DATA INCIDENT NOTIFICATION

What Happened

In January 2020, S&S Activewear (the "Company") acquired Technosport Canada. After the acquisition, the Company was victimized by a cyberattack that impacted two email accounts (the "Incident") on the legacy email server of Technosport Canada. Both email accounts were those of Technosport Canada employees, and the Incident was only linked to Technosport Canada data. As soon as we became aware of the Incident, we immediately commenced an investigation of it, with assistance from third-party experts, for the purpose of determining its scope, the impact on our information systems, and the identities of those the Incident potentially affected.

On or about August 12, 2020, we determined that the two accounts impacted by the Incident contained personal information that related to an identified set of individuals. Our investigation revealed that one of those accounts was subject to unauthorized access on June 6, 2020, and the other from June 6 through June 12, 2020. We have not found any evidence that the personal information contained in the impacted accounts was misused.

What Information Was Involved

A subset of the emails subject to the Incident contained one or multiple data elements of personal information including names, Social Security Numbers or Social Insurance Numbers, dates of birth, passport numbers, salary information, positions of employment, locations of employment, employee personnel files and employee identification numbers, race, national or ethnic origin, financial account information, and/or health and medical information.

What We Are Doing

We are providing notice to potentially affected individuals so that they can take steps to minimize the risk that their information will be misused. As an added precaution, we have arranged for Experian to provide potentially affected individuals 12 months of free credit monitoring and related services.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since learning of the attack, we have taken a number of steps to further secure our systems. Specifically, we have, among other things: disabled the compromised user account; deprecated and disabled the compromised password database; geoblocked access to the password vault; geofenced the password vault to the United States with multifactor authentication; implemented widespread changes to passwords associated with Company user accounts (including IT accounts), workstations, firewall and infrastructure devices, API/FTP, and the impacted domain; enabled multifactor authentication; strengthened password controls; disabled sending and access privileges within the impacted domain; disallowed permission elevation by users on workstations; limited permission elevation throughout the Company tenant; implemented alerts to the Company's Information Technology department; enabled notifications for large file deletions; enabled notifications for new user account creation; replaced all workstations with new Azure/Intune enrolled devices using Microsoft Defender ATP; and limited remote access privileges.

What You Can Do

In addition to enrolling in the free credit monitoring and related services mentioned above, we recommend that you remain vigilant and take the following steps to protect your personal information:

1. Contact the credit-reporting agencies as soon as possible to:

    - Add a fraud alert statement to your credit file at all three credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
    - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
    - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
    - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax Canada Co. National Consumer Relations Box 190 Montreal, Quebec H1S 2Z2 www.consumer.equifax.ca	Experian 2 Bloor St. E., Suite 3501 Toronto, Ontario Canada M4W1A8 Databreachinfo@experian.com www.experian.com/	TransUnion Attention: Consumer Relations 3115 Harvester Road, Suite 201 Burlington ON L7N3N8 https://members.transunion.ca/tucan_en/orderStep1_form.page?offer=CANTUM10011&CID=TRANSUNION:HPB www.transunion.ca

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Office of Consumer Affairs ("OCA") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The OCA can be contacted either by visiting https://www.canada.ca/en/services/finance/fraud.html, or by calling 1-800-328-6189. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Canadian Anti-Fraud Centre, which will collect all information and make it available to law enforcement agencies. You can report identity theft to the Canadian Anti-Fraud Centre at 1-888-495-8501.

For More Information

If you have questions or concerns, please contact 855-914-4669 Monday through Friday, 9am to 9pm ET. We apologize for this situation and any inconvenience it may cause you.