Date:
2023-08-28

File No.:
HW00263

To:

idtheft@oag.state.md.us
Office of the Attorney General
200 St. Paul Place, Baltimore, MD 21202

RE : Security Breach Notification

Henri & Wolf Inc. ("Counsel") represents Louis Garneau Sports Inc. ("Client") concerning a data security incident involving Garneau's online shopping pages.

On behalf of our Client, we write to inform you of a recent data security incident ("Matter") that may concern some personal information (collectively the "Information") as required by Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504. While we currently have no evidence of actual misuse of the Information, we are sharing what we know about the Matter, our Client's response to it, and steps taken by Client to help protect the Information.

What happened?
On or about July 26, 2023, the Client became aware of unusual activity on their website when they received a notice from law enforcement. The Client engaged their incident response process and began investigation of the Matter. On or about July 28, 2023, the Client determined that malicious code was on the website and was present from June 8, 2023, to July 28, 2023. The investigation determined that the malicious code was potentially able to skim personal information from customers of the Client's website, when they engaged in the purchasing process at checkout. The Client conducted a further investigation to confirm what data and who's Information was potentially impacted. That investigation concluded on August 7, 2023, and confirmed that there was unauthorized exfiltration of Information. The Client has no evidence of actual misuse of the Information. Notice to consumers will occur on August 28, 2023. The number of Maryland residents notified is 42.

Phone.
+1 514 360 3481
Fax.
+1 514 447 5532
Email.
contact@henriwolf.law
Web.
henriwolf.law
Address.
731, Rue de la Commune
Ouest, Bureau 100,
Montréal, Québec H3C 1X7

What Information was involved?

The Information that may be impacted includes:

- First and Last Name
- Email Address
- Address
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account or transaction, or used without security code

What are we doing?

Upon learning of the matter, the Client engaged their incident response process, which investigated the Matter and took a number of risk mitigation steps. In addition, they engaged data security professional experts to assist in the investigation. The Client changed login credentials and implemented various security measures.

The Client is providing potentially impacted individuals with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide alerts for twelve (12) months from the date of enrollment when changes occur to the credit file. This notification is sent the same day that the change or update takes place with the Bureau. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

Attached:

- Template notice

Please contact me with any questions.

Shawn Ford, LL.M.
Incident Response and Privacy Lawyer
C: 905-409-1385
E: sf@henriwolf.law

Phone. +1 514 360 3481
Fax. +1 514 447 5532
Email. contact@henriwolf.law
Web. henriwolf.law
Address. 731, Rue de la Commune Ouest, Bureau 100, Montréal, Québec H3C 1X7

Louis Garneau Sports Inc.
30 rue des Grands-Lacs
Saint-Augustin-de-Desmaures
Québec G34 2E6
Attn: Notification

August 24, 2023

000002

[redacted]

Notice of Data Breach

Dear [redacted]

We write to inform you of a recent data security incident ("Matter") that may concern some of your personal information (collectively the "Information"). While we currently have no evidence of actual misuse of your Information, we are sharing what we know about the Matter, our response to it, and steps you can take to help protect your personal Information.

What happened?

On or about July 26, 2023, we became aware of unusual activity on our website when they received a notice from law enforcement. We engaged their incident response process and began investigation of the Matter. On or about July 28, 2023, we determined that unauthorized code was present from June 8, 2023, to July 28, 2023. The investigation determined that the unauthorized code was potentially able to skim personal information during the purchasing process at checkout. We conducted a further investigation to confirm what Information was potentially impacted. That investigation concluded on August 7, 2023, and confirmed that there was unauthorized exfiltration of Information. Again, we have no evidence of actual misuse of your Information, however, out of an abundance of caution, we are notifying you because your Information may have been impacted.

What Information was involved?

The Information that may be impacted includes:

- First and Last Name
- Email Address
- Address
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account or transaction, or used without security code

What are we doing?

Upon learning of the matter, we engaged our incident response process, which investigated the matter and took a number of risk mitigation steps. In addition, we engaged data security professional experts to assist in the investigation. We changed login credentials and implemented various security measures. We are proud of the quick response by our team.

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide alerts for twelve (12) months from the date of enrollment when changes occur to the credit file. This notification is sent the same day that the change or update takes place with the Bureau. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://[redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of eighteen (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 can you do?

We encourage you to remain vigilant in reviewing your Information, such as reviewing your account statements, and monitor credit reports for any suspicious activity. We encourage you to enroll to receive identity and credit monitoring services. Please note that you must enroll directly. We are unable to enroll in these services for you.

For More Information.

Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-[redacted] and supply the fraud specialist with your unique code listed above.

We apologize for any inconvenience this may have caused.

Sincerely,

Jean-Marc Jahoo
Président-Directeur général/CEO
Louis Garneau Sports Inc.
30 rue des Grands-Lacs
Saint-Augustin-de-Desmaures
Québec G3A 2E6
1-800-463-8356

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a **12-month** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://[redacted]

You will be prompted to enter the following activation code:

[redacted]

Please ensure that you redeem your activation code before 12/22/2023 to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud.[1]
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-[redacted].

Steps You Can Take To Protect Your Information

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

[1] Underwritten by certain Underwriters at Lloyd's, under a master group policy issued in the name of Cyberscout Limited, Sontiq Inc. and all subsidiaries for the benefit of program members. Expense reimbursement insurance is only available upon successful enrollment in the online monitoring service. Please see www.sontiq.com/terms-of-use for details.

In order 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, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For more information on identify theft, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us.

For New Mexico residents, individuals have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in the individual's credit file has been used against the individual, the right to know what is in an individual's credit file, the right to ask for an individual's credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to an individual's file is limited; an individual must give consent for credit reports to be provided to employers; an individual may limit "prescreened" offers of credit and insurance an individual would get based on information in a credit report; and an individual may seek damages from violator. An individual may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage individuals to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are seven (7) Rhode Island residents impacted by this incident.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and https://oag.dc.gov/, where you can obtain information about avoiding identity theft.