



December 2, 2022

Notice - Cyber Incident

[Ms./Mr. NAME]

This notice is in response to the email we sent on November 30, 2022, informing you of a cyber incident involving Les Entreprises La Canadienne Inc. (**La Canadienne**). This incident affected some of your personal information and we would like to inform you of the measures available to you to better protect you, as well as the measures we are taking to continue protecting your personal information.

In our November 30th email, we asked you to take the necessary steps to **immediately cancel the credit card used to pay for your online order** placed between November 21 and November 25, 2022 on our website <https://www.lacanadienneshoes.com>. **We reiterate the importance of doing this to avoid any potential fraudulent activity.**

We want to reassure you that we have no confirmation that your personal information, including your credit card information, has been misused. That said, protecting your personal information and that of all our customers remains our priority. That is why we offer you a credit monitoring service with TransUnion, the details of which are explained below.

We take your privacy seriously, and we sincerely apologize for any inconvenience this incident may cause you.

What happened and what personal information was involved

On November 25, 2022, we discovered that La Canadienne was subject to a cybersecurity incident that resulted in the compromise by an unauthorized third party of certain transactions made online on our website <https://www.lacanadienneshoes.com> between November 21 and November 25, 2022. Our investigation reveals that the unauthorized third party was able to gain real-time access to these transactions and therefore all of the information you entered when ordering online during this period may have been stolen. Specifically, this information includes :

- Information about the credit card used to pay for your order, i.e., cardholder, number, expiry date and three-digit security code (CVV)
- Email address, billing address associated to the credit card

With the assistance of our IT specialists, we immediately conducted an investigation to determine the extent of the personal information involved. Following this investigation, we immediately notified you by email on November 30th and are sending you the present notice.

It is important to note that at this time, we have no confirmation that your personal information as identified above has been misused. However, since the security of your personal information is an ongoing priority, we wanted to make you aware of this incident and the steps we and you can take to protect yourself in the circumstances.

Measures taken by the Canadian

Upon discovering this incident, La Canadienne immediately retained the services of IT specialists to contain the incident and investigate the circumstances and impacts surrounding it.

Please be assured that we are taking all the necessary measures to prevent such an event from happening again. In particular, additional security parameters have been implemented in our system and we are

conducting regular cyber security assessments. Furthermore, we are currently contacting all relevant authorities.

We would like to point out that La Canadienne does not store any payment information on its servers once the transaction has been completed. The unauthorized third party was able to steal this payment information only because it was present on our network at the time you entered this information. We assure you that this third party is no longer on our network at this time and that your personal information is in a secure environment. Any future transactions on our website are secure.

Monitoring your credit file

Although there is no indication that your personal information may have been misused, La Canadienne offers you, at its expense, a twelve (12) month subscription to online monitoring service with Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

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://secure.identityforce.com/benefit/stst>

You will be prompted to enter the following activation code:

[Insert unique activation code].

Please make sure you use your activation code before March 31, 2023 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
- ✓ 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 1-800-405-6108 from Monday to Friday 8:00 a.m. – 8:00 p.m. EST, excluding holidays.

What you can also do

We encourage you to always remain vigilant and to adopt the following preventive measures:

- Take the necessary steps to **immediately cancel the credit card used to pay for your online order** placed between November 21 and November 25, 2022 on our website <https://www.lacanadienneshoes.com>.
- Monitor your bank accounts. If you have any doubts or spot any fraudulent or suspicious transactions on your credit or debit card, we recommend that you contact your financial institution.
- Change your passwords regularly and make sure they are secure – especially when an account is linked to your social insurance number. Don't use the same passwords.
- Be careful when sharing your personal information in an unsolicited manner whether by phone, email or on a website.
- Avoid clicking on links or downloading attachments in suspicious emails.
- If you notice any suspicious activity, report the incident to the appropriate authorities.
- Sign up for the above services.

The following website offers additional tips and resources to help you protect your identity: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/.

For more information

If you would like further information about the incident, please contact Nadia Niro at privacy@lacanadienneshoes.com or at 1-800-838-3943.

Sincerely,

Nicholas Niro
President
Les Entreprises La Canadienne Inc.



January 24, 2023

Follow-up Cyber incident

«First_Name» «Last_Name»
«Billing_Address»
«City», «State_Province», «Zip»

Dear «First_Name» «Last_Name»,

We previously mailed you a letter on December 2, 2022 informing you of a cyber incident involving Les Entreprises La Canadienne Inc. (**La Canadienne**). As indicated in that letter, this incident affected some of your personal information. We are following up with some additional information on what you can do to protect your information. Again, we have no confirmation that your information has been or will be misused.

What Happened

As described in our previous letter, we discovered that La Canadienne was subject to a cybersecurity incident that resulted in the compromise by an unauthorized third party of certain transactions made online on our website <https://www.lacanadienneshoes.com> between November 21 and November 25, 2022.

What Information Was Involved

The investigation revealed that the unauthorized third party gained real-time access to transactions made on our website and therefore the information you entered when placing your order during this time may have been accessed. Specifically, this information includes your name and:

- Information about the credit card used to pay for your order, i.e., cardholder, number, expiry date and three-digit security code (CVV)
- Email address, billing address associated to the credit card

It is important to note that at this time, we have no confirmation that your personal information has been or will be misused. However, since the security of your personal information is our priority, we wanted to make you aware of this incident and the steps we and you can take to protect yourself in the circumstances.

What We Are Doing

Upon discovering this incident, La Canadienne immediately retained the services of Information Technology specialists to contain and investigate the incident. Additionally, to prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our network, systems, and data. In particular, additional security parameters have been implemented in our systems and we are conducting regular cyber security assessments.

We would like to point out that La Canadienne does not store payment information on its servers once the transaction has been completed. The unauthorized third party was able to steal this payment information only because it was present on our network at the time you entered this information. We assure you that this

third party is no longer on our network at this time and that your personal information is in a secure environment.

What You Can Do

Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

As an added precaution, to help protect your personal information, we are offering a complimentary a twelve (12) month subscription to online monitoring service with Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

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.

If you have not already done so, we encourage you to take advantage of this service and help protect your identity. To activate your service, please follow the steps below:

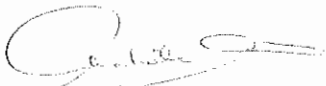
- (1) Ensure that you **enroll by March 31, 2023** (Your code will not work after this date)
- (2) **Visit** the TransUnion IdentityForce website to enroll:
<https://secure.identityforce.com/benefit/stst>
- (3) Provide your **activation code: «Coupon»**

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-800-405-6108 from Monday to Friday 8:00 a.m. – 8:00 p.m. EST, excluding holidays.

For More Information

We take your privacy seriously, and we sincerely apologize for any inconvenience this incident may cause you. If you would like further information about the incident, please contact Nadia Niro at privacy@lacanadienneshoes.com or at 1-800-838-3943.

Sincerely,



Nicholas Niro
President
Les Entreprises La Canadienne Inc.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111	Phone: 1-888-397-3742	Phone: 1-888-909-8872
P.O. Box 740256	P.O. Box 9554	P.O. Box 105281
Atlanta, Georgia 30348	Allen, Texas 75013	Atlanta, GA 30348-5281
www.equifax.com	www.experian.com	www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about

additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.