Morgan Lewis

Ezra D. Church
Partner
215.963.5710
ezra.church@morganlewis.com

VIA FIRST CLASS MAIL

December 12, 2019

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Security Breach Notification

Re: *Notification of Potential Personal Information Breach Involving 9 New Hampshire Residents*

Dear Office of the Attorney General:

This Firm represents ShopRunner, Inc. ("ShopRunner"), which offers a membership program whereby members receive free two-day shipping, free returns and other member-only deals on participating retailers' websites. It came to ShopRunner's attention that, on rare occasions, users of ShopRunner Express Checkout who were adding new payment card information and experienced some error (e.g., loss of internet connection) may have had their credit or debit card information appended to and transferred to the relevant retailer in URL logs. When this did occur, the information in the URLs was transmitted with encryption, which means it was not accessible to any third parties. However, in some cases, ShopRunner's retail partners captured plain text URLs of that information, which was then available in turn to their website vendors, such as ad technology and analytics companies.

Upon learning of the situation, ShopRunner promptly investigated, identified the issue and took steps to contain it by scrubbing logs, deploying a fix to prevent this issue in the future, and notifying its retail partners to also review and ensure their own logs do not contain payment card information. At this time, ShopRunner has not received any reports of improper use of any of payment card information. Nonetheless, ShopRunner is sending notification letters out to its affected members. In addition, ShopRunner is offering a two-year subscription to Experian's identity theft and credit monitoring services.

Further information about what ShopRunner has done and what we are recommending to the individuals in question can be found in the enclosed notification letter that ShopRunner sent to **9** New Hampshire residents. If you have any questions, please feel free to contact me.

Regards,

Ezra Church /TMS

Ezra D. Church

Enclosure

SHOPRUNNER

Re: **Personal Information Potentially Compromised**

Dear ShopRunner Member:

We are writing to tell you about an incident that may have exposed some of your personal information. While we have no reason to believe that this information was accessed, or has been or will be used inappropriately, we would like to let you know what happened, what information was involved, what we have done to address the situation, and to remind you of what you can do to protect your continued privacy.

What Happened

It has come to our attention that, on rare occasions, users of ShopRunner Express Checkout who were adding new payment card information and experienced some error (e.g., loss of internet connection) may have had their credit or debit card information appended to and transferred to the relevant retailer in URL logs. When this did occur, the information in the URLs was transmitted with encryption, which means it was not accessible to any third parties. However, our retail partners in some cases captured plain text URLs of that information, which was then available in turn to their website vendors, such as ad technology and analytics companies.

What Information Was Involved

The information that could have been accessed as a result of that transmission consisted solely of your name, address, and credit or debit card information (number, expiration date and possibly CVV code, which is the three or four-digit number typically printed on the back of your card). We are not aware of and have no reason to believe there to have been improper use of any of this information.

What We Are Doing

ShopRunner takes these types of situations very seriously and promptly investigated the incident. We identified the issue and took steps to contain it by scrubbing logs, deploying a fix to prevent this issue in the future, and notifying our retail partners to also review and ensure their own logs do not contain payment card information.

What You Can Do

First, we sincerely apologize for any inconvenience or concern this has caused you and we want you to be assured that we are taking steps to

prevent a similar occurrence. We understand the importance of the situation and we stand ready and willing to help you. We are offering two (2) free years of credit monitoring services to our customers who have received this notice. You may redeem this offer until March 31, 2020. For details regarding these credit monitoring services please contact us at 1-866-798-7767.

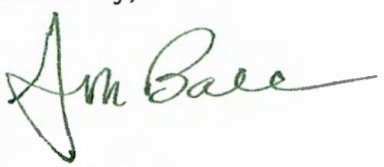
Second, contact any financial institutions that you bank with and advise them of this situation. Regularly check your accounts online or via telephone for any potential fraudulent activity. Always and promptly upon receipt, check your monthly/periodic statements from each of your financial institutions and credit card companies and immediately report to that company any unauthorized or suspicious transactions. Many credit card companies also offer potential fraud alerts that you can receive by text or email, usually for no charge. Sign up for any such program.

For More Information
For general information on protecting your privacy and preventing unauthorized use of your personal information, you may visit the U.S. Federal Trade Commission's website, http://ftc.gov, or contact your state office of consumer affairs or attorney general. You can also see the "Reference Guide" below for more information.

* * *

We are committed to maintaining the security and privacy of the personal information you entrusted to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, or if you encounter any problems that you believe to be related to this incident, please call us at 1-866-798-7767.

Sincerely,



Greg Ball
Chief Technology Officer

* * *

Reference Guide

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report: To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com

TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File: You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. 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 law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding

credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission: If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's
Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov