DLA Piper LLP (US)
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801-1147
www.dlapiper.com

Edward J. McAndrew
Ed.McAndrew@dlapiper.com

August 26, 2020

VIA E-MAIL: SECURITYBREACH@ATG.WA.GOV

The Honorable Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Security Incident Notification

Dear Attorney General Ferguson:

We are providing notice on behalf of Stericycle, Inc. ("Stericycle") to the Office of the Attorney General, pursuant to Wash. Rev. Code § 19.255, regarding an incident involving 1284 Washington residents.

On or about April 8, 2020, Stericycle's IT security team discovered a suspicious forwarding rule on a Stericycle email account during routine system maintenance. Stericycle immediately launched an investigation into the incident with the assistance of a leading cybersecurity firm. As of May 5, 2020, Stericycle had identified indicia of unauthorized access into additional employee email accounts. The dates of potential unauthorized access varied by email account, but the overall period of potential unauthorized access to the accounts was between October 2019 and April 2020. Stericycle conducted an analysis of the contents of the relevant employee email accounts to determine whether the accounts contained personal information. On July 27, 2020, we determined that the personal information of 1284 Washington residents contained in at least one of the email accounts. Our investigation revealed no evidence that any particular email message containing personal information was actually accessed by any unauthorized individual.

The types of personal information contained in the email accounts varied by individual, and not all of the types of data listed below were implicated for affected residents. In general, a limited number of emails contained in the email accounts may have included one or more of the following types of personal information: Name, Social Security Number, Driver's License Number, Passport Number, Financial Account/Payment Card Number, and Medical or Health Insurance Information.

Upon discovery of the initial suspicious forwarding rule on one email account, Stericycle immediately launched an investigation, secured each impacted employee email account, and has

VIA E-MAIL

continued to monitor for suspicious activity. Stericycle has also reviewed and updated its employee email security controls where appropriate and has continued to train its workforce regarding cybersecurity issues.

In an abundance of caution, Stericycle is notifying potentially affected individuals and providing them with access to 24 months of MyIDCare™ credit monitoring and identity protection services at no cost, through ID Experts. MyIDCare services include: 24 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

A sample of the notification letter is enclosed.

If you should have any questions or if we can provide further assistance to the Washington residents affected by this incident, please feel free to contact me at (302) 468-5685 or ed.mcandrew@dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

Edward J. McAndrew
An Attorney for Stericycle, Inc.

Enclosure

Stericycle

C/O ID Experts
PO Box 4600
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

SEQ
CODE 2D
Ver 1GE

To Enroll, Please Call:
(833) 431-1281
Or Visit:
https://ide.myidcare.com/stericycleprotect
Enrollment Code: <<XXXXXXXX>>

August 26, 2020

RE: Notice of Data Security Incident

Dear <<First Name>>:

We write to share important information with you about a data security incident that may have impacted your personal information. The protection of confidential information is among Stericycle's highest priorities.

We want to begin by emphasizing that we have no evidence that your personal information has been accessed without authorization or compromised. In an abundance of caution, we are providing this notice to you so you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? We have conducted an investigation, with the assistance of a leading cybersecurity firm, into email phishing attempts targeting Stericycle employees. These phishing attempts sought to compromise Stericycle employee email accounts. On July 27, 2020, we determined that your personal information was contained in at least one of the email accounts that appears to have been accessed by an unauthorized individual. The dates of potential unauthorized access varied by email account, but the overall period of unauthorized access to the email accounts was between October 2019 and April 2020. Although the employee email accounts themselves appear to have been accessed by an unauthorized individual, our investigation revealed no evidence that any email message containing your personal information was actually accessed by an unauthorized individual.

What Information Was Involved? The types of personal information contained in the email accounts varied by individual. In general, a limited number of emails contained in the impacted email accounts may have included one or more of the following types of personal information: Name, Social Security Number, Tax ID Number, Driver's License Number, Passport Number, financial account/payment card account number, and medical or health insurance information.

What We Are Doing. Stericycle utilizes robust measures to protect your personal information. These measures are reviewed and frequently updated, as appropriate, by our internal Information Technology team and external experts that support us. We strive to continually improve our data security and maintain a secure environment for confidential and personal information.

Stericycle immediately launched an investigation into the suspected phishing activity, secured each impacted employee email account, and has continued to monitor for suspicious activity. We have also reviewed and updated our employee email security controls where appropriate and have continued to train our workforce regarding cybersecurity issues.

As an added precaution, we are providing access to 24 months of MyIDCare™ credit monitoring and identity protection services at no cost to you, through ID Experts. MyIDCare services include: 24 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve any issues, if your identity is compromised.

What You Can Do: We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 431-1281 or going to https://ide.myidcare.com/stericycleprotect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is November 26, 2020.

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: For general questions about the incident or the MyIDCare service, please call (833) 431-1281 or go to https://ide.myidcare.com/stericycleprotect. You also may consult the resources included on the enclosed form, which provides additional information about protecting your personal information online.

I would like to reiterate that the security of your personal information is among our highest priorities. We sincerely regret any inconvenience caused to you by this incident.

Sincerely,

S. Cory White
Executive Vice President and Chief Commercial Officer

Steps You Can Take to Protect Against Identity Theft and Fraud

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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
800-349-9960	888-397-3742	888-909-8872

Websites:
www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stud, or W2;
8. 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.

SEQ
CODE 2D

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.