



Christopher Ballod
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Christopher.Ballod@lewisbrisbois.com
Direct: 215.977.4077

June 26, 2020

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent BCycle, LLC (“BCycle”), a supplier of equipment and services to bicycle sharing systems operating in approximately 40 cities across the United States. BCycle, itself, is based in Waterloo, Wisconsin. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21 because the personal information of New Hampshire residents may have been affected by a recent data security incident. The incident may have involved unauthorized access to names, addresses, card numbers, card expiration dates, and security codes for certain customers who used their credit cards for online purchases between January 24, 2020 and April 26, 2020.

On or about April 24, 2020, BCycle learned that it may have been the victim of a malware attack after detecting and investigating suspicious activity on websites for membership enrollment for a number of bicycle sharing systems. Upon discovering this, BCycle promptly took steps to secure the impacted system and launched a forensic investigation with the assistance of an external digital forensics firm. The forensics firm subsequently reported that an unauthorized actor may have accessed or acquired payment card information during the above-referenced window. BCycle then worked to identify potentially impacted customers based on transaction data during the relevant timeframe. On June 2, 2020, BCycle identified four (4) New Hampshire residents as among the potentially affected population. BCycle has reported this incident to law enforcement and contacted payment card brands (Visa, Mastercard, American Express, Discover) so steps could be taken prevent fraudulent activity on any affected cards.

BCycle is not aware of any unauthorized credit card transactions or fraudulent activity as a result of this incident. In addition to removing the malware from the impacted system, BCycle has implemented enhanced security measures to minimize the likelihood that an event like this might occur again in the future. BCycle notified the potentially affected New Hampshire residents via the attached sample letter on June 26, 2020. Out of an abundance of caution, BCycle is offering twelve

June 26, 2020
Page 2

(12) months of complimentary credit and identity monitoring services to the potentially affected residents through ID Experts.

Please contact me should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. Ballod', written in a cursive style.

Christopher Ballod of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Consumer Notification Letter



C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-579-1113
Or Visit:
<https://ide.myidcare.com/bcycle>
Enrollment Code: <<XXXXXXXXXX>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

June 26, 2020

Re: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a data security incident experienced by BCycle LLC, the equipment and software provider for <<Operator Name>>, involving suspected unauthorized access to a system containing your name, address, and credit card information. In an abundance of caution, we wanted to notify you of the incident, offer you identity protection services, and inform you about steps that can be taken to help protect your personal information.

What Happened? On April 24, 2020, BCycle learned that malicious software was present on the <<Operator Name>> website for membership enrollment. Upon discovering this, BCycle promptly took steps to secure the affected system and launched an internal investigation. BCycle also engaged a leading digital forensics firm to investigate. The investigation subsequently determined that the malicious software may have enabled unauthorized parties to access payment card information used for transactions between January 24, 2020 and April 26, 2020. On June 2, 2020, BCycle identified your information as being potentially within this window of exposure. BCycle is not currently aware of any unauthorized credit card transactions or fraudulent activity having occurred as a result of this incident. We are notifying you now out of an abundance of caution.

What Information Was Involved? The information involved may have included names, addresses, and credit card numbers with card security codes and expiration dates.

What We Are Doing. As soon as BCycle discovered this incident, we took the measures referenced above, reported the incident to the credit card companies, and implemented enhanced security measures to better safeguard all sensitive data in our possession and to help prevent a similar incident from occurring in the future. BCycle also reported the matter to law enforcement and will provide whatever cooperation is necessary to hold the perpetrator accountable. In addition, BCycle is providing you information about steps you can take to protect your personal information, as well as covering the costs of identity theft protection services through ID Experts®, a data security and recovery services expert. Your complimentary one-year enrollment in MyIDCare™ includes: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Additional information about these services is included with this letter. Please note the deadline to enroll is September 26, 2020.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information. You can also enroll in the complimentary services being provided to you through ID Experts. Activation instructions and a description of the services being provided are included with this letter.

For More Information. If you have any questions or need assistance, please call 1-833-579-1113 Monday through Friday from 9 am - 9 pm Eastern Time. Please accept our sincere apologies and know that we deeply regret any worry or convenience that this may cause you.

Sincerely,

Morgan Ramaker
Executive Director

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 740241
Atlanta, GA 30374
1-866-349-5191
www.equifax.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

**Maryland Attorney
General**

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



One-Year Enrollment in MyIDCare™

Website and Enrollment. Please visit <https://ide.myidcare.com/bcycle> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

Telephone. Contact MyIDCare at 1-833-579-1113 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This MyIDCare enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.