MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 8, 2018

INTENDED FOR ADDRESSEE(S) ONLY

VIA US MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Mr. MacDonald:

We represent Saris Cycling Group, 5253 Verona Rd, Fitchburg, WI 53711 ("Saris"), and are writing as a follow-up to our notice to you on November 6, 2017 regarding an incident that may affect the security of personal information relating to two (2) New Hampshire residents. By providing this notice, Saris does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about October 18, 2017, Saris discovered that an employee had clicked on a phishing email and entered his or her credentials. Saris immediately took steps to secure the employees' email account and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired.

Saris subsequently determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to the Saris employee's email account. Saris immediately began an investigation into the contents of the email account and, on November 2, 2017, initially identified a subset of individuals whose information was in the email account. On November 30, 2017, Saris determined, after its continued in-depth programmatic and manual review of the some of the contents of the email account, the types of protected information contained in the

email account and to which individuals the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. While there is no evidence that the individual(s) accessed or acquired personal information from the employees' email account, access to the information contained therein could not be ruled out. The email account may have contained the name, address, and Social Security Number of the affected New Hampshire residents.

Notice to New Hampshire Residents

On November 15, 2017, Saris provided written notice of this incident to those individuals it identified initially as having their information in the email account. Saris continued its investigation and identified additional individuals impacted by this incident, and is providing written notice to these individuals on January 4, 2018. Written notice is provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Saris is providing all potentially affected individuals access to one free year of credit and identity monitoring services, including identity restoration services, through Kroll, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Saris is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

Exhibit A

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a recent event that may affect the security of your personal information. As an employee of Saris Cycling Group ("Saris"), you provided Saris with certain personal information, and the security of your information is important to us. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about a recent incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On or about October 18, 2017, we discovered that Saris had become the target of a phishing email campaign and that an employee had clicked on phishing emails and entered their credentials. We immediately took steps to secure the employee's email account and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired.

We subsequently determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to the employee's email account. On October 27, 2017, Saris determined that information related to certain current and former employees was included in the email account and immediately launched a review of our files to ascertain address information for the impacted individuals.

While we currently have no evidence that anyone accessed or acquired this information, access to the information in the email account cannot be ruled out.

What Information Was Involved? While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name, address, <<ClientDef1 (additional data element(s)>> were accessible to the unknown actor during this event.

What We Are Doing. We take the security of information in our care very seriously. Since discovering this event, we have been working diligently with third-party forensic investigators to determine what happened and what information was accessible to the unknown actor. This involved a time consuming, programmatic and manual data review process. We are providing notice of this event to you, and to certain regulators and consumer reporting agencies as required. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
You have until April 4, 2018 to activate your identity monitoring services.
Membership Number: <<Member ID>>

What You Can Do. In the event you are not already receiving credit monitoring and wish to do so, you can enroll and receive the free credit monitoring and identity restoration services we are offering by calling the number below.

You can also review the enclosed Privacy Safeguards Information for additional information on how to better protect against identity theft and fraud.

For More Information. We are sorry for any inconvenience or concern this incident causes you. As a valued Saris employee, the security of your information is a top priority to us. Should you have any questions about the content of this letter, ways you can better protect yourself from the possibility of identity theft, or to enroll in credit monitoring services, please call 1-866-599-4455 between 9:00 am and 6:00 pm ET, Monday through Friday, excluding major holidays.

Sincerely,

Bill Shager
Executive Vice President
Saris Cycling Group

PRIVACY SAFEGUARDS

In addition to enrolling to receive the free monitoring and restoration services we are offering to you, we encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit bureau from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit bureau with a valid police report, the credit bureau cannot charge to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit bureaus separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze
www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. This notice was not delayed as the result of a law enforcement investigation.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.