



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

May 31, 2018

VIA ELECTRONIC SUBMISSION

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

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Temecula Motorsports, Inc. ("Temecula") in connection with a recent data security incident which is described in greater detail below. Temecula takes the security and privacy of personal information very seriously and is taking steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On March 30, 2018, Temecula learned of a potential data security incident involving the unauthorized installation of malware on its e-commerce web platform resulting in potential access to and / or acquisition of some personal information. Upon learning of the incident, Temecula took immediate steps to remove the malware and secure its system. Temecula also launched an investigation and engaged an independent forensics firm to determine what happened and whether personal information was accessed or acquired without authorization. In addition, Temecula notified the payment card brands that certain payment card information may have been impacted to help prevent credit card fraud. The forensics firm ultimately determined that the accessed information may have included names, card numbers, expiration dates, and security codes.

2. Number of New Hampshire residents affected.

Temecula notified 7 New Hampshire residents regarding this data security incident. Notification letters were mailed beginning on May 31, 2018. A sample copy of the notification letter is included.

3. Steps taken relating to the incident.

Temecula has taken affirmative steps to prevent a similar situation from arising in the future and to protect the privacy and security of all personal information. These steps have included working with a leading forensics firm to remove malicious code from its web platform and blocking traffic to / from malicious domains. Temecula has also taken steps to bolster the security of its web platform.

4. Contact information.

Temecula is dedicated to protecting the sensitive information that is in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@LewisBrisbois.com.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure



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

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

Subject: Notice of Data Breach

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

I am writing to inform you of a data security incident that may have affected your payment card information. At Temecula Motorsports, Inc. ("Temecula"), we take the privacy and security of your payment card information very seriously and regret any concern that this incident may cause you. That is why we are contacting you and informing you about steps that can be taken to protect your information.

What Happened? On March 30, 2018, Temecula learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. As soon as we discovered the incident, we took immediate steps to remove the malware and to secure all payment card information. We also launched an investigation and retained a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization. This letter serves to inform you of the incident and to share with you steps that you can take to protect your information.

What Information Was Involved? We believe that the malware could have comprised payment card information belonging to customers who utilized our web platform to purchase products from February 9, 2018 to March 30, 2018. The affected payment card information may have included names, card numbers, expiration dates, and security codes.

What Are We Doing? As soon as Temecula discovered the incident, we took the steps described above. We also reported the matter to the payment card brands in order to protect your payment card information and prevent fraudulent activity. In addition, we are providing you with information about steps that you can take to protect your personal information. Finally, we take the security of all information that we store in our systems very seriously and have taken steps to enhance the security of Temecula customer information and our e-commerce web platform in order to help prevent similar incidents from occurring in the future.

What You Can Do: You can follow the recommendations on the following page to protect your information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions please call 1-833-221-9228 Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time.

Thank you for your loyalty to Temecula and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Robert Vegter
Parts and Service 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 and review 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 should also 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 (the "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 can also contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion	Free Annual Report
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.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: In some U.S. states, you have the right to put a security freeze on your credit file. 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. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. 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 knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.