McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Christine Czuprynski
Direct Dial: 248.220.1360
cczuprynski@mcdonaldhopkins.com

February 16, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: TK Classics, LLC – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents TK Classics, LLC ("TK Classics"). I am writing to provide notification of an incident at TK Classics that may affect the security of personal information of approximately one (1) New Hampshire resident. TK Classics' investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, TK Classics does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

TK Classics recently discovered that e-commerce websites owned by TK Classics were modified with malicious code that acted to capture payment card data as it was entered on the websites in connection with a purchase. TK Classics immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, TK Classics determined that the payment card information potentially accessed and/or acquired related to transactions made through its online stores between January 24, 2020 and August 6, 2020. The information that may have been accessed and/or acquired in this incident included customer names, credit or debit card numbers, card expiration dates and CVVs (3 or 4 digit codes on the front or back of the cards). TK Classics discovered on January 6, 2021 that the affected resident completed a transaction at one of TK Classics' websites during the window of compromise and their card information may be at risk. No other personal information is at risk as a result of this incident.

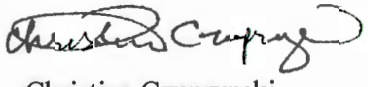
Out of an abundance of caution, TK Classics wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. TK Classics is providing the affected resident with written notification of this incident commencing on or about February 12, 2021 in substantially the same form as the letter attached hereto. TK Classics is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit

reports. The affected resident is being advised to contact their financial institutions to inquire whether new cards should be issued to them. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At TK Classics, protecting the privacy of personal information is a top priority. TK Classics has implemented enhanced security safeguards to help protect against similar intrusions. TK Classics is also conducting ongoing monitoring of its website to ensure that it is secure and cleared of any malicious activity.

Should you have any questions, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Christine Czuprynski

Encl.

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to make you aware of a recent data security incident involving potential unauthorized access to some of our customers' payment card data used at websites owned by TK Classics, LLC. The privacy and security of your personal information is of utmost importance to us and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

We discovered that e-commerce websites owned by TK Classics, LLC were modified with malicious code that acted to capture payment card data as it was entered on the websites in connection with a purchase. We immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, we determined that the payment card information potentially accessed and/or acquired related to transactions made through our online stores between January 24, 2020 and August 6, 2020.

The information that may have been accessed and/or acquired in this incident included customer name, credit or debit card number, card expiration date and CVV (3 or 4 digit code on the front or back of the card). We discovered on January 6, 2021 that you completed a transaction at one of our websites during the window of compromise and your card information may be at risk. No other personal information of yours is at risk as a result of this incident.

Because we value our relationship with you, we wanted to make you aware of the incident. We also wanted to let you know what we are doing to further secure your information, and suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect against similar intrusions. We are also conducting ongoing monitoring of our websites to ensure that they are secure and cleared of any malicious activity.

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

Your trust is a top priority for us and we deeply regret the inconvenience this may have caused. The privacy and protection of our customers' information is a matter we take seriously.

If you have any further questions regarding this incident, please contact [redacted].

Thank you,

[redacted]

– OTHER IMPORTANT INFORMATION –

Placing a Fraud Alert.

You may place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax, P.O. Box 105069, Atlanta, GA 30348
www.equifax.com, 1-800-525-6285

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

TransUnion LLC, P.O. Box 2000, Chester, PA 19016
www.transunion.com, 1-800-680-7289

Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348
https://www.freeze.equifax.com, 1-800-349-9960

Experian Security Freeze, PO Box 9554 Allen, TX 75013
http://experian.com/freeze, 1-888-397-3742

TransUnion Security Freeze, P.O. Box 2000, Chester, PA 19016
http://www.transunion.com/securityfreeze, 1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: 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 York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-775 (TDD/TYY: 800-788-9898)
https://ag.ny.gov/consumer-frauds-bureau/identity-theft.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.