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

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

August 3, 2017

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Juliska – Incident Notification

Dear Attorney General Foster:

McDonald Hopkins PLC represents Juliska. I write to provide notification concerning an incident that may affect the security of personal information of seventeen (17) New Hampshire residents. Juliska's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Juliska does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

After a security scan discovered some suspicious content on Juliska's e-commerce site, *www.juliska.com*, Juliska immediately identified and permanently removed a malicious script that was placed through unauthorized access of the site. Upon learning of the situation and promptly removing the malicious code, Juliska initiated a full investigation with a team of digital forensic experts, which was concluded on July 18, 2017.

Through this investigation, Juliska has learned that orders placed on its website, from October 27, 2016 through May 24, 2017, may have been affected by this malicious content. During this time period, the information associated with website orders, including names, addresses, email addresses, phone numbers, credit/debit card numbers, card expiration dates and CVV2/CVC2/CID/CVDs (security codes on the front or back of the card) may have been compromised. Debit PIN numbers were not involved in this incident. Moreover, purchases through Juliska's Customer Care department, physical retail store locations or a Juliska reseller were not affected by this incident.

To date, Juliska is not aware of any reports of improper use of information as a direct result of this incident. Nevertheless, Juliska wanted to make you (and the potentially affected residents) aware of the incident and explain the steps Juliska is taking to safeguard the residents against identity fraud. Juliska provided the New Hampshire residents with written notice of this incident commencing on August 3, 2017, in substantially the same form as the letter attached hereto. Juliska has advised the residents to remain vigilant in reviewing financial and credit/debit card account statements for fraudulent or irregular activity on a regular basis, and to

immediately report any unauthorized charges to their financial institutions. Juliska has also advised the residents about the process for obtaining a free credit report and placing a fraud alert and/or security freeze on their credit files. Juliska is providing dedicated call center support to answer questions. The residents also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Since learning of the incident, Juliska has implemented enhanced security safeguards to protect from similar intrusions. Juliska is also conducting ongoing monitoring of its website and payment portal to ensure that they are secure. In addition, Juliska has been working with the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

DAP/sdg
Encl.

[redacted]

August 3, 2017

Dear Juliska Valued Customer:

Juliska greatly values the relationship we have with our customers and understands the importance of protecting personal information. We are writing to inform you about an incident that may involve some of your information.

What Happened?

A recent security scan discovered some suspicious content on *www.juliska.com*. We immediately identified and permanently removed a malicious script that was placed through unauthorized access of the site.

What Information Was Involved?

Since learning of the incident and promptly removing the malicious code, we initiated a full investigation with a team of digital forensic experts, which was concluded on July 18, 2017. Through this investigation, we learned that orders placed on our website, from October 27, 2016 through May 24, 2017 may have been affected by this malicious content. During this time period, the information associated with website orders including name, address, email, phone number, and payment card information (including card number, expiration date and security code), may have been compromised. Purchases made through our Customer Care department directly, through our retail stores, or at a Juliska reseller were not affected by this incident.

What We Are Doing.

We have implemented enhanced security safeguards to protect from similar intrusions. We are also conducting ongoing monitoring of our website and payment portal to ensure that they are secure. In addition, we have notified law enforcement and have been working with the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

What You Can Do.

You should always remain vigilant in reviewing your financial account statements and payment card statements for fraudulent or irregular activity on a regular basis. You should immediately report any unauthorized charges you identify to your financial institution, as payment card network rules generally state that cardholders are not responsible for such charges. The phone number to call is usually on the back of your payment card.

You should also review the additional information on the following page on ways to protect yourself. Please note that only the card you used for your transaction may be affected due to this incident.

Earning your loyalty and trust is vital to us at Juliska, and we sincerely apologize for any inconvenience this may have caused you.

For More Information.

To help address any additional questions or concerns please contact [redacted]. This dedicated response line is available Monday through Friday, 9 a.m. to 6 p.m. EST.

Yours Sincerely,

David Gooding
CEO

- OTHER IMPORTANT INFORMATION -

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), https://www.identitytheft.gov/