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
E-mail: dpaluzzi@mcdonaldhopkins.com

May 17, 2021

VIA U.S. MAIL

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

Re: Stampin' Up! – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Stampin' Up!. I am writing to provide notification of an incident at Stampin' Up! that may affect the security of personal information of approximately thirty-four (34) New Hampshire residents. Stampin' Up!'s 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, Stampin' Up! does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Stampin' Up! recently discovered that its e-commerce website *www.paperpumpkin.com* was modified with malicious code, which acted to capture payment card data as it was entered on the website in connection with a purchase. Upon learning of the issue, Stampin' Up! promptly opened an investigation. As part of its investigation, Stampin' Up! has been working closely with external cybersecurity professionals. After an extensive forensic investigation, Stampin' Up! determined that the payment card information that potentially may have been accessed was information related to transactions between June 12, 2020 and November 17, 2020 made at its website *www.paperpumpkin.com*. Stampin' Up! determined on April 14, 2021, that the information that potentially may have been acquired included the residents' full names, credit or debit card numbers, and card expiration dates. It is important to note that CVVs (3 or 4 digit code on the front or back of the card) were not acquired. Thus, the information that potentially may have been acquired cannot be used for payment transactions where CVVs are required.

To date, Stampin' Up! is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Stampin' Up! wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Stampin' Up! is providing the affected residents with written notification of this incident commencing on or about May 14, 2021 in substantially the same form as the letter attached hereto. Stampin' Up! is advising the affected residents about the process for placing fraud alerts and/or security freezes

on their credit files and obtaining free credit reports. The affected residents whose credit or debit card information was impacted are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Stampin' Up!, protecting the privacy of personal information is a top priority. Stampin' Up! is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Stampin' Up! continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information. Stampin' Up! has implemented enhanced security safeguards to help protect against similar intrusions and is also conducting ongoing monitoring of its website *www.paperpumpkin.com* to ensure that it is secure and cleared of any malicious activity.

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

Sincerely,

Dominic A. Paluzzi

Encl.

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]:

We write to make you aware of a recent data security incident involving the potential unauthorized access to some of our customers' payment card data used at our website *www.paperpumpkin.com*. The privacy and security of your personal information is of utmost importance to Stampin' Up!, and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

We recently discovered that our e-commerce website *www.paperpumpkin.com* was modified with malicious code, which acted to capture payment card data as it was entered on the website 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 that potentially may have been accessed was information related to transactions between June 12, 2020 and November 17, 2020 made at our website *www.paperpumpkin.com*.

What Information Was Involved?

The information that potentially may have been acquired in this incident included customer name, credit or debit card numbers, and card expiration dates. We have confirmed, however, that CVVs (3 or 4 digit code on the front or back of the card) were **not** acquired in this incident. Thus, the information that potentially may have been acquired cannot be used for payment transactions where CVVs are required.

We discovered on April 14, 2021 that you completed a transaction at our website www.paperpumpkin.com between [redacted], and your card information may be at risk. No other personal information of yours is at risk because of this incident.

What We Are Doing

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 website www.paperpumpkin.com to ensure that it is secure and cleared of any malicious activity.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant and should review 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.

For More Information

Your trust is a top priority for Stampin' Up!, 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 call our dedicated and confidential toll-free response line to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Thank you,

Stampin' Up!

– OTHER IMPORTANT INFORMATION –

1. 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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Consider 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	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

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 personal identification number (PIN) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

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 with your local law enforcement agency.

3. 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.

4. 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 Federal Trade Commission (FTC) by contacting them on the internet 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.

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; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, https://oag.dc.gov/consumer-protection, Telephone: 1-202-727-3400.