

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

August 15, 2022

VIA ONLINE SUBMISSION

Aaron Frey
Maine State Attorney General's Office
Attn: Security Breach Notification
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, ME 04330

To Whom It May Concern:

McDonald Hopkins PLC represents Malley's Candies, Inc. ("Malley's"), of Cleveland, Ohio. I am writing to provide an update to our submission to your office dated May 6, 2022 (hereinafter, the "Preliminary Notification") concerning an incident at Malley's that may affect the security of personal information of a limited number of Maine residents. By providing this notice, Malley's does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

As discussed in our Preliminary Notification, Malley's recently learned that its e-commerce website - www.malleys.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, Malley's promptly opened an investigation. As part of its investigation, Malley's has been working closely with external cybersecurity professionals.

Since our Preliminary Notification, Malley's has determined, with assistance from external forensic experts, that the window of exposure began on April 11, 2021 and ended on July 1, 2022 (at the time the Preliminary Notification was made, the end of the window of exposure was understood to be March 2, 2022 pursuant to the external forensic investigation).

Due to the updated window of exposure, an additional nineteen (19) Maine residents have been determined to have been impacted, bringing the approximate total number of Maine residents impacted by this incident to approximately twenty-six (26).

Malley's provided the affected Maine residents who were not previously notified of the incident with written notification of this incident commencing on or about August 5, 2022 in substantially the same form as the letter attached hereto. Malley's is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Malley's is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free

August 15, 2022

Page 2

credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Malley's, protecting the privacy of personal information is a top priority. Malley's is committed to maintaining the privacy of personal and financial information in its possession and has taken many precautions to safeguard it. Malley's continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

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

Very truly yours,



Dominic A. Paluzzi

Encl.



CHOCOLATES
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



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 www.malleys.com. The privacy and security of your personal information is of utmost importance to Malley's Chocolates 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 former e-commerce website was modified with malicious code that potentially 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 potentially accessed and/or acquired related to transactions made through our online store between April 11, 2021, through July 1, 2022.

What Information Was Involved.

We discovered on July 21, 2022 that the information that may have been accessed and/or acquired in this incident included your name, contact information, credit or debit card number, card expiration date, and CVV (3 or 4 digit code on the front or back of the card). No other personal information of yours is at risk as a result 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 taken action to prevent a similar event from occurring in the future, including shifting all of our ecommerce transaction processing onto a new ecommerce platform hosted by Shopify.

What You Can Do.

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.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any questions regarding th [REDACTED] **lease call our dedicated and confidential toll-free response line that we have set up 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, 9am to 9pm Eastern.

Sincerely,

Malley's Chocolates

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) 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 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. 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
P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

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

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
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.

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 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 1-202-727-3400.

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.

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.

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, Consumer Protection Division, 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