

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

May 10, 2023

VIA EMAIL: Idtheft@oag.state.md.us

Brian E. Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: General Wax & Candle Company – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents General Wax and Candle Company (“General Wax”) of North Hollywood, California. I am writing to provide notification of an incident that may affect the security of personal information of approximately six (6) Maryland residents who recently made a purchase from General Wax’s retail website, www.generalwax.com. By providing this notice, General Wax does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

General Wax recently discovered that the purchase page on General Wax’s retail 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. General Wax removed the malicious code and commenced a prompt and thorough investigation into the incident in consultation with external forensic investigators and data privacy professionals. As a result of this review, on or about April 7, 2023 General Wax determined that the payment card information that was potentially accessed and/or acquired related to certain transactions made through General Wax’s website check out page between February 16, 2023 through March 2, 2023.

General Wax is providing the affected residents with written notification of this incident commencing on or about May 10, 2023 in substantially the same form as the letter attached hereto. General Wax will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. General Wax will advise the affected residents to remain vigilant and to call their bank or card issuer if they see any suspicious transactions. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At General Wax, protecting the privacy of personal information is a top priority. General Wax is committed to maintaining the privacy of personal and financial information in its possession and has taken many precautions to safeguard it. Should you have any questions

May 10, 2023

Page 2

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

Very truly yours,



Encl.

Dominic A. Paluzzi

General Wax & Candle Co
Return Mail to IDX
4145 SW Watson Ave, Suite 400
Beaverton, OR 97005



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

May 10, 2023

Dear [REDACTED]

We are writing with important information regarding a recent data security incident experienced by General Wax & Candle Company ("General Wax") involving unauthorized access to a limited subset of our customers' payment card data used at www.generalwax.com. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently discovered that the purchase page on our retail 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 removed the malicious code and commenced a prompt and thorough investigation into the incident in consultation with external forensic investigators and data privacy professionals. As a result of this review, we determined that the payment card information that was potentially accessed and/or acquired related to certain transactions made through our website check out page between February 16, 2023 through March 2, 2023.

What Information Was Involved?

The information that was potentially accessed and/or acquired in this incident included customer names, contact information, credit or debit card numbers, card expiration dates and CVV numbers (3 or 4 digit code on the front or back of the card). On April 7, 2023 we determined that you completed a transaction at our website during the window of compromise and that your card information and contact information may potentially be at risk.

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 to ensure that it is secure and cleared of any malicious activity.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide you with steps you can take to protect your information further. 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 apology that this incident occurred. We are committed to maintaining the privacy of our customer's information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our customer's information, and have taken steps to prevent further unauthorized access to customer records.

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

Sincerely,

General Wax & Candle Company

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

You may place an initial 90-day “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. **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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>
(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.

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: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

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, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.