

Karen Bridges
Direct Dial: 312.642.7127
E-mail: kbridges@mcdonaldhopkins.com

October 7, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: Name Badges, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Name Badges, LLC (“Name Badges”). Located in Cooper City, Florida,¹ Name Badges is a provider of custom name badges, name tags, and identification products. I am writing to provide notification of an incident at Name Badges that may affect the security of personal information of approximately thirty-eight (38) Maryland residents. By providing this notice, Name Badges does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On May 9, 2024 Name Badges’ credit card processing company informed Name Badges of a potential breach of credit card information from December 9, 2023 to December 23, 2024. Upon learning of the potential unauthorized activity, Name Badges immediately commenced a thorough investigation. As part of its investigation, Name Badges engaged a third party cybersecurity firm to confirm whether information from that period was actually impacted and identify what personal information, if any, was involved.

After an extensive forensic investigation and manual document review, Name Badges discovered on or about July 17, 2024 that a limited number of files potentially acquired by the unauthorized party, from November 27, 2024 to February 9, 2024, contained personal information pertaining to a limited number of individuals, such as full names, addresses, and payment card information.

Name Badges is providing the affected residents with written notification of this incident commencing on or about October 7, 2024 in substantially the same form as the letter attached hereto. Name Badges will advise the affected individuals to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected

¹ 12240 SW 53rd Street, Suite 511, Cooper City, FL 33330

October 7, 2024

Page 2

individuals will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

If you have any additional questions, please contact me at (312) 642-7127 or kbridges@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in dark ink that reads "Karen Bridges". The signature is written in a cursive, flowing style.

Karen Bridges

KB/efg

Name Badges, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



IMPORTANT INFORMATION - PLEASE REVIEW CAREFULLY

Dear [REDACTED],

We are writing to inform you of a data security incident at Name Badges, LLC involving some of your information. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On May 9, 2024, our credit card processing company informed us of a potential breach of credit card information from December 6, 2023 to December 23, 2024.

What Are We Doing?

Upon learning of the potential unauthorized activity, we promptly commenced an immediate and thorough investigation. As part of our investigation, we engaged a third-party cybersecurity firm to conduct a forensic investigation to confirm whether information from that period was actually impacted and to identify what personal information, if any, was involved.

What Information Was Involved?

After an extensive forensic investigation and manual document review, we discovered on or about July 17, 2024 that one or more of the files potentially acquired by the unauthorized party may have contained your [REDACTED]. Please note that your information was not identified in the December 6, 2023 to December 23, 2023 time frame. However, we are notifying you out of an abundance of caution.

What Can You Do?

We have no evidence that any personal information has been or will be misused as a direct result of this incident. This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information

Please accept our apologies that this incident occurred. We are 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 and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please 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, from 8:00 a.m to 8:00 p.m. Eastern Time, excluding holidays.

Sincerely,

Name Badges, LLC

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert.

We recommend that you 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 30348-5069
<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.



00001020280000

P

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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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, <https://www.marylandattorneygeneral.gov/>, 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.