

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

February 22, 2022

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: IAM Acquisition, LLC dba Coregistics – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents IAM Acquisition, LLC dba Coregistics (Coregistics). I am writing to provide notification of an incident at Coregistics that may affect the security of personal information of approximately one (1) Maryland resident. Coregistics' 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, Coregistics does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Coregistics recently became aware of potential unauthorized access to its email environment. Upon learning of the issue, Coregistics immediately commenced a prompt and thorough investigation. As part of the investigation, Coregistics has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, Coregistics discovered on January 20, 2022 that the email accounts that may have been accessed between May 31, 2021 and July 19, 2021 may have potentially contained personal information such a resident's full name and health insurance information.

Coregistics is providing notification of this incident commencing on February 22, 2022, in substantially the same form as the notice attached hereto. Coregistics is advising affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

February 22, 2022

Page 2

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

Sincerely,



Dominic A. Paluzzi

Encl.

IAM Acquisition LLC

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



[REDACTED]
[REDACTED]
[REDACTED]

February 22, 2022

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to Coregistics. We are writing to provide you with information regarding a data security that may have involved your personal information. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect personal information.

What Happened?

Coregistics recently became aware of potential unauthorized access to its email environment.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on January 20, 2022 that the email accounts that may have been accessed between May 31, 2021 and July 19, 2021 may have potentially contained some of your personal information.

What Information Was Involved?

The impacted email accounts may have contained some of your personal information, specifically your full name and [REDACTED]

What You Can Do.

We have no forensic evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident.

This letter provides 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.

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 personal information.

If you have any further questions regarding this incident, please call our toll-free response line at [REDACTED]
This response line is available Monday through Friday, 9 am – 9 am Eastern Time.

Sincerely,

[REDACTED]

[REDACTED]

Coregistics

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 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 105788
Atlanta, GA 30348
<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 LLC

P.O. Box 6790
Fullerton, PA 92834-6790
<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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

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

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
(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 monitoring 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.

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

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 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.

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.