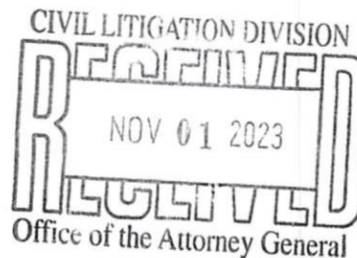


Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com



McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

October 26, 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: PMA Financial Network, LLC – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents PMA Financial Network, LLC (“PMA”). I am writing to provide notification of an incident at PMA that may impact the security of personal information of one (1) Maryland resident. By providing this notice, PMA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

PMA Financial Network has learned that an unauthorized actor briefly and temporarily obtained access to part of our network as a result of a sophisticated cybersecurity incident. Upon learning of this issue, PMA contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, PMA worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any sensitive data had been compromised because of the incident. After an extensive forensic investigation, PMA discovered on October 12, 2023 that the systems, which were accessed between June 12, 2023 and June 13, 2023, contained some personal information. The information involved includes individual name and Social Security number.

PMA has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, PMA wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. PMA is providing the affected resident with written notification of this incident commencing on or about October 26, 2023 in substantially the same form as the letter attached hereto. PMA is also offering the affected resident complimentary one-year membership with a credit monitoring service. PMA will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. PMA will advise the affected resident about the process for placing a fraud alert and/or security freeze

on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General Consumer Protection Division.

At PMA, protecting the privacy of personal information is a top priority. PMA is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. PMA 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) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'BLD', followed by a long horizontal flourish.

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl.

PMA Financial Network, LLC
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to PMA Financial Network. We are writing with important information regarding a recent data security incident that involved some of your information. We want 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?

PMA Financial Network has learned that an unauthorized actor briefly and temporarily obtained access to part of our network as a result of a sophisticated cybersecurity incident.

What We Are Doing.

Upon learning of this issue, we contained and secured the threat and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any sensitive data had been compromised because of the incident. After an extensive forensic investigation, we discovered on October 12, 2023 that the systems, which were accessed between June 12, 2023 and June 13, 2023, contained some of your personal information as described in more detail below.

What Information Was Involved.

The unauthorized actor gained access to some of your personal information, specifically [REDACTED] and [REDACTED].

What You Can Do.

We have no reason to believe that your information has been or will be misused as a direct result of this incident. Out of an abundance of caution, and to protect you from potential misuse of your information, we are offering a complimentary [REDACTED]-month membership of Equifax Complete™ Premier. For more information on identity theft prevention and Equifax Complete™ Premier including instructions on how to activate your complimentary [REDACTED] month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or 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.

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 toll-free response line at [REDACTED]. The response line is available Monday through Friday, 9:00 A.M. to 9:00 P.M.

Sincerely,

PMA Financial Network, LLC
[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary [REDACTED]-Month Credit Monitoring.**

Go to www.equifax.com/activate

Enter your unique Activation Code of [REDACTED] by [REDACTED], then click "Submit" and follow these 4 steps:

- **Register:**
 - Complete the form with your contact information and click "Continue".
 - *If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.*
 - *Once you have successfully signed in, you will skip to the Checkout Page in Step 4*
- **Create Account:**
 - Enter your email address, create a password, and accept the terms of use.
- **Verify Identity:**
 - To enroll in your product, we will ask you to complete our identity verification process.
- **Checkout:**
 - Upon successful verification of your identity, you will see the Checkout Page.
 - Click 'Sign Me Up' to finish enrolling.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary [REDACTED]-month credit monitoring services, 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

3. **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

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.

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 you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. 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.

5. 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.

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.

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.

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.

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.