



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

September 19, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Wright, Moore, DeHart, Dupuis & Hutchinson, LLC - Notice of Data Event

To Whom It May Concern:

We represent Wright, Moore, DeHart, Dupuis & Hutchinson, LLC (“WMDDH”) located at 100 Petroleum Drive Lafayette, LA 70508 and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately eighty-five (85) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WMDDH does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On or about July 11, 2023, WMDDH became aware of unusual network activity and immediately took steps to secure our systems. WMDDH launched an investigation with the assistance of leading cybersecurity experts to determine what happened and whether sensitive or personal information may have been affected during the incident. As a result of the investigation, WMDDH identified that certain data may have been acquired without authorization. WMDDH then engaged an independent team to conduct a comprehensive review of all potentially affected data, which review determined that personal information may have been affected. WMDDH then worked diligently to identify contact information to effectuate notification and prepare the services being offered to affected individuals, as provided in more detail below.

On September 10, 2024, WMDDH became aware of eighty-five (85) Maryland residents within the notification population. The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number, driver’s license number, passport number, medical/treatment information, and health insurance information.

2. Notice to Maryland Residents

On or about September 19, 2024, WMDDH provided written notice of this incident to approximately eighty-five (85) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Other Steps Taken and To Be Taken

Upon discovering the event, WMDDH moved quickly to investigate and respond to the incident, assess the security of WMDDH systems, and identify potentially affected individuals. WMDDH is also working to implement additional safeguards and training to its employees. WMDDH is providing access to credit monitoring services for 12 months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WMDDH is providing impacted individuals with guidance on how to better protect against identity theft and fraud. WMDDH is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

WMDDH is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-770-4234.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Aubrey Weaver', with a stylized, flowing script.

Aubrey Weaver of
Constangy, Brooks, Smith & Prophete LLP



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Re: Notice of Data <<Variable Data 1>>

Dear <<Full Name>>,

We are writing to inform you of a recent data security incident experienced by Wright, Moore, DeHart, Dupuis & Hutchinson, LLC ("WMDDH") that may have involved your personal information. At WMDDH, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened. On or around July 11, 2023, WMDDH became aware of unusual network activity and immediately took steps to secure our systems. We launched an investigation with the assistance of leading cybersecurity experts to determine what happened and whether sensitive or personal information may have been affected during the incident. As a result of the investigation, we identified that certain WMDDH data may have been acquired without authorization. WMDDH then engaged an independent team to conduct a comprehensive review of all potentially affected data, and on May 8, 2024, that review determined that your personal information may have been affected. WMDDH then worked diligently to identify contact information to effectuate notification and prepare the services being offered to affected individuals, as provided in more detail below. This process was completed on July 18, 2024.

What Information Was Involved. The information involved may have included your name, <<Breached Elements>>.

What We Are Doing. As soon as WMDDH learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are also providing you with information about steps you can take to help protect your personal information.

Additionally, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary <<CM Duration>> month membership in Equifax Credit Watch Gold. Equifax Credit Watch Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax Credit Watch Gold including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through Equifax® at no cost to you. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can enroll in the Equifax® identity protection services by visiting www.equifax.com/activate and using the Enrollment Code provided. Representatives are also available by calling 888-378-4329 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time and Saturday and Sunday 8:00 a.m. to 5:00 p.m. Central Time. Please note the deadline to enroll is <<Enrollment Deadline>>.

For More Information. If you have questions about the incident, please call the response line at 866-572-9678, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Wright, Moore, DeHart, Dupuis & Hutchinson, LLC

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Enroll in Monitoring Services



<<Full Name>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **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

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400
There were <<RI Count>> RI
residents affected.

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.