

# WOODS ROGERS VANDEVENTER BLACK

ATTORNEYS AT LAW

F. ELIZABETH BURGIN WALLER  
(540) 983-7625  
Beth.Waller@wrvblaw.com

**May 17, 2024**

**Via E-mail (Idtheft@oag.state.md.us)**

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann. § 14-3504(h)(1), I am writing on behalf of my client, Redmon, Peyton & Braswell LLP, ("RP&B") to notify you regarding the nature and circumstances of a recent data security incident. RP&B's mailing address is 510 King Street, Suite 301, Alexandria, VA 22314.

On or about April 8, 2024, RP&B learned that an unauthorized user had accessed its computer systems. Specifically, a cybercriminal contacted RP&B claiming to have removed certain information from the RP&B network. Immediately, RP&B took steps to triage the incident and protect the interests of their clients. As part of the incident response, my firm engaged outside cybersecurity experts to investigate this matter and confirm the continued security of RP&B's systems. Those experts have confirmed that RP&B's environment is presently secure – this incident did not interrupt the ability of any RP&B attorneys to represent their clients.

Simultaneous to fortification of the RP&B environment, RP&B attorneys reviewed and analyzed information residing on their systems to identify any potential risks to their clients and to determine the extent of any personally identifiable information that might have been accessed in this incident. As described in detail in the attached notification letter, personal information involved may have included one or more of the following types of information: names, information pertaining to RP&B representation, driver's license numbers, passport numbers, military identification numbers, and/or Social Security numbers.

As a precaution, RP&B has decided to offer all individuals with personally identifiable information impacted by this matter with 12 months of complimentary credit monitoring services through Kroll. We have notified and are cooperating with the FBI Cyber Crimes Division and the Cyber Intelligence Team of the Virginia State Police's Virginia Fusion Center.

In total, one (1) Maryland resident was impacted by this incident. We have worked expeditiously to identify and notify those with information potentially impacted. Attached for your reference is a sample of the notice letter that was sent by mail on May 16, 2024.

If you have any questions, please contact me.

Very truly yours,



F. Elizabeth Burgin Waller  
Principal  
Woods Rogers Vandeventer Black PLC

Enclosures



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

Dear <<First\_Name>> <<Last\_Name>> ,

Like many organizations around the country, Redmon, Peyton & Braswell LLP, (“RP&B”) recently discovered it was the victim of unauthorized access to our firm’s computer systems. We are writing to share with you how this incident may have affected your information, and, as a precaution, to provide you with steps you can take to help protect your information. While we cannot be certain your information was accessed for a malicious purpose, out of an abundance of caution we have arranged to offer identity monitoring services at no cost to you.

### **What Happened?**

On or about April 8, 2024, RP&B learned that an unauthorized user had accessed our firm’s computer systems. Specifically, a cybercriminal contacted us claiming that they had removed certain information from our network. Immediately, RP&B took steps to triage the incident and protect the interests of our clients. We engaged outside cybersecurity experts to investigate this matter and confirm the continued security of our systems. **Importantly, the ability of RP&B attorneys to provide our clients with high-quality representation has not been interrupted.** Simultaneous to the fortification of our environment, we rapidly reviewed and analyzed the information residing on our systems to determine any potential risks to our clients and to determine those clients whose information might have been accessed in this incident.

### **What Information Was Involved?**

Based on our review, we have determined that your personal information and/or information pertaining to your engagement of our legal services may have been accessed in this incident. In particular, your name in combination with information involving your representation by our firm or your driver’s license number, passport number, military identification number, and/or Social Security number may have been subject to unauthorized access.

### **What We Are Doing.**

We have notified the FBI Cyber Crimes Division and the Cyber Intelligence Team of the Virginia State Police’s Virginia Fusion Center. RP&B will fully support any law enforcement investigation. We take our obligation to safeguard client information very seriously and are continuing to evaluate additional actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

While we cannot be certain that your information was removed from our systems, as a precaution, we are offering 12 months of complimentary identity monitoring services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

### **What You Can Do.**

We encourage you to stay vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed Identity Theft and Protection Guide for additional information on how to help protect against identity theft and fraud. You may also take advantage of the identity monitoring services being offered through Kroll. Information regarding the identity monitoring services is included in the attached Identity Theft and Protection Guide.

**For More Information.**

If you have any further questions regarding this matter or the identity monitoring services provided, please call <<Kroll TFN>> toll-free Monday through Friday from 9:00 AM to 6:30 PM Eastern Time, excluding major U.S. holidays. Please have your Membership Number ready: <<Membership Number (S\_N)>>.

Please also note that RP&B is utilizing Kroll's return mail service, so the return address on this letter is to their mailing center, which is not based in Virginia.

We deeply regret that this event occurred and are committed to supporting you.

Sincerely,

A handwritten signature in black ink, appearing to read "J.F.R.", is positioned above the typed name.

John F. Rodgers  
Managing Member  
Redmon Peyton & Braswell LLP

## **IDENTITY THEFT PROTECTION GUIDE AND INFORMATION**



We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

### **Activate Your Identity Monitoring Services**

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until <<b2b\_text\_6 (ActivationDeadline)>> to activate your identity monitoring services.*

Membership Number: <<Membership Number (S\_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

### **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

#### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

### **Review Your Account Statements and Obtain and Monitor Your Credit Report**

As a precautionary measure, we recommend that you remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft resulting from the security incident. You may periodically obtain your free credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 9701  
Allen, TX 75013-9701  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 1000  
Chester, PA 19016-1000  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for inaccurate information, such as a home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

### **Notify Law Enforcement of Suspicious Activity**

You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To file a complaint with the FTC, use the below contact information or website.

**The Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.IdentityTheft.gov](http://www.IdentityTheft.gov)

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which the account is maintained.

### **Credit Freezes**

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact **all three** major consumer reporting agencies listed below.

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016-2000  
1-800-916-8800  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Your full name, with middle initial and any suffixes;
- 2) Your Social Security number;
- 3) Your date of birth (month, day, and year);

- 4) Your current address and previous addresses for the past five (5) years;
- 5) A copy of your state-issued identification card (such as a state driver's license or military ID);
- 6) Proof of your current residential address (such as a current utility bill or account statement); and
- 7) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request. More information regarding credit freezes can be obtained from the FTC and the major consumer reporting agencies.

### **Fraud Alerts**

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file one (1) year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the three major consumer reporting agencies listed above. The agency you contact will then contact the other two. More information regarding fraud alerts can be obtained from the FTC and the major consumer reporting agencies.

### **Monitor Your Personal Health Information**

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number. You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records.

### **Additional Resources and Information**

You can obtain additional information and further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state attorney general or the FTC. The FTC's contact information and website for additional information is:

**The Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For Virginia residents:** You may contact the Virginia Attorney General's Office at 202 North Ninth Street, Richmond, VA 23219; 1-804-786-2071; or <https://www.oag.state.va.us/contact-us/contact-info>.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; or <https://portal.ct.gov/ag>.

**For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; or <https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy>.

**For Iowa residents:** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at 1305 E. Walnut Street, Des Moines, IA 50319; 15152815164; or [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; 1-888-743-0023 (toll free), or <https://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General at 1 Ashburton Place, Boston, MA 02108; 1-617-727-8400; or <https://www.mass.gov/orgs/office-of-the-attorney-general>. You have the right to obtain a police report if you are a victim of identity theft.

**For New Mexico residents:** You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your credit file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit

[https://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf) or [www.ftc.gov](http://www.ftc.gov).

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>. You may also contact the Bureau of Internet and Technology (BIT) at 28 Liberty Street, New York, NY 10005; 21241684331; or <https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>.

**For North Carolina residents:** The North Carolina Attorney General’s Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 919-716-6400; or <https://ncdoj.gov/contact-doj/>.

**For Oregon residents:** We encourage you to report suspected identity theft to the Oregon Attorney General at 1162 Court Street NE, Salem, OR 97301; 18778779392; 15033784400; or [www.doj.state.or.us](http://www.doj.state.or.us).

**For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or <https://riag.ri.gov/>. You have the right to obtain a police report if you are a victim of identity theft. Zero Rhode Island residents were impacted by this breach.