POLSINELLI

2100 Southbridge Pkwy, Suite 650, Birmingham, AL 35209

June 25, 2024

Adam Griffin
(205) 963-7139
(615) 523-2397 (Fax)
agriffin@polsinelli.com

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

Re: Notice of a Security Incident

Dear Attorney General Brown:

Pursuant to Md. Code. Ann., Com. Law § 14-3504(h), I am writing to report a security incident on behalf of our client, Dial, Grimm, and Rupert, LLC, ("DGR" or the "Firm"). DGR is a full-service law firm that assists clients with real estate matters.

On January 16, 2024, DGR discovered suspicious activity in a single employee's e-mail account. Upon discovering the situation, DGR immediately secured the account and engaged external cybersecurity experts to investigate. The investigation determined that on or around October 30, 2023, an unauthorized third party gained temporary access to the e-mail account in an attempt to commit financial fraud against DGR.

DGR subsequently determined on April 22, 2024, that the threat actor may have accessed certain files within the e-mail account that contained the personal information of four (4) Maryland residents. While the exact information tended to vary by record and individual, DGR identified documents that included individual name, financial account information, and/or social security number.

DGR notified affected individuals on June 20, 2024 via U.S. mail to inform them of the situation and provide resources to monitor and protect their personal information, including 12 months of complimentary credit and identity monitoring services. A copy of the individual notice is enclosed.

DGR has been working with cybersecurity experts to investigate what happened and to further strengthen its computer network. DGR has no indication that any personal information has been acquired or misused as a result of this incident. As part of its ongoing commitment to information security, DGR will continue to evaluate and prioritize enhancing its cybersecurity defenses.

Very truly yours,

Adam Griffin

Enclosure

DIAL
GRIMM
RUPERT

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Dial Grimm and Rupert, LLC ("DGR") is notifying you of a recent security incident that may have involved your personal information. DGR is a full service law firm that assists clients with real estate matters. You may have provided information to DGR as part of a recent real estate transaction. We take this event and the security of information in our care seriously.

DGR has been investigating this situation with the help of external cybersecurity experts. We have no indication that <u>any</u> personal information has been misused as a result of this incident. However, as a precautionary measure, you can enroll in a credit and identity monitoring solution through Kroll at no cost to you. DGR will provide identity monitoring services to you for 12 months free of charge.

Additional information about the incident, our ongoing response, and the resources that are available to help protect your information can be found below.

What Happened? On January 16, 2024, DGR discovered suspicious activity in a single employee's email account, and immediately began an investigation with the help of outside cybersecurity experts. The investigation determined that an unauthorized third party gained temporary access to the employee's email account on or around October 30, 2023, in an attempt to commit financial fraud against DGR. We subsequently learned on April 22, 2024 that although not the target of the fraud attempt, the fraudsters potentially had access to certain files within the employee's email account containing your personal information.

What Information Was Involved? The information identified within these files included your <<b2b_text_1 (data elements)>>.

What We Are Doing. We have been working with external cybersecurity experts to investigate what happened and to further bolster our cybersecurity defenses. These efforts are all ongoing. We are notifying you now that we know what information was involved.

What You Can Do. We are providing an Identity Protection Reference Guide that includes information on general steps you can take to monitor and protect your personal information. You will also find information enclosed on how to activate the credit and identity monitoring services if you are interested in these services.

For More Information. If you have any questions or concerns, please reach out to our dedicated support team at (866) 898-2377 between 8:00 am and 5:30 pm CST, Monday through Friday (excluding major holidays).

Sincerely,

Matthew Rupert
Member

Chad Dial
Member

Robert J. Grimm
Member

<u>Columbia Central</u>
121 Executive Center Dr. Suite 218
Columbia, SC 29210
803-828-7661

<u>Columbia Northeast</u>
1120 Sparkleberry Ln. Extension Suite C
Columbia, SC 29223
803-828-7661

<u>Sumter</u>
106 Broad Street
Sumter, SC 29153
803-418-5700

<u>Orangeburg</u>
161 Centre Street
Orangeburg, SC 29115
803-828-7661

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax https://www.equifax.com/personal/credit-report-services/ 1-888-298-0045 Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian https://www.experian.com/help/ 1-888-397-3742 Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion https://www.transunion.com/credit-help 1-800-916-8800 TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no cost to place a security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438- 4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-866-366-8343 or (410) 576-6491, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

Rhode Island Residents: You can obtain additional information about identity theft prevention and protection from the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. There is approximately 1 Rhode Island resident that may be impacted by this event.

To help relieve concerns and restore confidence following this incident, 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, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6 (activation deadline)>> 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.

Additional information describing your services is included with this letter.

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.