

Melissa K. Ventrone
T (312) 360-2506
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

January 27, 2023

Via Electronic Mail to IDTheft@oag.state.md.us

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

To Whom it May Concern:

We represent the law firm of Gordon, Dodson, Gordon & Rowlett (“GDGR”) as Outside Counsel with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. GDGR, a law firm located in Chesterfield, VA, is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

After identifying suspicious activity associated with one of its firm email accounts, GDGR implemented its incident response protocols and engaged an independent computer forensic vendor to assist with an investigation. On December 14, 2021, the investigation found unauthorized access to three email accounts but was unable to determine whether any information in the accounts was compromised. GDGR then hired a vendor to conduct an in-depth review of the email accounts to identify any personal information that may have been present. This review was recently completed, and it appears the information in the email accounts may have included individuals’ names, addresses, financial account information, Social Security numbers, and limited medical information.

2. Number of residents affected.

Four (4) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on January 26, 2023. A copy of the form notification letter is enclosed.

January 27, 2023

Page 2

3. Steps taken in response to the incident.

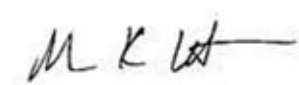
Since this incident, GDGR changed the passwords to the affected firm email accounts and implemented multifactor authentication for remote access. Additionally, impacted individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact Information

GDGR takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read "M K Ventrone", with a horizontal line extending to the right.

Melissa K. Ventrone



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 23, 2023

NOTICE OF DATA SECURITY INCIDENT

Dear <<First Name>> <<Last Name>>,

Gordon, Dodson, Gordon & Rowlett (“GDGR”) is writing to let you know about a data security incident that may have affected your personal information. GDGR may have been provided with your information in the course of litigation or to provide other legal services. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about what occurred, steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

We discovered suspicious activity associated with one of our email accounts, implemented our incident response protocols and hired an independent computer forensics firm to help us investigate. On December 14, 2021, the investigation found unauthorized access to three email accounts but was unable to determine whether any information in the accounts was accessed. Thus, out of an abundance of caution, we hired a vendor to review the contents of the accounts to determine whether any personal information was present. This review was recently completed at which point we learned that your personal information was present in the affected accounts.

What Information Was Involved?

From our review, it appears that your name, <<variable text>> may have been contained in the impacted accounts.

What We Are Doing

We want to assure you that we have taken steps to prevent a similar incident from happening in the future, including changing passwords on the impacted email accounts and implementing multi-factor authentication for remote access.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services provider, at no charge to you. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 23, 2023. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-800-939-4170 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Gordon, Dodson, Gordon & Rowlett

Gordon, Dodson, Gordon & Rowlett



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at **1-800-939-4170** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. 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. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only 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 will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the 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. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: 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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. [XX] Rhode Island residents were notified of this incident. You have the right to obtain any police report filed regarding this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.