



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:lmventrone@ClarkHill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

July 15, 2021

VIA ONLINE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Aaron Frey:

We represent Gilmore Rees & Carlson, PC (“GRC”) with respect to a security incident involving the potential exposure of certain personally identifiable information described in more detail below. GRC, located in Wellesley, Massachusetts, is a law firm advising on trust and estate matters. GRC is committed to answering any questions you may have about the security incident, its response, and steps taken to minimize the risk of a similar incident in the future.

1. Nature of security incident.

On March 17, 2021, GRC experienced a security incident that interrupted access to its systems. As soon as GRC learned of the incident, GRC began an internal investigation and hired independent cybersecurity specialists to help determine what occurred and whether any information was at risk. The cybersecurity specialists determined that an unauthorized actor gained access to certain GRC systems and deployed malware within the environment. The investigation also determined that certain files containing employee and client personal information may have been accessed or taken by the unauthorized actor. GRC reviewed the contents of the files, and on June 30, 2021, GRC completed the review and identified all potentially impacted individuals. For affected individuals, one or more of the following personal identifiers were impacted, including names, dates of birth, driver’s license numbers, Social Security numbers, and financial account information.

2. Number of residents affected.

Ten (10) Maine residents may have been affected and were notified of the incident. A notification letter was issued to all impacted on July 15, 2021 via regular mail. A copy of the template notification letter is enclosed.

3. Steps taken relating to the incident.

Since the incident, GRC has taken steps to minimize the risk of this happening in the future, including but not limited to resetting all passwords and fully deploying advanced endpoint threat detection and

July 15, 2021

Page 2

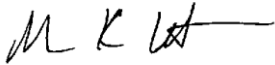
monitoring on all network-connected systems. Credit monitoring and identity protection services through IDX were offered at no cost. Finally, the Federal Bureau of Investigation was notified of this incident, and GRC is cooperating with its investigation.

4. Contact information.

GRC 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.

Very truly yours,

CLARK HILL

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

Melissa K. Ventrone
Partner

(Enclosure)

GILMORE REES & CARLSON PC

ATTORNEYS AT LAW

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-909-3922
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<XXXXXXXX>>

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

July 15, 2021

Notice of Data Security Incident

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

I am writing to inform you of a data security incident experienced by Gilmore Rees & Carlson, PC (“GRC”) that may have impacted your personal information, including your name, <<variable data 1>>, and other information described in greater detail below. GRC takes the privacy and security of your information seriously, and sincerely apologizes for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened:

On March 17, 2021, GRC experienced a security incident that interrupted access to its systems. As soon as GRC learned of the incident, GRC began an internal investigation and hired independent cybersecurity specialists to help determine what occurred, and whether any information was at risk. Unfortunately, the investigation recently determined that some files may have been taken by the unauthorized actor. We reviewed the contents of the files, and on June 30, 2021, determined that your personal information may have been impacted by this incident.

What information was involved:

From our investigation, the files may have contained your name, <<variable data 2>>.

What we are doing:

GRC wants to assure you that it is taking steps to minimize the risk of this happening in the future. Since the incident, GRC conducted a password reset for all users and has also fully deployed advanced endpoint threat detection and monitoring on all network-connected systems. GRC has also notified and is cooperating with federal law enforcement. In addition, while GRC is not aware of any misuse of your information, GRC has arranged for you to receive credit monitoring and identity protection services at no cost to you, as a precautionary measure.

What you can do:

GRC is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

GRC encourages you to remain vigilant against incidents of identity theft by reviewing account statements for unusual activity. You should immediately report any suspicious activity.

How to enroll in IDX: You can sign up online or via telephone

GRC encourages you to contact IDX with any questions and to enroll in free services by calling 1-833-909-3922 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is October 14, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

If you have questions about this incident:

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, 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.

For enrollment assistance and any questions regarding this incident, please contact IDX at 1-833-909-3922 Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://app.idx.us/account-creation/protect> for enrollment assistance.

Your trust is a top priority for me and all of GRC, and I deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Robert J. Morrill
Managing Partner
Gilmore Rees & Carlson, PC



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 1-833-909-3922 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.

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/>.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

Texas Residents: Office of the Attorney General of Texas, P.O. Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, Telephone: 1-800-621-0508.

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.