

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

October 5, 2023

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Anthony Brown

We represent Greater Rochester Independent Practice Association, Inc. (“GRIPA”) with respect to a data security incident involving personal information as described below. GRIPA provides delegated provider credentialing services to various health plans. GRIPA takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On May 31, 2023, GRIPA learned of the global exploit on Progress Software Company’s file transfer program, MOVEit. GRIPA stopped access to MOVEit and conducted an investigation to determine what occurred and whether any data was compromised. The investigation was completed on June 5, 2023. At that point GRIPA determined that files were taken from the MOVEit server. A vendor was engaged to review the at-risk files for any personal or protected health information. This process was completed on August 14, 2023, at which point GRIPA determined that personal information was impacted.

Impacted information includes names with some combination of the following: addresses, Social Security numbers, dates of birth, and tax identification numbers.

2. Number of residents affected

Ten (10) Maryland residents were notified of the incident. A notification letter was sent to the potentially affected individuals on October 5, 2023, via regular mail (a copy of the template notification is enclosed).

3. Steps taken in response to the incident

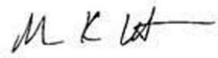
Immediately after learning of the MOVEit compromise, GRIPA stopped access to the MOVEit service, securely restored their servers from backups, and applied the patch(es) provided by the MOVEit software provider, Progress. Additionally, affected individuals were offered twelve months of credit monitoring and identity protection services through IDX.

4. Contact information

GRIPA takes the security of the information in its control seriously and is committed to ensuring information within its control 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
Member

cc: Sunaina Ramesh



4145 SW Watson Ave., Suite 400
Beaverton, OR 97005

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

October 5, 2023

Notice of Data Security <<Breach/Incident>>

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

We wanted to let you know of a recent security incident at Greater Rochester Independent Practice Association, Inc. ("GRIPA"). GRIPA provides credentialing services to various health plans and would have obtained your information to perform these services. GRIPA uses the file transfer tool MOVEit to send and received files, and recently learned that it was impacted by the global attack on MOVEit. Your personal information was included in files transferred via MOVEit.

We take the privacy and security of your information seriously. We apologize 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 May 31, 2023, we learned of the global attack on the file transfer tool called MOVEit. We immediately stopped access to MOVEit. We then conducted a forensic investigation to understand what occurred and whether any data was compromised. The investigation was completed on June 5, 2023. At that point we determined that files were taken from the MOVEit server. We then worked with a vendor to review these files for any personal information. This process was completed on August 14, 2023, when we learned that some of your personal information was impacted. We have no indication that any of your personal information has been misused, but wanted to let you know about this incident and provide you with resources to protect yourself.

What Information Was Involved?

From our review, it appears that your name, <<Data Elements>> may have been affected.

What We Are Doing:

Immediately after learning of the MOVEit attack, we stopped access to the MOVEit service. We securely restored our servers from backups and applied the patch provided by the MOVEit software provider, Progress. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. 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 recover services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-888-743-6538 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 January 5, 2024.

You should also review the enclosed information, which describes additional steps you can take to help protect yourself, 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. You should also regularly review your credit reports and financial statements, and immediately report any suspicious activity.

For More Information:

If you have questions, please call 1-888-743-6538, Monday through Friday from 9 am - 9 pm Eastern Time. Please have your Enrollment Code ready. Protecting your information is important to us. We sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Greater Rochester Independent Practice Association, Inc

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 1-888-743-6538 to gain additional information about this incident 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.

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.

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

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/201504_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.

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.

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.