

Nicholas A. Kurk, CIPP/US
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

September 14, 2022

VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Saggar & Rosenberg, P.C. – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Saggar & Rosenberg, P.C. (“S&R”). S&R is a CPA firm located in Rockville, Maryland that provides specialized tax, accounting and business advisory services to its clients. I am writing to provide notification of an incident that may affect the security of personal information of two hundred and four (204) Maryland residents. S&R’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, S&R does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On May 15, 2022, S&R detected potential unauthorized access to its network. Upon learning of this issue, S&R contained and secured the threat, commenced a prompt and thorough investigation, and notified law enforcement. S&R immediately launched an investigation in consultation with outside cybersecurity professionals to help determine whether any sensitive data had been compromised because of the incident. S&R’s investigation determined that the unauthorized individual(s) potentially accessed certain files and folders from portions of its network between May 4, 2022 and May 13, 2022. The system intrusion did not affect the majority of S&R’s data, which resides with cloud-based third-party service providers that were not impacted by the security incident. Nor did this incident affect individual tax return files in any way.

On August 15, 2022, following an extensive review and analysis of the data at issue, S&R determined that certain files and folders potentially accessed from its network contained the residents’ full name and Social Security number. While the cybersecurity professionals could not conclusively establish that any data was removed from S&R’s network, we nonetheless wanted to inform you (and the affected residents) of this incident

At the time of this notification, S&R is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, we wanted to explain the steps that it is taking to help safeguard the affected residents against identity fraud. S&R is providing the affected residents with written notification of this incident commencing on or about September 14, 2022 in substantially the same form as the letter attached hereto. Where, as here, a Social Security number was impacted, S&R is offering the affected residents complimentary one-year membership with a credit monitoring service. S&R will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. S&R will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At S&R, protecting the privacy of personal information is a top priority. S&R is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. S&R continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,



Nicholas A. Kurk, CIPP/US

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

September 14, 2022

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to Saggar & Rosenberg, P.C. (“S&R”). We are writing with important information regarding a recent data security incident that may potentially have involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On May 15, 2022, S&R detected a system intrusion that began encrypting certain select files that contained personal information related to individuals that were stored on S&R’s local network. The system intrusion did not affect the majority of S&R’s data, which resides with cloud-based third-party service providers that were not impacted by the security incident. Nor did this incident affect individual tax return files in any way.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network, restored any encrypted data, and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Though the investigation is ongoing, S&R determined on August 15, 2022 that unknown individual(s) may have had access to certain files and folders that were stored on our network. While the cybersecurity professionals could not conclusively establish that any data was removed from our network, we nonetheless wanted to make you aware of this incident.

What Information Was Involved.

The impacted files contained some of your personal information, specifically your name, [REDACTED]
[REDACTED]

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership in identity theft protection services through IDX, the data breach and recovery services provider. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy through IDX, and fully managed id theft recovery services. With this protection, IDX

will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

Saggar & Rosenberg, P.C.
One Church Street
Suite 700
Rockville, MD 20850

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

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. 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. Please note that the enrollment deadline is [REDACTED].

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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069

Atlanta, GA 30348-5069

[https://www.equifax.com/personal/credit-report-services/credit-](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

[fraud-alerts/](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

[https://www.experian.com](https://www.experian.com/fraud/center.html)

[/fraud/center.html](https://www.experian.com/fraud/center.html)

(888) 397-3742

TransUnion

Fraud Victim Assistance

Department

P.O. Box 2000

Chester, PA 19016-2000

[https://www.transunion.com/fra](https://www.transunion.com/fraud-alerts)

[ud-alerts](https://www.transunion.com/fraud-alerts)

(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

[https://www.equifax.com/personal/c](https://www.equifax.com/personal/credit-report-services/credit-freeze/)

[redit-report-services/credit-freeze/](https://www.equifax.com/personal/credit-report-services/credit-freeze/)

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

[http://experian.com/freez](http://experian.com/freeze)

[e](http://experian.com/freeze)

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

[https://www.transunion.com/cre](https://www.transunion.com/credit-freeze)

[dit-freeze](https://www.transunion.com/credit-freeze)

(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There was 1 Rhode Island resident impacted by this incident.