

420 Main St Suite 1100, Buffalo, New York 14202
75 S. Clinton Ave., 510 Clinton Square, Suite 555, Rochester, New York 14604
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300, #704, Bala Cynwyd, Pennsylvania 19004



716.898.2102
octillolaw.com
info@octillolaw.com

April 26, 2023

VIA Email only to ldtheft@oag.state.md.us

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

Dear Sir or Madam:

On behalf of NYSARC Columbia County Chapter ("COARC"), and pursuant to the Personal Information Protection Act ("PIPA"), Md. CodeAnn. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, COARC does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of the Maryland data notification laws or personal jurisdiction.

On July 19, 2022, COARC experienced a ransomware incident that impacted a limited number of devices and systems. COARC immediately launched an investigation, reported the matter to law enforcement, and retained leading cybersecurity and privacy professionals. Our investigation determined that for a brief amount of time in July 2022, an unauthorized actor obtained access to COARC systems, seemingly for the sole purpose of encrypting certain data with ransomware. The nature of the unauthorized actor and their attack extended the amount of time required to investigate the data involved in this matter and identify individuals involved. COARC immediately implemented measures to further improve the security of systems and practices and continues to work with leading data security and privacy professionals to continue to improve their security and environment. COARC has identified four (4) Maryland individuals who may have been affected by the security incident. The personal information identified in relation to these individuals is: financial account information.

Since the incident, COARC took numerous steps to recover from the criminal attack and bolster its security program, including revising policies and protocols, enhancing data security controls and applying additional multifactor authentication.

Attached for your convenience is a copy of the template notification that was sent to the impacted Maryland residents, today, April 26, 2023.

Please feel free to contact me with any questions at 716-898-2102 or dgreene@octillolaw.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel P. Greene".

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encls.

COARC
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



[REDACTED]
[REDACTED]
[REDACTED] B-1

April 26, 2023

Dear [REDACTED]:

I am writing to inform you that we, NYSARC Columbia County Chapter (“COARC”) recently experienced a data security incident (“Incident”), which potentially involved your personal information (“Information”). This letter provides you with information about this Incident, the extent of the Incident, and if you have any concerns, information on where to direct your questions. Additionally, although we are unaware of any misuse of your Information, as a precaution we also provide steps you can take to protect your Information.

What Happened?

On July 19, 2022, COARC experienced a ransomware incident that impacted a limited number of our devices and systems. We immediately launched an investigation and retained leading cybersecurity and privacy professionals to assist us in identifying the scope of the incident and resuming business. We have since been working to fully understand the scope of the unauthorized activity and determine what data was impacted. Our investigation concluded and determined limited information was potentially affected as a result of the Incident. Our investigation determined that for a brief amount of time in July, an unauthorized actor obtained access to our systems, seemingly for the sole purpose of encrypting certain data with ransomware. While COARC is unaware of any misuse of your information, we are providing this notification out of an abundance of caution.

What Information Was Involved?

We determined the following data related to your information was present: Social Security number, financial account and medical information.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices and notified law enforcement. We worked with a leading privacy and security firm to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

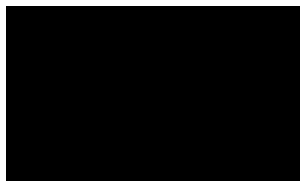
What Can You Do?

It is always recommended that you regularly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

You can contact COARC at [REDACTED] with questions about this matter or to seek further assistance. Alternatively, please call [REDACTED] Monday through Friday, from 8:00 a.m. to 5:00 p.m. Eastern (excluding some U.S. national holidays).

Sincerely,

A large black rectangular redaction box covering the signature area.

Chief Executive Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. 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, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, 445 Minnesota Street, Suite 1400, St. Paul, MN 55101, www.ag.state.mn.us, 1-651-296-3353.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <http://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. Submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.