



LEGAL + TECH

Liberty Building, 420 Main Street, Suite 1110, 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

August 12, 2022

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Sir or Madam:

On behalf of Lewis Johs Avallone Aviles LLP (“Lewis Johs”), and pursuant to the Personal Information Protection Act (“PIPA”), this letter provides notice of a recent data security incident. By providing this notice, Lewis Johs does not waive any rights or defenses regarding the applicability of Maryland law, and the applicability of the Maryland data notification laws or personal jurisdiction.

In December 2021, Lewis Johs detected irregular activity, identified as a ransomware attack, that impacted a limited number of Lewis Johs’ systems (the “Incident”). Upon becoming aware of the Incident, Lewis Johs immediately began an investigation and took measures to address and contain the Incident, including contacting law enforcement and engaging data privacy and security experts. At the conclusion of the investigation, in June, it was determined that for a limited period of time in December, an unauthorized actor obtained access to and acquired certain files from Lewis Johs’ systems. At this time, there is no evidence information has been misused; nevertheless, Lewis Johs is providing this notice.

The investigation determined the following types of information, in combination with a first name or initial and last name, may have been impacted: address; date of birth; Social Security Number; driver’s license number or other government issued identification; passport number; financial account number in combination with any required security code, access code, or password; payment card number; health insurance information or other medical information. Note that this describes general categories of information involved in this Incident, and that not all data elements were present for each potentially affected individual.

Since the Incident, Lewis Johs has implemented measures to further improve the security of its systems and practices including implementing two-factor authentication for all employees to protect the PCs and servers for remote and local logins, implementing two-factor authentication for all email accounts, and working with third-party experts to provide additional trainings to employees and staff on phishing emails and cybersecurity best practices.

Maryland Attorney General

August 12, 2022

Page 2

Attached for your convenience is a copy of the template notification that is being sent to the impacted Maryland residents, today, August 12, 2022. 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 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

Lewis Johs Avallone Aviles, LLP
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



NOTICE OF DATA BREACH



I am writing to inform you that we, Lewis Johs Avallone Aviles LLP (“Lewis Johs” or “we”), recently experienced a data security incident (“Incident”) which potentially involved your personal information (“Information”). This letter provides you with information about this Incident, the investigation, and although we are unaware of any misuse of your Information, steps you can take to protect your Information.

What Happened?

In December 2021, Lewis Johs detected irregular activity, identified as a ransomware attack, that impacted a limited number of our systems. Upon becoming aware of the Incident, we immediately began an investigation and took measures to address and contain the Incident, including contacting law enforcement and engaging data privacy and security experts. At the conclusion of our investigation, in June, it was determined that for a limited period of time in December, an unauthorized actor obtained access to and acquired certain files from our systems. At this time, there is no evidence Information has been misused; nevertheless, we are providing this notice.

What Information Was Involved?

Our investigation determined the following types of Information including your name may have been impacted: address; date of birth; Social Security Number, driver’s license number or other government issued identification; passport number; financial account number in combination with any required security code, access code, or password; payment card number, health insurance Information or other medical Information. Note that this describes general categories of Information involved in this Incident, and it likely includes categories that are not relevant to you.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. 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 monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

If you have any questions about the Incident, please call 888-605-3029, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Central (excluding some U.S. national holidays).

Sincerely,

A handwritten signature in black ink, appearing to read 'F. Johs', with a stylized, flowing script.

Frederick C. Johs

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 twelve (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.

For New Mexico residents: 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 may 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 or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

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 Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

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 Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

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, <https://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 Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

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 Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon 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.