

Buffalo
New York
Washington D. C.

www.octillolaw.com



June 2, 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 Alan J. Straus, P.C., ("Straus"), and pursuant to the Personal Information Protection Act ("PIPA"), Md. Code Ann. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, Straus 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.

In March 2023, Straus discovered suspicious activity related to one (1) employee's email account (the "Account") and immediately began an investigation and took steps to contain and remediate the situation, including changing passwords, engaging cybersecurity professionals to assist, and notifying the Internal Revenue Service, state tax authorities, and law enforcement. Straus also engaged a leading data security and privacy firm to assist its investigation and implemented additional safeguards on top of the firm's existing protections.

The investigation found that unauthorized actors accessed the Account and one (1) system used for the storage of tax information. The investigation concluded that tax information related to four (4) Maryland residents could have been present in the affected systems and accessed without authorization at the time of the incident.

Accordingly, Straus is providing written notification to the four (4) potentially affected Maryland residents via U.S. mail, beginning on June 2, 2023. A copy of that individual notice is attached for your review.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Patrick D. McNally", written in a cursive style.

Patrick D. McNally, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear [REDACTED],

In March 2023, we wrote to advise you of a potential data security incident (the “Incident”) that may have affected your personal information. We are writing now to provide an update on our investigation and remediation of the Incident, and, as a precaution, provide you with further resources and steps you can take to help protect your information.

What Happened?

In March 2023, we discovered suspicious activity related to one (1) employee’s email account (the “Account”). We immediately began an investigation and took steps to contain and remediate the situation, including changing passwords, engaging cybersecurity professionals to assist, and notifying the Internal Revenue Service, state tax authorities, and law enforcement. Out of an abundance of caution, we also engaged a leading data security and privacy firm to assist our investigation and implemented additional safeguards on top of our existing protections.

Our investigation concluded that unauthorized actors accessed the Account and one (1) system used for the storage of tax information. Your tax information could have been present in that system at the time of the Incident. Based on the findings of our investigation, it is possible that your personal information and, if applicable and present in your tax file, the personal information of your dependents, was accessed without authorization during the Incident.

What Information Was Involved?

We have determined that unauthorized actors may have accessed information included within your tax file relating to you and, if applicable, your dependents, including Social Security numbers, tax identification numbers, dates of birth, banking information, and health insurance policy numbers.

What We Are Doing.

After discovering the suspicious activity, we immediately began an investigation and notified tax authorities and law enforcement. We have since worked with the Internal Revenue Service to share information and take steps to protect our clients’ information. Internally, we have added additional security measures to our existing protections and have worked to strengthen our systems and practices further to prevent similar events from occurring in the future. We are also working with leading data security professionals to aid in our investigation and response and have reported the Incident to relevant authorities.

To help relieve concerns, we have also secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

What You Can Do.

Experts encourage simple steps for protecting your personal information, including changing your passwords regularly, monitoring your personal accounts closely, reporting suspicious activity to your financial institutions, and never sharing your personal information with unknown or untrusted sources. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

For More Information.

If you have questions, please call our office at [REDACTED], Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "A. Straus", with a long, sweeping horizontal line extending to the right.

Alan J. Straus
Alan J. Straus, P.C.

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.

For 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.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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.