



July 25, 2024

Dominik Cvitanovic
(504)-702-1710

Dominik.Cvitanovic@wilsonelser.com

Via Electronic Mail: Idtheft@oag.state.md.us

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Cybersecurity Incident Involving Law Office of Manning Zimmerman & Oliveira, PLLC

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Law Office of Manning Zimmerman & Oliveira, PLLC (“MZO”), with respect to a recent cybersecurity incident that was first discovered by MZO on December 21, 2023, (hereinafter, the “Incident”). MZO takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that MZO has taken in response to the Incident. We have also included with this letter a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services. By providing this notice, MZO does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Incident

On December 21, 2023, MZO detected suspicious activity in one staff member’s email. Upon discovery of this incident, MZO promptly took steps to secure the email account and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, MZO learned that an unauthorized actor accessed one email account, which included emailed documents and data.

Upon learning this, MZO began a time-consuming and detailed reconstruction and review of the data within this one email account (including previously deleted items) at the time of this incident to understand whose information was affected. On July 7, 2024, MZO identified persons whose reportable sensitive data was included within the impacted data. At this time, we have no evidence any of the information has been misused by a third party. The following types of reportable information may have been impacted: Name, Social Security number, driver’s license, and in some cases passport number. The type of information at issue varies for each person.

2. Number of Maryland residents affected.

A total of 3 Maryland residents may have been potentially affected by this incident. Notification letters to these individuals began to be mailed on July 25, 2024. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

MZO is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MZO moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals known at that time. Specifically, MZO engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. MZO informed our law firm and began identifying the potentially affected individuals in preparation for notice. Although MZO is not aware of any actual or attempted misuse of the affected personal information, MZO offered 12 months of complimentary credit monitoring and identity theft restoration services.

As part of its ongoing commitment to the security of information, MZO is reviewing and enhancing its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. MZO is notifying impacted individuals for whom MZO has a valid mailing address via U.S. mail and offering them credit monitoring and identity protection services. MZO is also notifying applicable regulators.

4. Contact information

MZO remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@wilsonelser.com or 504-702-1710.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in blue ink, appearing to read "D. Cvitanovic", is positioned above the printed name.

Dominik J. Cvitanovic, Esq.

Law Office of Manning Zimmerman & Oliveira, PLLC
c/o Cyberscout
PO Box 179
Manchester, NH 03105



Anna Goulet Zimmerman
Licensed in NH & ME
Michella Oliveira
Allison Stucki
Maureen Raibe Manning
Of Counsel

July 25, 2024

NOTICE OF DATA BREACH

Dear [REDACTED]

We are writing to provide you with important information regarding a cybersecurity incident that may have resulted in unauthorized access to your personal information. The Law Office of Manning, Zimmerman & Oliveira, PLLC ("MZO") is sending this letter to you as part of our commitment to protecting your privacy. **We are not aware of any instances of fraud or identity theft that have occurred as a result of this incident.** However, this letter provides some additional information about the incident and steps you can take to protect yourself from the misuse of your information.

What Happened? On December 21, 2023, we detected suspicious activity within our email environment. Upon discovery of this incident, we promptly took steps to secure our email environment and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, we learned that an unauthorized actor had accessed one of our staff member's email accounts between November 18, 2023 and December 20, 2023. We immediately changed her password and have since forced two-factor authentication on all email accounts.

As we could not rule out that the unauthorized actor made a copy of the full email inbox, we performed an extensive and comprehensive review of the mailbox to identify all persons with personal information in the mailbox in an abundance of caution.

What Information Was Involved? The affected personal information within the mailbox varies by the individual and their association with MZO (for example as our vendor, client, family member of client, or expert witness), and included case-related documents. The following reportable data as to you may have been subject to unauthorized access and acquisition: name and Social Security number. For more information regarding your data that may have been affected, you may contact our dedicated assistance line using the contact information provided under "For More Information" on the second page of this letter.

What We Are Doing: Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation to remediate the incident and confirm the security of our email environment. We take the protection and proper use of personal information very seriously and have enhanced the security of our systems moving forward in an effort to prevent any further similar incidents.

As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident, and we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for <<service length>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau.



000010103G0500

P

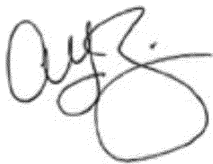
What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: 3 [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled, you will have 12 months of monitoring services. At the end of 12 months, the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information. We take our responsibility to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience. If you have questions or would like additional information, you may call our dedicated assistance line at 1-800-405-6108, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. This excludes all major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read 'AGZ', with a large loop at the end.

Anna Goulet Zimmerman

Enclosure

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- ◆ Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- ◆ TransUnion (<https://www.transunion.com/fraud-alerts>); or
- ◆ Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves <<x>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

