

June 14, 2022

Ross M. Molina, Esq.
504.702.1726 (direct)
Ross.Molina@WilsonElser.com

Via Email
IDTheft@oag.state.md.us

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

Re:	Our Client	:	Noll Law Office, LLC
	Matter	:	Data Security Incident on April 1, 2022
	Wilson Elser File #	:	16516.01833

Dear Attorney General:

We represent Noll Law Office, LLC (“Noll Law”), located in Springfield, Illinois, with respect to a potential data security incident described in more detail below. Noll Law takes the security and privacy of the information in its control 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 security breach, the number of Maryland residents being notified, what information has been compromised, and the steps that Noll Law is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

It appears that on or around April 1, 2022, Noll Law was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate Noll Law’s computer systems. This incident may have resulted in the exposure of personal information that is located on Noll Law’s systems, including including names, driver’s license numbers, medical records, and in some instances social security numbers.

Noll Law, however, is not aware of any evidence that information has been misused. Noll Law has not received any reports of related identity theft since the date of the incident (April 1, 2022 to present).

2. Number of Maryland Residents Affected

A total of one resident of Maryland was potentially affected by this security incident. A notification letter to this individual will be mailed on June 14, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, Noll Law moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. Noll Law has reviewed, altered and enhanced its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management.

4. Contact Information

Noll Law 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 Ross.Molina@WilsonElser.com or 504.702.1726.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Ross M. Molina

Enclosure: *Sample Notification Letter*

Noll Law Firm
P.O. Box 3923
Syracuse, NY 13220

NOLL LAW OFFICE, LLC
at the Lincoln Depot



930 E. Monroe • Springfield, Illinois 62701

[REDACTED]
[REDACTED]
[REDACTED]

June 14, 2022

Sent via United States Mail

Re: Notice of Data Incident

[REDACTED]

This letter is to notify you that we recently discovered that a data security incident may have resulted in the possible unintentional exposure of your personal information.

This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself. Please rest assured that the Noll Law Office takes the protection and proper use of your personal information very seriously. Law enforcement has been notified and we sincerely apologize for any inconvenience this may cause.

What Happened

On April 1, 2022, the Noll Law Office detected suspicious activity within its network environment. Upon discovery, the information technology (IT) support team was notified. We immediately engaged a law firm specializing in cybersecurity and data privacy to investigate. Additionally, the Noll Law Office retained a third-party forensic specialists to assist the Noll Law Office in its analysis of any unauthorized activity. The forensic investigation concluded on April 26, 2022. While the potentially impacted information varies by individual, the investigation concluded that certain personal information – including names, driver's license numbers, medical records, and in some instances social security numbers – were accessed by an unknown party that is not authorized to handle or view such information.

At this time, the Noll Law Office cannot verify whether any of your personal information has been or will be misused as a result of this incident. The Noll Law Office is notifying you of this incident out of an abundance of caution.

What We Are Doing

Although we are not aware of any misuse of your information as a result of this incident, we are offering you Single Bureau Credit Monitoring* services at no charge provided by Cyberscout, a company specializing in fraud assistance and remediation services. This is because we take the protection and proper use of personal information extremely seriously. As part of our ongoing

commitment to information privacy and the security of information, we are notifying you of this incident.

Cyberscout's services include: access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft..

To enroll in Credit Monitoring* services at no charge, please log on to **<https://www.myidmanager.com>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **l47ahu6rotxr** 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. 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.

We encourage you to contact Cyberscout with any questions by calling 1-800-405-6108 from 8:00 am to 8:00 pm, Monday through Friday, excluding holidays. Representatives are available for 90 days.

What You Can Do:

Further, as a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, and to monitor your credit reports for suspicious activity. This letter also includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

For More Information:

If you have additional questions, please call 1-800-405-6108 from 8:00 am to 8:00 pm, Monday through Friday, excluding holidays. Representatives are available for 90 days. The Noll Law Office values the security of your personal data, and we sincerely apologize for any inconvenience this incident causes you.

Very Truly Yours,

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

Daniel Noll
Managing Partner
Noll Law Office

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 1-800-909-8872 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you 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 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.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.