

December 1, 2022

Sent Via Email Only

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

Re: *Notice of Data Security Breach – Patton Law Offices, PLLC*

Dear Attorney General Frosh:

I am writing on behalf of our client, Patton Law Offices, PLLC, a North Carolina solo-practitioner law firm located at 1435 N. Bridge Street, Elkin, NC 28621 (the “Firm”). I write to notify you, pursuant to Md. Comm. Code § 14-3504, of a data security incident involving two (2) Maryland residents.

Discovery and Nature of Breach

On Saturday, September 17, 2022, the Firm fell victim to a cyber-attack that encrypted the data stored in certain firm systems. The Firm immediately contacted its third-party information technology team to secure its systems and investigate the nature and scope of the event. A ransomware attack was suspected. This was confirmed on Monday, September 19, 2022, when a ransomware notice was discovered on the desktop computer of one of the Firm’s staff members. Following consultation with third-party data privacy experts and a careful review of the encrypted information and attack vector utilized, the Firm determined on October 18, 2022, that personal information may have been exposed to unauthorized persons as a result of this incident.

The Firm’s Response

Fortunately, at the time of the incident, the Firm had sufficient backups to recover virtually all of the encrypted data. The Firm initiated the recovery process and was able to continue servicing its clients with little-to-no disruption. The Firm did not pay the ransom or otherwise acknowledge to the perpetrators that it had received the ransomware notice. The perpetrators have not contacted the Firm since the initial ransom event.

With help from qualified third-party information technology experts, the Firm confirmed that there was no malicious software present on or suspicious activity in the Firms’ servers following the recovery from backups. Moreover, the Firm has implemented additional

cybersecurity and access management features and redoubled its efforts at sharing best practices in security with attorneys and staff.

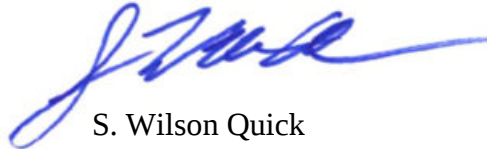
Moving forward, the Firm is offering one year of complementary identity theft protection services through IDX, a trusted recovery services expert, to all potentially affected current and former clients. This offering includes CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Additionally, all adults who register with IDX will receive credit monitoring for the duration of the identity theft protection services.

Notice to Affected Persons

On December 2, 2022, the Firm will mail formal notice of this incident to the two (2) affected Maryland residents in substantially the same form as Attachment 1 to this letter.

If you have any other questions or need additional information, please let me know.

Sincerely yours,



S. Wilson Quick

Attachment

1 – Sample Consumer Notification Letter

PATTON LAW

Patton Law Offices, PLLC
Return Mail to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-814-1785

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

December 2, 2022

Notice of Data Security Incident

Dear <<FIRST NAME>> <<LAST NAME>>,

Patton Law Offices, PLLC (the “Firm”) recently discovered an incident that may impact the privacy of some of your personal information. Although we are currently unaware of any misuse of your information, we take this incident seriously, and write to provide you with information about the incident, steps we are taking in response, and steps you can take to protect against misuse of your information.

What Happened? On Saturday, September 17, 2022, the Firm was impacted by a ransomware attack that encrypted the data stored in certain firm systems. We immediately contacted our third-party information technology and cybersecurity team to secure our systems and conduct an investigation into the nature and scope of the event. Fortunately, the Firm maintains secure backups that were sufficient to recover virtually all of the encrypted data. We initiated the recovery process and were able to continue serving our clients with very little disruption. We did not pay a ransom or otherwise acknowledge to the perpetrators that we had been impacted. We have received no further communication from the perpetrators of the attack. Following consultation with third-party cybersecurity experts and a careful review of the encrypted information, we determined on October 18, 2022, that your personal information may have been exposed to unauthorized persons as a result of this incident.

What Information Was Involved? As a law firm representing clients at all levels of the disability claims process, we receive and maintain a wide variety of information about our clients. The personal information that relates to you that may have been exposed through this incident could include your name, Social Security Number, driver’s license or other state identification number, date of birth, address, and, in some clients’ cases, checking account information provided to the Social Security Administration. While we do not have any evidence of misuse of your information, out of an abundance of caution, the Firm is providing notice of the incident so that you may take steps to better protect your personal information, should you feel it is appropriate to do so.

What We Are Doing? We take this incident and the security of the personal information we maintain seriously. With help from qualified third-party cybersecurity and information technology experts, we confirmed that there was no malicious software present on or suspicious activity in our servers following the recovery from backups. We have implemented additional security and access management features and redoubled our efforts at sharing best practices in information security with our attorneys and staff. We continue to review and update firm email and file retention policies to help reduce the risk of this type of incident in the future.

In addition, although we are unaware of any actual or attempted fraudulent misuse of your information as a result of this incident, we are offering complimentary identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

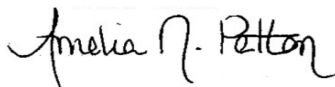
What You Can Do. You are encouraged to remain vigilant against identity theft and fraud by regularly reviewing your account statements, explanation of benefits forms, and free credit reports for suspicious activity and to detect errors. We also encourage you to contact IDX with any questions and to enroll in the complimentary identity protection services being offered by calling 1-833-814-1785 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. You will need to reference the Enrollment Code when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is March 2, 2023.

You may also want to review the enclosed “Recommended Steps to Help Protect Your Information” for detailed instructions on how to enroll and to learn about additional steps you may take to help protect your personal information.

For More Information. We understand there may be questions that are not answered by this letter or the enclosed information. You may contact an IDX representative by calling 1-833-814-1785 Monday through Friday from 9 AM to 9 PM Eastern Time to speak with someone familiar with this incident and the identity protection enrollment process.

We sincerely regret that this incident occurred, and we apologize for any inconvenience or concern it may have caused you.

Respectfully,

A handwritten signature in black ink that reads "Amelia N. Patton". The signature is fluid and cursive, with the first name "Amelia" being more prominent.

Amelia N. Patton
Patton Law Offices, PLLC

(Enclosure)



Recommended Steps to Help Protect Your Information

Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 1-833-814-1785 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Watch for Suspicious Activity. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus online or by phone. 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. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

Notify law enforcement of any suspicious activity. You should also notify the appropriate law enforcement authorities or your state attorney general if you suspect identity theft or 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state attorney general.

Additional resources to protect against identity theft. You can find additional information to help protect against identity theft by contacting the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. Depending upon your state residency you may also be able to obtain additional information from the agencies below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400