Shaheen &Gordon
ATTORNEYS AT LAW

Office: 603-749-5000
Fax: 603-749-1838
353 Central Ave, Suite 200, Dover, NH 03820

October 3, 2024

[redacted]

Enrollment Code: [redacted]

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

https://app.idx.us/account-creation/protect

Notice of Data Security Incident/Possible Data Breach

Dear [redacted]

We write to notify you of an incident in which your personal information may have been exposed to unauthorized actors who temporarily accessed an account of one of our firm's lawyers. While, to date, we have no evidence that your information was taken from the firm's systems or has been misused, we provide you with information about the event, our response to it, and resources available to you to help protect your information and identity, should you feel it appropriate to do so. We take seriously the confidentiality of information you provide to our firm, and we regret any inconvenience this may cause you.

What Happened

On or about April 15, 2024, one of our firm lawyers received an email that appeared to be sent from an expected sender. Unbeknownst to our firm lawyer, the sender's email account had been compromised and the email was in fact a phishing attack that exposed our lawyer's account login credentials. Shortly before 8:00 am on April 16, 2024, the unauthorized actors used our lawyer's credentials to sign into his account. The unauthorized access was discovered by the firm's information technology security vendor around 11:00 am on April 17, 2024, and that access was terminated immediately. The unauthorized actor's access was limited to just one account; they did not access other firm systems or data.

An investigation followed to determine if any personal information was copied from our systems. Aspects of the investigation suggest that no personal data was taken, but our external IT security vendor cannot rule out entirely the possibility that personal information was taken. And, during the time that the unauthorized actor had access to our systems, personal information might have been viewed by people

outside of our firm. Because there is a chance that your information was accessed or viewed, we have opted to provide this notice to you.

What Information Was Involved

You are receiving this letter because our lawyer's account contained your name and your social security number and/or a number assigned to you on a government-issued identification card (such as a driver's license or passport number).

What We Are Doing

Our IT security vendor conducted a scan of the lawyer's account to locate any personally identifiable information, and the result of that scan has caused us to send this letter to you. We are taking other steps to improve the firm's security, mitigate these types of risks, and protect against further unauthorized access. For example, we have implemented additional safeguards to improve data security on our web server infrastructure. We are taking additional steps to protect client related data from theft or similar criminal activity in the future. We are also ensuring that all personally assigned portable computers utilize encryption software for patient data protection.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, at no cost to you. IDX identity protection services include: 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

We encourage you to enroll in free IDX identity protection services by going to https://app.idx.us/account-creation/protect, calling 1-800-939-4170, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is December 14, 2024. You will need to reference the enrollment code at the top of this letter when enrolling, so please do not discard this letter.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information

In addition to enrolling in the credit protection services, we encourage you to remain vigilant against incidents of identity theft and fraud. If you are concerned about the potential implications of this breach there are a number of steps you can take to avoid any adverse impact. Information on additional steps you can take to protect yourself from identity theft can be found at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft. Please review the information contained in the enclosed "Protecting Your Personal Information."

Again, we apologize for any inconvenience this may cause you. Please feel free to call me at 603-609-0600 if you have any questions.

Sincerely,

Joseph G. Shoemaker
Director of Operations
Shaheen & Gordon, P.A.

(Enclosure)

Protecting Your Personal Information

We are providing this notice to you so that you can take steps to monitor your credit activity, report any suspicious activity, and take any additional action you believe is necessary. You may consider placing a fraud alert on your credit file, reviewing credit reports for suspicious activity, and reviewing credit card and other financial account information for unauthorized activity.

1. **Website and Enrollment in Credit Monitoring.** Scan the QR image or 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.

2. 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.

3. Review your credit reports. 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. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

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.

You should also know that you have the right to file a police report if you ever 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 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 the Attorney General.

4. 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 by phone and also via Experian's or Equifax's website. An initial fraud alert is a 1- year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. 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:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

5. Security Freeze. As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. 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. Therefore, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact **each** of the three major credit reporting bureaus above. There is no cost to freeze or unfreeze your credit files.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 and your state Attorney General.

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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

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; https://ag.ny.gov/.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.