

November 15, 2023

VIA ELECTRONIC MAIL (IDTHEFT@AOG.STATE.MD.US)

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

Re: *Notice of Business Email Compromise*

Dear Maryland Office of the Attorney General:

We represent Solomon Law Firm, PLLC ("Solomon") and write to provide notice of a business email compromise ("BEC") that may have impacted its clients' personal information.

On August 3, 2023, Solomon discovered that on or about June 12, 2023, a threat actor gained access to an employee email account via a phishing attack. A forensic investigation revealed that the threat actor had access to the account until July 21, 2023. During the course of Solomon's forensic investigation, document review, and subsequent data enrichment efforts, it discovered on October 18 that personal information belonging to 22 Maryland residents may have been temporarily accessible to the threat actor. Importantly, there is no indication that the threat actor viewed or downloaded any information from the mailbox.

The following information associated with Maryland residents was temporarily accessible to the threat actor: SSNs, financial information, health information, health insurance information, and usernames and passwords for online accounts. We cannot confirm whether this information was accessed, and we are notifying clients out of an abundance of caution.

Upon learning of the BEC, Solomon immediately initiated a password reset for the impacted email account and launched a forensic investigation to determine the nature and scope of the compromise. Solomon also took steps to enhance its threat monitoring capabilities and harden its systems to minimize the risk of similar incidents in the future. In addition, it is providing cybersecurity awareness training to all employees.

Maryland Office of the Attorney General
November 15, 2023
Page 2

To mitigate any potential impact on those affected, Solomon is offering identity theft protection services through IDX. The 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.

The attached notification letter was mailed to Maryland residents on November 15, 2023. Solomon apologizes for any inconvenience this incident may have caused and remains steadfast in its commitment to protect personal information.

Very truly yours,

BOND, SCHOENECK & KING, PLLC

A handwritten signature in dark ink, appearing to read "Mario Ayoub", written over a horizontal line.

Mario Ayoub

(Attachment)

SOLOMON LAW FIRM **PLLC**

4145 SW Watson Ave, Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

November 15, 2023

Notice of a Business Email Compromise

Dear <<First Name>> <<Last Name>>:

We are sending this letter to you as part of Solomon Law Firm PLLC's ("Solomon" or "we") commitment to respect our client's privacy. We take the protection of our client's personal information very seriously and it is important to us that you are made fully aware of a recent business email compromise ("BEC") that may have impacted your personal information. This letter provides details about the BEC, explains the services we are making available to you, and describes our response efforts designed to safeguard your information. Importantly, as of the date of this mailing, there is no evidence of misuse of your information.

What Happened?

On August 3, 2023, we discovered that on or about June 12, 2023, a threat actor gained access to an employee email account via a phishing attack. A forensic investigation revealed that the threat actor had access to the account until July 21, 2023. During the course of our forensic investigation, document review, and subsequent data enrichment efforts, we discovered on October 18 that some of your personal information may have been temporarily accessible to the threat actor. There is no indication that the threat actor either viewed or was able to download any information from the mailbox.

What Information Was Involved?

The following information was temporarily accessible to the threat actor: <<VariableData1>>. We cannot confirm whether this information was accessed, and we are notifying you out of an abundance of caution.

What Are We Doing?

As soon as the BEC was discovered, we immediately initiated a password reset for the impacted email account and launched a forensic investigation to determine the nature and scope of the compromise. We are also taking steps to enhance our threat monitoring capabilities and harden our systems as appropriate to minimize the risk of similar incidents in the future. Additionally, we are providing cybersecurity awareness training to all employees.

To protect you from any potential misuse of your information, and to demonstrate our commitment to the protection of your personal information, we are offering identity theft protection services through IDX. 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.

What You Can Do.

We encourage you to enroll in the free IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or by calling 1-800-939-4170 and using the enrollment code provided above. IDX representatives are available Monday through Friday from 6 am to 6 pm Pacific Time. Please note that the deadline to enroll is February 15, 2024. This letter also provides other precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information.

You will find detailed instructions for enrollment on the enclosed “Other Important Information” document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

If you have any further questions regarding this issue, please call 1-800-939-4170 for assistance or for any additional questions you may have. We apologize for any inconvenience that this BEC has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Ariel Solomon", with a stylized flourish at the end.

Ariel E. Solomon, Esq.
Founding & Managing Partner – Solomon Law Firm PLLC

(Enclosure)



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. 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. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. 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.

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 our 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.

5. 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. 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
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.

6. 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.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

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.