

WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

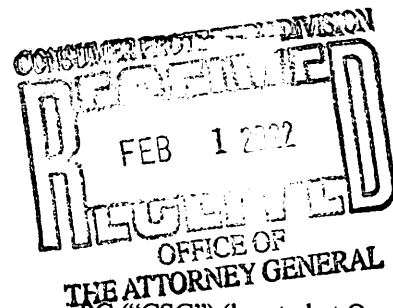
DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

January 28, 2022

Privileged and Confidential
VIA EMAIL AND FIRST CLASS MAIL

Hon. Brian E. Frosch
Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: idtheft@oag.state.md.us
Re: Security Breach Notification



Dear Attorney General Frosch:

We are writing on behalf of our client, Chiesa Shahinian & Giantomasi PC ("CSG") (located at One Boland Drive, West Orange, NJ 07052), to notify you of a data security incident involving approximately three (3) Maryland residents.¹

Nature

On December 10, 2021, CSG discovered suspicious activity in one of its employee's email accounts. At that time, CSG took immediate steps to stop the threat and understand the full scope of the situation. This included hiring third-party forensic experts to conduct a thorough investigation, remediation efforts, and contacting the FBI to seek assistance with the incident. The investigation is ongoing, but CSG believes that unauthorized access began on November 24, 2021, which was during the time period that the user's email account was being migrated and the user had received an additional means of access. We believe that that particular means of access was compromised only for that user and until December 10 when CSG learned of the incident and changed passwords systemwide.

At that time, CSG began a comprehensive search of the data to determine what information was involved and the individuals the incident impacted. CSG, with the assistance of counsel, recently concluded its review and we determined that the incident involved personal information related to approximately three (3) Maryland residents. *However, as of now, there is no evidence indicating identity theft or financial harm involving any of the information.*

The personal information included first and last names, Social Security Numbers, driver's license or passport numbers, and financial account information.

¹ By providing this notice, CSG does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland's data event notification statute, or personal jurisdiction.

Notice and CSG's Response to the Event

On January 31, 2022, CSG will mail a written notification to the potentially affected Maryland residents, pursuant to Md. Code Ann., Com. Law § 14-3504, in a substantially similar form as the enclosed letter (attached as Exhibit A).²

Additionally, CSG is providing these potentially impacted individuals the following:

- Free access to credit monitoring services at the three nationwide credit reporting agencies for one year through Sontiq;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank.
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, CSG provided the notice to the applicable government regulators, officials, and other Attorneys General (as necessary).

Finally, CSG is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,



Spencer S. Pollock, Esq., CIPP/US, CIPM

² Please note that because some of the impacted individuals are current or former adversaries in legal proceedings who had counsel, CSG is in the first instance going to seek permission from counsel to contact the impacted individuals. Those emails will be sent on January 31, 2022. In the event that counsel authorizes CSG to contact the impacted individual, notice will go out the next business day. In the event that counsel does not respond to the outreach, notice will be sent to the impacted individual six business days after January 31, 2022.

EXHIBIT A

Chiesa Shaninian and Giantomasi PC
One Boland Drive
West Orange, NJ 07052



CHIESA SHAHINIAN & GIANTOMASI PC

ONE BOLAND DRIVE
WEST ORANGE, NJ 07052

csglaw.com

[REDACTED]
[REDACTED]
[REDACTED]

January 31, 2022

Re: Notice of Data Breach

Dear [REDACTED]:

At Chiesa Shahinian & Giantomasi PC, we value transparency and respect the privacy of your information. That is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your and/or your dependents' protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information including enrolling in credit monitoring services being provided for one year free of charge.

While such incidents unfortunately have become all too common, and while we have no reason to believe your personal information has been misused, we recognize that this news can be unsettling. We take this incident extremely seriously and, because of the personal relationship that exists between you and our firm, want you to have all the information you need to respond appropriately.

What Happened

On December 10, 2021, we discovered suspicious activity in one of our employee's email accounts. After learning of the incident, we took immediate action to assure the security of our systems and operations. In addition, we promptly engaged outside forensic and incident response experts to conduct a thorough investigation and assist with any necessary remediation efforts.

With the help of these experts, we began a comprehensive review of the information that might have been compromised. We have completed our review and determined that your and/or your dependents' personal information may have been exposed. ***Please know that as of now, we have no evidence indicating any such information has been used improperly.*** However, out of an abundance of caution, we wanted to notify you of the incident and provide information about how you can protect yourself and your family from identity theft and fraud.

What Information Was Involved

The protected personal information could potentially involve your first and last name, date of birth, Social Security Number, IRS Pin number and driver's license or state issued identification number.

What We Are Doing

As described above, we took immediate steps to assure the security of our systems including hiring outside forensic and incident response experts to investigate. While we had robust, state-of-the-art cybersecurity measures at the time, we are implementing additional cybersecurity safeguards and enhancing our cybersecurity training, policies, procedures, and protocols to further minimize the likelihood of this type of incident occurring again.

What You Can Do

The security and privacy of your personal information are a top priority for us. Therefore, while we have no evidence that your or your dependents' information was misused, we strongly recommend you remain vigilant. Monitor and review all your financial and account statements, and immediately report any unusual activity to the institution that issued the record and to law enforcement. In addition, please see "**OTHER IMPORTANT INFORMATION**" on the following pages for guidance on how to best protect your identity.

Maintaining the safety and security of your and your loved ones' personal information is important to us, and we sincerely regret any concern or inconvenience this incident may cause. Because your peace of mind is of paramount importance, we are providing you with access to Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Non-Credit Public Records monitoring/Cyber Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition to credit related data, the services will also monitor any changes to your non-credit public records including: Change of Address, Court Records and Social Security number trace. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

Please see "**OTHER IMPORTANT INFORMATION**" on the following pages for a list of the services available to you at no cost.

To enroll in these credit monitoring services, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]. To receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

For More Information

If you have additional questions, please contact me by phone (973-530-2006), email (pcostello@csglaw.com), or mail (One Boland Drive, West Orange, NJ 07052).

Sincerely yours,

s/Patricia K. Costello

Patricia K. Costello, A.J.S.C. (ret.)
Managing Member
Chiesa Shahinian & Giantomasi PC

PKC:lb

* Services marked with an "*" require 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.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax (888) 766-0008 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 P.O. Box 1000 Chester, PA 19016 www.transunion.com
--	---	---

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box. 380 Woodlyn, PA 1904 https://www.transunion.com/credit-freeze
---	---	---

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Free Credit Monitoring through Cyberscout. Chiesa Shahinian & Giantomasi PC is offering access to Cyberscout's Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Non-Credit Public Records monitoring/Cyber Monitoring for twelve (12) months at no charge. Cyberscout's exhaustive credit monitoring will provide you with:

- Triple bureau credit monitoring with the three nationwide credit reporting agencies (notifications to you when changes to your credit file occur (for twelve months from the date of enrollment)
- Dark web monitoring;
- Credit freeze assistance;
- Change of address monitoring;
- Court records monitoring;
- SSN trace monitoring;
- Identity theft protection services;
- Access to identity theft specialists;
- Credit file review;
- Credential assistance; and
- \$1,000,000 in identity theft expense reimbursement insurance.

The service also provides identity theft resolution services, including assistance:

- Tax fraud;
- Unemployment fraud;
- Employment fraud;
- Criminal identity theft;
- Estate and deceased fraud;
- Financial and medical identity theft;
- Fraudulent account takeover;
- Social media account takeover.

To enroll in these Credit Monitoring services, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED] To receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf0009_identitytheft_a_recovery_plan.pdf.

New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, <https://ag.ny.gov/internet/resource-center> and or *NYS Department of State's Division of Consumer Protection*, (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>.