

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

DANIEL J. HAIER
dhaier@c-wlaw.com

KATIE GORA
kgora@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

March 5, 2025

Via Email (idtheft@oag.state.md.us)

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

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for Salzmann Hughes, P.C. ("Salzmann"), located at 79 St Paul Drive, Chambersburg, PA 17201. We write to provide notification of a recent data security incident. By providing this notice, Salzmann does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On October 1, 2024, Salzmann identified unusual activity associated with an employee email account and immediately began an investigation with the assistance of third-party specialists. The investigation determined that an unknown party potentially accessed information contained within the email account without authorization between September 25, 2024 and October 1, 2024. Salzmann then began a comprehensive review of the contents of the email account to determine the type of information it contained and to whom the information related. The review determined that the potentially impacted information included the names of seven (7) Maryland residents in combination with Social Security numbers.

Salzmann notified potentially impacted individuals of this incident via First Class mail on March 5, 2025. A copy of the notice is attached as ***Exhibit A***. Salzmann has no reason to believe any information has been or will be misused because of this incident. However, in an abundance of caution, Salzmann is offering the potentially impacted resident of Maryland complimentary access to 12 months of credit monitoring and identity protection services.

In response to this incident, Salzmann promptly terminated access to the email account and engaged outside cybersecurity specialists to determine the scope of this incident. Salzmann is also reviewing its policies and procedures related to data protection.

Thank you for your attention to this matter and please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

A handwritten signature in black ink, appearing to read 'D Haier', with a stylized, cursive script.

Daniel Haier, Esq.
610-215-2288
dhaier@c-wlaw.com

EXHIBIT A



0000122

Salzmann Hughes, P.C.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS437

0 0000122



[REDACTED]
[REDACTED]
[REDACTED]

March 5, 2025

Dear [REDACTED]

Salzmann Hughes, P.C. (“Salzmann Hughes”) writes to notify you of an incident that may affect the privacy of certain information provided to us. We take this incident seriously and are providing you with information about the incident, our response, and steps you can take to help safeguard your information.

On October 1, 2024, we observed unusual activity in an employee email account and immediately began an investigation with the assistance of third-party specialists. The investigation determined that an unknown party accessed the employee’s email account without authorization between September 25, 2024 and October 1, 2024. Therefore, we reviewed the contents of the email account to determine the type of information it contained and to whom the information related. This review determined that information in the email account included [REDACTED]
[REDACTED].

In response to this incident, we promptly terminated access to the employee email account and engaged outside cybersecurity specialists to determine the scope of this incident and ensure implementation of appropriate remediation measures. We also continue to review our policies and procedures related to data protection and have taken additional steps to help prevent a similar incident from occurring in the future.

Please note that we have no reason to believe there has been or will be any fraud or misuse of information as a result of this incident. Nonetheless, in an abundance of caution we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

We encourage you to enroll in the complimentary credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services along with

additional resources available to you are included in the attached *Steps You Can Take to Help Protect Your Information*.

We understand you may have questions about this incident. You may contact our assistance line within 90 days from the date of this letter at [REDACTED], between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, or write to us at 79 St Paul Drive, Chambersburg, PA 17201.

We regret any concern this incident may cause you.

Sincerely,

Salzmann Hughes, P.C.



STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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