



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 25, 2023

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Creese, Smith, Hune & Co. LLC (“CSH”) located at 8150 Perry Highway, Suite 105, Pittsburgh, PA 15236, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twelve (12) Maryland residents. The investigation into this matter has recently concluded. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CSH does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around June 23, 2023, CSH became aware of suspicious activity within its systems. With the assistance of third-party cyber security specialists, CSH immediately launched an investigation into the nature and scope of the event. Through the investigation, it learned there was unauthorized access to its systems at various times between June 19 to June 23, 2023, during which an unauthorized actor potentially viewed or copied certain files stored within the systems.

The information that could have been subject to unauthorized access includes name, Social Security number and financial account information.

Notice to Maryland Residents

On September 25, 2023, CSH provided written notice of this incident to twelve (12) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, CSH moved quickly to investigate and respond to the incident, assess the security of CSH systems, and identify potentially affected individuals. Further, CSH notified federal law enforcement regarding the event. CSH is also working to implement additional safeguards and training to its employees. CSH is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CSH is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. CSH is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

CSH is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/ogf
Enclosure

EXHIBIT A

Creese, Smith, Hune & Co. LLC
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07954 1-1



September 25, 2023

NOTICE OF SECURITY INCIDENT

Dear _____ :

Creese, Smith, Hune & Co. LLC (hereinafter “CSH”) is writing to inform you of a recent event that may affect the security of some of your information. Although we are unaware of any attempts to misuse your information for identity theft in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around June 23, 2023, CSH became aware of suspicious activity within its systems. With the assistance of third-party cyber security specialists, we immediately launched an investigation into the nature and scope of the event. Through the investigation, we learned there was unauthorized access to CSH’s systems at various times between June 19 to June 23, 2023, during which an unauthorized actor potentially viewed or copied certain files stored within our systems.

In an abundance of caution, we conducted a thorough review of the potentially impacted files to determine whether they may contain personal information and to whom it related. You are receiving this notice because we determined your information may have been impacted.

What Information Was Involved? Our review determined that the following types of your information may have been impacted:

Additionally, please be advised that if you previously provided CSH with your spouse’s and/or dependent minor’s information, such as name, date of birth and Social Security number, that information may have also been impacted.

What We Are Doing. CSH takes this event and the security of information in our care seriously. We want to assure you that the privacy and security of employee information is one of our top priorities. Upon discovering this event, we promptly took steps to investigate the incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the privacy of personal information in our care, while we have safeguards in place to protect data in our care, we are working to review and further enhance these protections as part of our ongoing commitment to data security. We also reported this event to federal law enforcement and government regulators where required.

As an additional precaution, CSH is offering you 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. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

Please contact the phone number provided below should you have questions about receiving such services for a potentially impacted family member if you previously provided us with their information.

What You Can Do. As a precautionary measure, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Additional resources can be found below in the *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information. You may also enroll in the complimentary credit monitoring services being offered.

For More Information. If you have additional questions, you may contact our dedicated assistance line toll-free at 1-833-570-2581. This toll-free line is available Monday through Friday 8:00 am – 8:00 pm EST, (excluding major U.S. holidays).

We take the privacy and security of personal information in our care very seriously, and sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Hune", written in a cursive style.

Jim Hune
Member
Creese, Smith, Hune & Co. LLC

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/cshllc> and follow the instructions provided. When prompted please provide the following unique code to receive services:

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

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

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 consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission,

or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.