



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Michele T. Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

411 Theodore Fremd, Ste 206S
Rye, NY 10580

October 17, 2024

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 Leaders Staffing located at 4912 Lima Road, Fort Wayne, Indiana, 46808 and are writing to notify your office of an incident that may affect the security of certain personal information relating to eight (8) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Leaders Staffing 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 January 11, 2024, Leaders Staffing became aware of unusual activity in its network. Leaders Staffing immediately took steps to secure its systems and reviewed the nature and scope of the activity. With the assistance of third-party forensic specialists, the investigation determined that Leaders Staffing's network was subject to unauthorized access on January 11, 2024, and that certain files were potentially accessed by an unknown actor who accessed the network. As a precaution, Leaders Staffing undertook a lengthy and comprehensive review of the files stored on its network at the time of the incident to identify any sensitive information and to whom that information pertained. On or about, August 7, 2024, Leaders Staffing determined that information related to certain Maryland residents was potentially accessed by an unknown actor. Leaders Staffing then worked to locate current mailing addresses, in order to provide an accurate notification.

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

Notice to Maryland Residents

On or about October 17, 2024, Leaders Staffing began providing written notice of this incident to eight (8) 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, Leaders Staffing moved quickly to respond to the incident and assess the security of Leaders Staffing systems. After the investigation determined that a third party potentially accessed files on its network but could not confirm the precise files potentially accessed, Leaders Staffing took steps to identify individuals whose information was potentially accessed. Leaders Staffing implemented additional technical security measures designed to prevent similar future incidents. Leaders Staffing is providing access to credit monitoring services for twelve (12) months through Cyberscout, a TransUnion company to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Leaders Staffing 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 fraud to their credit card company and/or bank. Leaders Staffing 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.

Leaders Staffing 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.

Office of the Attorney General

October 17, 2024

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at (267) 930-4775.

Very truly yours,

A handwritten signature in blue ink that reads "Michele Veltri". The signature is written in a cursive, flowing style.

Michele T. Veltri of
MULLEN COUGHLIN LLC

MTV/ekw

Enclosure

EXHIBIT A

Return mail will be processed by: IBC

PO Box 847
Holbrook, NY 11741

[REDACTED]
[REDACTED]
[REDACTED]

October 17, 2024

NOTICE OF SECURITY INCIDENT

Dear [REDACTED]:

Leaders Staffing (“Leaders”) writes to inform you of a data event that may affect the security of your personal information. This letter provides details of the event, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened?

On January 11, 2024, Leaders became aware of unusual activity in our network. We immediately took steps to review the activity and secure our systems. After conducting an investigation with the assistance of third-party forensic specialists, we determined that our network was subject to unauthorized access on January 11, 2024, and that certain files were potentially accessed by an unknown actor who accessed the network. While we could not confirm what files were potentially accessed, out of an abundance of caution, we decided to notify anyone whose personal information was stored in files on our network at the time of the incident. As such, we undertook a lengthy and comprehensive review of the files on our network, which concluded on or about August 7, 2024. As we identified individuals, we began taking steps to verify current mailing addresses for those individuals, in order to provide an accurate notification. This process also took time and required the assistance of a third-party mailing vendor.

What Information Was Involved?

The information that was potentially subject to unauthorized access because it was stored on our network at the time of the incident includes your name, address, Social Security number, and one or more of the following: driver’s license number, financial account information, and medical information.

What We Are Doing.

We take this incident and the security of personal information in our care seriously. Upon discovering the unusual activity, we took steps to further increase the security of our network. As part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to prevent similar future incidents. We are also reviewing and enhancing existing policies and procedures. As an added precaution, Leaders is offering you access to credit monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Help Protect Personal Information*. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the offered identity monitoring services.

What You Can Do.

Please review the enclosed *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. We encourage you to remain vigilant against potential incidents of identity theft and fraud, to review your account statements, report any suspected incidents of fraud to your credit card company and/or bank, and to monitor your credit reports for suspicious activity. You will also find information on how to enroll in the credit monitoring services offered.

For More Information.

We understand that you may have questions that are not addressed in this letter. If you have additional questions, please call (888) 445-7043, which is available Monday through Friday, between the hours of 9:00 am - 7:00 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Nate Golm

Nate Golm

President

Leaders Staffing LLC

LEAD-ADT-CM-L01

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

In response to the incident, 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 12 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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> 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
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) 442-9828; 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.