



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Justin Schiff
Office: (267) 930-4256
Fax: (267) 930-4771
Email: jschiff@mullen.law

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

July 31, 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 Accountable Healthcare Staffing (“Accountable”) located at 999 Yamato Rd., Suite 210, Boca Raton, FL 33431, and write to notify your office of an event that may affect the security of certain personal information relating to certain Maryland residents. By providing this notice, Accountable 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 February 5, 2024, Accountable became aware of suspicious activity related to an employee email account. Accountable immediately took steps to secure the email account, and launched an extensive investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the event. Through its investigation, Accountable determined that an unknown actor gained access to one (1) employee email account and was able to view and/or download certain data within that account between January 31, 2024 and February 2, 2024.

Upon becoming aware of the unauthorized access, Accountable began a diligent and comprehensive review process to identify sensitive information that may have been contained within the impacted email account, and to identify the individuals whose information may have been impacted. Accountable then worked to identify appropriate contact information for the impacted individuals. That process recently completed, and Accountable provided notification to individuals whose information was contained within the impacted email account.

The personal information that could have been subject to unauthorized access for Maryland residents includes name, Social Security number, and medical information.

Notice to Maryland Residents

On or about July 31, 2024, Accountable began providing written notice of this incident to approximately ten (10) 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 becoming aware of the event, Accountable moved quickly to investigate and respond, assess the security of its computer systems, and identify potentially affected individuals. In addition, Accountable is working to implement additional safeguards and training to its employees. Accountable is also providing access to credit monitoring services for twelve (12) months, through CyEx, to individuals whose personal information was potentially affected by this event, at no cost to these individuals. Accountable also established a toll-free call center to address any questions from notified individuals.

Additionally, Accountable is providing potentially affected 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. Accountable 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.

Accountable is providing written notice of this event to appropriate state privacy regulators and the three major consumer 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) 930-4802.

Very truly yours,

A handwritten signature in black ink, appearing to read "Justin Schiff".

Justin Schiff of
MULLEN COUGHLIN LLC

JXS/reh
Enclosure

EXHIBIT A



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Accountable Healthcare Staffing (“Accountable”) writes to inform you of an event that may have impacted the privacy of some of your information. While we are unaware of any attempted or actual misuse of your information at this time, we are providing you this notice to inform you of the event, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On or around February 5, 2024, Accountable became aware of suspicious activity related to an employee email account. We immediately took steps to secure the email account, and launched an extensive investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the event. Through our investigation, we determined that an unknown actor gained access to one (1) employee email account and was able to view and/or download certain data within that account between January 31, 2024 and February 2, 2024.

Upon becoming aware of the unauthorized access, we began a diligent and comprehensive review process to identify sensitive information that may have been contained within the impacted email account, and to identify the individuals whose information may have been impacted. We then worked to identify appropriate contact information for the impacted individuals. That process recently completed, and we are providing you with notification given that your information was contained within the impacted email account.

What Information Was Involved? Our investigation determined that at the time of the event, your name and <<Breached Elements>> were stored within the impacted account and may have been affected by this event. We are unaware of any attempted or actual misuse of your information at this time.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this event very seriously. Upon becoming aware of the activity, we immediately took steps to secure our environment and initiated a comprehensive incident response. We also reviewed our security policies and procedures and are enhancing our security measures to reduce the risk of similar future events.

As an added precaution, we are offering you access to credit monitoring and identity restoration services for <<CM Length>> months at no cost to you, through Epiq. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Personal Information*. You may also enroll in the complementary credit-monitoring services available to you.

For More Information. If you have additional questions, please contact our toll-free assistance line at 833-215-2902. This toll-free line is available Monday through Friday from 9:00 am ET to 9:00 pm ET (excluding U.S. holidays). You may also write to Accountable (Attn: General Counsel) at 999 Yamato Rd., Suite 210, Boca Raton, FL 33431.

Sincerely,

Accountable Healthcare Staffing, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services



<<Full Name>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Deadline>>
Service Term: <<CM Length>>*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit <<URL>>

Enter your unique Activation Code <<Activation Code>>

Enter your Activation Code and click 'Redeem Code'.

1. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
2. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
3. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Deadline>>. After <<Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 one-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. Consumers should be aware, however, 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. 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 Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately <<RI>> Rhode Island residents that may be impacted by this event.