



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

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

July 20, 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 The Mission Essential Group (“Mission Essential”) located at 6530 West Campus Oval, Suite 190, New Albany, Ohio 43054, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately five hundred ninety-four (594) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Mission Essential 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

In September 2022, Mission Essential was notified by federal law enforcement authorities of a potential incident wherein certain Mission Essential email accounts may have been accessed and/or acquired by an unauthorized actor. Upon learning of the potential incident, Mission Essential quickly commenced an investigation with the assistance of industry leading cybersecurity specialists into the security of its email environment. After a thorough and comprehensive investigation, on December 13, 2022, Mission Essential was unable to validate the reports from law enforcement and confirm unauthorized access to Mission Essential email accounts occurred. However, Mission Essential decided to provide notice of this alleged incident out of an abundance of caution to all individuals whose information may have been contained in an email account. Working with its human resources vendor, Mission Essential prepared a list of

all current and former employees, contractors and their spouses and dependents. This review was recently completed on April 19, 2023.

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

Notice to Maryland Residents

On July 20, 2023, Mission Essential provided written notice of this incident to approximately five hundred ninety-four (594) 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 learning of the potential incident, Mission Essential moved quickly to investigate and validate the potential incident, assess and confirm the security of Mission Essential systems, and identify potentially affected individuals. Further, Mission Essential continues to cooperate with law enforcement investigations regarding the potential incident. Although Mission Essential is unable to validate any potential unauthorized access to Mission Essential email accounts, out of an abundance of caution, Mission Essential is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose information may have been contained within Mission Essential email accounts, at no cost to these individuals.

Additionally, Mission Essential 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. Mission Essential is also 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.

Mission Essential is providing written notice of this incident to relevant state regulators, as necessary.

Office of the Attorney General

July 20, 2023

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/dle
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 20, 2023

J6695-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of [Variable Header]

Dear Sample A. Sample:

The Mission Essential Group (“Mission Essential”) writes to inform you of a potential incident that may affect the privacy of some of your information. You are receiving this notice because you are a current or former Mission Essential employee or contractor, or you are a spouse, dependent, or beneficiary of a current or former Mission Essential employee or contractor. Although Mission Essential is unaware of any actual or attempted misuse of your information, Mission Essential is providing you notice of the potential incident, steps Mission Essential is taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened?

In September 2022, Mission Essential was notified by federal law enforcement authorities of a potential incident wherein certain Mission Essential email accounts may have been accessed and/or acquired by an unauthorized actor. Upon learning of the potential incident, Mission Essential quickly commenced an investigation with the assistance of industry leading cybersecurity specialists into the security of its email environment. After a thorough and comprehensive investigation, Mission Essential was unable to validate the reports from law enforcement and confirm unauthorized access to Mission Essential email accounts occurred. However, Mission Essential decided to provide notice of this alleged incident out of an abundance of caution to all individuals whose information may have been contained in an email account. Therefore, working with our human resources vendor, Mission Essential prepared a list of all current and former employees, contractors and their spouses and dependents. This review was completed on April 19, 2023.

What Information Was Involved?

As indicated above, Mission Essential is unable to validate any potential unauthorized access to Mission Essential email accounts but Mission Essential is notifying individuals out of an abundance of caution. The types of information potentially present in Mission Essential email accounts may relate to Mission Essential current or former employees or contractors, or those individuals’ spouses, dependents, or beneficiaries and include: [data elements], and name.

INNOVATION.

PERFORMANCE.

COMMITMENT.

ENGAGE#

missionessential.com

0000002



J6695_L02

What We Are Doing.

Mission Essential treats its responsibility to safeguard information in its care as an utmost priority. As such, Mission Essential responded immediately to the potential incident and has worked diligently to provide you with this notice as soon as possible and out of an abundance of caution. As part of Mission Essential's ongoing commitment to the privacy and security of personal information in its care, Mission Essential is reviewing and updating existing policies and procedures relating to data protection and security. Mission Essential is also investigating additional security measures to further enhance its data protections.

As an additional measure to assist you with protecting and safeguarding your information, Mission Essential is providing you with ## months of complimentary access to credit monitoring and identity restoration services through Experian, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although Mission Essential is covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do.

Mission Essential is unable to validate the alleged incident and there is no evidence of any actual or attempted misuse of your information, but Mission Essential encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information.

We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at: 833-281-4832, Monday to Friday, from 6am to 8pm PST; Saturday and Sunday, from 8am to 5pm PST (excluding major US holidays). You may also write to us directly at 6530 West Campus Oval, Suite 190, New Albany, OH 43054.

Sincerely,

The Mission Essential Group

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring and Identity Restoration:

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-281-4832 by October 31, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your 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, DC 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; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are approximately 11 Rhode Island residents impacted by this incident.



