



&lt;&lt;Date&gt;&gt; (Format: Month Day, Year)

 <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country>>

Re: Notice of Data Security Incident

Dear &lt;&lt;first\_name&gt;&gt; &lt;&lt;middle\_name&gt;&gt; &lt;&lt;last\_name&gt;&gt; &lt;&lt;suffix&gt;&gt;,

MESVision manages vision benefits on behalf of &lt;&lt;b2b\_text\_2 (your employer or Name of Covered Entity)&gt;&gt;. MESVision takes the privacy and confidentiality of your information very seriously. We are writing to inform you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken in response, and steps you can take as well.

#### What happened?

MESVision uses a secure file-transfer program called MOVEit. On August 23, 2023, MESVision discovered that an unauthorized individual had accessed information on its MOVEit server by exploiting a vulnerability in MOVEit's system. MESVision immediately took the server offline, launched an investigation into the incident, and engaged a cybersecurity firm. It was determined that the unauthorized individual exfiltrated information from the server on May 28, 2023, and May 31, 2023. We also reported the incident to the FBI.

#### What information was involved?

The server contained information about individuals who are enrolled in vision benefit plans managed by MESVision. Following a detailed analysis and review of all potentially compromised files, we recently determined that the information affected may have included: &lt;&lt;b2b\_text\_2 (your name, impacted data elements)&gt;&gt;.

#### What are we doing in response?

MESVision has rebuilt the MOVEit system in accordance with vendor requirements and with our gold standard build requirements. Before reactivating the system, we took a number of technical measures to validate the security protections put in place.

 To help relieve concerns and restore confidence following this incident, we are offering complimentary credit monitoring and identity restoration services through Kroll. To take advantage of these free credit monitoring and identity theft protection services, please follow the instructions in [Attachment A](#). You must enroll by <<b2b\_text\_6 (Activation Deadline)>> to receive these services.

#### What can you do?

 It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account, credit report, or EOB. Additional information about how to protect your identity is contained in [Attachment B](#).

#### For More Information:

MESVision has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call (866) 347-8463 Monday through Friday from 9:00am to 8:00pm Eastern Time.

Sincerely,

Jennifer L Volk

**MES Privacy Officer**

## ATTACHMENT A

### IDENTITY MONITORING SERVICES

We have secured the services of Kroll to provide identity monitoring at no cost to you. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services<sup>1</sup> include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

#### How to Activate Your Identity Monitoring Services

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6 (Activation Deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number (S\_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

#### Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services from Kroll:

##### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

##### Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

##### Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

##### Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

##### \$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

##### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

##### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari, and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ATTACHMENT B

### ADDITIONAL INFORMATION

Below are additional helpful tips you may want to consider to protect your personal information.

#### **Review Your Credit Reports and Account Statements & Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission (“FTC”) and/or the Attorney General’s office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
<http://www.identitytheft.gov/>  
1-877-IDTHEFT (438-4338)

#### **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:  
[equifax.com](http://equifax.com)  
[equifax.com/personal/credit-report-services](http://equifax.com/personal/credit-report-services)  
P.O. Box 740241  
Atlanta, GA 30374  
800-685-1111

Experian: [experian.com](http://experian.com)  
[experian.com/help](http://experian.com/help)  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742

TransUnion:  
[transunion.com](http://transunion.com)  
[transunion.com/credit-help](http://transunion.com/credit-help)  
P.O. Box 1000  
Chester, PA 19016  
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

#### **Fraud Alert**

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

#### **Security Freeze**

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

## **Federal Fair Credit Reporting Act Rights**

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies 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 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 violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to [www.ftc.gov/credit](http://www.ftc.gov/credit) or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

### **Additional Information**

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

**For Colorado and Illinois residents:** You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

**For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, <https://www.oag.dc.gov/>, 1-202-727-3400.

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

**For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

**For Massachusetts residents:** You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For New York residents:** For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at <http://www.dos.ny.gov/consumerprotection> or (800) 697-1220 or NYS Attorney General at <http://www.ag.ny.gov/home.html> or (800) 771-7755.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at [www.dfcs.oregon.gov/id\\_theft.html](http://www.dfcs.oregon.gov/id_theft.html) and click "How to get a security freeze."

**For Rhode Island residents:** The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://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 event. There are 70 Rhode Island residents impacted by this event.

**For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).