

NEW YORK
LONDON
SINGAPORE
PHILADELPHIA
CHICAGO
WASHINGTON, DC
SAN FRANCISCO
SILICON VALLEY
SAN DIEGO
LOS ANGELES
TAIWAN
BOSTON
HOUSTON
AUSTIN
HANOI
HO CHI MINH CITY

DuaneMorris®

FIRM and AFFILIATE OFFICES

SANDRA A. JESKIE
DIRECT DIAL: 215.979.1395
PERSONAL FAX: 215.689.2586
E-MAIL: jeskie@duanemorris.com

www.duanemorris.com

SHANGHAI
ATLANTA
BALTIMORE
WILMINGTON
MIAMI
BOCA RATON
PITTSBURGH
NEWARK
LAS VEGAS
CHERRY HILL
LAKE TAHOE
MYANMAR
OMAN
A GCC REPRESENTATIVE OFFICE
OF DUANE MORRIS
ALLIANCES IN MEXICO
AND SRI LANKA

November 12, 2024

VIA E-MAIL - idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: **Breach Notification Pursuant to Maryland Personal Information Protection Act**

Dear Sir/Madam:

This firm is counsel to the Miller Edge Inc. ("Miller Edge"). I am writing to provide information pursuant to the Personal Information Protection Act.

On October 3, 2024, Miller Edge experienced a ransomware attack. Cybersecurity experts were promptly engaged and Miller Edge took quick action to address the attack, begin remediation and launch an investigation. The affected computers remain offline and new computers were purchased.

Based on the results of the investigation, it was determined that the personal information of four (4) Miller Edge employees in Maryland were affected. The compromised information relates to the employees' personnel file which included name, address, date of birth, social security number, banking information and health information only to the extent it was provided by the employees.

Miller Edge promptly retained Experian to provide complimentary access to Experian IdentityWorksSM for 12 months. By email on October 15, 2024, Miller Edge notified all affected employees about the incident and the offering of Experian credit monitoring and fraud protection services. In addition, breach notification letters are being mailed today.

Office of the Attorney General
Attn: Security Breach Notification
November 12, 2024
Page 2

Enclosed for your reference is a sample copy of breach notification letter that is being provided to affected Maryland residents.

Please feel free to contact me directly should the need arise.

Sincerely,



Sandra A. Jeskie

SAJ/sfm/
Attachment



November 11, 2024

Re: Notice of Data Breach

Dear ,

First, I would like to express our appreciation for your employment with Miller Edge. As reflected in our email dated October 15, 2024, Miller Edge was the victim of a ransomware attack, and we offered each employee 1 year of complimentary access to Experian IdentityWorks. Our investigation is now complete, and we confirmed that your personal information appears to have been affected by this cyberattack. We are providing this letter to provide further information about your personal information and the efforts we are taking to help you ensure that your personal data is protected. Please carefully review this letter as it contains information regarding this event and important steps which you should take right away to protect your personal data.

What Happened

On October 3, 2024, Miller Edge experienced a ransomware attack. We promptly engaged cybersecurity experts, took quick action to address the attack, communicated with law enforcement, began remediation and launched an investigation. The forensic investigation is now complete, and we believe that your personal information was affected.

What Information Was Involved

Based on the investigation to date, we believe that the following information and your personnel file held on our system was affected and this includes name, address, date of birth, social security number, banking information, health information. While we do not have direct knowledge that your personal information has been improperly used or that improper activity will occur, in an abundance of caution, we felt that it was important to advise you of these facts and the steps you may wish to take to help protect yourself (listed below).

What are We Doing

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 1 year, as detailed below. We encourage you to promptly sign up for this complimentary service.

What You Can Do

Please be vigilant about monitoring your personally identifiable information, in particular your credit report information and financial accounts, to protect against fraudulent activity. Please also take care and attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf.

To assist you in this effort, you are being provided with complimentary credit monitoring and identity theft prevention services through Experian. If you are concerned about identity theft, please sign up for the complimentary monitoring and protection services by following the instructions enclosed or provided below from Experian. The deadline to sign up for this complimentary monitoring and protection service is **January 31, 2025**.

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 12 months 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 12-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 January 31, 2025** by no later than 5:59pm CT. (Your code will not work after this date/time.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
Your unique activation code, code, is required to enroll.

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 1-(833) 931-7577 by **January 31, 2025** by no later than 5:59pm CT. Be prepared to provide **engagement number B133522** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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 ExtendCARE™:** 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.

For More Information

On behalf of Miller Edge, we sincerely regret any inconvenience or concern caused by this incident. As noted above, if you have questions about the Experian 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) 931-7577 by January 31, 2025** by no later than 5:59pm CT. Be prepared to provide engagement number listed above as proof of eligibility for the Identity Restoration services by Experian. You can also reach me with questions at 610-869-4422 ext.119.

Sincerely,

Lisa Bardsley
Human Resources Manager

Information about Identity Theft Protection

Monitor Your Accounts

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

Credit Reports

Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348- 5281. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 916-8800

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 the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877- IDTHEFT (438-4338)
www.ftc.gov/idtheft

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Credit Freeze

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports?

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses above. You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze?

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Fraud Alerts

There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two credit bureaus, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to do so.

For More Information

For more information, we recommend that you review the FTC's Identify Theft website at <https://www.identitytheft.gov/>