



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

June 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 Edgewood Summit located at 300 Baker Lane, Charleston, WV 25302, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, Edgewood Summit 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 about January 25, 2024, Edgewood Summit discovered that it had been the target of a wire fraud scheme perpetrated by an unknown actor. In response, Edgewood Summit immediately launched an investigation to determine the full nature and scope of this incident. On February 22, 2024, Edgewood Summit's investigation determined that an unknown individual had access to an Edgewood Summit email account between January 9, 2024, and February 7, 2024. In response to the unauthorized access, Edgewood Summit undertook a comprehensive review of information contained within the subject email account. Through the review, which was completed on April 24, 2024, we determined that sensitive information was present in the account at the time of the incident, and thus potentially accessed without authorization.

The information that could have been subject to unauthorized access includes name and medical information.

Notice to Maryland Resident

On or about June 17, 2024, Edgewood Summit provided written notice of this incident to one (1) Maryland resident. 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, Edgewood Summit moved quickly to investigate and respond to the incident, assess the security of Edgewood Summit systems, and identify potentially affected individuals. Further, Edgewood Summit notified federal law enforcement regarding the event. Edgewood Summit is also working to implement additional safeguards and training to its employees. Edgewood Summit is providing access to credit monitoring services for 1 year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Edgewood Summit 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. Edgewood Summit is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Edgewood Summit is providing written notice of this incident to relevant state and federal regulators, and posting a notification on its website. Edgewood Summit is also notifying the U.S. Department of Health and Human Services, attached here as ***Exhibit B***.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/hkl
Enclosure

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [SECURITY INCIDENT] / [DATA BREACH])>>

Dear <<first_name>> <<last_name>>:

Edgewood Summit is writing to notify you of an incident that may affect the privacy of some of your information. We take this incident very seriously and are providing details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about January 25, 2024, Edgewood Summit discovered that it had been the target of a wire fraud scheme perpetrated by an unknown actor. In response, we immediately launched an investigation to determine the full nature and scope of this incident. On February 22, 2024, our investigation determined that an unknown individual had access to an Edgewood Summit email account between January 9, 2024, and February 7, 2024. In response to the unauthorized access, Edgewood Summit undertook a comprehensive review of information contained within the subject email account. Through the review, on April 24, 2024, we determined that sensitive information was present in the account at the time of the incident, and thus potentially accessed without authorization.

What Information Was Involved? While we have no evidence that any of your information has been subject to actual or attempted misuse, we are notifying you out of an abundance of caution and providing information and resources to help protect your personal information. The following types of your information were present in the accessed account: your <<b2b_text_2(name, data elements)>>.

What We Are Doing. Upon discovery of this incident, we immediately took steps to secure the account by changing passwords and conducted a diligent investigation to confirm the nature and scope of the incident. As part of Edgewood Summit's ongoing commitment to the security of information, our policies and procedures regarding information security are being reviewed and enhanced, additional safeguards have been implemented, and additional training is being conducted to reduce the likelihood of a similar event in the future.

As an added precaution, we are also offering you complimentary access to <<Monitoring Term Length (Months)>> of identity monitoring and identity theft restoration services, through Kroll. You will need to activate yourself in these services if you wish to do so, as we are not able to activate them on your behalf. The deadline to enroll is <<b2b_text_6(activation deadline)>>. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Personal Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements for suspicious activity and to detect errors, and to review your credit reports for suspicious activity. You may also review the enclosed *Steps You Can Take to Help Protect Your Personal Information* for additional guidance to better protect against the possibility of identity theft and fraud. We also encourage you to activate in the complimentary identity monitoring services we are offering you.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact <<TFN>>, **Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding U.S. holidays.**

Sincerely,

Edgewood Summit

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Activate in 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.

Additional information describing your services is included with this letter.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have 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.

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.

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.

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
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. 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 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. [There are approximately \[#\] Rhode Island residents that may be impacted by this event.](#)

EXHIBIT B

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov.

- * Breach Affecting: Fewer Than 500 Individuals
- * Report Type: Initial Breach Report
- * Are you a Covered Entity filing on behalf of your organization? Yes

Covered Entity

- * Name of Covered Entity: Edgewood Summit
- * Type of Covered Entity: Healthcare Provider
- * Street Address Line 1: 300 Baker Lane
- Street Address Line 2:
- * City: Charleston
- * State: West Virginia
- * ZIP: 25302

Covered Entity Point of Contact Information

- * First Name: Diane * Last Name: Gouhin
- * Email: dgouhin@edgewoodsummit.com
- * Phone Number: Contact Phones
- (Include area **Phone Number Usage**
code): (304) 346-2323 Work
- * Breach Start Date: 01/09/2024 * Breach End Date: 02/07/2024
- * Discovery Start Date: 02/22/2024 * Discovery End Date: 04/24/2024
- * Approximate Number of Individuals Affected by the Breach: 171

-
- * Type of Breach: Unauthorized Access/Disclosure

-
- * Location of Breach: Email

-
- * Type of Protected Health **Clinical**
Information Involved in
Breach: * Clinical

Diagnosis/Conditions

*** Brief Description of the Breach:**

On or about January 25, 2024, Edgewood Summit discovered that it had been the target of a wire fraud scheme perpetrated by an unknown actor. In response, Edgewood Summit immediately launched an investigation to determine the full nature and scope of this incident. On February 22, 2024, Edgewood Summit's investigation determined that an unknown individual had access to an Edgewood Summit email account between January 9, 2024, and February 7, 2024. In response to the unauthorized access, Edgewood Summit undertook a comprehensive review of information contained within the subject email account. Through the review, on April 24, 2024, Edgewood Summit determined that sensitive information was present in the account at the time of the incident, and thus potentially accessed without authorization.

*** Safeguards in Place Prior to Breach:**

Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)

*** Individual Notice Provided Start Date:**

06/17/2024

Individual Notice Provided
Projected/Expected End Date: 06/17/2024

Was Substitute Notice Required?

Yes

10 or more

Was Media Notice Required?

No

*** Actions Taken in Response to Breach:**

Changed password/strengthened password requirements
Implemented new technical safeguards
Provided individuals with free credit monitoring
Revised policies and procedures
Took steps to mitigate harm
Trained or retrained workforce members

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Edward J. Finn Date: 06/17/2024

