



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: Jsjohnson@mullen.law

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

November 17, 2022

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

Dear Sir or Madam:

We represent Myriddian, LLC (“Myriddian”) located at 8510 Corridor Road, Savage, Maryland 20763, and are writing to notify your office of an incident that may affect personal information relating to twenty-seven (27) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Myriddian 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 July 30, 2022, Myriddian became aware of suspicious activity related to certain systems within its network. Myriddian promptly took steps to secure the identified systems, disconnected its entire network from the internet, and with the assistance of third-party forensic specialists, began an investigation to determine the full nature and scope of the suspicious activity. The investigation determined that a specific portion of Myriddian’s network was subject to unauthorized access between July 29, 2022, and July 31, 2022. Given that unauthorized access to specific information in the environment occurred, Myriddian then undertook a comprehensive review of the data within the affected portion of its network in order to understand the specific information potentially impacted and to whom it related for purposes of providing notification to potentially impacted individuals. After this phase of the process was completed, Myriddian worked diligently to review its internal records to identify complete and accurate address information for potentially impacted

individuals in order to provide notification. All such efforts were completed on October 19, 2022, after which Myriddian worked to disseminate notification.

The information related to the twenty-seven (27) Maryland residents that could have been subject to unauthorized access varies by name, but includes name, Social Security number, driver's license number, financial account information, and passport number.

Notice to Maryland Residents

On or about November 17, 2022, Myriddian began providing written notice of this incident to potentially impacted individuals, which includes twenty-seven (27) Maryland residents. Written notice is being provided in substantially the same form as the letters attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon identifying the event, Myriddian promptly began a diligent investigation, which was aided by third-party forensic specialists, to assess the scope of the event, the security of Myriddian's systems, and to identify potentially affected individuals. Further, Myriddian notified federal law enforcement regarding the event. Moreover, as part of its ongoing commitment to information security, Myriddian is reviewing and enhancing its existing policies and procedures, instituting additional security measures to better protect against future similar incidents, and providing additional training to employees regarding the importance of safeguarding data. Myriddian is also notifying other requisite regulatory authorities regarding this event.

Additionally, Myriddian is providing access to credit and/or identity monitoring services for two (2) years, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Myriddian is also providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

Office of the Attorney General
November 17, 2022
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-4005.

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/rmm
Enclosure

EXHIBIT A



<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

November 17, 2022

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

Re: Notice of Data [Breach // Event]

Dear <<Name 1>> <<Name 2>>:

Myriddian, LLC ("Myriddian") is writing to notify you of an incident that may affect the privacy of some of your personal information. We write to provide you with information about the incident, our response, and steps you can take to help protect against the possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On July 30, 2022, Myriddian became aware of suspicious activity related to certain systems within our network. In response, we promptly took steps to secure the identified systems, disconnected our entire network from the internet, and began an investigation to determine the full nature and scope of the suspicious activity. Our investigation determined that a specific portion of our network was subject to unauthorized access between July 29, 2022, and July 31, 2022. Given that unauthorized access to specific information in our environment occurred, we then undertook a comprehensive review of the data within the affected portion of our network in order to understand the specific information potentially impacted and to whom it related for purposes of providing notification to potentially impacted individuals. After this phase of the process was completed, we worked diligently to review our internal records to identify complete and accurate address information for potentially impacted individuals in order to provide notification. This process was completed on or around October 19, 2022, and we are notifying you because your information was present in the portion of our network that was subject to unauthorized access.

What Information Was Involved? Our investigation determined that the information related to you that may have been impacted includes your name, [Data Elements]. While we have no evidence that any of your information was used for identity theft or fraud, we are notifying you out of an abundance of caution and providing information and resources to assist you in helping protect your personal information, should you feel it appropriate to do so.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the suspicious activity, we promptly took steps to confirm the security of our systems, and conducted a comprehensive investigation of the incident to confirm its nature, scope, and impact. Moreover, we notified federal law enforcement regarding the event. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing our existing policies and procedures, instituting additional security measures beyond those already in place to better protect against future similar incidents, and providing additional training to employees regarding the importance of safeguarding data. We are also notifying relevant regulatory authorities, as required.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for 24 months through IDX at no cost to you. If you wish to activate these complimentary services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information* section of this letter. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any such activity to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information contained in the *Steps You Can Take to Help Protect Personal Information* section of this letter for additional information and resources.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please contact me at 410-913-9563 or jmyers@myriddian.com.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason Myers", with a horizontal line extending from the end of the signature.

Jason Myers
Myriddian, LLC

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Offered Monitoring Services

As an added measure, we are offering you access to credit monitoring and identity theft protection services for 24 months through IDX at no cost to you. Please follow the below steps to enroll in the monitoring services.

1. **Website and Enrollment.** Please go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code below. You may also call 1-800-939-4170 to enroll as well.

Your Unique Enrollment Code: **[Monitoring Code]**

2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Please note, the above code must be redeemed by June 1, 2023.

IDX's MyIDCare will include two-year enrollments into the following service components:

Single Bureau Credit Monitoring – Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CyberScan™ – Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

Identity Theft Insurance – Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

Fully-Managed Identity Recovery – ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

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	833-395-6938
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 www.oag.state.md.us. Myriddian is located at 8510 Corridor Road, Savage, MD 20763.



To the Parent or Guardian of <<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

November 17, 2022

Re: Notice of Data Event

To the Parent or Guardian of <<Name 1>> <<Name 2>>:

Myriddian, LLC (“Myriddian”) is writing to notify you of an incident that may affect the privacy of some of your minor’s personal information. We write to provide you with information about the incident, our response, and steps you can take to help protect against the possible misuse of your minor’s information, should you feel it is appropriate to do so.

What Happened? On July 30, 2022, Myriddian identified suspicious activity related to several servers on its network. In response, we promptly took steps to secure the impacted servers, disconnected our entire network from the internet, and with the assistance of third-party forensic specialists, began an investigation to determine the full nature and scope of the suspicious activity. Our investigation confirmed a portion of our network was subject to unauthorized access between July 29, 2022, and July 30, 2022. We then undertook a comprehensive review of the data within the affected portion of our network in order to understand the specific information potentially impacted and to whom it related for purposes of providing notification to potentially impacted individuals. After this phase of the process was completed, we worked diligently to review our internal records to identify complete and accurate address information for potentially impacted individuals in order to provide notification. This process was completed on or around October 19, 2022, and we are notifying you because your minor’s information was present in the portion of our network that was subject to unauthorized access.

What Information Was Involved? Our investigation determined that the information related to your minor that may have been impacted includes your minor’s [Data elements]. While we have no evidence that any of your minor’s information was used for identity theft or fraud, we are notifying you out of an abundance of caution and providing information and resources to assist you in helping protect your minor’s personal information, should you feel it appropriate to do so.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the suspicious activity, we promptly took steps to confirm the security of our systems, and conducted a comprehensive investigation of the incident to confirm its nature, scope, and impact. Moreover, we notified federal law enforcement regarding the event. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing existing policies and procedures, instituting additional security measures beyond those already in place to better protect against future similar incidents, and providing additional training to employees regarding the importance of safeguarding data. We are also notifying relevant regulatory authorities, as required.

As an added precaution, we are offering your minor access to monitoring and identity theft protection services for 24 months through IDX at no cost to you. If you wish to activate these complimentary services on behalf of your minor, you may follow the instructions included in the *Steps You Can Take to Help*

Protect Your Minor's Personal Information section of this letter. We encourage you to enroll your minor in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and free credit reports, if any, for suspicious activity and to detect errors. You should report any such activity to law enforcement. You can also enroll your minor to receive the complimentary monitoring services that we are offering. Please also review the information contained in the *Steps You Can Take to Help Protect Your Minor's Personal Information* section of this letter for additional information and resources.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please contact me at 410-913-9563 or jmyers@myriddian.com.

We sincerely regret any inconvenience or concern this incident may cause you or your minor.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jason Myers', with a stylized flourish at the end.

Jason Myers
Myriddian, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR'S PERSONAL INFORMATION

Enroll in Offered Monitoring Services

As an added measure, we are offering your minor access to identity theft protection services for 24 months through IDX at no cost to you. Please follow the below steps to enroll in monitoring services.

Website and Enrollment. Please go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using the below unique Enrollment Code for your minor. You may also call 1-800-939-4170 to enroll as well.

Your Minor's Unique Enrollment Code: **[Monitoring Code]**

Please note, the above code must be redeemed by June 1, 2023.

IDX's MyIDCare will include two-year enrollments into the following service components:

CyberScan™ – Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

Identity Theft Insurance – Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

Fully-Managed Identity Recovery – ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

Monitor Your Minor's Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report or to request a manual search for your minor's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit the below websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/education/identity-theft/child-identity-theft/	www.experian.com/fraud/form-minor-child.html	https://www.transunion.com/fraud-victim-resources
888-298-0045	888-397-3742	833-395-6938
P.O. Box 105788 Atlanta, GA 30348-5788	P.O. Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19094

To request information about the existence of a credit file in your minor's name, search for your minor's Social Security number, place a security freeze on your minor's credit file, place a fraud alert on your

minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide some or all of the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor's birth certificate;
- A copy of your minor's Social Security card;
- Your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor's date of birth; and
- Your minor's previous addresses for the past two years.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps individuals can take to protect 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 and/or your minor have the right to file a police report if your minor ever experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you or your minor will likely need to provide some proof that your minor has 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 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 www.oag.state.md.us. Myriddian is located at 8510 Corridor Road, Savage, MD 20763.