



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

December 23, 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 Exostar LLC (“Exostar”) located at 2325 Dulles Corner Blvd., Suite 600, Herndon, Virginia 20171, and are writing to notify your office of an event that may involve certain personal information relating to approximately four (4) Maryland residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Exostar 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 November 22, 2024 Exostar determined that certain personal information was accessible within a third-party provided system to unauthorized actors. Exostar learned through its investigation that the system was accessed without authorization by actors between October 16, 2023 and April 11, 2024 and that during this time certain files and information were copied from the system.

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

Notice to Maryland Residents

On or about December 23, 2024, Exostar provided written notice of this event to approximately four (4) 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 event, Exostar moved to investigate and respond appropriately, including assessing and confirming the security of Exostar systems and working to identify potentially affected individuals. Exostar also has worked with its vendors to implement enhanced security measures and additional monitoring tools. Exostar is providing access to credit monitoring services to individuals for 24 months, through IDX, a Zerofox company, to individuals whose Social Security numbers and/or driver's license numbers were potentially involved in this event, at no cost to these individuals.

Additionally, Exostar is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Exostar is 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:ncs
Enclosure

EXHIBIT A

To Enroll, Please Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXXXX>>

<<Exostar Letterhead/Logo>>

<<First Name>> <<Middle Initial/Name>> <<Last Name>>

<<Address 1>>

<<Address 2>>

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

<<Date>>

Re: Notice of Data Incident

Dear <<First Name>> <<Middle Initial/Name>> <<Last Name>>:

Exostar LLC (“Exostar”) writes to inform you of an incident that may involve some of your information. You are receiving this letter because you are a current or former Exostar employee or contractor. This letter provides information about the incident, steps Exostar has taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? In October 2023, Exostar was alerted of a potential incident involving exposure of certain information from a third party system. Upon learning of the potential incident and with the assistance of its third party vendor and federal law enforcement, Exostar quickly began an investigation to understand the full nature and scope of the incident. Exostar’s investigation confirmed that unauthorized actors exploited a configuration issue with the third party system that allowed the actors to access and/or copy certain files and information from the third party system between October 2023, and April 2024. Exostar then worked with the appropriate specialists to remediate the configuration issue to prevent similar incidents in the future. To understand what information was contained in the affected files, Exostar subsequently conducted a thorough review of the contents of the affected files to determine whether it contained sensitive information and to whom that information relates. On November 22, 2024, Exostar concluded the review and determined that your information was in the files and information that was accessed and/or copied by the unauthorized actors.

What Information Was Involved? Exostar has no indication that the data affected by this incident has been used to commit identity theft, fraud, or other financial harm to individuals. However, Exostar is notifying you because the files and information involved contained your <<data elements>>, and name.

What We Are Doing. Exostar prioritizes its responsibility to safeguard the information in its possession. As such, Exostar responded upon learning of this incident and has worked diligently with the proper specialists and authorities to conduct a comprehensive investigation in order to provide you with accurate and complete notice of the incident as soon and accurately as possible. As part of its ongoing commitment to the privacy and security of information in its care, Exostar continues to review its existing policies and training protocols relating to data protection on an ongoing basis. Exostar also implemented enhanced security measures and additional monitoring tools to mitigate any risk associated with this incident and to better prevent similar incidents in the future.

As an added precaution, Exostar is providing you complimentary access to identity theft protection services through IDX, a ZeroFox company, as well as guidance on how to better protect your information. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Although Exostar is covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions enclosed.

What You Can Do. In accordance with best practices, as would be recommended in response to any data incident, Exostar encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next 12 to 24 months. Any questionable activity detected should be reported to the associated insurance company, health care provider, or financial institution immediately. You can also find out more about how to safeguard your information in the enclosed *Steps You Can*

Take to Protect 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, you may reach Exostar at privacy@exostar.com.

Sincerely,

Privacy Office
Exostar LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

We encourage you to enroll in complimentary IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or calling **1-800-939-4170** and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is **December 31, 2025**.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

IDX Identity enrollments will include two-year enrollments into the following service components:

SINGLE BUREAU CREDIT MONITORING (adults*) - 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.

CYBERSCANTM - 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.

*Enrolled minors will receive all other service components listed above.

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 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 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>.