
March 7, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Anthony G. Brown,

We are writing to notify you of a data security incident that may have affected certain personal information maintained by SES Space & Defense, Inc (“S&D”). This incident may have involved personal information maintained by S&D related to five (5) Maryland residents. At this time, we have no indications that the personal information has been subject to fraudulent use as a result of this incident.

On or about March 31, 2023, S&D became aware of an IT security incident impacting certain company IT systems. S&D started an investigation, retained leading experts, notified certain law enforcement and governmental authorities, and implemented measures to assess and contain the incident. These measures include disabling certain VPN accounts and accounts within administrative privileges, deploying enhanced Endpoint Detection and Response protection, and performing an enterprise password reset.

The investigation has determined that an unauthorized third-party accessed certain S&D systems and accessed and/or acquired certain data. We undertook a detailed review of the affected data with the assistance of third-party specialists. Based on that review, we determined that the personal information of five (5) Maryland residents may have been impacted, including the individual’s name and, varying by individual, driver’s license number, passport number, and/or Social Security Number. A sample individual notice is enclosed, which will be mailed to each of the five (5) Maryland residents.

As an added precaution and as set forth in the attached notification letter, S&D is offering the individuals complimentary access to 24 months of credit monitoring, web monitoring, and identity theft restoration services.

If you have any questions, please do not hesitate to contact me at brian.pedati@sessd.com.

Sincerely,

Brian Pedati
General Counsel
SES Space & Defense, Inc

Brian D. Pedati
General Counsel

SES Space & Defense
11790 Sunrise Valley Drive, Suite 300 • Reston • VA • 20191 • US
Mobile +1 571 665 0344
brian.pedati@sessd.com



Connect with us at www.sessd.com

[LinkedIn](#) • [Twitter](#) • [Facebook](#)

DISCLAIMER: This e-mail contains proprietary information, some or all of which may be legally privileged. It is for the intended recipient only. If an addressing or transmission error has misdirected this e-mail, please notify the author by replying to this e-mail. If you are not the intended recipient, you must not use, disclose, distribute, print or rely on this e-mail.

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

SES Space & Defense, Inc.

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

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

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to let you know about a data security incident that may have affected certain information in our possession. At this time, we have indications that an unauthorized party may have accessed and/or acquired certain of your personal information. However, we have no indication of fraudulent use of such personal information as a result of this incident. We are writing to explain the circumstances of the incident and to inform you of the steps we have taken and the resources we are making available to you.

What Happened?

We investigated the incident, retained leading experts, notified certain law enforcement and governmental authorities, and implemented measures to assess and contain the incident.

The investigation revealed that an unauthorized third-party accessed certain S&D systems and accessed and/or acquired certain data. We undertook a detailed review of the affected data with the assistance of third-party specialists, and through that review recently identified that certain of your personal information may have been impacted.

What Information Was Involved?

Based on our investigation, we understand that your <<b2b_text_1(data elements)>> may have been accessed and/or acquired by the unauthorized third party.

What We Are Doing.

We took prompt steps to investigate the incident and notified law enforcement. As part of our investigation, we have taken, and continue to take, measures to further secure our systems.

As an added precaution, we are offering you complimentary access to 24 months of identity monitoring services through Kroll. Additional information describing these services is included on page three of this letter. To activate these services, please take the following steps:

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>>

What You Can Do.

At this time, we have no indication of fraudulent use of your personal information as a result of this incident. Nevertheless, we recommend that you remain vigilant for fraud and identity theft.

Further steps you can take can be found on the “Additional Ways to Help Protect Your Identity” document we have included on the following pages.

For More Information

If you have questions, please feel free to call [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major bank holidays).

Sincerely,

SES Space & Defense, Inc.

Description of 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.

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.

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.

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some you may consider:

Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian 1-888-397-3742 Experian.com Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion 1-800-680-7289 Transunion.com TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094
---	---	--

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322- 8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing, or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Maryland and New York.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.marylandattorneygeneral.gov>, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 1.800.771.7755.