

Jena M. Valdetero
Tel 312.456.1025
jena.valdetero@gtlaw.com

December 2, 2022

Attorney General Brian E. Frosh

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

VIA EMAIL

Dear Attorney General Frosh:

We are writing to inform you that our client, BAE Systems, Inc., ("BAE Systems") is notifying approximately four hundred and ten (410) individuals who reside in Maryland of a data security incident that may have impacted some of their personal information.

On November 6, 2022, BAE Systems discovered that certain personal information entrusted to a vendor was the subject of unauthorized access. BAE Systems immediately began investigating the incident and worked with the vendor to determine what information may have been at risk and completed that review on November 21, 2022. The vendor confirmed the earliest date of unauthorized access to their systems occurred on September 25, 2022. We have no information that the data has or will be misused, and the vendor has confirmed that the data files have been recovered and the information no longer is accessible.

The impacted personal information contained one or more of the following: name, address, health and medical information, passport number, and Social Security numbers. BAE Systems mailed notifications to all potentially affected individuals on December 2, 2022. An example of the notifications is attached. Information to assist impacted individuals, including a complimentary credit monitoring package for individuals with impacted Social Security numbers, was included in the notice.

Please contact me for any additional information.

Best regards,



Jena Valdetero
Shareholder

Greenberg Traurig, LLP | Attorneys at Law

77 West Wacker Drive | Suite 3100 | Chicago, Illinois 60601 | T +1 312.456.8400 | F +1 312.456.8435

Albany. Amsterdam. Atlanta. Austin. Berlin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Las Vegas. London.[†] Los Angeles. Mexico City.[†] Miami. Milan.[‡] Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.[‡] Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.[†] Tokyo.[‡] Warsaw.[‡] Washington, D.C. West Palm Beach. Westchester County.

Operates as: [†]Greenberg Traurig Germany, LLP; ^{*}A separate UK registered legal entity; [†]Greenberg Traurig, S.C.; [‡]Greenberg Traurig Santa Maria; [∞]Greenberg Traurig LLP Foreign Legal Consultant Office; [^]A branch of Greenberg Traurig, P.A., Florida, USA; [¤]GT Tokyo ^{www.gtlaw.com}
Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubegoshi Jimusho; [~]Greenberg Traurig Grzesiak sp.k.ACTIVE 683779517v1

October 28, 2022
Page 2

BAE SYSTEMS

P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-5725

Or Visit:

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

Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

<<Notice of Data Breach CA Only>>

December 2, 2022

Dear <<First Name>> <<Last Name>>,

We are writing with important information regarding a recent data security incident experienced by a BAE Systems vendor that may have included some of your personal information. This incident did not impact BAE Systems' own systems, and we are working with the vendor to ensure that they take steps to prevent a similar occurrence in the future. We have no information that the data has been or will be misused, and the vendor has obtained assurance that the unauthorized third party no longer has access to the data. We take the security of your information very seriously and sincerely apologize for any concern this incident may cause. This letter contains information about steps you can take to protect your information.

What Happened?

On November 6, 2022, BAE Systems discovered that certain personal information entrusted to a vendor was the subject of unauthorized access. We immediately began investigating the incident and have been working with the vendor to determine what information may have been at risk. The vendor confirmed the earliest date of access to their systems by the unauthorized third party occurred on September 25, 2022.

What Information Was Involved?

This incident may have impacted your name, address, and <<variable 1, 2, 3, 4, 5, 6>>. We understand that the vendor has recovered the data, and, after a thorough investigation, we believe it is no longer accessible.

What We Are Doing

We take the security of personal information very seriously, and we want to assure you that we have already taken steps to prevent a reoccurrence by disconnecting our systems from the vendor's and by reviewing vendor security protocols. Additionally, as a safeguard, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of credit monitoring 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.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-896-5725 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 2, 2023.

In addition, please review the enclosed “Additional Important Information” section included with this letter, which contains steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

We and the third party vendor deeply regret that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken steps to ensure additional precautions have been taken to safeguard it. If you have any questions, please contact IDX at 1-833-896-5725.

Sincerely,

Jeffrey C. Dodson
Vice President and Chief Security Officer
BAE Systems, Inc.

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Office of Attorney General
441 4th St NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 www.ncdoj.com	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

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

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.experian.com/freeze/center.html
1-800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com/credit-freeze
1-800-680-7289

BAE SYSTEMS

P.O Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

December 2, 2022

<<Notice of Data Breach CA Only>>

Dear <<First Name>> <<Last Name>>,

We are writing with important information regarding a recent data security incident experienced by a BAE Systems vendor that may have included some of your personal information. This incident did not impact BAE Systems' own systems, and we are working with the vendor to ensure that they take steps to prevent a similar occurrence in the future. We have no information that the data has been or will be misused, and the vendor has obtained assurance that the unauthorized third party no longer has access to the data. We take the security of your information very seriously and sincerely apologize for any concern this incident may cause. This letter contains information about steps you can take to protect your information.

What Happened?

On November 6, 2022, BAE Systems discovered that certain personal information entrusted to a vendor was the subject of unauthorized access. We immediately began investigating the incident and have been working with the vendor to determine what information may have been at risk. The vendor confirmed the earliest date of access to their systems by the unauthorized third party occurred on September 25, 2022.

What Information Was Involved?

This incident may have impacted your name, address, and <<variable 1, 2, 3, 4, 5, 6>>. We understand that the vendor has recovered the data, and, after a thorough investigation, we believe it is no longer accessible.

What We Are Doing

We take the security of personal information very seriously, and we want to assure you that we have already taken steps to prevent a recurrence by disconnecting our systems from the vendor's and by reviewing vendor security protocols.

What You Can Do

Please review the enclosed "Additional Important Information" section included with this letter, which contains steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

We and the third party vendor deeply regret that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken steps to ensure additional precautions have been taken to safeguard it. If you have any questions, please contact 1-833-896-5725.

Sincerely,

Jeffrey C. Dodson
Vice President and Chief Security Officer
BAE Systems, Inc.

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Office of Attorney General
441 4th St NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 www.ncdoj.com	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

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

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.experian.com/freeze/center.html
1-800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com/credit-freeze
1-800-680-7289

