



Lindsay B. Nickle
1201 Elm Street, Suite 2550
Dallas, TX 75270
lnickle@constangy.com
Direct: 806.535.0274

March 29, 2023

VIA E-MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Elbit Systems of America, LLC (“Elbit America”) in connection with a recent data security incident described in greater detail below. Elbit America is a technology and engineering firm for defense and commercial applications headquartered in Fort Worth, Texas. Elbit America takes the protection of all information within its possession very seriously and has taken significant steps to help prevent a similar incident from occurring in the future.

1. Nature of the Security Incident.

On June 8, 2022, Elbit America discovered unusual activity in its network environment. Elbit America immediately shut down its network and took steps to secure its environment. Elbit America also engaged a leading, independent cybersecurity firm to assist Elbit America with safely restoring its operations, investigating the incident, and to determine if any personal information was affected as quickly as possible. Through this investigation, Elbit America learned that personal information belonging to certain current and former employees and contractors and their dependents may have been acquired without authorization.

2. Number of Maryland Residents Affected.

At the outset of the incident, out of an abundance of caution, Elbit America notified all employees. On February 22, 2023, Elbit America learned additional individuals may have had their information impacted in the incident and that the personal information of two (2) residents of Maryland was potentially acquired without authorization. The impacted information varies by individual but may

include: names, addresses, Social Security numbers, tax identification numbers, driver's license numbers, passport numbers, information related to physical or mental health, usernames and passwords, payment for the provision of healthcare, and health account, subscriber, or identifier numbers.

On March 16, 2023, a notification letter was mailed to two (2) Maryland residents. The letter advised the recipient about steps they can take to help protect their information. In addition, Elbit America offered complimentary credit monitoring and identity protection services for 12 months through IDX. The identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident.

Elbit America has taken steps in response to this incident to help prevent similar incidents from occurring in the future. Elbit America has worked since discovering this incident with leading cybersecurity experts to enhance the security of its network environment and deployed endpoint detection and monitoring software throughout its environment.

4. Contact Information.

Elbit America remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (806) 535-0274 or via email at lnickle@constangy.com.

Very truly yours,



Lindsay B. Nickle of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 16, 2023

Re: Notice of Data Security <<VariableText1>>

Dear <<First name>> <<Last Name>>:

We are writing to inform you of a data security incident experienced by Elbit Systems of America, LLC (“Elbit America”) that may have involved your personal information. At Elbit America, we take the privacy and security of personal information very seriously. As such, we are notifying you of the incident, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened? On June 8, 2022, someone attempted to interfere with Elbit America’s cyber operations. We immediately shut down our network and took steps to secure our environment. We also engaged a leading cybersecurity firm to assist with safely restoring our operations, to investigate the incident, and to determine if any personal information was affected. The investigation revealed that an unknown actor gained access to and obtained certain data from the Elbit network. On February 22, 2023, we determined that your personal information may have been impacted. We have no reason to believe that your personal information has been misused as a result of this incident.

What Information Was Involved? The following information may have been impacted: your <<VariableText2>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also notified law enforcement and are cooperating with the resulting investigation. We are providing you with information about steps you can take to help protect your personal information. In addition, we are offering you complimentary credit and identity monitoring and recovery services for <<12 or 24>> months through IDX as described below.

What You Can Do: We recommend that you review the guidance included with this letter about how to protect your personal information. We also encourage you to enroll in the complimentary credit monitoring and identity monitoring services, which are free to you upon enrollment. These services include a subscription for the following: single bureau credit monitoring, CyberScan dark web monitoring, fully-managed identity recovery services, and \$1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

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 information describing your services is included with this letter.

Please note you must enroll by June 16, 2023. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For More Information: If you have any questions about the complimentary services or need assistance, please contact customer service for IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We want to emphasize that we are taking this situation extremely seriously as the privacy and protection of personal information is a top priority for Elbit America. We have taken and continue to take steps to protect against a similar incident from occurring in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Raanan Horowitz". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Raanan Horowitz
President and CEO
Elbit Systems of America, LLC

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 740256
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft 1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

**New York Attorney General Bureau
of Internet and Technology
Resources**

28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street Providence,
RI 02903 <http://www.riag.ri.gov> 1-401-274-4400

Washington D.C. Attorney General

400 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf.

