

# KING & SPALDING

RECEIVED

JAN 03 2019

CONSUMER PROTECTION

King & Spalding LLP  
1700 Pennsylvania Ave, NW  
Suite 200  
Washington, D.C. 20006-4707  
Tel: +1 202 737 0500  
Fax: +1 202 626 3737  
www.kslaw.com

Scott Ferber  
Partner  
Direct Dial: +1 202 626 8974  
Direct Fax: +1 202 626 3737  
sferber@kslaw.com

December 28, 2018

## **BY U.S. MAIL**

To: Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Data Security Incident Affecting General Dynamics Information Technology

Dear Attorney General MacDonald:

On behalf of General Dynamics Information Technology (“GDIT”), I write to inform you of GDIT’s investigation into a recent data security incident and to explain the steps GDIT is taking to notify potentially affected individuals and to provide them ways with which to protect their personal information.

GDIT recently discovered that from approximately October 31, 2018 to November 13, 2018, a now former employee obtained unauthorized access to a limited number of consumer records held in a computer system. Upon discovery, GDIT immediately began investigating the incident to determine the scope and identify the information that was potentially affected and determined that a limited amount of personal information was accessed in the system without authorization. This information may have included name, address, date of birth, gender, social security number, marketplace user ID number, and/or email address.

GDIT has taken steps to strengthen the security and processes of employee system access. The individual who obtained the unauthorized access is no longer employed by the company. GDIT has notified appropriate law enforcement authorities. GDIT is sending notification letters to the potentially impacted individuals on December 28, 2018, including 32 New Hampshire residents. An unaddressed copy of the notification letter is attached as Exhibit A. In an abundance of caution, GDIT is also offering identity theft protection services at no cost for 24 months from AllClear ID. Please do not hesitate to contact me if you have any questions regarding this letter.

Office of the Attorney General  
December 28, 2018  
Page 2

Please do not hesitate to contact me if you have any questions regarding this letter.

Very truly yours,

A handwritten signature in black ink, appearing to read "Scott Ferber", with a long horizontal line extending to the right.

Scott Ferber

Attachment

**GENERAL DYNAMICS**  
Information Technology

Processing Center • P.O. BOX 141578 • Austin, TX 78714



JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

December 28, 2018

NOTICE OF DATA BREACH

Dear John Sample:

We are writing to inform you of a data security incident that may have involved some of your personal information. You are receiving this letter, along with an offer for identity theft protection services at no cost to you, out of an abundance of caution.

**What happened**

General Dynamics Information Technology (“GDIT”) recently discovered that from approximately October 31, 2018 to November 13, 2018, a now former employee obtained unauthorized access to a limited number of consumer records held in a computer system. Upon discovery, GDIT immediately began investigating the incident to determine the scope and identify the information that was potentially affected and determined that a limited amount of personal information was accessed in the system without authorization.

**What information was involved**

Based on our investigation, we determined that some of your personal information was included in the accessed computer system. This information may have included name, address, date of birth, gender, Social Security number, marketplace user ID number, and/or email address.

**What we are doing**

The security and confidentiality of your information is of critical importance to us and a responsibility we take very seriously. As discussed above, upon discovery, GDIT immediately began investigating the incident. We have taken steps to strengthen the security and processes of employee system access. The individual is no longer employed by the company. GDIT has also notified appropriate law enforcement authorities and intends to cooperate with any investigation. In an abundance of caution, we are offering you identity theft protection services at no cost to you for 24 months from AllClear ID. Information on how to enroll in these services is included below and additional information is enclosed with this notice. We also want to make you aware of steps you may take to help guard against identity theft or fraud. Please review the enclosed Identity Theft Prevention Tips.



## **What you can do**

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 24 months.

**AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-263-1695, and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.

**AllClear Fraud Alerts with Credit Monitoring:** This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-263-1695 using the following redemption code: **Redemption Code**.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

## **For more information**

If you have further questions or concerns about this incident, you can contact us at 1-855-263-1695, Monday through Saturday from 8 a.m. to 8 p.m. Central Time (excluding national holidays). We are committed to protecting your personal information and we sincerely regret any inconvenience or concern caused by this incident.

Enclosures:   Identity Theft Prevention Tips  
                  AllClear Identity Repair Terms of Use

## Identity Theft Prevention Tips

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

Equifax  
P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
800-685-1111

Experian  
P.O. Box 9532  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
P.O. Box 1000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)  
800-888-4213

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission**  
Bureau of Consumer Protection  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

State Attorneys General: Information on how to contact your state attorney general may be found at [www.naag.org/naag/attorneys-general/whos-my-ag.php](http://www.naag.org/naag/attorneys-general/whos-my-ag.php).

**PLEASE NOTE** that under recent federal legislation under the Economic Growth, Regulatory Relief, and Consumer Protection Act, fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies. You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.



As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services>

<https://www.experian.com/freeze/center.html>

<https://www.transunion.com/credit-freeze>

### **IF YOU ARE A MARYLAND RESIDENT**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the State of Maryland Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

### **IF YOU ARE A NEW MEXICO RESIDENT**

Under New Mexico law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

### **IF YOU ARE A NORTH CAROLINA RESIDENT**

You may obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)



## AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

### **Services Provided**

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

### **Coverage Period**

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

### **Eligibility Requirements**

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

### **How to File a Claim**

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

### **Coverage under AllClear Identity Repair Does Not Apply to the Following:**

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

### **Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

### **Opt-out Policy**

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

<b>E-mail</b> support@allclearid.com	<b>Mail</b> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	<b>Phone</b> 1.855.434.8077
---	--	--------------------------------

