June 9, 2023

<Name>
<Address>
<City>, <State> <Zip>

Notice of Data Breach

Dear <Name>:

We are writing to inform you of a security incident that involved your personal information. The security incident affected systems operated by Diligent Corp. ("Diligent"). Diligent is a third-party service provider to Leidos and hosts Leidos' enterprise case management system ("ECMS"), which includes information gathered in connection with internal investigations. Your personal information was among the information in the ECMS that may have been exposed as a result of this incident. Please read this notice carefully to learn more about the incident and what you can do to protect yourself.

What Happened

On November 11, 2022, Diligent notified Leidos that an unauthorized individual was able to exploit a vulnerability in Diligent's platform to download documents from the system, possibly as early as September 30th. On February 9, 2023, Diligent informed Leidos that an unauthorized person was able to exploit a second vulnerability in Diligent's platform to view the information submitted by individuals to Leidos through the ECMS, possibly as early as October 1, 2022.

Upon learning of the first phase of this incident, Leidos worked with Diligent to understand the scope of the incident. Diligent provided Leidos with copies of the affected documents but was unable to provide any information about their contents or whether any personal information was impacted by this incident. Leidos promptly began a manual review of the documents to determine if they contained any personal information and to identify affected individuals. When Diligent notified Leidos of the second phase of this incident, Leidos requested that Diligent provide it with a copy of all impacted information, which Leidos manually reviewed to determine if any personal information was affected. As a result of these reviews, Leidos has determined that the documents or forms affected by this incident included your personal information.

What Information Was Involved

Our investigation has revealed that this incident affected the following types of personal information about you:

- <Data Types>

What We Are Doing

Upon first learning of this incident, Leidos worked with Diligent to understand how the incident occurred. Diligent reviewed its security measures, identified the vulnerabilities that were exploited to gain access to the documents and information in the ECMS, and implemented multiple patches to address those vulnerabilities. Leidos also restricted its use of the ECMS while it re-evaluated the system's security.

Similarly, upon learning of the second phase of this incident, Diligent identified the exploited vulnerabilities and implemented several patches to address them.

While Leidos continues to review the effectiveness of Diligent's security measures, we are also examining our processes around our use of the ECMS. Leidos is currently requiring all new reports to be submitted directly to Leidos and has instructed all Leidos employees with access to the ECMS to refrain from uploading any new documents to the ECMS. At Leidos' request, Diligent took the ECMS offline to prevent further access to Leidos data from the internet.

What You Can Do

We encourage you to carefully review the Additional Resources appendix to this letter, as it contains information about the steps you can take to protect yourself against fraud and identity theft. We are offering you two (2) years of complimentary credit monitoring and identity protection services. Please review the enrollment instructions provided below for information about activating these services. Please note that you must activate these services prior to the enrollment deadline provided with the enrollment instructions.

We encourage you to remain vigilant by reviewing your account statements, credit reports, and explanation of benefits for unauthorized activity. If you believe you may be the victim of identity theft, you should contact your local law enforcement representative, your state attorney general, and/or the Federal Trade Commission.

More Information. If you have any questions about this incident, you can contact us at privacy@leidos.com or by phone at 571-526-7200. We regret any inconvenience this incident may have caused you. Leidos takes the protection of your personal information very seriously and has taken steps to prevent a similar incident from occurring again.

Sincerely,

Leidos, Inc.

<First Name> <Last Name>
Enter your Activation Code: **<Activation Code>**
Enrollment Deadline: December 31, 2023

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of **<Activation Code>** then click "Submit"

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Resources

Free Credit Report. You can obtain a free copy of your credit report once every 12 months from each of the three nationwide credit bureaus. We have provided the contact information for each of the nationwide credit bureaus below. You can also obtain a free credit report by visiting www.annualcreditreport.com or by calling, toll-free, (877) 322-8228.

Equifax P.O. Box 105069 Atlanta, GA 30348 800-525-6285 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 800-680-7289 www.transunion.com

If you see anything on your credit report that you do not understand, you should notify the credit bureau that sent you the report immediately. If you find any suspicious activity on your credit report, call your local police or sheriff's office, and file a police report for identity theft. You have a right to obtain a copy of the police report, which you may need to provide to creditors to clear up your records. Please note that Leidos has not delayed providing notice due to a law enforcement investigation.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. 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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Additional Information. You can learn more about protecting yourself from identity theft and fraud, including how to request that a fraud alert or security freeze be placed on your credit report, from the Federal Trade Commission at http://www.ftc.gov/idtheft. You can also call the FTC at 1-877-IDTHEFT (438-4338) or contact the FTC by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. You can obtain information about requesting a fraud alert or security freeze from the nationwide credit bureaus by contacting them using the information provided above.

Your state's attorney general may also have resources about protecting yourself from identity theft and fraud. We encourage you to check the website for your state's attorney general for more information on how to protect yourself and your information.

If you live in any of the following states, please review the information below that pertains to your state.

For District of Columbia Residents: You have a right to obtain a security freeze, which restricts access to your credit report. Please review the information provided above to understand how you can request a security freeze. You may also obtain information about preventing and avoiding identity theft from the District of Columbia Office of the Attorney General: District of Columbia Office of the Attorney General, 400 6th Street, NW Washington, DC 20001, (202) 727-3400, https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

For Iowa Residents: You may report suspected incidents of identity theft to local law enforcement or contact the Iowa Office of the Attorney General: Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, 515-281-6771, https://www.iowaattorneygeneral.gov/for-consumers/.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For Massachusetts Residents: By law, you have a right to obtain a police report filed relating to these incidents (if any), and 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 also have the right to request a security freeze, at no charge, as described above. You may contact and obtain information from the Massachusetts Attorney General at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/internet/privacy-and-identity-theft.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For Oregon Residents: You may also report suspected identity theft to local law enforcement, including the Oregon Office of the Attorney General: Oregon Office of the Attorney General, Consumer Protection, 1162 Court St. NE, Salem, OR 97301, 1-877-877-9392, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/.

For Rhode Island Residents: By law, you have a right to obtain a police report filed relating to these incidents (if any), and 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 contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.