

Serco Inc.
12930 Worldgate Drive
Suite 600
Herndon, VA 20170



July 31, 2023

NOTICE OF DATA BREACH

Dear **SAMPLE**,

Serco is committed to maintaining the integrity and security of our employees' personal information. As a follow-up to our July 5, 2023 email to you, we are writing to notify you of an incident that affected our third-party benefits administrator, CBIZ, Inc. ("CBIZ") and some of your personal information. We take this situation seriously and sincerely regret any concern that this incident may cause.

WHAT HAPPENED?

On June 30, 2023, Serco was made aware that our third-party benefits administration provider, CBIZ, experienced a ransomware attack and data breach involving their MOVEit file transfer platform. This incident was associated with the exploit of a critical security vulnerability in MOVEit Transfer, a tool used by enterprises to share large files over the internet. Ransomware attacks on the MOVEit platform have been reported to have affected several hundred organizations. We understand from CBIZ that the incident began in May 2023 and CBIZ took steps to mitigate the incident on June 5, 2023. To be clear, the breach of CBIZ's systems did not affect the safety and security of Serco's systems.

WHAT INFORMATION WAS INVOLVED?

The personal information that may have been accessed includes one or more of the following: your name, U.S. Social Security Number, date of birth, home mailing address, Serco and/or personal e-mail address, and the health benefits you elected for the year. To date, we have no evidence to suggest that any other personal information was involved or that your personal information was misused in any way.

WHAT WE ARE DOING

After being notified by CBIZ of the data breach, we promptly began an investigation and took action to address the incident with CBIZ. Our Information Security team is actively working with CBIZ to investigate the extent of the incident and to ensure that CBIZ has implemented necessary security measures to prevent similar occurrences in the future.

As a precaution, we have also secured the services of NortonLifeLock to provide credit and identity theft monitoring services at no cost to you for eighteen (18) months. The identity theft monitoring services include primary identity alert, dark web monitoring, three-bureau credit monitoring, For more information about NortonLifeLock and your identity theft monitoring services, you can visit LifeLock.norton.com/US. Please find details on signing up for a complimentary membership to NortonLifeLock's identity theft protection services and additional information describing their services at the end of this letter.

WHAT YOU CAN DO

As noted above, we have no evidence that your information has been misused. As a best practice, you should remain vigilant and carefully review your personal and work accounts for any suspicious activity. If you detect any unauthorized activity on an account, you should change the password and security questions associated with the account. We encourage you to contact NortonLifeLock and take advantage of the identity theft monitoring services we are providing to you free of charge. In addition, please continue to report any unusual activity on your Serco email accounts or Serco-related text messages to the Information Security team at ServiceDesk-IT@serco-na.com so that our Information Security team can investigate.

If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection, details on how to place a fraud alert or a security freeze on your credit file, and the toll-free telephone numbers and addresses of the major credit reporting agencies.

FOR MORE INFORMATION

We sincerely regret any inconvenience that this matter has caused you. If you have any questions, please contact Serco's Benefits Help Desk at 703-263-6010 Monday through Friday from 8:00 AM EST to 5:00 PM EST.

Sincerely,

Serco Benefits Team

Complimentary Credit Monitoring and Identity Protection Services

Serco, Inc has retained **NortonLifeLock** to provide Eighteen (18) Months of complimentary **LifeLock Defender™ Preferred** identity theft protection

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **Norton.com/Offers**
2. Below the THREE protection plan boxes, you may enter the **Promo Code: SERC230718** and click the **“APPLY”** button.
3. Your complimentary offer is presented. Click the Orange **“START MEMBERSHIP”** button.
4. A Popup will appear to enter your Member ID **80066226** and click **“APPLY”**
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: (800) 995-3086

You will have until October 31st, 2023, to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Defender™ Preferred** membership includes:

- ✓ Primary Identity Alert System[†]
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring^{**}
- ✓ Norton™ Security Deluxe² (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to \$25,000^{††}
- ✓ Personal Expense Compensation up to \$25,000^{††}
- ✓ Coverage for Lawyers and Experts up to \$1 million^{††}
- ✓ U.S.-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores^{1**}
The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring^{1**}
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts^{†**}

¹ If your plan includes credit reports, scores, and/or credit monitoring features (“Credit Features”), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is

successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.

²Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

** These features are not enabled upon enrollment. Member must take action to get their protection.

††† Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender Choice. And up to \$1 million for coverage for lawyers and experts if needed, for all plans. Benefits provided by Master Policy issued by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission (“FTC”) and/or the Attorney General’s office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

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

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 <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

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

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

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

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, <http://www.ag.ny.gov/home.html>, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at (202) 442-9828; 400 6th Ave NW, Washington DC 20001 or <https://oag.dc.gov/>.

For Rhode Island residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, <http://www.riag.ri.gov>, (401) 274-4400.