



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

January 19, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

By Email

To Whom It May Concern:

I am writing on behalf of Sirius Federal, LLC ("the Company"), a small subsidiary of CDW-G, to notify you that the Company recently experienced a data security incident impacting the personal information of Maryland residents.

On August 2, 2023, the Company's security protocols detected unusual activity on an internal environment as part of continuous network monitoring. Upon detection, the Company promptly triggered its incident response processes, and an investigation was launched with the assistance of third-party cybersecurity experts. The investigation identified evidence that an unauthorized party had conducted a successful brute force password attack against the Company's virtual private network and, between July 31 and August 2, 2023, had acquired data that was held on a few servers dedicated to internal support of the Company.

A leading data mining vendor was engaged to help analyze the data identified in the investigation as impacted. On December 20, 2023, the Company learned that the impacted data included personal information of Maryland residents. As of the date of this letter, 1,691 Maryland residents have been identified as impacted. The impacted information varied by individual and may have included names, addresses, Social Security numbers or individual taxpayer identification numbers, dates of birth, health insurance information, medical information, and other government-issued identification numbers. Financial account and payment card information were involved for a small subset of individuals.

Upon learning that Company systems were accessed by an unauthorized party, the Company promptly took steps to secure the systems and contain the incident, including by disabling the credentials associated with the unauthorized activity. An investigation was also launched with the support of third-party cybersecurity experts, and law enforcement was notified regarding the incident. To reduce the risk of similar events happening in the future, the Company is working to further enhance its security controls, including by further strengthening security monitoring and enhancing authentication protocols where feasible and appropriate.

The Company plans to provide notice by mail to affected Maryland residents, and a sample copy of such notice is attached. In addition to providing information regarding credit reporting agencies, government resources, security freezes, fraud alerts, and other identity protection tools, the Company is offering credit monitoring and identity protection services for two years through Experian, at no cost to the impacted individuals.

Please feel free to contact me at the contact information below if you have any questions or require additional information.

Sincerely,

/s/ Paul Otto

Paul Otto
paul.otto@hoganlovells.com
(202) 637-5887



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>>,

We are writing on behalf of Sirius Federal, a small subsidiary of CDW-G, to notify you of an incident that impacted your information that was held on a few servers dedicated to internal support of Sirius Federal. We are providing this letter to help you understand what happened and what we are doing in response. We are taking this matter very seriously and sincerely regret any concern that it may cause you.

What Happened? On August 2, 2023, our security protocols detected and contained unusual activity on an internal environment as part of continuous network monitoring. As soon as we detected the unusual activity, we took immediate steps to investigate the event. We subsequently determined that, between July 31 and August 2, 2023, some of the files stored in that internal environment were obtained by an unauthorized actor.

What Information Was Involved? On December 20, 2023, our review determined that the affected files contained information related to a small number of individuals. The impacted information varied by individual and may have included names, addresses, Social Security numbers or individual taxpayer identification numbers, dates of birth, health insurance information, medical information, and other government-issued identification numbers. Financial account information and credit/debit card information were involved for a small subset of individuals.

The information was maintained as part of the normal course of business of Sirius Federal, including various Human Resources and other business operations.

What We Are Doing. Upon learning that Sirius Federal systems were accessed by an unauthorized party, we promptly took steps to secure the systems and contain the incident. An investigation was also launched with the support of third-party cybersecurity experts. To reduce the risk of similar events happening in the future, Sirius Federal has taken steps to further enhance its security controls, including by further strengthening security monitoring and enhancing authentication protocols where feasible and appropriate. Sirius Federal is also offering two years of complimentary credit monitoring and identity protection services through Experian. If you would like to take advantage of the services that we are providing to you free of charge, please follow the instructions in Attachment 1.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and errors. We also encourage you to review the information contained in the Attachments and to activate the complimentary identity monitoring services we are offering.

For More Information. If you have additional questions, please call our dedicated assistance line at <<TFN>>, which is available from 9:00 AM to 6:30 PM Eastern Time Monday through Friday (excluding major U.S. holidays).

Sincerely,

Ben Bourbon
Vice President, Government Sales
Sirius Federal

Attachment 1: Credit Monitoring Services Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6 (activation date)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code s_n>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by <<b2b_text_6 (activation date)>>. Be prepared to provide engagement number <<b2b_text_1 (Engagement Number)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

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. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
<https://www.experian.com/help/>

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
<https://www.transunion.com/credit-help>

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, North Carolina, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. Residents of all other states can find information on how to contact your state attorney general at <https://www.naag.org/find-my-ag/>.

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
www.ftc.gov/idtheft

Oregon Department of Justice

1162 Court Street NE
Salem, OR 97301
1-877-877-9392
<https://justice.oregon.gov>

New York Attorney General's Office

The Capitol
Albany, NY 12224-0341
1-800-771-7755
<https://ag.ny.gov/consumer-frauds-bureau/identity-theft>

North Carolina Department of Justice

114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
<https://ncdoj.gov/protecting-consumers/identity-theft/>

Office of the Attorney General for the District of Columbia

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

Maryland Attorney General's Office

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

Consumer Protection Division**Office of the Attorney General of Iowa**

1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926
www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free security freeze (aka "credit freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348
<http://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

TransUnion Security Freeze PO Box

2000
Chester, PA 19016
<https://www.transunion.com/credit-freeze>
1-888-909-8872

Experian Security Freeze

PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.