Hogan Lovells

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

September 2, 2023

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

By electronic mail

To Whom It May Concern,

I am writing on behalf of Ciena Corporation ("Ciena") to inform you that Ciena experienced a security incident impacting the personal information of four (4) Maryland residents.

The incident resulted from a previously unknown critical security vulnerability in a third-party software application used by Ciena. The application involved is MOVEit Transfer, a file transfer application provided by Progress Software Corporation that Ciena and many other organizations around the world use. This vulnerability allowed an unauthorized party to gain access to confidential, proprietary, and sensitive data of companies that use MOVEit Transfer. The joint CISA/FBI advisory issued on June 7, 2023, associates the widespread exploitation of this MOVEit vulnerability with the CL0P Ransomware Gang, also known as TA505.

On May 30, 2023, Ciena observed unauthorized activity on one of its MOVEit Transfer servers. Ciena promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems. Through the investigation, Ciena learned that the unauthorized party accessed one of its MOVEit Transfer servers on May 29, 2023, and downloaded certain files. A review of the impacted files was conducted to identify any individuals affected by this incident, and that review was completed on July 24, 2023. Through this review, Ciena determined that the files contained personal information of four (4) Maryland residents including name, date of birth, Social Security number, and health benefits and enrollment information.

Ciena takes the security of personal information in its care seriously. Upon learning of the incident, Ciena took several steps to respond quickly, including implementing vendor-recommended actions to patch the vulnerability, initiating an investigation, and notifying law enforcement. In response to this event, Ciena is actively seeking a replacement product to better service its data sharing needs for itself and its customers, and is also reviewing and enhancing its information security policies and procedures as appropriate.

Ciena expects to complete its provision of individual notice on or about September 8, 2023. 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, Ciena is offering credit monitoring and identity protection services for two years through Experian, at no cost to impacted individuals.

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

Sincerely,

/s/

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

7035 Ridge Road
Hanover, Maryland 21076

800 921 1144 phone
410 694 5750 fax
www.ciena.com

[Date]

Notice of Data Incident

[Name],

Ciena takes the protection of its employees' personal information seriously. This notice concerns a data incident that involved some of your information. It explains the circumstances of the incident and how your data was impacted. We are also sharing with you further details about our response and the additional measures you can take to help protect yourself.

What Happened?

On May 31, 2023, Progress Software Corporation, notified users of a critical security vulnerability in its MOVEit Transfer file transfer application, used by Ciena and many other organizations globally. This vulnerability allowed an unauthorized party to gain access to the data of companies that use MOVEit Transfer. Ciena promptly took mitigation steps and launched an investigation with cybersecurity experts into the impact of the MOVEit vulnerability. Through the investigation, we learned that an unauthorized party downloaded certain files on May 28, 2023. We have completed a review of the impacted files and individuals potentially affected by this incident.

What Information Was Involved?

Our investigation determined that the impacted files contained the following categories of information about you:

- Employee information such as Employee ID, salary and compensation information, date of birth, contact information including telephone number and home address, and other related internal and personnel management files.
- Government identification number such as a social security number or foreign equivalent, passport number, or a driver's license number.
- Health and benefits information such as enrollment information, flexible spending account information, care giver leave, health insurance plan, group, and policy numbers, and other related information.
- Financial account information such as financial account numbers and routing numbers.

How Did We Respond?

We are committed to maintaining the privacy and security of personal information in our care and are taking this incident very seriously. Upon learning of the incident, we took several steps to respond immediately, including implementing vendor-recommended mitigation actions, initiating an investigation, engaging expert advisors, and notifying law enforcement and relevant data protection authorities.

To assist in protecting you, we are offering you access to an additional 12 months of complimentary identity monitoring services.

Please reach out to your People Connect team by [date] if:

- If you would like for your complimentary services to be extended for an additional 12 months.
- If you have misplaced your original email and need your code again.

What Can I Do?

We encourage you to remain vigilant with respect to incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed Steps You Can Take to Help Protect Personal Information, which contains information on what you can do to safeguard against possible misuse of your information. You can also activate the identity monitoring services that we are offering.

For More Information

- To sign up for an additional 12 months of complimentary identity monitoring services, please reach out to your People Connect Team by [date].
- For all other questions, please call: [call center number]

We encourage you to avail yourself to the resources we have provided above.

Sincerely,

Sheela Kosaraju
Sr. Vice President and General Counsel, Acting Chief People Officer

Ryan Hammer
Chief Information Security Officer

Steps You Can Take to Help Protect Personal 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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/ credit-report-services	www.experian.com/ fraud/center.html	www.transunion.com/fraud- victim-resource/place-fraud-alert

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. 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, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents 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) / https://www.consumer.ftc.gov/identity-theft-and-online-security

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

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
https://riag.ri.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.