Cynthia J. Larose
617 348 1732
cjlarose@mintz.com

MINTZ

One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

September 20, 2023

VIA E-MAIL TRANSMISSION (IDTHEFT@OAG.STATE.MD.US)

Attorney General Anthony G. Brown
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Reporting of Security Incident Pursuant to Maryland Code. § 14-3505

Dear Attorney General Brown:

We are writing on behalf of Cedar Fair, L.P. (the "Company") to advise you of a third-party security incident at a vendor of the Company that may affect the security of personal information relating to approximately four (4) Maryland residents. Sovos Compliance, LLC ("Sovos") provides unclaimed property reporting services to many companies, including the Company, and is a leading provider of these services. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature of the Security Incident

On or around May 31, 2023, Progress Software Corporation, the provider of MOVEit Transfer software, disclosed a vulnerability in its software that had been exploited by an unauthorized third party. Sovos utilizes MOVEit in the regular course of its business operations to securely transfer files. Sovos informed the Company that it promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems. Through the investigation, Sovos learned that the third party accessed one of its MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. Sovos then conducted a manual review of its records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. On June 20, 2023, the Company received a formal notice of the event from Sovos (attached), wherein Sovos disclosed that it had reviewed the Company's affected files and identified the individuals impacted and types of personally identifiable information exposed.

Sovos' investigation determined that the information involved in this event that could have been subject to unauthorized access by the threat actor includes the impacted person's name, address, Social Security number, and date of birth.

Notice to Maryland Residents

On September 22 2023, Kroll, LLC will begin to provide Sovos' written notice of this event to potentially affected individuals on the Company's behalf. This mailing includes notice to Maryland residents impacted by the event who are former employees of the Company.

Sovos is providing written notice in substantially the same form as the letter attached as Exhibit A.

Other Steps Taken and To Be Taken

Sovos informed the Company that it investigated the incident and undertook an assessment of the security of Sovos' systems, including its MOVEit Transfer servers. Sovos is providing affected individuals access to 24 months of fraud counseling, credit monitoring, and identity restoration services through Kroll, LLC, at no cost to these individuals. Sovos is also establishing a toll-free call center for notified individuals to address any questions related to this event. The incident had no impact on the Company's network or systems.

Please contact the undersigned at cjlarose@mintz.com or 617-348-1732 should you need further information or have any additional questions.

Sincerely,

Cynthia J. Larose

Cynthia J. Larose
Member

Attachments

SOVOS

SOVOS COMPLIANCE, LLC ("SOVOS") MOVEit INCIDENT FACT SUMMARY

On May 31, 2023, Progress Software announced a previously unknown vulnerability in its MOVEit Transfer application. Sovos uses MOVEit for purposes of secure file transfer for a subset of its Unclaimed Property customers.

When Sovos became aware of unauthorized activity on the MOVEit application, it immediately took the affected application offline, and an investigation was commenced into indicators of potential exploitation of this vulnerability, with assistance from third-party forensics experts. Although the data stored in the MOVEit application was encrypted[1], the security vulnerability in the application allowed the threat actor to bypass the encryption and access the data.[2]

Importantly, MOVEit is cloud-based and segmented from Sovos' corporate network and other cloud resources. Sovos does not have evidence that the threat actor moved laterally within the Sovos environment. As such, this issue did not and does not present any risk to Sovos' broader corporate network.

Timeline:

- **May 27, 2023:** Date of first unauthorized access to Sovos' MOVEit Transfer web application, which Sovos uses for purposes of secure file transfer.
- **May 30, 3023:** Date of last unauthorized activity on Sovos' MOVEit transfer web application. On this same day, the threat actor downloaded certain Sovos customer files from the MOVEit application.
    - Sovos' impacted customer data relates to unclaimed property claims that Sovos processes in connection with its Unclaimed Property Premium Services, Enhanced Services, and Consulting Services.
    - This same day, Sovos identified certain of the unauthorized activity on its MOVEit transfer application as suspicious, immediately took the affected application offline, and activated its incident response procedures.
    - Sovos' affected MOVEit application remains offline.
- **May 31, 2023:** Progress Software informed Sovos, along with many other organizations, of a previously unknown vulnerability in Progress Software's MOVEit platform. Outside advisors and cybersecurity experts were retained to assist in the evaluation of potential exploitation of this vulnerability.

---

[1] MOVEit uses 256-bit AES encryption.

[2] Please refer to this NIST article for additional information on the vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

- Publicly available threat intelligence indicates that the threat actor responsible for the mass MOVEit exploitation is CL0P.

- **June 1, 2023**: Sovos began notifying clients that used the affected MOVEit Transfer web application of the MOVEit vulnerability, noting that an investigation into potential exploitation of the vulnerability was underway.

- **June 12, 2023**: Sovos began updating clients that the affected files had been identified and a data analysis process was underway.

- **July 20, 2023**: Affected data became available to customers via the Kroll portal.

[DATE]

[FIRST NAME] [LAST NAME]
[STREET ADDRESS 1]
[STREET ADDRESS 2]
[CITY], [STATE] [ZIP CODE]

RE: NOTICE OF <<DATA BREACH / SECURITY EVENT>>

Dear [FIRST NAME],

We're writing to inform you that some of your personal information was recently involved in a security event. Please read this notice carefully, as it provides up-to-date information on what happened, what we are doing in response, and no-cost support services available to you.

What happened?

On May 31, 2023, Progress Software announced a previously unknown vulnerability in its MOVEit Transfer application (SecureFT), which we utilize to help [SOVOS CUSTOMER NAME] deliver services related to an unclaimed property claim associated with an account or payment belonging to you. When we became aware of this incident, we immediately took the affected application offline and activated our incident response procedures. Outside advisors and cybersecurity experts were retained to assist in the evaluation of the situation, and we notified law enforcement. We recently determined that unauthorized actors exploited the then-unknown MOVEit vulnerability to download a file containing some of your personal information.

What information was involved?

The unauthorized third party downloaded your [CUSTOMIZED LIST OF CATEGORIES OF PERSONAL INFORMATION].

What are we doing?

We are offering two years of complimentary credit monitoring and identity restoration services through Kroll Information Assurance. To take advantage of these credit monitoring and identity restoration services, please follow the instructions in Attachment A. You must enroll within [[●] days after [MAILING DATE]] to receive these services. In addition to these actions, Sovos has deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of our network.

What can you do?

It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. If you identify suspicious activity, you should contact the company that maintains the account on your behalf. Additional information about how to protect your identity is contained in Attachment B.

For more information:

Sovos has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call [1-XXX-XXX-XXXX] Monday through Friday from 9:00am to 6:30pm Eastern Time.

Sincerely,

Sovos Compliance, LLC

Attachment A - Identity Monitoring Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **[Activation Deadline]**.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **[Activation Code]** and Your Verification ID: **[Verification ID]**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari, and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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
http://www.identitytheft.gov/
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:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	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 Avenue N.W., Washington, D.C. 20580.

Additional Information

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

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state 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. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding 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.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus 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 credit 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 violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_ your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

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 more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx and click "Place a credit freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are [NUMBER] Rhode Island residents impacted by this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia 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).