Orrick, Herrington & Sutcliffe LLP
401 Union Street
Suite 3300
Seattle, WA 98101-2668

+1 206 839 4300
orrick.com

Joseph C Santiesteban

E jsantiesteban@orrick.com
D +1 206 839 4352
F +1 206 839 4301

September 22, 2023

BY EMAIL
Office of the Attorney General of Iowa
consumer@ag.iowa.gov

To Whom It May Concern:

I am writing to follow up on our letter dated August 23, 2023, in which we provided notice that Sovos Compliance, LLC ("Sovos") recently determined unauthorized actors exploited the then-unknown MOVEit vulnerability to download files containing personal information. Sovos is making this notification on behalf of the entity listed in Exhibit A.

On May 31, 2023, Progress Software announced a previously unknown vulnerability in its MOVEit Transfer application (SecureFT), which Sovos utilizes as part of its Unclaimed Property Premium Services, Enhanced Services, and Consulting Services. When Sovos became aware of this incident, it immediately took the affected application offline and activated its incident response procedures. Outside advisors and cybersecurity experts were retained to assist in the evaluation of the situation, and Sovos notified law enforcement. The incident was limited to the MOVEit application that Sovos utilizes to deliver a sub-set of its services. MOVEit is cloud-based and segmented from Sovos' corporate network and other cloud resources. Other Sovos systems and services were not affected.

Sovos recently determined that, on May 30, 2023, unauthorized actors exploited the then-unknown MOVEit vulnerability to download files containing personal information. Once we identified the affected files, we began a process to determine what personal information was impacted and to whom it belonged.

Sovos' clients were informed about the incident, and Sovos then worked with its customers to identify individuals with affected personal information and their contact information. Depending on the individual, the types of affected data include one or more of the following: account number, Social Security Number, phone number, driver's license number, and date of birth.

We are writing to inform you that Sovos is notifying an additional 9 Iowa residents whose personal information has been affected. Sovos anticipates notifying these individuals on behalf of the Exhibit A entity beginning on September 22, 2023. Sovos is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft restoration services. Sovos has also established a dedicated call center to answer questions related to this incident. A sample individual notice is attached as Exhibit B.

In addition to these actions, Sovos has deployed additional security measures and tools to strengthen the ongoing security of its network. Sovos is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at +1 (408) 772-0709 or at jsantiesteban@orrick.com.

Respectfully yours,

/s/ Joseph C. Santiesteban
Partner, Orrick Herrington & Sutcliffe LLP

Exhibit A

Iowa

Atlantic Shareholder Services

Exhibit B

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

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

<<b2b_text_1 (Notice of [Data Breach / Security Event])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

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 <<b2b_text_3 (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?

Your personal information that was downloaded by the unauthorized third party included: <<b2b_text_2 (Data Elements)>>.

What are we doing?

We are offering two years of complimentary credit monitoring and identity restoration services through Kroll. 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.

Please see activation instructions in Attachment A. You have until <<b2b_text_6 (activation date)>> to activate your services.

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 (866) 373-7132 Monday through Friday from 9:00am to 6:30pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Sovos Compliance, LLC

Attachment A - Identity Monitoring Services

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

You have been provided with access to the following services 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.

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.

Attachment B – Information for U.S. Residents

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.

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).