EXHIBIT 1

By providing this notice, Sitzberger & Company ("Sitzberger") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 6, 2021, Sitzberger discovered that its network had been impacted by a malware attack that encrypted certain systems. Sitzberger immediately launched an investigation to determine the nature and scope of the event. Sitzberger quickly worked to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption and (3) investigate what happened and whether this resulted in any access to, or theft of, information by the unknown actor. Through the investigation, it was determined that the unknown actor gained access to certain systems between February 24, 2021 and March 6, 2021. The investigation determined that certain files on those systems were viewed and exfiltrated by the unknown actor.

Sitzberger then worked to perform a comprehensive review of all information stored on the impacted systems to determine what personal information was contained in the systems and to whom the information related. Upon completion of our review, Sitzberger then conducted a manual review of their records to determine the identities and contact information for potentially impacted individuals. On or about April 26, 2021, Sitzberger confirmed address information for affected individuals to provide notifications.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maine Residents

On or about July 7, 2021, Sitzberger provided written notice of this incident to all affected individuals, which includes three (3) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Sitzberger moved quickly to investigate and respond to the incident, assess the security of Sitzberger systems, and notify potentially affected individuals. Sitzberger is also working to implement additional safeguards and training to its employees.

Additionally, Sitzberger is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Sitzberger is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

SITZBERGER
CPAs and Business Advisors

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

Sitzberger & Company ("Sitzberger") writes to inform you of an incident that may affect the privacy of some of your personal information. While we have no evidence of actual or attempted misuse of your information, we wanted to provide you with information about the incident, steps we are taking in response, and steps you may take to better protect your information, should you feel it is appropriate to do so. Please know we take this incident very seriously and have been working diligently to investigate and respond.

What Happened? On or about March 6, 2021, Sitzberger discovered that its network had been impacted by a malware attack that encrypted certain systems. Sitzberger immediately launched an investigation to determine the nature and scope of the event. Sitzberger quickly worked to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption and (3) investigate what happened and whether this resulted in any access to, or theft of, information by the unknown actor. Through our investigation, we determined that the unknown actor gained access to certain systems between February 24, 2021 and March 6, 2021. The investigation determined that approximately 6 gigabytes out of a possible 16,800 gigabytes on those systems were viewed and exfiltrated by the unknown actor. Please note that we have no evidence of any actual misuse of any information as a result of this incident.

We then worked to perform a comprehensive review of all information stored on the impacted systems to determine what personal information was contained in the systems and to whom the information related. Upon completion of our review, we then conducted a manual review of our records to determine the identities and contact information for potentially impacted individuals. On or about April 26, 2021, we confirmed address information for affected individuals to provide notifications.

What Information Was Involved? Our investigation determined that this information may include your name and Social Security number. Again, we have no evidence of any actual or attempted misuse of your information; rather, we are letting you know in an abundance of caution and providing information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we continue to assess and update security measures and training to our employees to safeguard the privacy and security of information in our care. We also notified law enforcement and we will be notifying regulatory authorities, as required by law.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 262-860-1724 between 9:00 AM and 5:00 PM CST Monday through Friday. You may also write to Sitzberger at 611 N. Barker Road, Suite 200, Brookfield, WI 53045.

Again, please know we take this incident very seriously and have been working diligently to investigate and respond. We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Frederick J. Sitzberger, CPA, CVA
CEO
Sitzberger & Company

Steps You Can Take to Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. 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. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Sitzberger is located at 611 N. Barker Road, Suite 200, Brookfield, WI 53045.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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 incident. There are [#] Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, 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 Fair Credit Reporting Act, 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 violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act 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 Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.