EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WELBRO Building Corporation ("WELBRO") 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 November 19, 2023, WELBRO became aware of suspicious activity on its network. WELBRO immediately took steps to secure its network and initiated an investigation into the nature and scope of the event with the assistance of third-party cybersecurity specialists. The investigation determined that WELBRO's network was subject to unauthorized access between November 14, 2023, and November 19, 2023, and that certain files were accessed or acquired by an unknown actor while on the network. Once becoming aware that employee information may have potentially been impacted, WELBRO provided preliminary notice and offered credit monitoring to all potentially impacted individuals out of an abundance of caution on December 14, 2024.

WELBRO undertook a thorough and time-consuming review of the data determined to be at risk, to assess the type of information at issue, and to whom that information relates. WELBRO completed this review on February 6, 2024, and confirmed that the files contained sensitive information related to a Maine resident. WELBRO then promptly took steps to locate necessary contact information to notify affected individuals. The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maine Resident

On or about April 29, 2024, WELBRO provided written notice of this incident to one (1) Maine resident. 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, WELBRO moved quickly to investigate and respond to the incident, assess the security of WELBRO systems, and identify potentially affected individuals. Further, WELBRO notified federal law enforcement regarding the event. WELBRO is also working to implement additional safeguards and training to its employees. WELBRO provided access to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WELBRO 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. WELBRO is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

WELBRO is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Return Mail Processing
PO Box 999
Suwanee, GA 30024

4 1 692 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

April 29, 2024

NOTICE OF [EXTRA1]

Dear Sample A. Sample:

The WELBRO Building Corporation ("WELBRO") writes to follow up on our December 14, 2023, letter and to provide additional information regarding an incident that may affect some of your personal information. Safeguarding information is among WELBRO's highest priorities, and this letter provides details of the incident, our response to it, and steps you may take to better protect against the possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On November 19, 2023, WELBRO became aware of suspicious activity on our computer network. We immediately took steps to secure our network and minimize any disruption to our operations. We launched an investigation into the nature and scope of the incident with the assistance of third-party cybersecurity specialists. The investigation determined that an unknown actor gained access to certain parts of our network between November 14, 2023 and November 19, 2023, and that certain files were accessed or acquired by an unknown actor while on the network. Following this determination, we began an in-depth process to identify the information that may have been contained in the impacted environment, identify the individuals whose information may have been impacted, and reviewed our internal records to identify address information for potentially impacted individuals. This process was completed on February 6, 2024. We are notifying you out of an abundance of caution because the investigation determined that certain information relating to you may have been accessed or acquired by an unknown, unauthorized person.

What Information Was Involved? Our investigation determined the following types of personal information may have been accessed without authorization: your name and [Extra2]. WELBRO is not aware of any fraud or identity theft related to this event.

What We Are Doing. Information security is among WELBRO's highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems, including the deployment of an advanced threat protection and monitoring tool. We are reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward. We reported this incident to federal law enforcement. We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory authorities, as required.

As an added precaution, we previously offered you access to three bureau credit monitoring and identity theft protection services for twelve (12) months at no cost to you, through Epiq. You were eligible to enroll in these services until March 31, 2024.

What You Can Do. We encourage you to remain vigilant against 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 information contained in the enclosed "*Steps You Can Take to Help Protect Your Information.*" You can also write to us at 2301 Maitland Center Parkway, Suite 250 Maitland, FL 32751

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 833-918-6271 Monday through Friday from 8am to 8pm Central Time, excluding major U.S. holidays. Be prepared to provide your engagement number B117291. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

WELBRO Building Corporation

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been

a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

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.