EXHIBIT 1

By providing this notice, EGC does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

Nature of the Data Event

On September 20, 2020, EGC discovered certain data on its systems was encrypted due to a malware infection. EGC immediately worked to restore its systems and launched an investigation, with assistance from third party computer forensics specialists, to determine the nature and scope of the incident. The investigation determined that certain EGC information was accessed and acquired by an unknown actor during the incident. Therefore, EGC conducted a comprehensive review of the potentially impacted information to determine the type of information and to whom it related. On October 12, 2020, EGC completed the review and began obtaining contact information to notify potentially impacted individuals about this incident. EGC also worked to engage additional services and resources for these individuals.

The types of personal information potentially impacted vary by individual but include name and the following: Social Security number and driver's license number.

Notice to Maine Residents

On October 14, 2020, EGC began providing written notice of this incident to affected individuals, which includes four (4) 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 learning of this incident, EGC moved quickly to investigate and respond to this incident, assess the security of its systems, restore functionality to its environment, and notify potentially affected individuals. As part of its ongoing commitment to the security of information, EGC notified federal law enforcement and is reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

As an added precaution, EGC is offering impacted Maine residents access to twelve (12) months of free credit monitoring and identity protection services through CyberScout. EGC is also providing impacted Maine residents with guidance on how to better protect against identity theft and fraud. Such guidance includes information on how to place a fraud alert and security freeze on one's credit file, contact details for the national consumer reporting agencies, information on how to obtain a free credit report, reminders to remain vigilant for incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and recommendations regarding how to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

Date

[First Name] [Last Name]
[Address1]
[City, State Zip]

Re: Notice of Data breach

Dear [First Name] [Last Name]:

EWIE Group of Companies ("EGC") writes to notify you of an incident that may affect the privacy of some of your personal information. While, to date, we have no evidence of actual or attempted misuse of personal information potentially affected by this incident, this letter provides details of the incident, our response, and steps you may take to protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On September 20, 2020, EGC discovered certain data on its systems was encrypted due to a malware infection. We immediately worked to restore our systems and launched an investigation, with assistance from third-party computer forensics specialists, to determine the nature and scope of the incident. Our investigation determined that certain EGC information was accessed and acquired by an unknown actor during the incident. Therefore, we conducted a comprehensive review of the potentially impacted information to determine the type of information and to whom it related. On October 12, 2020, we completed the review and began obtaining contact information to notify potentially impacted individuals about this incident. We also worked to engage additional services and resources for these individuals.

What Information was Involved? The investigation determined that the type of information potentially impacted by this incident includes your name and the following data elements: [TYPE OF INFORMATION IDENTIFIED].

What We Are Doing. The security of personal information within our care is among our highest priorities. Upon discovering this incident, we diligently worked to securely restore our systems, investigate, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we also notified law enforcement and are reviewing and enhancing existing policies and procedures. We are also notifying potentially affected individuals, including you, so you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

What You Can Do. In response to the incident, we are offering you services provided by CyberScout. EGC is providing you with access to the following services:

CyberScout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the CyberScout help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

Please review of the enclosed *Steps You Can Take to Protect Your Information* for additional information and enrollment instructions.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions or concern regarding this incident, please call our dedicated assistance line at XXX-XXX-XXXX, [hours of operation].

We sincerely regret any inconvenience this incident may cause you. EGC remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

[SIGNATURE]
Virginia Angerer
Human Resources Manager
EWIE Group of Companies

Steps You Can Take to Protect Your Information

Enroll in Identity Monitoring

To enroll in Credit Monitoring* services at no charge, please log on to **https://www.myidmanager.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE.>** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

For guidance with the CyberScout services, or to obtain additional information about these services during or after enrollment, please call the CyberScout help line 1-800-405-6108 and supply the fraud specialist with your unique code. Representatives are available to assist you from 8:00 am to 5:00 pm Eastern time, Monday through Friday.

Monitor Your Accounts

In addition to enrolling in the above offered services, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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

* * Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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