EXHIBIT 1

We previously notified this Office of this event on June 7, 2023 This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CGM, Inc. ("CGM") 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 December 28, 2022, CGM observed unusual activity related to certain systems within its information technology network. Upon learning of the incident, we quickly began investigating to better understand the nature and scope of this activity. The investigation determined that an unauthorized actor may have accessed a limited amount of information stored on CGM's systems between December 15, 2022, and December 28, 2022. CGM then conducted a thorough and time-consuming review of the potentially affected data to determine whether any sensitive information was accessed and to whom the data relates, and this review concluded on March 23, 2023. After notifying data owners of this event by April 2023, CGM obtained approval from certain data owners to provide notification of this event to affected individuals on the data owners' behalf, and the first wave notification was completed by June 7, 2023. However, for certain data owners, in order to ensure that the appropriate individuals were accurately identified from the affected data, CGM engaged a third-party data analytics specialist to conduct a comprehensive review of the affected data relating to the data owners and used internal CGM data to identify mailing addresses for affected individuals. This review process concluded on December 18, 2023. By December 21, 2023, CGM received approval from data owners to provide notice to affected individuals and regulatory authorities on the data owners' behalf.

The information that could have been subject to unauthorized access includes name and state identification card number.

Notice to Maine Resident

CGM previously provided written notice of this incident to one (1) resident on June 7, 2023, and on February 14, 2024, CGM subsequently provided written notification to an additional 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, CGM moved quickly to investigate and respond to the event, assess the security of CGM systems, and identify potentially affected individuals. As part of CGM's initial response, CGM notified federal law enforcement regarding the event. CGM is providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CGM 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. CGM 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.

CGM 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

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Notice of Data <<Breach/Incident>>

Dear <<Name 1>> :

CGM Inc. ("CGM") writes to notify you of an event that may affect the privacy of some of your personal information. CGM provides solutions to wireless and broadband companies that participate in the federal Affordable Connectivity Program and Lifeline Program. CGM stores certain information related to you through your services with <<Data Owner>>. **Although we have no evidence of misuse of your personal information**, we write to provide you with information about the event, our response, and steps you can take to help protect against the possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On December 28, 2022, we observed unusual activity related to certain systems within our network. We quickly began investigating to better understand the nature and scope of this activity. Working with third-party specialists, we determined that an unknown actor accessed our network <<between December 15, 2022, and December 28, 2022>>. We promptly took steps to contain the threat and ensure the security of our systems. We simultaneously launched a full investigation designed to understand the nature and scope of what occurred and what information was stored on impacted systems at the time of the event. An intensive and time-consuming review of the contents of the affected data was subsequently performed by an external subject matter specialist to determine whether the data contained any sensitive information and to identify affected individuals. We also undertook an additional internal review to locate missing mailing address information for potentially affected individuals. This comprehensive review process recently concluded, and it was determined that certain information related to you was found within the affected systems.

What Information Was Involved? Our investigation determined that the information related to you that was subject to unauthorized access includes your name, <<data elements>>. Although we have no evidence that any of your information was used for identity theft or fraud, we are notifying you in an abundance of caution and providing information and resources to assist you in helping protect your personal information, should you feel it appropriate to do so.

What We Are Doing. We take this event and the obligation to safeguard the information in our care very seriously. After learning of the suspicious activity, we promptly took steps to confirm our system security and engaged third-party specialists to assist in conducting a comprehensive investigation of the event to confirm its nature, scope, and impact. CGM also promptly notified federal law enforcement of the event. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing existing policies and procedures relating to data protection and security. We instituted additional security measures to minimize the likelihood of similar events in the future. We are also notifying relevant regulatory authorities, as required.

Although there is no evidence of any actual or attempted misuse of your information, as an added precaution, we are offering you access to credit monitoring and identity theft protection services for <<CM Length>> months through Equifax at no cost to you. If you wish to activate these complimentary services, you may follow the instructions included in the attached

Steps You Can Take to Help Protect Personal Information. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and by monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Any suspicious activity should be reported to the appropriate financial institution, insurance company, or health care provider. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring and how to enroll.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call us at 844-566-1548, Monday through Friday 9am to 9pm Eastern Time. You may also write to Credit Protection Inquiry at CGM, LLC, 104 Sloan Street, Roswell, GA 30075.

We sincerely regret any inconvenience or concern this event may cause.

Sincerely,

CGM, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring

<<Name 1>>
Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of ***<ACTIVATION CODE>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 one-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 credit 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, 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 a 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
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

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 Street, 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 https://www.marylandattorneygeneral.gov/.

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.

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, individuals have the right to obtain any police report filed in regard to this event. There are approximately two Rhode Island residents that may be impacted by this event.