Exhibit A1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CHRISTINA CAIN, DARRON DANNA, STEPHANIE YOUNGBLOOD, JOSHUA WOLF, KIM WHITE, BRANDON GUERRA, and CHARLES WILLIAMS, on behalf of themselves, and all others similarly situated, ***Plaintiffs*** **v.** **CGM, L.L.C. d/b/a CGM, INC.** ***Defendant***	**Case No.: 1:23-cv-02604-SEG**

PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Christina Cain, Darron Danna, Stephanie Youngblood, Joshua Wolf, Kim White, Brandon Guerra, and Charles Williams, (hereinafter, "Plaintiffs"), on behalf of themselves, and all others similarly situated, for his causes of action against Defendant, CGM, L.L.C. d/b/a CGM, INC. ("Defendant" or "CGM"), allege upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of Defendant's unauthorized disclosure of the

confidential personal information, Personally Identifying Information[1] ("PII" or "Private Information") of Plaintiffs and the proposed Class Members, approximately 279,063 persons, from December 15, 2022 to December 28, 2022 in a cyberattack on CGM's systems, including their names, driver's license or state identification numbers, and Social Security numbers (the "Data Breach").[2]

2. CGM, headquartered in Roswell, Georgia, provides services to wireless and broadband telecommunications companies to assist them in participating in the Affordable Connectivity Program (ACP) and Lifeline Program, federal benefit program(s) assisting individuals with obtaining broadband internet and related services.[3]

3. In connection with performing these services, CGM collects massive amounts of PII regarding its customers and their clients, including Plaintiffs and the Class Members.

---

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] *See*: CGM Notice of Data Event to Maine Attorney General, including sample notice to consumers (Ex. A) ("Data Breach Notice") available at https://apps.web.maine.gov/online/aeviewer/ME/40/fdc0a65c-9a4c-401a-b278-5a83284956c7.shtml (last acc. Sept. 26, 2023) **attached as Exhibit 1.**

[3] *See* CGM website, available at https://www.cgmllc.net/; https://www.fcc.gov/acp (last acc. Sept. 26, 2023).

4. On information and belief, CGM failed to undertake adequate measures to safeguard the PII of Plaintiffs and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

5. Although CGM discovered the Data Breach on or about December 28, 2022, Defendant failed to notify and warn Data Breach victims of the unauthorized disclosure of their PII until June 7, 2023[4].

6. As a direct and proximate result of Defendant's failures to protect Plaintiffs' and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class have suffered widespread injury and damages necessitating Plaintiffs seeking relief on a class wide basis.

PARTIES

7. Plaintiff Christina Cain is a resident and citizen of Arkansas. Plaintiff Cain received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

8. Plaintiff Darron Danna is a resident and citizen of the State of

[4] *See* Maine Attorney General, CGM Data Breach Notification to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/fdc0a65c-9a4c-401a-b278-5a83284956c7.shtml (last acc. Sept. 26, 2023).

Louisiana. Plaintiff Danna received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

9. Plaintiff Stephanie Youngblood is a resident and citizen of the State of California. Plaintiff Youngblood received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

10. Plaintiff Joshua Wolf is a resident and citizen of the State of California. Plaintiff Wolf received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

11. Plaintiff Kim White is a resident and citizen of the State of Ohio. Plaintiff White received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

12. Plaintiff Brandon Guerra is a resident and citizen of the State of California. Plaintiff Guerra received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

13. Plaintiff Charles Williams is a resident and citizen of the State of Ohio.

Plaintiff Williams received a letter dated June 7, 2023, from Defendant CGM notifying Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

14. Defendant CGM is a for profit limited liability company organized and existing under the laws of the State of Georgia headquartered in Roswell, Georgia in Fulton County. CGM's principal place of business is located at 104 Sloan Street, Roswell, Georgia 30075 in Fulton County. CGM, LLC's Registered Agent for service of process is Kevin Murphy, 104 Sloan Street, Roswell, Georgia 30075.

JURISDICTION AND VENUE

15. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this state; it maintains its principal places of business and headquarters in Georgia; and committed tortious acts in Georgia.

16. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendant.

17. The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law under 28 U.S.C. § 1367.

18. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant CGM

19. Founded in 1997, CGM is a company which "help[s] wireless and broadband companies participate in the federal Affordable Connectivity Program (ACP) and Lifeline Program," including "…deliver[ing] tools to confirm subscriber eligibility, enroll low-income households, track agent and distribution activity, calculate and file federal and state reimbursements, and provide audit support to our Service Provider clients."[5]

20. The ACP is a Federal Communications Commission ("FCC") benefit program for low income and eligible persons which "helps ensure that households can afford the broadband they need for work, school, healthcare and more," providing eligible participants with discounts towards internet services, and computers.[6]

21. The Lifeline Program, instituted in 1985, and as revised in 2016, is an FCC program assisting low income consumers in affording access to telephone and

[5] https://www.cgmllc.net/ (last acc. Sept. 26, 2023).
[6] Federal Communications Commission website, "Affordable Connectivity Program," available at https://www.fcc.gov/acp (last acc. Sept. 26, 2023).

internet services.[7] As described by the FCC, "Lifeline provides subscribers a discount on qualifying monthly telephone service, broadband Internet service, or bundled voice-broadband packages purchased from participating wireline or wireless providers [… to] ensure that low-income consumers can afford 21st century broadband and the access it provides to jobs, healthcare, and educational resources."[8]

22. CGM assists telecommunications communicating in participating in the ACP and Lifeline programs, providing services including: program compliance through a "Subscriber Enrollment Platform" which "connects to a number of third-party and private billing systems, has successfully navigated over a thousand FCC and state audits, and maintains on-going compliance with ever-changing federal and state regulations and rule interpretations[;]" monthly reimbursement filings; "audit support services," including "pulling together data necessary to respond to the myriad of audits Service Providers receive each year," and training on program compliance; as well as providing a "CGM Distribution Management Database (DMD)."[9]

23. To provide these ACP and Lifeline enrollment and reimbursement filing

[7] https://www.fcc.gov/general/lifeline-program-low-income-consumers (last acc. Sept. 26, 2023).
[8] FCC website, "Lifeline Support for Affordable Communications," avail. at https://www.fcc.gov/lifeline-consumers (last acc. Sept. 26, 2023).
[9] https://www.cgmllc.net/ (last acc. Sept. 26, 2023).

services, CGM requires that its customers, including program applicants and participants, provide their and their customers' PII to Defendant, including their names, driver's license or state identification numbers, and Social Security numbers, either directly or through its telecommunications clients.

24. In exchange for this information, CGM promises to safeguard its client's customers' PII, and to only use this confidential information for authorized purposes.

25. Defendant acknowledges the importance of properly safeguarding the private data and PII of individuals, stating in the Data Breach Notice (Ex. A, sample notice), that "[w]e take this event and the obligation to safeguard the information in our care very seriously."[10]

26. Plaintiffs and the proposed Class Members are current and former customers of CGM's telecommunications clients, and of CGM itself, and would not have allowed their PII to be entrusted to Defendant had they known CGM would not adequately safeguard that information.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiffs, and the members of the Proposed Class, and knew or should have known that they were responsible for protecting their PII from unauthorized

[10] *See* sample notice, **Exhibit 1.**

disclosure.

28. At all times Plaintiffs and the members of the Proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiffs and the proposed Class Members, relied on Defendant to keep their PII confidential and securely maintained.

B. CGM Fails to Adequately Safeguard PII—the Data Breach

29. Plaintiffs and the proposed Class Members are current and former customers of CGM and of its telecommunication clients, whose personal information, PII, was entrusted to CGM, directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

30. CGM collected and maintained this PII in its computer information technology systems and networks.

31. On information and belief, from December 15, 2022, and December 28, 2022, CGM's systems network was unauthorizedly accessed by an unknown cybercriminal during an external system breach hacking attack, resulting in the compromise and disclosure and the PII of its telecommunications clients' customers, including Plaintiffs and the proposed Class Members, that was stored therein, including their names, driver's license or state ID numbers, and Social Security numbers—the Data Breach.[11]

[11] *See* Notice of Data Event to Maine Attorney General, **Exhibit 1.**

32. According to Defendant, "[o]n December 28, 2022, CGM observed unusual activity related to certain systems within its information technology network," after which it conducted an investigation showing 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," "assess[ed] the security of [their] systems."[12]

33. Thereafter, on information and belief, CGM, through a third-party "external data analytics specialist," further investigated and reviewed the potentially affected data to determine "whether any sensitive information was accessed and to whom the data relates to," which was completed by March 23, 2023.[13]

34. Following the three (3)-month investigation, Defendant identified those individuals whose PII was impacted in the Data Breach and their "respective data owners," Defendant's telecommunications clients, and began notifying these data owners/clients of the Data Breach beginning on April 15, 2023.[14]

35. As of "May 18, 2023, CGM [had] received approval from data owners to provide notice to affected individuals and regulatory authorities on their

[12] *See Id.*
[13] *See Id.*
[14] *See Id.*

behalf."[15]

36. Despite over five (5) months having passed since CGM initially identified the Data Breach, only beginning on or about June 7, 2023, did CGM began sending written notices to affected persons notifying them of the Data Breach[16] (hereinafter, "Data Breach Notice") [17].

37. Defendant's Data Breach Notice, sent on or about June 7, 2023 to affected consumers, generally described the occurrence of the Data Breach, but failed to explain *when* the cyberattack occurred (December 15th to 28th, 2022), the nature of the cyberattack, or how the cyberattack was perpetrated (i.e., an external system breach (hacking) attack), obfuscating the nature of the Data Breach.[18]

38. Further, the Data Breach Notice stated that after discovering the Data Breach, CGM "review[ed] and enhance[ed] existing policies and procedures relating to data protection and security [and] instituted additional security measures to minimize the likelihood of similar events in the future." [19]

39. CGM's Data Breach Notice admitted that affected consumers' PII, including their names, driver's license or state ID numbers, and Social Security

---

[15] *See Id.*
[16] *See Id.*
[17] *See*: Notice of Data Event to Maine Attorney General, **Exhibit 1**; sample notice to Vermont Attorney General, attached as **Exhibit 2.**
[18] *See Id.*
[19] *See Id.*

numbers were subject to unauthorized access in the Data Breach.[20]

40. The Data Breach Notice was careful to qualify, in bold and underlined type, that "…**we have no evidence of misuse of your personal information**," downplaying the severity and consequences of the Data Breach, but encouraged affected victims to "remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring [their] free credit reports for suspicious activity and to detect errors," to report such fraud to law enforcement, and informed them of their abilities to place a fraud alert on their credit files and a credit freeze on their credit reports.[21]

41. CGM offered victims of the Data Breach credit monitoring and identity theft protection services through TransUnion for either twelve (12) or twenty-four (24) months.[22]

42. Only on or about June 7, 2023 did Defendant provide notification of the Data Breach to regulatory authorities, including the Maine Attorney General and Vermont Attorney General, reporting to the Maine Attorney General that the Data Breach occurred on December 15, 2022; that it involved an "external system breach (hacking)" attack; inconsistently, that it was discovered on May 18, 2023; that 279,063 persons were affected; and that the information acquired included full

[20] *See Id.*
[21] *Id.*
[22] *See Id.*

names in combination with "Driver's License Number or Non-Driver Identification Card Number."[23]

43. Defendant did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the cyberattack on CGM's systems and accessing the voluminous PII of Plaintiffs and the proposed Class Members in the Data Breach.

44. Further, CGM failed to adequately train its employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over individuals' PII in the Data Breach.

45. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning CGM had no effective means to detect and prevent attempted data breaches.

46. As a result of CGM's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Accordingly, CGM's identity theft protection through TransUnion is wholly insufficient to compensate Plaintiffs and the Class Members for their damages caused by the Data Breach.

---

[23] *See* CGM Data Breach Notification to Maine Attorney General, avail. at https://apps.web.maine.gov/online/aeviewer/ME/40/fdc0a65c-9a4c-401a-b278-5a83284956c7.shtml (last acc. Sept. 26, 2023).

47. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiffs and the proposed Class Members have suffered injury and damages, as set forth herein.

C. Plaintiffs' Experiences

i. Plaintiff Cain

48. Plaintiff Cain's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

49. Plaintiff Cain received CGM's Data Breach Notice dated June 7, 2023, informing her that her name and driver's license number and/or state ID number had been compromised in the Data Breach.

50. To her knowledge, Plaintiff Cain has never been the victim of a prior data breach.

51. As a direct result of the Data Breach, Plaintiff Cain has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her PII that can be directly traced to Defendant.

52. On information and belief, Plaintiff Cain's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

53. Plaintiff Cain has received an increase in spam calls and emails since

the Data Breach.

54. Plaintiff Cain has spent time mitigating the effects of the Data Breach by researching the Data Breach and speaking with her bank to inquire about fraudulent charges to her account.

55. In addition, Plaintiff Cain must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring her credit reports, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

56. Plaintiff Cain was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

57. As a result of CGM's Data Breach, Plaintiff Cain faces a lifetime risk of additional identity theft.

ii. Plaintiff Danna

58. Plaintiff Danna's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

59. Plaintiff Danna received CGM's Data Breach Notice dated June 7, 2023, informing him that his name and Social Security Number had been compromised in the Data Breach.

60. To his knowledge, Plaintiff Danna has never been the victim of a prior data breach.

61. As a direct result of the Data Breach, Plaintiff Danna has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

62. On information and belief, Plaintiff Danna's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

63. Plaintiff Danna has spent time mitigating the effects of the Data Breach by researching the Data Breach and monitoring accounts regularly to protect against the Breach.

64. In addition, Plaintiff Danna must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury

and harm to a Data Breach victim that is contemplated and addressed by law.

65. Plaintiff Danna was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

66. As a result of CGM's Data Breach, Plaintiff Danna faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

iii. Plaintiff Youngblood

67. Plaintiff Youngblood's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

68. Plaintiff Youngblood received CGM's Data Breach Notice dated June 7, 2023, informing her that her name and Social Security Number had been compromised in the Data Breach.

69. To her knowledge, Plaintiff Youngblood has never been the victim of a prior data breach.

70. As a direct result of the Data Breach, Plaintiff Youngblood has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her PII that can be directly traced to Defendant.

71. On information and belief, Plaintiff Youngblood's PII unauthorizedly

disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

72. Plaintiff Youngblood has received an increase in spam calls and emails since learning about the Data Breach.

73. Plaintiff Youngblood has spent time mitigating the effects of the Data Breach by researching the Data Breach and attempting to set up credit monitoring to protect against the Breach.

74. In addition, Plaintiff Youngblood must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring her credit reports, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

75. Plaintiff Youngblood was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

76. As a result of CGM's Data Breach, Plaintiff Youngblood faces a lifetime risk of additional identity theft, as it includes sensitive information that

cannot be changed, like her Social Security number.

iv. Plaintiff Wolf

77. Plaintiff Wolf's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

78. Plaintiff Wolf received CGM's Data Breach Notice dated June 7, 2023, informing him that his name and Social Security Number had been compromised in the Data Breach.

79. To his knowledge, Plaintiff Wolf has never been the victim of a prior data breach.

80. As a direct result of the Data Breach, Plaintiff Wolf has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

81. On information and belief, Plaintiff Wolf's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

82. Plaintiff Wolf has received an increase in spam calls and emails.

83. Plaintiff Wolf has spent time and effort researching and mitigating the effects of the Data Breach.

84. In addition, Plaintiff Wolf must now spend time and effort attempting

to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

85. Plaintiff Wolf was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

86. As a result of CGM's Data Breach, Plaintiff Wolf faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

v. ***Plaintiff White***

87. Plaintiff White's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

88. Plaintiff White received CGM's Data Breach Notice dated June 7, 2023, informing her that her name and Social Security Number had been compromised in the Data Breach.

89. To her knowledge, Plaintiff White has never been the victim of a prior

data breach.

90. As a direct result of the Data Breach, Plaintiff White has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her PII that can be directly traced to Defendant.

91. On information and belief, Plaintiff White's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

92. Plaintiff White has received an increase in spam calls and emails.

93. Plaintiff White has spent time and effort researching and mitigating the effects of the Data Breach.

94. In addition, Plaintiff White must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring her credit reports, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

95. Plaintiff White was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

96. As a result of CGM's Data Breach, Plaintiff White faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her Social Security number.

vi. Plaintiff Guerra

97. Plaintiff Guerra's sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

98. Plaintiff Guerra received CGM's Data Breach Notice dated June 7, 2023, informing him that his name and Social Security Number had been compromised in the Data Breach.

99. To his knowledge, Plaintiff Guerra has never been the victim of a prior data breach.

100. As a direct result of the Data Breach, Plaintiff Guerra has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

101. On information and belief, Plaintiff Guerra's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

102. Plaintiff Guerra has received an increase in spam calls and emails since the Data Breach.

103. Plaintiff Guerra has spent time and effort researching and mitigating the effects of the Data Breach.

104. In addition, Plaintiff Guerra must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

105. Plaintiff Guerra was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

106. As a result of CGM's Data Breach, Plaintiff Guerra faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

vii. Plaintiff Williams

107. Plaintiff Williams' sensitive PII was entrusted and disclosed to CGM directly or indirectly, in connection with Defendant's ACP and Lifeline program services.

108. Plaintiff Williams received CGM's Data Breach Notice dated June 7,

2023, informing him that his name and Social Security Number had been compromised in the Data Breach.

109. To his knowledge, Plaintiff Williams has never been the victim of a prior data breach.

110. As a direct result of the Data Breach, Plaintiff Williams has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

111. On information and belief, Plaintiff Williams' PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

112. Plaintiff Williams has received an increase in spam calls and emails since the Data Breach.

113. In addition, Plaintiff Williams must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

114. Plaintiff Williams was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

115. As a result of CGM's Data Breach, Plaintiff Williams faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

D. This Data Breach was Foreseeable by CGM.

116. Plaintiffs' and the proposed Class Members' PII was provided to CGM with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

117. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiffs and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

118. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

119. Cyber-attacks against companies such as Defendant are targeted and frequent. Indeed, according to UpGuard, "[c]ybercriminals know that tech companies often have weaker data protection and overall cybersecurity measures than highly-regulated industries, like healthcare and finance. Instead of targeting these organizations directly for their valuable data, they focus their efforts on the poor data security often found in the first link of the supply chain – tech vendors that store and manage significant amounts of data from these industries."[24]

120. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[25]

121. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including CGM.

[24] UpGuard, Catherine Chipeta, "5 Ways Tech Companies Can Prevent Data Breaches," updated Mar. 2, 2023 available at https://www.upguard.com/blog/how-tech-companies-can-prevent-data-breaches (last acc. Jun. 15, 2023).
[25] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Sept. 26,, 2023Sept. 26, 2023).

According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[26]

122. Based on data from the Maine Attorney General, as of August 2022, "…at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[27]

123. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

124. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

125. Given the nature of the Data Breach, it was foreseeable that the

[26] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Sept. 26,, 2023).
[27] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. CGM Failed to Comply with FTC Guidelines

126. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

127. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted

from the system; and have a response plan ready in the event of a breach.[28]

128. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

129. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

130. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

[28] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Sept. 26, 2023).
[29] *See id*.

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

131. CGM failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

132. Defendant was at all times fully aware of its obligations to protect the PII of Plaintiffs and the Class Members. CGM was also aware of the significant repercussions that would result from its failure to do so.

F. CGM Fails to Comply with Industry Standards

133. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

134. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability

Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[30]

135. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their

[30] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Sept. 26, 2023).

personal risk in addition to their crucial role in the workplace.[31]

136. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[32]

---

[31] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Sept. 26, 2023).

[32] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Sept. 26, 2023).

137. Upon information and belief, CGM failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiffs' and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages

138. Plaintiffs and members of the proposed Class have suffered injury and damages from the exfiltration and misuse of their PII that can be directly traced to CGM, that has occurred, is ongoing, and/or imminently will occur.

139. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access and acquire the Plaintiffs' and the proposed Class Members' PII, which is now available to be imminently used for fraudulent purposes or has been sold for such purposes, causing widespread injury and damages.

140. The ramifications of CGM's failure to keep Plaintiffs' and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal

and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

141. Because CGM failed to prevent the Data Breach, Plaintiffs and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

e. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, which remains in the possession of CGM and is subject to further breaches so long as CGM fails to undertake the appropriate measures to protect the PII in its possession.

142. Furthermore, the Data Breach has placed Plaintiffs and the proposed Class Members at an increased risk of fraud and identity theft.

143. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents

having their identities stolen.[33]

144. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[34]

145. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud—just as occurred here—phone or utilities fraud, and bank/finance fraud.

146. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

---

[33] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Sept. 26, 2023).

[34] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. Sept. 26, 2023).

147. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

148. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated. [35]

149. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud

[35] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Sept. 26, 2023).

computing, PII is valuable property.[36]

150. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

151. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

152. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

153. Where the most PII belonging to Plaintiffs and Class Members was accessible from CGM's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial accounts for many years

[36] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

to come.

154. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[37]

155. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[38] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

156. Moreover, it is not an easy task to change or cancel a stolen Social

[37] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)
[38] *See id.*

Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[39]

157. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[40] ...Accordingly, the Data Breach has caused Plaintiffs and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the unauthorized disclosure, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

158. Another example of criminals using PII for profit is the development of

---

[39] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[40] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 27, 2023).

"Fullz" packages.[41]

159. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as Fullz packages.

160. The development of Fullz packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam

[41] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

161. CGM knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

114. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiffs bring this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

116. Plaintiffs propose the following Class definition ("Nationwide Class"), subject to amendment based on information obtained through discovery:

> **All persons whose PII was compromised as a result of the Data Breach experienced by CGM beginning on or about December 15, 2022, including all persons who received Defendant's Data Breach Notice.**

117. In addition, or in the alternative, Plaintiffs propose the following State Class ("State Classes") definitions, subject to amendment as appropriate (together

with the Nationwide Class, the "Class"):

Arkansas Class:

All Arkansas residents whose PII was compromised as a result of the Data Breach experienced by CGM beginning on or about December 15, 2022, including all persons who received Defendant's Data Breach Notice.

California Class:

All California residents whose PII was compromised as a result of the Data Breach experienced by CGM beginning on or about December 15, 2022, including all persons who received Defendant's Data Breach Notice.

Louisiana Class:

All Louisiana residents whose PII was compromised as a result of the Data Breach experienced by CGM beginning on or about December 15, 2022, including all persons who received Defendant's Data Breach Notice.

Ohio Class:

All Ohio residents whose PII was compromised as a result of the Data Breach experienced by CGM beginning on or about December 15, 2022, including all persons who received Defendant's Data Breach Notice.

118. Excluded from the Class are Defendant's members, officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

119. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

120. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

121. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

122. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the PII of approximately 279,063 individuals was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

123. **Commonality, Fed. R. Civ. Proc. 23(a)(2), and Predominance, Fed. R. Civ. Proc. 23(b)(3):** There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Class Members because CGM has acted on grounds generally

applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

e. Whether computer hackers obtained Plaintiffs' and Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant failed to adequately respond to the Data Breach, including failing to timely notify the Plaintiffs and the Class Members;

h. Whether Defendant's failures amounted to negligence;

i. Whether Defendant breached its contractual promises;

j. Whether Defendant was unjustly enriched;

k. Whether Defendant intruded into the private affairs of Plaintiffs and the Class Members;

l. Whether Plaintiffs and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant's acts violated the law, including the state consumer and privacy protection laws alleged herein; and

n. Whether Plaintiffs and the Class Members are entitled to damages including compensatory and punitive damages, and/or injunctive relief.

124. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach, and all arise from the same set of facts regarding CGM's failures:

a. to protect Plaintiffs' and Class Members' PII;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiffs and Class Members in a complete and timely manner information concerning the security breach and the theft of their Private Information.

125. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

126. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court

will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only

CGM's client's customers, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

127. **Injunctive and Declaratory Relief, Fed. R. Civ. Proc. 23(b)(2):** In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

128. Finally, all members of the proposed Class are readily ascertainable. CGM has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

130. Defendant collected the PII of Plaintiffs and the proposed Class

Members and stored this information in its computer information technology systems.

131. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiffs and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

132. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their data in Defendant's possession.

133. By collecting and storing this data in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

134. Defendant owed a common law duty of care to Plaintiffs and the Class Members to provide adequate data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiffs' and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiffs' and Class Members' PII;

f. Failing to timely notify Plaintiffs and Class Members about the

Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

137. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

138. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in one or more types of injuries to them.

139. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

140. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

141. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

142. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

143. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

144. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

145. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se.*

146. Plaintiff and Class Member are within the class of persons that the FTC Act was intended to protect.

147. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

148. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

149. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated and "impacted" individuals whose Private Information was accessed during the Data Breach, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) anxiety, annoyance

and nuisance, (i) nominal damages, and (j) the future costs of identity theft monitoring.

150. Moreover, Plaintiffs' and Class Members' Private Information remains at risk, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

151. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity theft monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

152. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

153. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for Defendant to provide services in connection with participating in the federal telecommunications and internet benefit programs, and that Defendant would deal with them fairly and in good faith, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII entrusted

to Defendant.

154. Specifically, Plaintiffs and the Class Members entered into valid and enforceable implied contracts with Defendant when they first applied to receive or received Defendant's services.

155. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendant included Defendant's promise to protect nonpublic PII given to Defendant, or that Defendant created on its own, from unauthorized disclosures. Plaintiffs and Class Members allowed their PII to be provided in reliance of that promise.

156. Defendant solicited and invited Plaintiffs and Class Members to provide their PII, directly or indirectly, as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

157. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

158. Plaintiffs and Class Members reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

159. Under the implied contracts, Defendant promised and was obligated to:

(a) provide services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII: (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiffs and Class Members agreed to pay money for these services and to turn over their PII.

160. Both the provision of these services, and the protection of Plaintiffs' and Class Members' PII, were material aspects of these implied contracts.

161. Plaintiffs and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected; nor would they have entrusted their PII to Defendant, directly or indirectly, in the absence of its implied promise to monitor its computer systems and networks to ensure that PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

162. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their PII to Defendant and/or paid for services, whether directly or indirectly, for, amongst other things, (a) the provision of such services and (b) the protection of their PII.

163. Plaintiffs and the Class Members performed their obligations under the contracts when they paid for services and/or provided their valuable Private Information to Defendant, directly or indirectly.

164. Defendant materially breached its contractual obligations to protect the nonpublic PII of Plaintiffs and Class Members which Defendant required and gathered.

165. Under Georgia law, good faith is an element of every contract. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

166. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Examples of bad faith are evasion of the spirit of the bargain and abuse of a power to specify terms.

167. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiffs and the Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

168. The Data Breach was a reasonably foreseeable consequence of

Defendant's conduct, by acts of omission or commission, in breach of these contracts.

169. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in the contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

170. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services from Defendant or entrusted their valuable Private Information to it.

171. As a direct and proximate result of the Data Breach, Plaintiffs and the Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they had struck with Defendant by paying for Defendant's services and/or entrusting their valuable Private Information to Defendant.

172. Plaintiffs and the Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

173. Plaintiffs and the Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF CONTRACT—THIRD PARTY BENEFICIARY
(On Behalf of Plaintiffs and the Class)

174. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

175. Plaintiffs bring this claim in the alternate to their claim for Breach of Implied Contract (Count II).

176. Defendant entered into valid and enforceable contracts with their telecommunications and internet service provider clients, including but not limited to, Assurance Wireless and Q Link Wireless, under which Defendant would provide services in connection with federal telecommunications and internet benefit programs, including ACP verification and enrollment, which contemplated the security and protection of the Private Information belonging to Plaintiffs and Class Members which was to be entrusted to it.

177. These contracts were entered into in exchange for payment, and included obligations for Defendant to implement data security adequate to

safeguard and protect the privacy of Plaintiffs' and Class Members' PII entrusted to Defendant.

178. Defendant solicited and invited its clients to pay monies in exchange for services, which expressly included terms requiring its clients to turn over Plaintiffs' and Class Members' PII in exchange for promises from Defendant that it would protect and safeguard such Private Information. These terms make up an integral part of Defendant's regular business practices, and CGM's partners accepted the offers and paid monies to CGM and provided Plaintiff's and Class Members' PII to Defendant.

179. Both the provision of these services and payment made, along with Defendant's promises of protection of Plaintiffs' and Class Members' PII, were material aspects of these contracts.

180. Plaintiffs and the Class Members were the intended beneficiaries of these contracts as facilitating their participation in the FCC ACP and Lifeline federal benefit programs and saving them money on telephone and internet services.

181. These valid and enforceable contracts included Defendant's promise to protect nonpublic PII of Plaintiffs and Class Members given to Defendant, or that Defendant created on its own, from unauthorized disclosures. Plaintiffs and Class Members allowed their PII to be provided in reliance on that promise.

182. Defendant materially breached its contractual obligations to protect the nonpublic PII of Plaintiffs and the Class Members which Defendant required and gathered when the information was unauthorizedly disclosed in the Data Breach.

183. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiffs and the Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

184. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts of which Plaintiffs and the Class Members were the intended beneficiaries.

185. As a result of Defendant's failure to fulfill the data security protections promised in these contracts in which Plaintiffs and the Class Members were the intended beneficiaries, Plaintiffs and Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering the loss of the benefit of the bargain they had struck with Defendant directly and/or indirectly through their telecommunications and internet service providers.

186. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

187. Plaintiffs and Class Members are also entitled to injunctive relief

requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

188. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

189. Plaintiffs bring this claim in the alternate to their claim for Breach of Implied Contract (Count II) and Breach of Contract—Third Party Beneficiary (Count III).

190. Plaintiffs and proposed Class Members conferred benefits upon Defendant in the form of monies received by CGM, and in the form of valuable PII entrusted to Defendant.

191. Defendant appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this Court should not allow Defendant to retain the full value of these benefits—specifically, the monies and PII of Plaintiffs and members of the Class.

192. After all, Defendant failed to adequately protect Plaintiffs' and Class Members' PII. And if such inadequacies were known, then Plaintiffs and the

members of the Class would never have conferred payment to Defendant, nor permitted the disclosure of their PII to Defendant.

193. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class Members.

194. As a direct and proximate result of Defendant's unjust enrichment set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; and the compromise and continuing publication of their PII and thus are entitled to damages as a result of the Data Breach.

195. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

196. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class Members in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds under circumstances making it inequitable to do so constitutes unjust enrichment.

197. The financial benefits derived by Defendant rightfully belong to Plaintiffs and Class Members. Defendant should be compelled to disgorge in a

common fund for the benefit of Plaintiffs and Class Members all wrongful or inequitable proceeds collected by Defendant. A constructive trust should be imposed upon all wrongful or inequitable sums received by Defendant traceable to Plaintiffs and Class Members.

198. Plaintiffs and the Class Members have no adequate remedy at law.

COUNT VI
INVASION OF PRIVACY—INTRUSION INTO PRIVATE AFFAIRS
(On Behalf of Plaintiffs and the Class)

199. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

200. The state of Georgia recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977).

201. Plaintiffs and the Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

202. Defendant owed a duty to Plaintiffs and the Class Members to keep their PII confidential.

203. Defendant failed to protect said PII and exposed the PII of Plaintiffs and the Class Members to unauthorized persons in the Data Breach.

204. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiffs and the Class Members, by way of Defendant's failure to protect the PII.

205. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Class Members is highly offensive to a reasonable person.

206. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs' and the Class Members' PII was disclosed to Defendant in connection with CGM's services relating to federal telecommunications and internet benefit programs, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

207. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiffs' and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

208. Defendant acted with a knowing state of mind when it permitted the

Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

209. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' PII.

210. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' PII.

211. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

212. As a direct and proximate result of the Defendant's invasion of privacy, the PII of Plaintiffs and the Class Members was disclosed to third parties without authorization, causing Plaintiffs and the Class Members to suffer injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; and compromise and continuing publication of their PII and, thus, are entitled to damages.

213. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

214. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

COUNT VII
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs Youngblood, Wolf and Guerra, and the California Class)

215. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

216. This claim is pleaded on behalf of Plaintiffs and the Class, or alternatively, the California Class.

217. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has

decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

218. As a result, in 2018, the California Legislature passed the California Consumer Privacy Act of 2018 ("CCPA"), giving consumers broad protections and rights intended to safeguard their personal information.

219. Among other things, the CCPA, Cal. Civ. Code §§ 1798.100(e), imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

220. On information and belief, CGM is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

221. Section 1798.150(a)(1) of the CCPA provides: "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

222. Through the above-detailed conduct, Defendant violated the CCPA by

subjecting the nonencrypted and nonredacted PII of Plaintiffs and Class Members to unauthorized access and exfiltration, theft, or disclosure as a result of CGM's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

223. Plaintiffs are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are natural persons residing in the state of California.

224. On information and belief, Defendant is a "business" as defined by Civ. Code § 1798.140(c) because it is a legal entity that does business in the state of California and has annual revenues in excess of $25,000,000.

225. The CCPA provides that "personal information" includes "[i]dentifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." *See* Civ. Code § 1798.140.

226. Plaintiffs' PII compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

227. Through the Data Breach, Plaintiffs' PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

228. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

229. On or around June 21, 2023, counsel for Plaintiff Guerra provided Defendant with written notice via certified mail of his intent to pursue claims under the CCPA and an opportunity for Defendant to cure. Defendant later sent a response thereto which failed to fully address and cure the violations alleged in the letter (which are now alleged herein).

230. On or around June 28, 2023, counsel for Plaintiff Wolf provided Defendant with written notice via certified mail of his intent to pursue claims under the CCPA and an opportunity for Defendant to cure. Defendant later sent a response thereto which failed to fully address and cure the violations alleged in the letter (which are now alleged herein).

231. On or around June 23, 2023, counsel for Plaintiff Youngblood provided Defendant with written notice via certified mail of her intent to pursue claims under the CCPA and an opportunity for Defendant to cure. Defendant later sent a response thereto which failed to fully address and cure the violations alleged in the letter (which are now alleged herein).

232. Defendant did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that they "cured" the above failures to

implement reasonable security procedures to prevent unauthorized access of Plaintiffs' and California Class members' PII through steps taken by Defendant "in response to the date security incident." These post- attack actions that Defendant allegedly took did not retroactively cure the unauthorized access, as they provide no assurance that CCPA Plaintiffs' and California Class members' PII was not viewed by—and/or is not still in the hands of—unauthorized third parties.

233. Furthermore, none of the steps Defendant asserts in its response demonstrates an actual cure of their failure to implement reasonable security measures to protect CCPA Plaintiffs' and California Class members' PII, as the steps they assert they have taken are not sufficient to protect CCPA Plaintiffs' and California Class members' PII into the future.

234. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect Plaintiffs' and California Class members' information.

235. As Defendant has not "actually cured" the violation, CCPA Plaintiffs and the California Class seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief, reasonable attorneys' fees and costs, and statutory damages. *See*

Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT VIII
VIOLATION OF CALIFORNIA'S CONSUMER RECORDS
Cal. Civ. Code §§ 1798.82, *et seq.* ("CCRA")
(On Behalf of Plaintiffs Youngblood, Wolf and Guerra, and the California Class)

236. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

237. This claim is pleaded on behalf of Plaintiffs and the Class, or alternatively, the California Class.

238. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under Section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay…"

239. The CCRA further provides: "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data *immediately* following discovery, if the personal information

was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b) (emphasis added).

240. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
>
> (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A)

and (B) of paragraph (1) of subdivision (h).

Cal. Civ. Code § 1798.82(d)(2).

241. The Data Breach described herein constitutes a "breach of the security system" of CGM.

242. As alleged herein, it took over five (5) months for Defendant to begin informing Plaintiffs and the Class or California Class Members about the Data Breach. CGM unreasonably delayed information to Plaintiffs and Class Members about the Data Breach, affecting their PII, after Defendant knew the Data Breach had occurred.

243. Defendant failed to disclose to Plaintiffs and California Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII, when CGM knew or reasonably believed such information had been compromised.

244. Defendant's ongoing business interests gave CGM incentive to conceal the Data Breach from the public to ensure continued revenue.

245. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiffs and California Class Members would impede its investigation.

246. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiffs and the California Class Members or Class Members were deprived of

prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class Members because their PII would have had less value to identity thieves.

247. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiffs and the California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

248. Plaintiffs and California Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to, to the damages suffered by Plaintiffs and Class Members as alleged above and equitable relief.

249. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to CGM conducted with the intent on the part of Defendant depriving Plaintiffs and Class Members of "legal rights or otherwise causing injury."

250. In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by CGM with a willful and conscious disregard of the rights or safety of Plaintiffs and Class Members and despicable conduct that has subjected Plaintiffs and Class Members to cruel and unjust hardship in conscious disregard

of their rights.

251. As a result, Plaintiffs and Class Members are entitled to punitive damages under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, Christina Cain, Darron Danna, Stephanie Youngblood, Joshua Wolf, Kim White, Brandon Guerra, and Charles Williams, on behalf of themselves, and all others similarly situated, pray for judgment as follows:

A. Trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

C. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, and statutory damages, and punitive damages, as allowed by law;

D. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of

Plaintiffs and the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiffs and the Class are entitled.

Dated: September 27, 2023

Respectfully submitted,

/s/ Andrew R. Tate
Andrew R. Tate – GA Bar # 518068
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
235 Peachtree Street NE, Suite 400
Atlanta, GA 30303
Telephone: (404) 282-4806
Email: atate@peifferwolf.com

Brandon M. Wise – IL Bar # 319580*
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Telephone: 314-833-4825
Email: bwise@peifferwolf.com

Joseph Alonso
ALONSO & WIRTH LAW, LLC
Georgia Bar No. 13627
1708 Peachtree Street NW
Suite 207

Atlanta, GA 30309
jalonso@alonsowirthlaw.com

Lynn A. Toops*
Amina A. Thomas*
Mary Kate Dugan*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com

Michael R. Hirsh, GBN 357220 2295
HIRSH LAW OFFICE, LLC
Towne Lake Pkwy.
Suite 116-181
Woodstock, Georgia 30189
Tel: 678-653-9907

E: Michael@Hirsh.law

Tyler J. Bean (admitted *pro hac vice*)
Mason A. Barney (admitted *pro hac vice*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

John A. Yanchunis*
jyanchunis@forthepeople.com
Ra O. Amen (Ga. Bar No. 368227)
ramen@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

Kenneth Grunfeld (admitted pro hac vice)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
65 Overhill Road
Bala Cynwyd, Pennsylvania 19004
Main: 954-525-4100
grunfeld@kolawyers.com

*Motion for *Pro Hac Vice* Admission forthcoming

Counsel for Plaintiffs and the Proposed Class

EXHIBIT 1

The investigation is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, 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, through an external data analytics specialist, 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 to, and this review concluded on March 23, 2023. A subsequent internal review was conducted to locate missing mailing addresses and associate identified individuals with respective data owners, and upon completion of this additional review, CGM completed notifying affected data owners on or about April 15, 2023. By May 18, 2023, CGM received approval from data owners to provide notice to affected individuals and regulatory authorities on their behalf.

The information that could have been subject to unauthorized access includes name, driver's license or state ID number, and Social Security number.

Notice to Maine Resident

On or about June 7, 2023, CGM began providing written notice of this incident to one (1) Maine resident on behalf of data owners. 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 incident, 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 incident. CGM is providing access to credit monitoring services for one (1) year, through TransUnion, 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

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 7, 2023

Re: Notice of Data <<Variable data 2/Variable Header>>

Dear <<First Name>> <<Middle Name/Initial>> <<Last Name>>:

CGM Inc. ("CGM") writes to notify you of a recent 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 or Entity /Carrier>>. **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 <<Variable data 1/Exposure language>>. 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.

Based on our investigation, we determined that certain information related to you was found within the impacted systems.

What Information Was Involved? Our investigation determined that the information related to you that was subject to unauthorized access includes your <<data elements>>, and name. 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 discovering the suspicious activity, we promptly took steps to confirm our system security and engaged third-party cybersecurity 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.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for <<12/24>> months through TransUnion 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 account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any such activity to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

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

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, asubsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and inthe space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Engagement number>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Enrollment Deadline>>** . Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with youronline enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 2,834 Rhode Island residents that may be impacted by this event.

EXHIBIT 2

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

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 7, 2023

Re: Notice of Data <<Variable data 2/Variable Header>>

Dear <<First Name>> <<Middle Name/Initial>> <<Last Name>>:

CGM Inc. ("CGM") writes to notify you of a recent 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 or Entity /Carrier>>. **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 <<Variable data 1/Exposure language>>. 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.

Based on our investigation, we determined that certain information related to you was found within the impacted systems.

What Information Was Involved? Our investigation determined that the information related to you that was subject to unauthorized access includes your <<data elements>>, and name. 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 discovering the suspicious activity, we promptly took steps to confirm our system security and engaged third-party cybersecurity 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.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for <<12/24>> months through TransUnion 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 account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any such activity to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

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

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, asubsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and inthe space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Engagement number>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Enrollment Deadline>>** . Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with youronline enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 2,834 Rhode Island residents that may be impacted by this event.