UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
URBANA DIVISION

RILDA FIRKINS, on behalf of herself and on behalf of all other similarly situated individuals, Plaintiff, v. **COMMUNICATIONS DATA GROUP, INC., DUO COUNTY TELEPHONE COOPERATIVE CORPORATION, INC. and CUMBERLAND CELLULAR, LLC D/B/A DUO BROADBAND**, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Rilda Firkins ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Communications Data Group, Inc. ("CDG"), Duo County Telephone Cooperative Corporation, Inc. and Cumberland Cellular, LLC d/b/a Duo Broadband (collectively, "Defendants") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to her own actions and her counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendants Duo County Telephone Cooperative Corporation, Inc. and Cumberland Cellular, LLC d/b/a Duo Broadband, communications companies that deliver telecom and communications

services, and Defendant Communications Data Group, Inc., a billing vendor for service providers such as Duo Broadband.[1]

2. Plaintiff brings this Complaint against Defendants for their failure to properly secure and safeguard the personally identifiable information that they collected and maintained as part of their regular business practices, including Plaintiff's and Class Members' first and last names, addresses, dates of birth, and Social Security numbers (collectively defined herein as "Private Information").

3. Upon information and belief, current and former customers of Defendants are required to entrust Defendants with sensitive, non-public Private Information, without which Defendants could not perform their regular business activities. Defendants retain this information for at least many years and even after the customer-provider relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Defendants failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect Plaintiff's and Class Members' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

---

[1] The "Notice Letter," attached hereto as ***Exhibit A***.

6. In breaching their duties to properly safeguard Plaintiff's and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendants' conduct amounts to negligence and/or recklessness and violates federal and state statutes.

7. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

8. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

9. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated

with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) invasion of their privacy; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

10. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

11. Plaintiff Rilda Firkins is a natural citizen of Kentucky, residing in the citizen of Columbia.

12. Defendant Communications Data Group, Inc. is a Delaware corporation. CDG is headquartered at 2107 S. Neil Street, Champaign, IL 61820. CDG's registered agent is Kim Belanger, who can be served at the same address.

13. Defendant Duo County Telephone Cooperative Corporation, Inc. is a nonprofit corporation organized under the state laws of Kentucky with its principal place of business located in Jamestown, Kentucky.

14. Defendant Cumberland Cellular, LLC is a limited liability company organized under the state laws of Kentucky with its principal place of business located in Jamestown, Kentucky.

15. Defendants Duo County Telephone Cooperative Corporation, Inc. and Cumberland Cellular, LLC collectively do business as Duo Broadband with their principal place of business located in Jamestown, Kentucky.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant Communications Data Group, Inc., including the Plaintiff.

17. This Court has personal jurisdiction over Defendants because Defendant Communications Data Group, Inc. is registered to do business in the State of Illinois; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District. Upon information and belief, the Data Breach giving rise to this lawsuit occurred in this District.

FACTUAL ALLEGATIONS

Background of Defendants.

19. Defendant Communications Data Group, Inc. is a for-profit company headquartered in Champaign, IL.

20. Defendant Duo County Telephone Cooperative Corporation, Inc. is a nonprofit corporation in Jamestown, Kentucky.

21. Defendant Cumberland Cellular, LLC is a for-profit company in Jamestown, Kentucky.

22. Plaintiff and Class Members are current and former customers of Defendants.

23. CDG produces billing and operational management solutions for use by its clients located in the United States and Canada.[2]

24. CDG's clients are service providers that offer telephone, cable, internet, and other services to their customers.[3]

25. Duo Broadband is one of CDG's clients.[4] Duo Broadband is an internet service provider based in Jamestown, Kentucky that sells phone, TV and internet service.[5]

26. It is estimated that CDG's annual revenue is $25 million per year.[6] In other words, CDG could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

27. As a condition of receiving services from Defendants, Plaintiff and Class Members were required to provide Defendants with their sensitive and confidential Private Information, including their first and last names, Social Security numbers, addresses, and dates of birth.

28. The information held by Defendants in their computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

---

[2] https://cdg.us/privacy/ (last accessed June 18, 2025).
[3] *Id*.
[4] The "Notice Letter," attached hereto as ***Exhibit A***.
[5] *See* https://www.comparitech.com/news/telecom-saas-firm-communications-data-group-notifies-42k-people-of-data-breach-on-behalf-of-duo-broadband/ (last accessed June 18, 2025).
[6] https://growjo.com/company/Communications_Data_Group_(CDG)#google_vignette (last accessed June 18, 2025).

29. Upon information and belief, Defendants made promises and representations to their current and former customers, including Plaintiff and Class Members, that the Private Information collected from them as a condition of receiving services would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

30. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

32. Defendants each had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendants each have a legal duty to keep their customers' Private Information safe and confidential.

33. Defendants each had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

34. Defendants each derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

The Data Breach.

36. Starting on or about May 15, 2025, Defendants began sending Plaintiff and other victims of the Data Breach a letter (the "Notice Letter"), informing them that:

> **What Happened?** On February 13, 2025, we discovered a data security incident in which a cyber threat actor attempted to disrupt our systems in a possible effort to deploy ransomware, and solicit a ransom payment from us. Upon discovery, we immediately took action to secure our systems, terminated any unauthorized access, and notified law enforcement as required by federal regulations. On March 17, 2025, we detected unauthorized access to certain sensitive personal information of Duo Broadband customers, described below.
>
> **What Information Was Involved?** The information subject to the incident may have included sensitive personal information, including your first and last name, address, date of birth, and Social Security Number.[7]

37. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, and the vulnerabilities exploited. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

[7] The "Notice Letter," attached hereto as ***Exhibit A***.

38. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

39. Despite Defendants' intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendants' networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendants' networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' names, Social Security numbers, addresses, and dates of birth for download and theft.

40. To be clear – there are numerous issues with Defendants' Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1) Defendants waited over ***three*** months to notify Plaintiff and Class members of the Data Breach; (2) Defendants fail to state whether they were able to permanently contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendants continue to maintain is secure; and (3) Defendants fail to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

41. Moreover, in their Notice Letter, Defendants failed to specify whether they undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether

Class Members should report their misuse to Defendants, and whether Defendants set up any mechanism for Class Members to report any misuse of their data.

42. Furthermore, Defendants' delay in notifying Plaintiff and Class members of the Data Breach is in direct violation of Defendants' responsibilities under the data breach notification statute in Illinois. *See* 815 ILCS § 530/10 (which requires that the disclosure notification be made "in the most expedient time possible and without unreasonable delay."[8]

43. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

44. The attacker targeted, accessed, and acquired files in Defendants' computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, addresses, dates of birth, and Social Security numbers. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

45. Plaintiff further believes that her Private Information and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable.

46. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

---

[8] While the definition of "reasonable" differs from state to state, the range is between 30-60 days. Defendants failed to meet this requirement by over ***60 days.***

47. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[9]

48. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders

[9] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed June 18, 2025).

supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

49. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

[10] *Id.* at 3-4.

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

50. Given that Defendants were storing the sensitive Private Information of their current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

51. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, thousands of thousands of individuals, including that of Plaintiff and Class Members.

Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information

52. As a condition of receiving Defendants' services, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendants.

53. Defendants retain and store this information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendants would be unable to perform their services.

54. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

---

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed June 18, 2025).

55. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

56. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

Defendants Knew or Should Have Known of the Risk Because Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

57. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

58. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information and other sensitive information, like Defendants, preceding the date of the breach.

59. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[12]

60. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million

[12] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024); https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last accessed June 18, 2025).

records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

61. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

62. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

63. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

64. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[13] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed June 18, 2025).

[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed June 18, 2025).

65. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to more than forty-two thousand individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data[15].

66. In the Notice Letter, Defendants make an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

67. Defendants' offering of credit and identity monitoring establishes that Plaintiff and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendants' computer systems.

68. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

69. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

---

[15] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792a1252b4f8318/943d1111-7f57-42a2-8259-b0de8e4ba981.html (last accessed June 18, 2025).

70. As a company in possession of Plaintiff's and Class Members' Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information.

71. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "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, employee-benefit management company or taxpayer identification number."[17]

72. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[18] For example, Personal Information can be sold at a price

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id.*
[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 18, 2025).

ranging from $40 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and date of birth.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

75. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

76. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have

---

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 18, 2025).

[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 18, 2025).

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 18, 2025).

> been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

77. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendants Fail to Comply with FTC Guidelines.

78. 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.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23]

80. 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

---

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed June 18, 2025).

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 18, 2025).

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.[24]

81. The FTC further recommends that companies not maintain Private Information 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.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee 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.

83. These FTC enforcement actions include actions against companies in possession of Private Information, like Defendants.

84. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

85. Defendants failed to properly implement basic data security practices.

---

[24] *Id.*

86. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

87. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of their customers, Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Fail to Comply with Industry Standards.

88. As noted above, experts studying cyber security routinely companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

89. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

90. Other best cybersecurity practices that are standard for companies like Defendants include installing appropriate malware detection software; monitoring and limiting the network

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

91. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These foregoing frameworks are existing and applicable industry standards for companies in possession of Private Information to safeguard their employees' data, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages.

93. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Victims' Risk of Identity Theft.

94. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

95. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

98. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to

perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[25]

99. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[26]

100. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[27] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[28]

101. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[29]

---

[25] *See* N.C. Gen. Stat. § 132-1.10(1).
[26] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers (last accessed June 18, 2025).
[27] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last accessed June 18, 2025).
[28] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last accessed June 18, 2025).
[29] "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 that can be made off of those credentials. Fullz are usually pricier than standard credit card

102. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information 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.

103. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' 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 Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

104. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

105. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

---

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://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last accessed June 18, 2025).

106. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud.

107. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

108. Thus, due to the actual and imminent risk of identity theft, Defendants, in their Notice Letter instruct Plaintiff and Class Members to protect themselves by offering enrollment in a free credit monitoring program.

109. Defendants' suggestion of steps that Plaintiff and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiff and Class Members must undertake in response to the Data Breach. Plaintiff's and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendants' Notice Letter.

110. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, freezing their payment cards, contacting credit bureaus to place freezes on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take

years to detect. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

111. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

112. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

113. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution of Value of Private Information.

114. Private Information is a valuable property right.[32] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy

---

[30] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed June 18, 2025).

[31] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed June 18, 2025).

[32] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;

prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

115. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[33]

116. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35,36] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[37]

117. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an

---

However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed June 16, 2025) ("GAO Report").

[33] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, 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) (last accessed June 18, 2025).

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed June 18, 2025).

[35] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed June 18, 2025).

[36] https://datacoup.com/ (last accessed June 18, 2025).

[37] https://digi.me/what-is-digime/ (last accessed June 18, 2025).

economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

118. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

119. The fraudulent activity resulting from the Data Breach may not come to light for years.

120. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

121. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

122. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary.

123. Given the type of targeted attack, the sophisticated criminal activity, and the type of Private Information involved in this case, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and

purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

124. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employee-benefit management company of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

125. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

126. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss of Benefit of the Bargain.

127. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide Defendants with their Private Information as a condition of receiving telecommunication and/or internet services, Plaintiff and other reasonable customers understood and expected that Defendants would properly safeguard and protect their Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

Plaintiff Experience

128. Plaintiff Rilda Firkins is a former customer of Defendants.

129. Upon information and belief, as a condition of receiving Defendants' services, Plaintiff was required to provide Defendants with her Private Information.

130. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in their system.

131. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

132. Plaintiff provided her Private Information to Defendants and trusted the companies would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law.

133. Plaintiff reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of Private Information.

134. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendants, dated May 15, 2025. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, address, and date of birth.

135. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, which instructs Plaintiff to monitor her free credit report for any authorized activity, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect.

136. As a result of the Data Breach, Plaintiff spent valuable time that she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

137. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

138. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

139. As a result of the Data Breach, Plaintiff anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

140. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

141. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

142. Plaintiff brings this action against Defendants on behalf of herself and all others similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **Nationwide Class**: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach, including those who received notice of the Data Breach (the "Class").

143. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

144. Plaintiff reserves the right to amend the definitions of the Class or Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

145. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

146. **Numerosity.** The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendants, upon information and belief, thousands of individuals were impacted. The Class is apparently

identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by sending them breach notification letters).

147. **Commonality and Predominance.** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

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

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of Defendants' wrongful conduct; and,

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

148. **Typicality.** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendants' uniform misconduct. Defendants' inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendants.

149. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

150. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical

of other Class Members. Plaintiff have retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

151. **Superiority and Manageability.** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

152. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

153. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

154. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

155. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

156. Further, Defendants have 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.

CAUSES OF ACTION

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

157. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

158. Defendants require their customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing their services.

159. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of their business of soliciting their clients, which solicitations and services affect commerce.

160. Plaintiff and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

161. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

162. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants have a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

163. Defendants each 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.

164. Defendants each owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

165. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, a necessary part of obtaining services from Defendants.

166. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

167. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

168. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information it was no longer required to retain pursuant to regulations.

169. Moreover, Defendants each had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

170. Defendants had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

171. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former customers' Private Information after they were no longer required to retain it pursuant to regulations, and;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

172. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

173. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

174. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

175. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

176. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

177. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting companies in possession of Private Information.

178. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

179. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

180. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

181. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

182. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

183. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

184. Defendants have admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

185. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

186. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

187. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of their privacy; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized

disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

188. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

189. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

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

191. Defendants' negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

192. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their 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 Plaintiff and the Class)

193. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

194. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

195. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

196. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

197. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

198. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

199. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

200. Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

201. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

202. CDG entered into uniform written contracts with Duo Broadband to provide billing services.

203. Pursuant these contracts, Defendants received from their clients and maintained Plaintiff's and Class Members' Private Information in the course of performing their contractual services, which Defendants could not perform without receiving and maintaining such Private Information.

204. Pursuant to these contracts, Duo Broadband agreed to provide CDG with compensation and Plaintiff's and Class Members' Private Information.

205. In exchange, Defendants agreed, in part, to implement adequate data security measures to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure, and to timely notify Plaintiff and Class Members of the Data Breach.

206. Defendants were required by statutes and regulations, including but not limited to the FTC Act and state consumer privacy and protection laws, to have contracts with its clients that required CDG to implement and maintain reasonable security procedures and practices to protect its clients' customers'—Plaintiff and Class Members—Private Information from unauthorized access, use, or disclosure.

207. The relevant statutes and regulations obligating Defendants to promise by contract to use reasonable data security for Plaintiff's and Class Members' Private Information create a class of intended beneficiaries whose members are implied into such agreements by operation of law. Plaintiff and Class Members are the intended beneficiaries of the contracts that Defendants entered into.

208. Upon information and belief, Defendants' contracts with their clients each contained a provision requiring CDG to implement and maintain reasonable security procedures and practices appropriate to the nature of Private Information Defendants collected, to protect the Private Information from unauthorized access, use, or disclosure.

209. These contracts between Defendants were made expressly for the benefit of Plaintiff and Class Members as the intended third-party beneficiaries of these contracts.

210. Defendants knew Plaintiff and Class Members were involved and would benefit from the transactions that were subject to these contracts between Defendants.

211. Defendants knew that if they breached its contractual obligation to adequately safeguard Plaintiff's and Class Members' Private Information, Plaintiff and Class Members would

be harmed. Defendants breached these contracts, by, among other acts and omissions: (a) failing to use reasonable data security measures, (b) failing to implement adequate protocols and employee training sufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure, and (c) failing to promptly or adequately notify Plaintiff and Class Members of the Data Breach.

212. As a direct and proximate result of Defendants' breaches of these contracts with its clients, Plaintiff and Class Members have suffered and will continue to suffer injuries as set forth herein and are entitled to damages sufficient to compensate for the losses they sustained.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

213. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

214. Defendants offered to provide telecommunication and internet services to their current and former customers, including Plaintiff and Class members, in exchange for payment.

215. Defendants also required Plaintiff and the Class members to provide their Private Information as a condition of receiving these services.

216. In turn, Defendants impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures, including by virtue of the promises in their privacy policies.[38]

[38] *See* https://duobroadband.com/legal-tariff-and-rights-information/privacy-statement/ ("DUO Broadband secures your personal information from unauthorized access, use or disclosure. DUO Broadband secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure.") (last accessed June 16, 2025); https://cdg.us/privacy/ ("To protect customer and company information from unauthorized access and use, CDG uses security measures that comply with federal / state law and standard industry practices. These measures include computer safeguards and secured files

217. Plaintiff and the Class members accepted Defendants' offer by providing Private Information to Defendants in exchange for their services.

218. Plaintiff and Class members would not have entrusted their Private Information to Defendants but for the above-described agreement with Defendants.

219. Defendants materially breached their agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

220. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendants.

221. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. 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 along with their form.

222. Defendants' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

223. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendants' breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

---

and buildings") (last accessed June 16, 2025).

224. Plaintiff and the Class were harmed by Defendants' breach of their contracts, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

225. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

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

226. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

227. This Count is pleaded in the alternative to the breach of implied contract (Count III).

228. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security.

229. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

230. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

231. Defendants acquired the Private Information through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

232. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information to Defendants.

233. Plaintiff and Class Members have no adequate remedy at law.

234. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their Private Information.

235. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

236. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the

compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix)nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

237. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

238. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

239. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

240. Given the relationship between Defendants and Plaintiff and Class members, where Defendants became guardian of Plaintiff's and Class members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and

disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

241. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendants' relationship with them—especially to secure their Private Information.

242. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members would not have entrusted Defendants, or anyone in Defendants' position, to retain their Private Information had they known the reality of Defendants' inadequate data security practices.

243. Defendants breached their fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

244. Defendants also breached their fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

245. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VII
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

246. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 156, as if fully set forth herein.

247. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those

alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

248. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

249. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to employ reasonable data security to secure the Private Information they possess, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendants continue to breach their duties by failing to employ reasonable measures to secure their customers' personal and financial information; and

c. Defendants' breach of their legal duty continues to cause harm to Plaintiff and the Class.

250. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect their customers' (i.e., Plaintiff's and the Class's) data.

251. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary

damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

252. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued.

253. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendants and that the Court grants the following:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

Vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees and costs as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

Dated: June 19, 2025

Respectfully submitted,

SHAMIS & GENTILE P.A.
/s/ Andrew Shamis
Andrew J. Shamis, Esq.
ashamis@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299

Leigh Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
Service only: service@eksm.com
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Phone: (888) 350-3931

* *Pro hac vice applications forthcoming*