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

ALEXIS MORGAN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CRICKET WIRELESS, LLC,

Defendant.

Case No.:_____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Alexis Morgan, ("Plaintiff") brings this Class Action Complaint against Defendant Cricket Wireless, LLC, ("Defendant") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") and/or customer proprietary network information ("CPNI")[1] that was accessed and exfiltrated in a data breach.

2. Defendant is a wireless telecommunications service provider that collects and/or creates personal information related to its subscribers, including information that relates to the

[1] Collectively, personally identifiable information and customer proprietary network information is referred to as "PII."

quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by its customers.

3. Defendant acknowledges its responsibility to protect the personal data it collects and assures customers, through its privacy policy, that their information and their privacy are important.[2]

4. Earlier this year, cybercriminals figured out that many major companies, including Defendant, have uploaded massive amounts of valuable and sensitive customer data to Snowflake servers. Snowflake is a third-party cloud platform. Cybercriminals targeted Snowflake accounts that did not require users to authenticate themselves prior to accessing sensitive data.[3]

5. On, or about, July 22, 2024, Defendant announced that customer data was illegally downloaded from its workspace on a third-party cloud platform (hereafter, the "Data Breach"). The compromised data included records of calls and texts of nearly all of Cricket Wireless's cellular customers from May 1, 2022 to October 31, 2022 and January 2, 2023. The compromised data also includes cell site identification numbers of the most frequently used cell tower(s), and phone numbers that Defendant's wireless customers interacted with during this time.

6. Upon information and belief, the Data Breach affected approximately 10 million Cricket Wireless customers and Snowflake is the third-party cloud platform involved.

7. Defendant completely and utterly failed to protect its customers' personal data and/or ensure that its third-party vendors protected customer data consistent with Defendant's

[2] *Cricket Wireless Privacy Policy*, effective January 1, 2023, https://www.cricketwireless.com/legal-info/privacy-policy-previous-version.html (last accessed July 22, 2024).

[3] *See, Crooks Steal Phone, SMS Records for Nearly All AT&T Customers*, https://krebsonsecurity.com/2024/07/hackers-steal-phone-sms-records-for-nearly-all-att-customers/ (last accessed July 16, 2024).

privacy notice. Upon information and belief, multi-factor authentication was not required to access the customer records that were exposed in the Data Breach.

8. Although Defendant learned of the Data Breach in April 2024, Defendant did not notify Plaintiff of the Data Breach until July 2024. Omitted from the data breach notice letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff, who retains a vested interest in ensuring the PII remains protected.

9. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take the necessary steps to secure the PII from those risks left the data in a dangerous condition.

10. The Data Breach was a direct result of Defendant's failure to implement reasonable safeguards to protect PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant implemented reasonable administrative, technical, and/or physical controls consistent with industry standards and best practices, it could have prevented the Data Breach.

11. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. Plaintiff suffered actual injury in the form of damages to and diminution in the value of the PII that was compromised as a result of the Data Breach. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

12. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

13. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a. **Data Type**: The data acquired in the Data Breach included unencrypted phone numbers and cell site identification numbers, which can be used to perpetuate fraud, identity theft, and other types of exploitation. For example, this data can be used in SIM swapping scams, port-out fraud,[4] and Smishing attacks.[5] These scams work as follows:
   - Subscriber Identity Module (SIM) Swapping – A bad actor convinces a victim's wireless carrier to transfer the victim's service from the victim's cell phone to a cell phone in the bad actor's possession. This is called "SIM swapping" because it involves an account being fraudulently transferred (or swapped) from a device associated with one SIM to a device associated with a different SIM.
   - Port-Out Fraud – A bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor.
   - Smishing Scams – Occurs when a bad actor uses deceptive text messages to lure consumers into providing their personal or financial information. The scam artists that send smishing messages often impersonate a government agency, bank, or other company to lend legitimacy to their claims. Smishing messages typically ask consumers to provide usernames and passwords, credit and debit card numbers, PINs, or other sensitive information that scam artists can use to commit fraud.

b. **Data Breach Type**: This was a targeted attack, orchestrated by a hacker that is part of the ShinyHunters hacking group. ShinyHunters has been linked to a string of high-profile data breaches resulting in millions of dollars in losses. In 2021, ShinyHunters stole a database of personal information regarding 70 million cellular customers and then sold the data on the dark web.[6] Furthermore, since

[4] https://www.ccmi.com/fcc-will-update-cpni-rules-to-stop-data-breaches/ (last accessed May 21, 2024).
[5] *See*, https://www.fcc.gov/avoid-temptation-smishing-scams (last accessed May 21, 2024).
[6] *See*, *Data allegedly stolen from 560 million Ticketmaster users*, https://www.bbc.com/news/articles/c899pz84d8zo (accessed June 11, 2024).

2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (*e.g.*, GitHub, AT&T, Pizza Hut). Upon information and belief, ShinyHunters has accumulated enough personal information from that series of data breaches to be able to commit identity theft, fraud, or other forms of exploitation.

c. **Data Misuse**: Upon information and belief, other Cricket Wireless users have been victims of SIM swapping scams.[7]

14. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff.

15. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused her to: (i) spend money on mitigation measures like credit monitoring services and/or dark web scans and monitoring; (ii) lose time and effort spent responding to the Data Breach, like finding where the data is exposed and at risk; (iii) spend money removing data from risky databases or deleting it from data broker databases; and/or (iv) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff suffered can be redressed by a favorable decision in this matter.

16. Plaintiff faces a substantial risk of future spam, phishing, or other social engineering attacks where full names, addresses, email addresses, locations, call/text details, and phone numbers can be readily accessed by cybercriminals known for stealing and reselling personal data on the dark web. The exposure of call data records is particularly alarming, according to Secure Cyber Defense CEO Shawn Waldman, because *this type of data allows hackers to pinpoint locations based on phone numbers*. Furthermore, Jake Williams, a former hacker for the

[7] *See, e.g., Hackers take over family's Cricket Wireless account, shut down phones and take over financial apps*, ABC News Chicago, https://abc7chicago.com/cricket-wireless-account-hacked-sim-swap-coinbase-crypto-app/14517218/ (last visited July 22, 2024).

National Security Agency, said *call data records* "are *a gold mine in intelligence analysis because they can be used to understand who is talking to who — and when*." This type of information can be used to craft highly sophisticated attacks. Additionally, threat actors may use the data to circumvent SMS-based multifactor authentication security measures.[8]

17. Names, telephone numbers, and cell site identification numbers can be used by cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information. Therefore, Plaintiff must incur out of pocket costs for purchasing products to protect from phishing, smishing (SMS message), vishing (voice messaging), pretexting, and other sophisticated attacks.

18. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit other forms of exploitation.

19. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (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) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk her PII will be further misused, where: (a) her data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

[8] *See, e.g.*, https://therecord.media/att-ransom-data-breach (accessed July 16, 2024).

20. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

21. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

JURISDICTION & VENUE

22. Plaintiff incorporates the allegations contained in the foregoing paragraphs as if fully set forth herein.

23. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

24. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, Defendant has purposefully availed itself of the laws, rights, and benefits of the forum state by registering to do business and selling products or services within this District, Defendant has sufficient minimum contacts with the forum state such that jurisdiction in this District is proper, and the events giving rise to Plaintiff's claims occurred in this District.

25. Venue is proper under 28 U.S.C §1391 because Defendant maintains a principal place of business in this District, a substantial part of the events and omissions giving rise to

Plaintiff's claims occurred in and emanated from this District, and Defendant is subject to personal jurisdiction in this District.

PARTIES

26. Plaintiff Alexis Morgan is an adult citizen of the State of South Carolina. At all relevant times, Plaintiff Morgan has been a resident of Lynchburg, Lee County, South Carolina. Plaintiff Morgan purchased telecommunications services from Defendant.

27. Defendant Cricket Wireless, LLC, is a Delaware limited liability company with a principal office or principal place of business at 1025 Lenox Park Boulevard, NE, Atlanta, Fulton County, Georgia 30319. Defendant's registered agent is CT Corporation System, 289 S. Culver Street, Lawrenceville, Georgia 30046-4805. Defendant provides wireless telecommunications services to over ten million subscribers in the United States.

FACTUAL ALLEGATIONS

28. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

29. To run its business, Defendant collects, maintains, and profits from the PII of millions of its U.S. consumers.

30. Upon information and belief, Defendant uses PII for Social Network Analysis on its customers' call logs and locations for marketing purposes. Social Network Analysis (SNA) characterizes networked structures in terms of nodes (individual actors, people, or things within the network) and the ties, edges, or links (relationships or interactions) that connect them.

31. Common SNA applications include data aggregation and mining, user attribute and behavior analysis, location-based interaction analysis, customer interaction and analysis, marketing, and business intelligence.

32. The Cricket Wireless Privacy Policy (the "Privacy Policy") applies to anyone who uses Defendant's products and services, including voice, data, mobile broadband, and applications.[9] The Privacy Policy provides that customer information is used to: (i) create engaging and customized experiences and offer new or improved products and services; (ii) design and deliver advertising and marketing campaigns to customers and measure their effectiveness; and (iii) customize advertisements, articles, videos, and marketing materials.[10]

33. In addition to listing the ways Defendant benefits and profits from its customers' personal information, the Privacy Policy states: "[we] work hard to safeguard your data using a range of technological and organizational security controls. We maintain and protect the security of computer storage and network equipment, and we use security procedures that require employees to authenticate themselves to access sensitive data. We also limit access to personal information only to those with jobs requiring such access. . . .We take steps to ensure that data is processed according to this Policy and to the requirements of applicable law of your country and of the additional countries where the data is subsequently processed."

34. Defendant promised to safeguard the PII it collected using technical and organizational safeguards. These promises were contained in the applicable privacy policy, the website, and through other disclosures in compliance with statutory privacy requirements.

35. Plaintiff and Class Members (later defined) are current and former customers of Defendant. Plaintiff and Class Members, as customers of Defendant, relied on these representations and on this sophisticated business entity to keep their PII confidential, securely maintained, and to make only authorized disclosures of this information.

[9] https://www.cricketwireless.com/legal-info/privacy-policy-previous-version.html (last accessed July 22, 2024).
[10] *Id.*

36. On, or about, July 22, 2024, Defendant announced that customer data was illegally downloaded from its workspace on a third-party cloud platform, which exposed the personal data of roughly 10 million customers. Upon information and belief, multi-factor authentication was not required to access the sensitive customer records that were exposed in the Data Breach.

37. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

38. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement identity and access management (IAM) policies and technology to ensure that the correct users have the appropriate access to technology resources; (iv) implement multifactor authentication in cloud environments and require users to provide more than one form of identification before accessing systems, applications, or services; (v) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (vi) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

39. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[11] Ransomware groups frequently implement a double extortion tactic, "where the

[11] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).

cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[12]

40. To prevent cyber-attacks like the one involved here, Defendant could and should have implemented ISO 27017, which is part of the ISO/IEC 27000 family and is an information security framework for organizations using cloud services. The standard advises both cloud service customers and cloud service providers, with the primary guidance laid out side-by-side in each section.

41. ISO/IEC 27017 is a standard that focuses on addressing the data privacy and security requirements for organizations using cloud services. An overview of the standard is as follows:

Overview of ISO/IEC 27017

a. **Scope**: ISO/IEC 27017 provides guidance to cloud service customers on the implementation of information security controls within the context of their use of cloud services. It complements the existing ISO/IEC 27001 standard, which is a broader information security management system (ISMS) standard.

b. **Objectives**: The standard aims to help organizations protect the confidentiality, integrity, and availability of their information in the cloud environment. It provides guidelines for addressing the risks associated with cloud computing and ensures that cloud service customers maintain control over their data.

c. **Data Classification & Handling**: ISO/IEC 27017 emphasizes the importance of classifying data based on its sensitivity and defining appropriate handling and security measures for each classification. It provides guidance on data encryption, access controls, data segregation, and data retention.

d. **Security Responsibilities**: The standard clarifies the division of security responsibilities between the cloud service customer and the cloud service provider. It outlines the areas where the customer retains control and where the provider assumes responsibility. This helps establish clear expectations and accountability for security measures.

[12] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

e. **Supplier Management**: ISO/IEC 27017 emphasizes the need for cloud service customers to assess the security capabilities of their cloud service providers. It provides guidance on selecting trustworthy providers, establishing contractual agreements, and monitoring the provider's compliance with security requirements.

f. **Incident Management**: The standard addresses incident management processes in the cloud environment. It provides guidance on incident reporting, investigation, and response to ensure timely and effective handling of security incidents.

g. **Continual Improvement**: ISO/IEC 27017 promotes a continual improvement approach to information security in the cloud. It encourages organizations to regularly review and update their security controls, assess emerging risks, and implement necessary improvements.

42. ISO/IEC 27017 provides guidance on multi-factor authentication (MFA) as a security control for cloud service customers. The standard provides, among other things, the following security requirements:

a. **Authentication Requirements**: The standard emphasizes the importance of strong authentication mechanisms for accessing cloud services. It recommends the use of MFA as an effective method to enhance the security of user authentication. MFA requires users to provide multiple forms of identification, such as a password and a unique code or biometric factor, to verify their identity.

b. **Risk Assessment**: ISO/IEC 27017 encourages cloud service customers to conduct a risk assessment to determine the level of authentication controls required based on the sensitivity of the data and the potential impact of unauthorized access. MFA is often recommended for high-risk or sensitive applications or data.

c. **Access Controls**: The standard provides guidance on implementing access controls in the cloud environment. It suggests that MFA should be used as an additional layer of security in conjunction with other access control measures such as strong passwords, role-based access control (RBAC), and least privilege principles.

d. **User Management**: ISO/IEC 27017 highlights the need for effective user management practices in the cloud. It recommends implementing MFA for user accounts with administrative privileges or access to sensitive data. This helps prevent unauthorized access even if the user's password is compromised.

e. **Supplier Management**: The standard advises cloud service customers to assess the authentication capabilities of their cloud service providers. It recommends selecting providers that offer robust MFA options and have appropriate controls in place to protect customer data.

f. **Compliance Monitoring**: ISO/IEC 27017 suggests that organizations should monitor and review the effectiveness of their MFA controls regularly. This includes monitoring user access logs, analyzing authentication success/failure rates, and promptly addressing any security incidents or vulnerabilities related to authentication.

43. By addressing MFA in these ways, ISO/IEC 27017 helps cloud service customers, like Defendant, strengthen their authentication processes, reduce the risk of unauthorized access, and enhance the overall security of their cloud services.

44. Defendant could and should have identified the risks and potential effects of collecting, maintaining, sharing, and storing PII in cloud environments as detailed above.

45. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and Class Members' PII.

46. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII in cloud environments and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and Class Members as a result.

47. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

48. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their PII was targeted by a sophisticated hacker known for

stealing and reselling sensitive data on the dark web. The substantial risk of future exploitation created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

49. Furthermore, Plaintiff and Class Members face a substantial risk of future spam, phishing, or other attacks designed to trick them into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime, where their cellular data and contact information were acquired in the Data Breach. The substantial risk of future spam, phishing, or other exploitation attempts created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

50. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[13] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

51. Given the type of targeted attack in this case, the sophistication of the criminal claiming responsibility for the Data Breach, the type of PII involved in the Data Breach, the hacker's behavior in prior data breaches, and the ability of criminals to link data acquired in the Data Breach with information available from other sources, it is reasonable for Plaintiff and the Class Members to assume that their PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

[13] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

52. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

53. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) 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); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[14]

54. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

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

[14] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

56. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[15] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[16] Sensitive PII can sell for as much as $363 per record.[17]

57. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

58. When agreeing to pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive.

59. Through this Complaint, Plaintiff seeks redress individually, and on behalf of all similarly situated individuals, for the damages that resulted from the Data Breach.

---

[15] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[16] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[17] *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).

CLASS ALLEGATIONS

60. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

61. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All Cricket Wireless customers from May 1, 2022, to October 31, 2022 and January 2, 2023, residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was reported by Defendant (the "Class").

South Carolina Subclass

All Cricket Wireless customers from May 1, 2022, to October 31, 2022 and January 2, 2023, residing in South Carolina whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was reported by Defendant (the "South Carolina Subclass").

Georgia Subclass

All Cricket Wireless customers from May 1, 2022, to October 31, 2022 and January 2, 2023, residing in Georgia whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was reported by Defendant (the "Georgia Subclass").

62. Collectively, the Class, Georgia Subclass, and South Carolina Subclass are referred to as the "Classes" or "Class Members."

63. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has 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.

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

65. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, 10 million individuals were impacted in Data Breach.

66. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

d. Whether Defendant required its third-party vendors to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

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

i. Whether Defendant adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;

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

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

67. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

68. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, 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 for the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenges of these policies hinge on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

69. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has 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 suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

70. 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 Defendant. 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.

71. 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 for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant 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 was exposed is representative of that experienced by the Classes 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.

72. The litigation of the claims brought herein is manageable. Defendant's 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.

73. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

74. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

75. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

76. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
c. Whether Defendant's (or its vendors') security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or its vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and
g. Whether adherence to ISO/IEC 27000 series recommendations and best practices or other relevant industry standards for protecting personal information in cloud environments would have prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE*

77. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

78. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

79. Defendant gathered and stored the PII of Plaintiff and Class Members as part of telecommunications service carrier-customer relationship. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

80. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

81. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

82. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology and/or cloud environments; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited vendors for compliance with contractual and other applicable data protection obligations; (vi) provided timely notice to individuals impacted by a data breach event; and (vii) required all employees and contractors to adhere to Defendant's security requirements and regularly update those requirements.

83. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade

practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

84. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII that Defendant was no longer required to retain.

85. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

86. Defendant violated Section 5 of the FTC Act by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff's and Class Members information. Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII. Defendant's violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitutes negligence *per se.*

87. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to implement organizational controls, including multifactor authentication in cloud environments.

b. Failing to encrypt personally identifying information in transit and at rest.

c. Failing to adopt, implement, and maintain adequate security measures to safeguard PII.

d. Failing to adequately monitor the security of their cloud services vendors.

e. Allowing unauthorized access to PII.

f. Failing to detect in a timely manner that PII had been compromised.

g. Failing to remove former customers' PII it was no longer required to retain.

h. Failing to timely and adequately notify Plaintiff and 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.

i. Failing to implement data security practices consistent with Defendant's published privacy policies and standards.

88. 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 statue was intended to guard against.

89. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

90. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of strong authentication mechanisms for accessing cloud services.

91. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

92. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect PII and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

93. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted

and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

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

95. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and credit monitoring to all affected by the Data Breach.

COUNT 2: BREACH OF IMPLIED CONTRACT

96. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

97. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

98. Defendant published a Privacy Policy to inform the public about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of those products or services.

99. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

100. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

101. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

102. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on Defendant's website, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

103. As a direct and proximate result of Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

104. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and credit monitoring to all affected by the Data Breach.

COUNT 3: UNJUST ENRICHMENT

105. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

106. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

107. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant used the PII to market, advertise, and sell additional services to Plaintiff and Class Members. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit.

108. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

109. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

110. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (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) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized

disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

111. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 4: UNAUTHORIZED DISCLOSURE OF CUSTOMER PROPRIETARY INFORMATION

112. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

113. Defendant collected information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications service subscribed to by its customers, including Plaintiff and Class Members.

114. Under the Telecommunications Act of 1996, 47 U.S.C. § 222, Defendant has a duty to protect the confidentiality of customer proprietary information and is prohibited from disclosing customer information, such as call location, except as required by law or with the customer's permission.

115. Defendant failed to protect the confidentiality of Plaintiff's and Class Members' information, which resulted in customer proprietary information being disclosed to an unauthorized third party in or around April 2024.

116. Defendant violated the Telecommunications Act of 1996, 47 U.S.C. §222, by failing to use reasonable measures to protect Plaintiff's and Class Members' proprietary information from disclosure and not complying with Defendant's own security standards, privacy policy, or other applicable industry standards. Defendant's conduct was particularly unreasonable

given the nature and amount of customer proprietary information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach.

117. Defendant breached its duties to Plaintiff and Class Members under the Telecommunications Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard CPNI. Furthermore, Defendant breached its duty to: (i) conduct privacy impact assessments for each cloud services vendor; (ii) examine each vendor's reputation regarding data breaches; (iii) determine whether each vendor has obtained industry certifications for their privacy practices; (iv) assess whether each vendor has adequate security measures (technical and administrative) to protect the data being shared; (v) ensure each vendor is contractually obligated to comply with the requirements of Defendant's Privacy Policy or other privacy/security obligations concerning the data; and, (vi) monitor the vendor's practices, annually, to ensure they continue to comply with its contractual privacy obligations and industry best practices.

118. As a result of Defendant's failure to adequately protect the CPNI from unauthorized disclosure, Defendant is liable for the full amount of damages sustained in consequence of its violation of the provisions of the Telecommunications Act, together with attorneys' fees and costs. *See*, 47 U.S.C. §206.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, and certainly impending targeted messaging (calls, texts, and emails) designed to deceive Plaintiff and Class Members into disclosing sensitive information, or otherwise perpetrate identity theft crimes, fraud, and other exploitation, resulting in monetary loss and economic harm; expenses and time spent erasing

addresses, phone numbers, and other details from the internet; expenses for purchasing a secondary phone number or purchasing applications used to create a secondary phone number to keep Plaintiff and Class Members actual phone numbers hidden; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of the privacy and the confidentiality of personal information; mitigation expenses and time spent in response to the Data Breach; lost work time; lost value of the CPNI or lost value of access to the CPNI permitted by Defendant; the amount of the actuarial present value of ongoing high-quality identity defense, credit monitoring services, and dark web monitoring services made necessary as mitigation measures because of Defendant's Data Breach; lost benefit of the bargain and overcharges for services or products; attorneys' fees, nominal and general damages and other economic and noneconomic harm.

COUNT 5: VIOLATION OF GEORGIA'S UNIFORM DECEPTIVE TRADE PRACTICES ACT {OCGA § 10-1-370 *et seq.*,}

120. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

121. Plaintiff and Class Members are consumers of Defendant's products and services. Defendant collects its customers' PII in the ordinary course of providing products or services.

122. Defendant created, collected, and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

123. Under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

Such behavior by Defendant also constitutes a false, misleading, or deceptive act under Georgia's Uniform Deceptive Trade Practices Act OCGA §10-1-370 *et seq*.

124. Defendant violated OCGA §10-1-370 *et seq*., by failing to adhere to its own privacy policy regarding the confidentiality and security of Plaintiff's and Class Members information. Defendant further violated the state consumer protection statute by failing to use reasonable measures to protect PII.

125. Defendant's unfair or deceptive acts affected public interests, including those of Plaintiff and Class Members. Defendant knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendant engaged in unfair or deceptive practices by breaching its duties to provide reasonable technical and organizational data security policies, procedures, and practices. Defendant knew or should have known that it was not adhering to its published privacy policies and procedures. Had Plaintiff and Class Members known Defendant would not follow its own published security practices, they would not have purchased (or continued to purchase) Defendant's products or services.

126. Defendant's data security measures remain inadequate. Plaintiff and Class Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendant's deceptive trade practices, which places Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury.

127. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable

prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

128. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose PII would be at risk of future unauthorized disclosures.

129. As a result of the Defendant's false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff, and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

130. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and/or credit monitoring to all affected by the Data Breach.

COUNT 6: VIOLATION OF SOUTH CAROLINA'S UNFAIR TRADE PRACTICES ACT {S. C. Code Ann. §§ 39–5–10 *et seq*.,}

131. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

132. Plaintiff and Class Members are consumers of Defendant's products and services. Defendant requires its customers, including Plaintiff and Class Members, to submit PII in the

ordinary course of providing products or services.

133. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

134. Under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies. Such behavior by Defendant also constitutes a false, misleading, or deceptive act under South Carolina's Unfair Trade Practices Act S. C. Code Ann. §§ 39–5–10 *et seq*.

135. Defendant violated S. C. Code Ann. §§ 39–5–10 *et seq*., by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff's and Class Members' information. Defendant further violated the state consumer protection statute by failing to use reasonable measures to protect PII.

136. Defendant's unfair or deceptive acts affected public interests, including those of Plaintiff and Class Members. Defendant knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendant engaged in unfair or deceptive practices by breaching its duties to provide technical and organizational data security policies, procedures, and practices. Defendant knew or should have known that it was not adhering to its published privacy policies and procedures. Had Plaintiff and Class Members known Defendant would not follow its own published security practices they would not have purchased (or continued to purchase) Defendant's products or services.

137. Defendant's data security measures remain inadequate. Plaintiff and Class

Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendant's deceptive trade practices, which places Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury.

138. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

139. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose PII would be at risk of future unauthorized disclosures.

140. As a result of the Defendant's false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff, and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

141. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive

relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and/or credit monitoring to all affected by the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web monitoring services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: July 23, 2024.

By: /s/ *Thomas Sizemore*
Thomas Sizemore, Esq.
GA Bar No.: 823195
Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
thomas.sizemore@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff
**Pro Hac Vice forthcoming*

ClassAction.org
