UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

TRINA STOCKTON, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

VERIFF OU and VERIZON VALUE, INC. d/b/a TOTAL WIRELESS,

Defendants.

Case No.: _____

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Trina Stockton ("Plaintiff") brings this Class Action Complaint against Defendants Veriff OU ("Veriff") and Verizon Value, Inc. d/b/a Total Wireless ("Total Wireless", and collectively, "Defendants") individually and on behalf of all others similarly situated, and alleges, 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 that compromised Plaintiff and Class Members' personally identifiable information ("PII" or "Private Information").

2. Defendant Veriff OU is a global identity verification company that provides services to clients, including Defendant Total Wireless ("Clients" or "Defendant Veriff's Clients").

3. Defendant Total Wireless is a budget-friendly, no-contract prepaid mobile service that runs on Verizon's extensive 5G network.

4. In their ordinary course of business operations, Defendants collect, store, and maintain sensitive Private Information, and have a resulting duty to securely maintain such information in confidence.

5. Defendant Veriff experienced a cyber incident, in which an unauthorized third-party gained access to its IT Network.[1] Upon discovery, Defendant Veriff launched an investigation to determine the nature and scope of the Data Breach.[2]

6. On December 10, 2025, Defendant Veriff notified Defendant Total Wireless that certain customers Private Information was compromised as a result of the Data Breach.[3]

7. Upon information and belief, the following types of Private Information were compromised: name, government-issued ID, date of birth, and address.[4]

8. On January 9, 2026, Defendant Total Wireless began issuing notice letters ("Notice") to impacted customers.

9. Upon information and belief, customers are required to entrust Defendants, either directly or indirectly, 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 relationships have ended.

10. 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.

11. Defendants failed to adequately protect Plaintiff's and Class Members' Private Information. This unencrypted, unredacted Private Information was compromised due to Defendants'

[1] *Exhibit A*, Plaintiff's Notice Letter.
[2] *Id.*
[3] *Id.*
[4] *Id.*

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.

12. 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.

13. 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.

14. 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.

15. 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 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) 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.

16. 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

17. Plaintiff is a resident and citizen of Denver, Colorado.

18. Defendant Veriff is an Estonian corporation maintaining its principal place of business at 110 Wall St, New York, New York, 10005.

19. Defendant Total Wireless is a Delaware corporation maintaining its principal place of business at 9700 Northwest 112th Avenue Miami, Florida, 33178.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants, namely Plaintiff.

21. This Court has personal jurisdiction over Defendants because Defendant Veriff maintains its principal place of business in this District, and Defendants regularly conduct business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

22. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant Veriff's principal place of business is in this District and because substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendants

23. Defendant Veriff OU is a global identity verification company that provides services to Clients, including Defendant Total Wireless.

24. Defendant Total Wireless is a budget-friendly, no-contract prepaid mobile service that runs on Verizon's extensive 5G network.

25. In order to obtain services from Defendants, Plaintiff and Class Members were required to provide Defendants, either directly or indirectly, with their sensitive and confidential Private Information.

26. 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.

27. Upon information and belief, Defendants made promises and representations to Plaintiff and Class Members, that the Private Information collected from them 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.

28. 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.

29. 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.

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

31. Defendants 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.

32. Defendants derived a substantial economic benefit from collecting and using Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants could not provide their services to Plaintiff and Class Members.

33. 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.

B. The Data Breach

34. Defendant Veriff experienced a cyber incident, in which an unauthorized third-party gained access to its IT Network.[5] Upon discovery, Defendant Veriff launched an investigation to determine the nature and scope of the Data Breach.[6]

35. On December 10, 2025, Defendant Veriff notified Defendant Total Wireless that certain customers Private Information was compromised as a result of the Data Breach.[7]

36. Upon information and belief, the following types of Private Information were compromised: name, government-issued ID, date of birth, and address.[8]

37. On January 9, 2026, Defendant Total Wireless began issuing Notice to impacted customers.

38. Omitted from the Notice were the identity of the cybercriminals who perpetrated this Data Breach, 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 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.

39. 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.

[5] *Exhibit A*, Plaintiff's Notice Letter.
[6] *Id.*
[7] *Id.*
[8] *Id.*

40. Despite Defendants' intentional opacity about the root cause of this Data Breach, several facts may be gleaned from the statement, including: a) that this Data Breach was the work of cybercriminals; and b) an unauthorized party gained access to a database containing Plaintiff and Class Members data.

41. To be clear — there are numerous issues with Defendants Data Breach, but the deficiencies in the statement exacerbate the circumstances for victims of the Data Breach: (1) Defendants fail to state whether they were able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendants continue to maintain is secure; and (2) 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.

42. Moreover, 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.

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. 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.

C. Data Breaches Are Preventable.

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

46. 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]

47. 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, customers 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.

---

https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Jan. 20, 2026)

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders 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]

48. 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;

Id. at 3-4

Apply principle of least-privilege

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

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]

49. Given that Defendants were storing the sensitive Private Information of Plaintiff and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

50. 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 individuals, including that of Plaintiff and Class Members.

D. Defendants Acquire, Collect, and Store Private Information

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

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

[11] See https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Jan. 20, 2026)

53. 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.

54. 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.

55. 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.

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

56. 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.

57. 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.

58. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[12] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage

[12] See 2023 Data Breach Annual Report, (https://www.idtheficenter.org/wp-content/uploads/2024/01/ITRC 2023) (last visited Jan. 20, 2026)

point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

59. 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 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.

60. 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]

61. 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.

62. 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.

63. 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

[13] https://www.federalreserve.govieconres/notes/feds -notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Jan. 20, 2026).
[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Jan. 20, 2026).

foreseeable consequences that would occur if Defendants data security system were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

64. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants server(s), amounting to several thousand individuals detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. 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.

66. 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.

67. As a company in possession 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. 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.

F. Value of Personally Identifying Information.

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 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."[15]

69. 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.[16] For example, Personal Information can be sold at a price ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

70. 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, address, and Social Security number.

71. 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."[18]

72. 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.

73. 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

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id*
[17] 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-s old-on-the -dark-web-how-much-it-costs/ (last visited Jan. 20, 2026).
[18] 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 visited Jan. 20, 2026).

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 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[19]

74. 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.

G. Defendants Fail to Comply with FTC Guidelines.

75. 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.

76. 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.

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[19] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 20, 2026).

78. 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.

79. 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.

80. These FTC enforcement actions include actions against companies like Defendants.

81. 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' duties in this regard.

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

83. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to 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.

84. Upon information and belief, Defendants were at all times fully aware of their obligation to protect individuals Private Information, 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.

H. Defendants Fail to Comply with Industry Standards.

85. As noted above, experts studying cyber security routinely identify 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.

86. 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.

87. Other best cybersecurity practices that are standard in the media industry 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.

88. 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.

89. These foregoing frameworks are existing and applicable industry standards in the media industry safeguarding their employees and customers' 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.

I. Common Injuries and Damages.

90. 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 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 fail to undertake appropriate and adequate measures to protect the Private Information.

J. The Data Breach Increases Victims' Risk of Identity Theft

91. 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.

92. 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.

93. 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.

94. 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.

95. One such example, is criminals ability to piece together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[20]

96. 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

[20] "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 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 ://kreb sonsecuritv.eotn/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 visited Jan. 20, 2026).

astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

97. 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.

98. 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.

99. 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.

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

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

101. 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.

102. Thus, due to the actual and imminent risk of identity theft, Defendant Total Wireless, in its Notice, instructs Plaintiff and Class Members to protect themselves by reviewing account statements and monitoring their credit reports, in addition to enrolling in the offered free credit monitoring program.

103. Defendant Total Wireless' extensive 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.

104. 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.

105. 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.[21]

[21] 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 visited Jan. 20, 2026).

106. 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.

107. 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."

L. Diminution of Value of Private Information.

108. Private Information is a valuable property right.[22] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

109. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[23]

110. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker

[22] See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 20, 2026).

[23] 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 visited Jan. 20, 2026).

who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[24]

111. 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 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.

112. 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 were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

114. 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.

115. 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 of individuals detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

[24] https://digi.me/what-is-digime/ (last visited Jan. 20, 2026).

116. 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.

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

117. 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.

118. 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.

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

120. 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.

N. Loss of Benefit of the Bargain.

121. Furthermore, Defendants poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain, goods and/or services from Defendants under

certain terms, Plaintiff and other reasonable individuals 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.

O. Plaintiff's Experience

122. Plaintiff is a customer of Defendant Total Wireless.

123. As a condition of obtaining services from Defendant Total Wireless, Plaintiff was required to provide Defendants, either directly or indirectly, her Private Information.

124. Defendants were in possession of Plaintiff's Private Information before, during, and after the Data Breach.

125. On or around January 9, 2026, Plaintiff received Notice that her Private Information was compromised as a result of the Data Breach.

126. Plaintiff reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she believed that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

127. Plaintiff greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

128. Plaintiff stores any and all documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

129. As a consequence of and following the Data Breach, Plaintiff has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

130. Subsequent to the Data Brech, Plaintiff received alerts that unauthorized individuals attempted to use her debit card on multiple occasions.

131. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendants' delay in noticing her of the fact that her Private Information was acquired by criminals as a result of the Data Breach.

132. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

134. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed

and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendants did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and likely published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that Defendants obtained from Plaintiff and (g) other economic and non-economic harm.

CLASS ACTION ALLEGATIONS

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

136. The Class that Plaintiff seeks to represent is 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 and received a Notice Letter from Defendant (the "Nationwide Class").

137. 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.

138. 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.

139. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

140. 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, at least hundreds of 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).

141. 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.

142. Typicality. Plaintiff's claims are typical of those of the other members of the Class 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 Class.

143. 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.

144. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she 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 she has suffered is 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.

145. 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 companies, 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.

146. 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 was 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.

147. 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.

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

149. 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.

150. 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.

151. Likewise, particular issues under Rule 23(c)(2) 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 Defendants failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard individuals Private Information; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

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

152. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 151, as if fully set forth herein.

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

154. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of their ordinary course of business.

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

156. 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.

157. 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 had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

158. Defendants 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.

159. Defendants 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.

160. 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 receiving services.

161. 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.

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

163. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

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

165. 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.

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard 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 Private Information it was no longer required to retain 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.

167. 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.

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

169. 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.

170. 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.

171. 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.

172. 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.

173. 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.

174. 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.

175. 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.

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

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

178. 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.

179. 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.

180. 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.

181. 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.

182. 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 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) 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.

183. 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.

184. 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.

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

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

187. 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 against Defendants)

188. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 151, as if fully set forth herein.

189. 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 Defendant's duty.

190. 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.

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

192. 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.

193. 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.

194. 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 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) 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.

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

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class against Defendants)

196. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 151, as if fully set forth herein.

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

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

199. 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.

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

201. 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 not have entrusted their Private Information at Defendants.

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

203. Defendants enriched themselves by saving the costs it 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.

204. 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.

205. 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 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) 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.

206. 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 wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

207. 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 IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class against Defendant Veriff)

208. Plaintiff restates and re-alleges all of the allegations stated above in paragraphs 1-151, as if fully set forth herein.

209. Defendant Veriff entered into contracts, written or implied, with its Clients, including Defendant Total Wireless, to perform services. Upon information and belief, these contracts are virtually identical between and among Defendant Veriff and its Clients around the country whose customers, including Plaintiff and Class Members, were affected by the Data Breach.

210. In exchange, Defendant Veriff agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

211. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant Veriff and its Clients. Defendant Veriff knew that if it were to breach these contracts with its Clients, its Clients' customers—Plaintiff and Class Members—would be harmed.

212. Defendant Veriff breached the contracts it entered into with its Clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

213. Plaintiff and the Class were harmed by Defendant Veriff's breach of its contracts with its Clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

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

PRAYER FOR RELIEF

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

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

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 Defendant 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 Defendant 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 its 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 their 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 S0C 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: January 20, 2026

Respectfully submitted,

By: */s/ Courtney Maccarone*

Courtney Maccarone (NY Bar No. 5030150)
KOPELOWITZ OSTROW P.A.
1 W Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
maccarone@kolawyers.com

Counsel for Plaintiff and the Proposed Class