UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

DARREN BARCOMB, DAVID SETTERS, CHARISE CARSON, JAYNAE COLE, JOSHUA DAVIS, RAVEN HARDEN, and MICHAEL BROADUS, individually and on behalf of others similarly situated, Plaintiffs, v. TRACFONE WIRELESS, INC, Defendant.	Civil Action No. **TRIAL BY JURY DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Darren Barcomb, David Setters, Charise Carson, Jaynae Cole, Joshua Davis, Raven Harden, and Michael Broadus (each a "Plaintiff" and collectively "Plaintiffs"), individually and on behalf of similarly situated persons defined below, allege the following against Defendant TracFone Wireless, Inc. ("Defendant" or "TracFone") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against TracFone for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former TracFone customers' confidential information from hackers.

2. TracFone is an American mobile phone provider and wireless service, and a wholly owned subsidiary of Verizon Wireless. Straight Talk Wireless, Simple Mobile, Net10 Wireless, Walmart Family Mobile, and Total Wireless are brand names owned and used by TracFone primarily to sell mobile phone services through stores and online.

3. On or before December 2021, hackers gained access to the personally identifiable information ("PII") and customer proprietary network information ("CPNI") (collectively, "confidential information") of thousands of TracFone customers (the "Data Breach") and used that confidential information to engage in widespread "port-out fraud." A user "ports" a mobile phone number when he or she transfers that number from one mobile service provider to another. It appears that the hackers used the confidential information to port class member mobile phone numbers to new accounts with other service providers without the TracFone customer's knowledge or permission. Not only does the transfer render the TracFone customer unable to use their mobile phone, but it opens the customer up to significant additional fraud. For example, once in full control of TracFone customers' mobile phone numbers, and with the use of their stolen confidential information, the hackers were able to access other accounts, such as email and financial accounts. On information and belief, the Data Breach is currently ongoing, and TracFone has failed to secure its internal systems.

4. The Data Breach meant that thousands of TracFone customers were without their mobile phone, unable to conduct business, and had their financial accounts compromised over the holidays.

5. Even though TracFone is aware of the Data Breach, it has misled customers as to the nature of the Data Breach and failed to take reasonable steps to mitigate customers' damages. In some cases, TracFone refused to take action to restore customers' phone numbers (for which customers had already paid) unless customers paid additional fees to TracFone, thereby profiting from the Data Breach and its own negligence.

6. Not only did hackers access customers' confidential information, on information and belief, the confidential information is currently up for sale on the dark web. Hackers frequently

offer for sale the unencrypted, unredacted, stolen information to criminals. Because of Defendant's Data Breach, it is believed that the customers' confidential information is still available on the dark web for criminals to access and abuse. As a result, the affected customers face a lifetime risk of identity theft.

7. Clearly, Tracfone failed to safeguard Plaintiffs' and other customers' confidential information.

8. Plaintiffs and similarly situated TracFone customers (the "Class Members" or the "Class") have suffered injury because of TracFone's conduct. The injuries suffered by Plaintiffs and the proposed Classes as a direct result of the Data Breach include, *inter alia*:

a. Theft of their confidential information;

b. Costs associated with the detection and prevention of identity theft;

c. Direct costs, and costs associated with time spent and the loss of productivity from having to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

d. The imminent and certainly impending injury flowing from fraud and identity theft posed by their confidential information being placed in the hands of criminals, which has already been misused via the port out fraud and the sale of Plaintiffs and the Class Members' information on the Internet black market;

e. Damages to and diminution in value of their confidential information entrusted to TracFone with the mutual understanding that TracFone would

safeguard Plaintiffs and the Class Members' data against theft and not allow access to and misuse of their confidential information by others;

f. Continued risk to their confidential information, which remains in the possession of TracFone, and which is subject to further breaches so long as TracFone continues to fail to undertake appropriate and adequate measures to protect Plaintiffs' and the Class Members' data in its possession;

g. Damages resulting from TracFone failing to provide mobile services for which Plaintiffs and the Class Members had paid;

h. Damages resulting from disruptions to their personal lives and businesses resulting from the Data Breach and the deactivation of their phone numbers; and

i. TracFone's failure to mitigate, and its own exacerbation of, the above damages by hiding information from customers or affirmatively misleading them regarding the Data Breach.

9. Plaintiffs bring this action on behalf of all persons whose confidential information was compromised due to TracFone's failure to: (i) adequately protect its users' confidential information, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor its internal systems for security vulnerabilities and incidents. Tracfone's conduct violates federal and state statutes.

II. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one member of the class is a citizen of a state different from TracFone.

11. This Court has personal jurisdiction over TracFone because it regularly conducts business in New York, has sufficient minimum contacts in New York, and intentionally avails itself of this jurisdiction by marketing and selling products and services in New York.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, including (upon information and belief) the Data Breach. TracFone caused harm to Plaintiffs and the Class Members through its actions in this District.

III. PARTIES

13. Plaintiff Darren Barcomb ("Plaintiff Barcomb") is a citizen of New York residing in Plattsburgh. Plaintiff Barcomb is a TracFone Customer and Straight Talk user (phone number: 518-335-XXXX).

14. Plaintiff David Setters ("Plaintiff Setters") is a citizen of Pennsylvania, residing in Dillsburg. Plaintiff Delcambre is a TracFone customer and Straight Talk user (phone number: 717-919-XXXX).

15. Plaintiffs Charise Carson ("Plaintiff Carson") is a citizen of Wisconsin residing in Kenosha. Plaintiff Carson is a TracFone customer and Straight Talk user (phone number: 262-771-XXXX).

16. Plaintiff Jaynae Cole ("Plaintiff Cole") is a citizen of Kansas residing in Manhattan. Plaintiff Cole is a TracFone customer and Net10 wireless user (phone number: 562-884-XXXX).

17. Plaintiff Joshua Davis ("Plaintiff Davis") is a citizen of Missouri residing in Odessa. Plaintiff Davis is a TracFone customer and Simple Mobile user (phone number: 816-263-XXXX).

18. Plaintiff Raven Harden ("Plaintiff Harden") is a citizen of Indiana residing in Gary. Plaintiff Harden is a TracFone customer and Total Wireless user (phone number: 773-701-XXXX).

19. Plaintiff Michael Broadus ("Plaintiff Broadus") is a citizen of Alabama residing in Mobile. Plaintiff Broadus is a TracFone customer and Walmart Family Mobile user (phone number: 251-605-XXXX).

20. Defendant TracFone Wireless, Inc. is a corporation organized under the laws of the State of Delaware, with a principal place of business at 9700 NW 112TH Ave., Miami, FL 33178. TracFone is a wholly owned subsidiary of Verizon Communications. TracFone advertises its services and sells products to customers nationwide through its website and various other channels, including Straight Talk, Simple Mobile, Net10 Wireless, Walmart Family Mobile, and Total Wireless.

IV. FACTUAL ALLEGATIONS

A. TracFone's Personal Information Collection Practices

21. TracFone is a mobile phone service provider known for providing prepaid no-contract mobile services to its customers. Straight Talk Simple Mobile, Net10 Wireless, Walmart Family Mobile, and Total Wireless are brand names for non-contract mobile services provided by TracFone and sold through stores nationwide.

22. As is the case with most mobile phone service providers, when a new customer signs up for mobile phone service through Defendant, the customer needs to provide a substantial amount of confidential information, including in most situations highly sensitive confidential information, such as the customers' home address, social security number, and/or credit or debit card information.

23. With regard to the confidential information, the TracFone website refer customers to the same "TracFone Wireless, Inc. Privacy Policy" (the "Privacy Policy").[1] The Privacy Policy opens up by stating in no uncertain terms: "TracFone Wireless, Inc. … is committed to your privacy." It says that the policy exists to inform "our customers, website visitors, and mobile application users" about their "rights" with regard to their data. It goes on to state that the Privacy Policy also exists "to inform you of the types and categories of personal information that TracFone, including its brands, affiliates, vendors, and service providers collect, use, share, and retain."

24. The Privacy Policy states that TracFone collects various types of confidential information, including but not limited to, customer name, alias, postal address, telephone number, e-mail address, partial or full social security number, telephone numbers, signature, credit or debit card information, credit or debit card expiration dates, and other financial records.

25. In its Privacy Policy, TracFone promises to only disclose customers' information in limited circumstances. Further, TracFone also claims that it "uses administrative, organizational, technical, and physical safeguards to protect the personal information it collects and processes," and that "TracFone, based on its reasonable judgment, will continue to enhance its security procedures as new technology becomes readily available."

B. <u>The Data Breach</u>

26. Despite Tracfone's representation that it had implemented several safeguards, Tracfone filed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and the Class Members' confidential information.

[1] *See* https://www.tracfonewirelessinc.com/en/Privacy+Policy/ (last visited on Nov. 15, 2024).

27. On or before December 2021, hackers gained access to the confidential information of TracFone customers, including Plaintiffs and Class Members.

28. Thereafter, the hackers used Plaintiffs and Class Members' confidential information to engage in a widespread port-out fraud. The hackers deactivated Plaintiffs and Class Members' TracFone accounts and ported their mobile phone numbers to other mobile phone service providers, including MetroPCS. Once in control of Plaintiffs and Class Members' mobile phone numbers, the hackers went to third parties, such as banks, social media companies, and credit card companies, and utilized what is commonly referred to as a 2-step verification code process (which allows users to access accounts through receiving a code sent to their mobile phone number) to access Plaintiffs and Class Members' other accounts, including but not limited to emails and financial accounts.

29. The Federal Communications Commission ("FCC") describes "port-out fraud" as follows:

> One way to hijack your phone number is through a porting-out scam. Mobile phone numbers can legally be ported from one provider to the next when you switch your phone service. Phone companies have established safeguards to protect this process, such as having account holders set up a PIN or a password they must provide when calling about their account. But scammers with enough of your personal information can interfere, hijacking your phone number and with it your identity.
>
> Scammers go after their target's personal information, such as their name, address, birth date, PINs or passwords, and the last four digits of their Social Security number. Scammers may try to get this information by calling their target and impersonating a trusted business or institution, then asking a series of questions to gather as much data as possible. In some cases, the information may already be stolen and available on the dark web.
>
> When scammers initiate a porting request, they con the victim's phone company into believing the request is from the authorized account holder. If the scam is successful, the phone number will be ported to a different mobile device or service account set up by the

> scammer. This typically begins a race where the scammer, by receiving the victim's private texts and calls, tries to reset the access credentials for as many of the victim's financial and social media accounts as possible before the victim realizes they have lost service on their device. Once the scammer has access, they attempt to drain the victim's bank accounts. In another variation, they attempt to sell or ransom back to the victim access to their social media accounts.[2]

30. Even though on information and belief TracFone became aware of the Data Breach relatively soon after it occurred, it has misled customers as to the nature of the Data Breach and failed to take reasonable steps to mitigate customers' damages. In some cases, TracFone has even refused to take action to restore customers' phone numbers (for which customers had prepaid plans) unless customers pay additional fees to TracFone, thereby allowing TracFone to profit from the Data Breach and TracFone's own unlawful conduct.

31. Not only did hackers access customers' confidential information, on information and belief, the confidential information is currently up for sale on the dark web. Hackers frequently offer for sale the unencrypted, unredacted, stolen confidential information to criminals. Because of Defendant's Data Breach, it is believed that the Class Members' confidential information is still available on the dark web for criminals to access and abuse. As a result, the affected Class Members face a lifetime risk of identity theft.

C. Plaintiff Barcomb's Allegations

32. On or around November 22, 2021, Plaintiff Barcomb paid $143.42 to TracFone for mobile phone service until on or around March 22, 2022.

33. On or around December 21, 2021, Plaintiff Barcomb's TracFone account was deactivated and his mobile phone number was fraudulently ported to MetroPCS without his

[2] *Port Out Fraud Targets Your Private Accounts*, FEDERAL COMMUNICATIONS COMMISSION (SEPT. 16, 2019), https://www.fcc.gov/port-out-fraud-targets-your-private-accounts (last visited on Nov. 15, 2024).

knowledge or permission. Shortly afterwards, hackers attempted to access his financial accounts, including Coinbase.

34. Plaintiff Barcomb called TracFone and they told him that his number was ported, but that TracFone would resolve the issue within 24 hours.

35. In the weeks following this initial call with TracFone, Plaintiff Barcomb spent countless hours over the following week on the phone with TracFone, and they continued to provide false assurances until his number was returned to him on or around December 27, 2021.

36. TracFone never informed Plaintiff Barcomb of the Data Breach and did not warn him of any risks to his financial accounts as a result of the Data Breach.

37. Plaintiff Barcomb uses his TracFone mobile phone for personal and business uses. The Data Breach disrupted his ability to speak with family and friends over the holidays.

38. Plaintiff Barcomb is a police officer and provides his own cell phone for use on the job. The Data Breach greatly disrupted his work, since his access to several applications was setup through his TracFone mobile phone number. It took him several days to resolve these issues.

39. In an attempt to mitigate his damages, Plaintiff Barcomb purchased a prepaid phone from AT&T for $96.12.

D. Plaintiff Setters' Allegations

40. Plaintiff Setters paid $55 to Straight Talk for wireless service.

41. As a result of the breach, Plaintiff Setters was without cell phone service for 22 days.

42. Plaintiff Setters was ultimately the victim of identity theft when his Coinbase account was hacked and the funds removed, funds that were to be used for the purchase of a new home.

43. Plaintiff Setters has had to spend countless hours on phone with non-responsive and misleading outsourced overseas Straight Talk reps (representing incident as a glitch while knowingly misleading and stalling identity theft victims).

44. Plaintiff Setters has further had to spend countless hours filing formal complaints with Straight Talk Legal in Miami, Coinbase, Pennsylvania Attorney General Consumer Affairs, Local Police Department, BBB, FTC, and the FBI.

45. Nevertheless, TracFone has not taken the necessary action to recover Plaintiff Setters' mobile phone number. Since Plaintiff Setters' mobile phone number has been associated with fraud. While TracFone continuously assures Plaintiff Setters that it has taken the necessary actions and will restore his services imminently, Straight Talk has confirmed to Plaintiff Setters that this is false.

46. Instead of restoring Plaintiff Setters' stolen service, Plaintiff was forced to spend $265 on a new phone and service provider.

47. Plaintiff Setters' financial well-being has been severely damaged and will continue to be damaged because of the Data Breach. Plaintiff Setters' Coinbase investment accounts are linked to his mobile phone number, which ultimately enabled the wrongdoers to access Plaintiff Setters Coinbase account and remove the $22,385 within it. Thus, Plaintiff Setters has tangible financial losses because of the Data Breach.

E. Plaintiff Carson's Allegations

48. Plaintiff Carson was a Straight Talk Wireless customer.

49. As a result of the Data Incident, Plaintiff Carson was without cell service for 6 days.

50. As a result of this loss of service, Plaintiff Carson experienced a $200 loss in business revenue, which is tied to her Straight Talk Wireless number.

51. Plaintiff Carson also had to buy a cheap phone until she was able to use her original number again.

52. In the weeks following the Data Incident, Plaintiff Carson has had to spend at least 10 hours dealing with attempting to get access to her original number and ensuring no fraudulent activity is occurring on any accounts linked to her Straight Talk Wireless number.

F. Plaintiff Cole's Allegations

53. Plaintiff Cole was a customer of Net10 Wireless and Tracfone.

54. Due to the Data Incident, Plaintiff Cole was without cellphone service for 60 days.

55. Plaintiff Cole has spent 8 hours dealing with the repercussions of the Data Incident, including conversations with Net10 wireless and monitoring her accounts tied to her phone number for fraudulent activity.

56. Plaintiff Cole also lost $360.00 in business income, as she used her phone for her business, as well as an additional $120 for a new phone and service provider as a result of this breach.

G. Plaintiff Davis' Allegations

57. Plaintiff Davis was a customer of Simple Mobile and Tracfone.

58. As a result of the Data Incident, Plaintiff Davis was without cellphone service for 2 days.

59. Plaintiff Davis has had to spend upwards to three hours on dealing with the repercussions of the Data Incident, including contacting Simple Mobile and monitoring his accounts tied to his wireless number for fraudulent activity.

60. Plaintiff Davis also had to spend $125 to get a new phone and wireless service provider.

H. Plaintiff Harden's Allegations

61. Plaintiff Harden was a customer of Total Wireless and Tracfone.

62. As a result of this Data Incident, Plaintiff Harden was without wireless service for 90 days.

63. Plaintiff Harden has had to spend at least 3 hours dealing with the repercussions of the Data Incident, including conversations with Total Wireless and monitoring her accounts tied to her Total Wireless number for fraudulent activity.

64. Plaintiff Harden also had to purchase a new phone to put a Sim Card in to restore her wireless service.

I. Plaintiff Broadus' Allegations

65. Plaintiff Broadus was a Tracfone and Walmart Family Mobile user.

66. As a result of the Data Incident, Plaintiff Broadus was without cellphone service for around 6 months off and on, which required Plaintiff Broadus to purchase a new phone in an attempt to restore service.

67. Ultimately, this step would only provide temporary relief, resulting in Plaintiff Broadus purchasing multiple phones.

68. Plaintiff Broadus has had to spend at least 5 hours dealing with the repercussions of the Data Incident, including conversations with Walmart Family Mobile and Tracfone to make sure his account was secure and wireless services available.

69. Plaintiff Broadus had difficulties performing his job as loss prevention at Walmart as a result of his inability to use his wireless phone.

70. Plaintiff Broadus ultimately had expenditures purchasing new phones for wireless service so he could go back to work.

J. TracFone's Legal Duty To Protect Customer Information, Including CPNI, Under the FCA.

71. TracFone is a large telecommunications company and provider of mobile phone services. As a common carrier,[3] TracFone is governed by the Federal Communications Act of 1934, as amended ("FCA"),[4] and corresponding regulations passed by the FCC.[5]

72. Recognizing the sensitivity of data collected by cell carriers, the FCA requires TracFone and other similar carriers to protect Plaintiffs and the Class Members' sensitive personal information to which it has access because of its unique position as a telecommunications carrier.[6]

73. Section 222 of the FCA requires TracFone to protect the privacy and security of information relating to its customers. Likewise, Section 201(b) of the FCA requires TracFone's practices related to the collection of information from its customers to be "just and reasonable," and declares unlawful any practice that is "unjust or unreasonable."[7]

74. The FCA also imposes more specific obligations on TracFone with regard to protecting customers' CPNI.[8] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[9]

75. Under the FCA, TracFone is liable for failures to protect its customers from unauthorized disclosures.[10] The FCC has also stated that "[t]o the extent that a carrier's failure to

[3] 47 U.S. Code § 153(51).
[4] 47 U.S.C. § 151 *et seq.*
[5] 47 C.F.R. § 64.2001 *et seq.*
[6] 47 U.S.C. § 222.
[7] 47 U.S.C. § 201(b).
[8] 47 U.S.C. § 222(a).
[9] Report and Order and Further Notice of Proposed Rulemaking, In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").
[10] 47 U.S.C. §§ 206, 207.

take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred."[11]

76. The FCA defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[12]

77. TracFone is not just liable for its own violations of the FCA, but also for violations that it "cause[s] or permit[s]."[13] By failing to secure Plaintiffs and the Class Members' accounts and protect their CPNI, TracFone has caused and/or permitted their CPNI to be accessed and used by third-party hackers.

78. TracFone also knew, or should have known, about the risk of port-out fraud presented to its customers. Port-out fraud has been a widespread problem for years. Indeed, on September 30, 2021, the FCC began rulemaking to combat port-out fraud.[14] The notice states that

[11] Declaratory Ruling, In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information, 28 F.C.C. Rcd. 9609 ¶ 30 (2013).
[12] 7 U.S.C. § 222(h)(1).

[13] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

[14] *See FCC Combating Scams Used to Commandeer Consumers' Cell Phone Accounts*, FEDERAL COMMUNICATIONS COMM'N (Sept. 30, 2021), https://www.fcc.gov/document/fcc-combating-scams-used-commandeer-consumers-cell-phone-accounts (last visited on Nov. 15, 2024).

"[t]he FCC has received numerous complaints from consumers who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. In addition, recent data breaches have exposed customer information that could potentially make it easier to pull off these kinds of attacks."

79. TracFone knew or should have known that it needed to take steps to protect its customers. The Federal Trade Commission ("FTC") published a report in 2016 stating that "mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking[.]"[15] The FTC urged carriers such as TracFone to "adopt a multilevel approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions." The FTC also specifically warned carriers, including TracFone, of the risk that, due to text message password reset requests and two-factor authentication, phone account hijacking put subscribers at risk of financial loss and privacy violations:

> Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen your phone number. Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.

[15] Lori Cranor, *Your mobile phone account could be hijacked by an identity thief*, FEDERAL COMMUNICATIONS COMM'N (June 7, 2016), https://www.ftc.gov/comment/605903 (last visited on Nov. 15, 2024).

K. FTC and NIST Guidelines on Protecting Customer Personal Information

80. Recently, the FTC has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act ("FTCA") (codified by 15 U.S.C. § 45).

81. Under the FTCA, TracFone is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.

82. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide").[16] In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of confidential information that is no longer needed;
- Businesses should encrypt confidential information on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and

[16] *See FTC Unveils Practice Suggestions for Businesses on Safeguarding Personal Information*, FEDERAL TRADE COMM'N (Mar. 8, 2007), https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding (last visited on Nov. 15, 2024).

- Businesses should have an emergency plan prepared in response to a breach.

83. On information and belief, TracFone failed to adequately address the foregoing requirements in the FTC Guide.

84. In 2015, the FTC supplemented the FTC Guide with a publication called "Start with Security" (the "Supplemented FTC Guide").[17] This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep confidential information stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and
- Businesses should be continuously monitoring for suspicious activity on their network.

85. Again, TracFone apparently failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

86. The FTC Guide is clear that businesses should, among other things: (1) protect the confidential information they acquire; (2) properly dispose of confidential information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large

[17] *Start with Security: A Guide for Business*, FEDERAL TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on Nov. 15, 2024).

amounts of data being transmitted from the system.[18] Plaintiffs believe that TracFone did not follow these recommendations and, as a result, exposed thousands of consumers to harm.

87. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

88. TracFone knew or should have known about its obligation to comply with the FTCA, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

89. Thus, among other things, TracFone's misconduct violated the FTCA and the FTC's data security pronouncements, led to the Data Breach, and resulted in harm directly and proximately to Plaintiffs and the Class Members.

90. Additionally, the National Institute of Standards and Technology ("NIST") provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities.[19] Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

---

[18] *See, e.g.*, *id.*; *see also Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Nov. 15, 2024).

[19] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited on Nov. 15, 2024).

91. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[20]

92. TracFone's failure to protect massive amounts of confidential information throughout breach period belies any assertion that TracFone employed proper data security protocols or adhered to the spirit of the NIST guidance.

L. Value of Personally Identifiable Information

93. Confidential information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that confidential information has considerable market value.

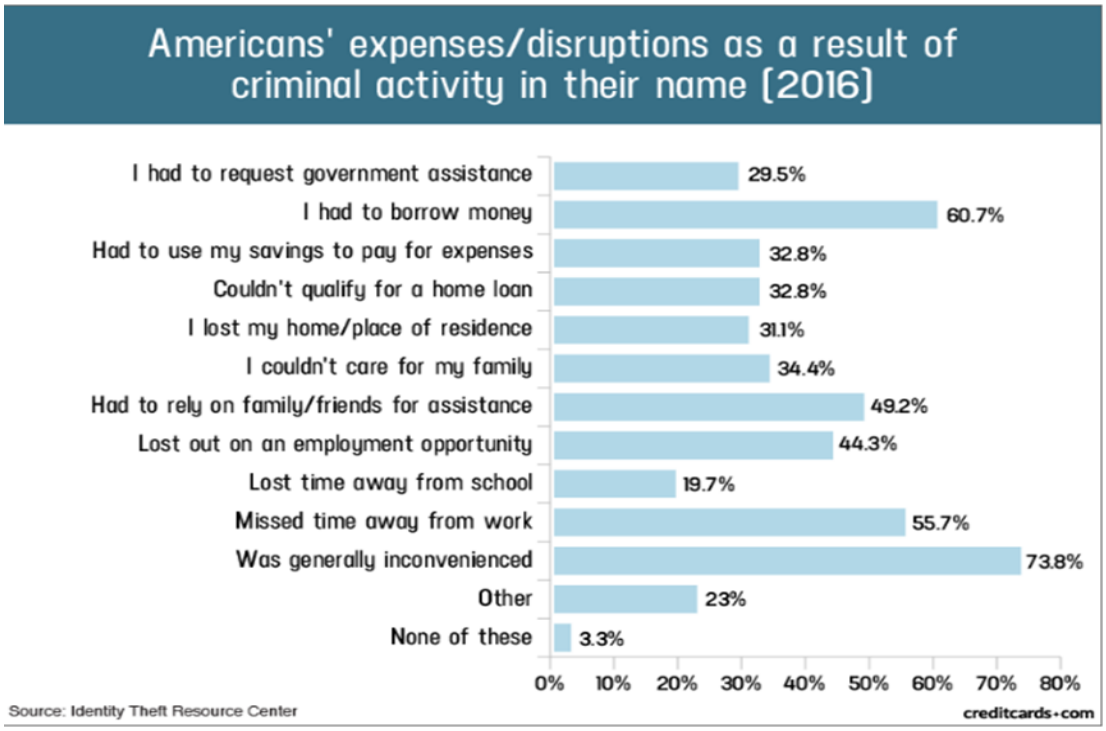
94. The confidential information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, confidential information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on

[20] *Id*. at Table 2 pg. 36-43.

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Nov. 15, 2024).

a fraud victim) sold for $30 in 2017.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

95. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of confidential information.[24] [Chart on next page]



96. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when confidential information is stolen and when it is used. According to the U.S. Government Accountability Office, 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,

---

[22] *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 on Nov. 15, 2024).

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on Nov. 15, 2024).

[24] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Nov. 15, 2024).

> 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.[25]

97. Therefore, given the importance of safeguarding confidential information and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach, TracFone was, or should have been, fully aware of its responsibilities towards protecting customer confidential information.

M. Damage to Plaintiffs and the Class Members Caused by the Data Breach

98. Plaintiffs and Class Members have been damaged because their confidential information was accessed by hackers in the Data Breach.

99. Plaintiffs and the Class Members have or will suffer actual injury as a direct result of the Data Breach.

100. As a direct and proximate result of TracFone's conduct, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiffs now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives.

101. TracFone has yet to issue a public notification to customers that their confidential information has been compromised. Further, TracFone appears to be doing nothing to remedy the harm caused by the Data Breach.

[25] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, Government Accountability Office (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited on Nov. 15, 2024).

102. Plaintiffs and the Class Members may also incur out-of-pocket costs for protective measures such as purchase of an alternative mobile phone number, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

103. Plaintiffs and the Class Members also suffered a loss of value of their confidential information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

104. Plaintiffs and the Class Members were also damaged via benefit-of-the-bargain damages. First, the Class Members paid for mobile phone service which they did not receive when their accounts were deactivated by TracFone. Second, the contractual bargain, express or implied, entered into between Plaintiffs and TracFone included TracFone's contractual obligation to provide adequate data security, which TracFone failed to provide. Thus, Plaintiffs and the Class Members did not get what they paid for.

105. Plaintiffs and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their confidential information;

b. Improper disclosure of their confidential information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' confidential information being placed in the hands of criminals and misused via the sale of such information on the Internet black market;

d. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, and the stress,

nuisance and annoyance of dealing with all issues resulting from the Data Breach;

e. Damages to and diminution in value of their confidential information entrusted to TracFone with the mutual understanding that TracFone would safeguard Plaintiffs and the Class Members' data against theft and not allow access to and misuse of their confidential information by others;

f. Continued risk to their confidential information, which remains in the possession of TracFone, and which is subject to further breaches so long as TracFone continues to fail to undertake appropriate and adequate measures to protect Plaintiffs and the Class Members' data in its possession;

g. Damages resulting from TracFone failing to provide mobile services for which Plaintiffs and the Class Members had paid;

h. Damages resulting from disruptions to their personal lives and businesses resulting from the Data Breach and the deactivation of their phone numbers; and

i. TracFone's failure to mitigate, and its exacerbation of, the foregoing damages by hiding information from customers or affirmatively misleading them regarding the Data Breach.

j. Ascertainable losses in the form of deprivation of the value of customers' confidential information for which there is a well-established and quantifiable national and international market.

V. CLASS ALLEGATIONS

106. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated.

107. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**: All individuals residing in the United States who had any confidential information compromised as a result of the Data Breach.

108. Excluded from each of the above Class are Defendant and their parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

109. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class, as well as add state subclasses, before the Court determines whether certification is appropriate.

110. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

111. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of at least thousands of TracFone customers whose confidential information was compromised in the Data Breach.

112. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether TracFone engaged in the conduct alleged herein;

b. Whether TracFone's conduct violated the consumer protection laws invoked below;

c. When TracFone actually learned of the Data Breach and whether its response was adequate;

d. Whether TracFone had a legal duty to adequately protect Plaintiffs and the Class Members' confidential information;

e. Whether TracFone breached its legal duty by failing to adequately protect Plaintiffs and the Class Members' confidential information;

f. Whether TracFone implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs and the Class Members' confidential information;

g. Whether TracFone knew or should have known that it did not employ reasonable measures to keep Plaintiffs and the Class Members' confidential information secure and prevent loss or misuse of that confidential information;

h. Whether TracFone adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

i. Whether Plaintiffs and the Class Members are entitled to recover actual and/or statutory damages;

j. Whether TracFone had a policy or practice of failing to mitigate, or of exacerbating, customers' damages following a hack like the Data Breach;

k. Whether Plaintiffs and the other Class Members are entitled to credit or identity monitoring and are entitled to other monetary relief; and

l. Whether Plaintiffs and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

113. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' confidential information, like that of every other Class Member, was compromised in the Data Breach.

114. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data breach class actions.

115. Predominance. TracFone has engaged in a common course of conduct toward Plaintiffs and the Class Members, in that all Plaintiffs' and the Class Members' confidential information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from TracFone's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

116. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact will be superior to multiple individual actions or piecemeal litigation. There is a significant cost to litigating a data breach matter. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for TracFone. In contrast, the conduct of this

action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

117. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). TracFone has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

118. Finally, all Class Members are readily ascertainable because TracFone has access to their confidential information.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

119. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

120. TracFone solicited and gathered confidential information of Plaintiffs and the Nationwide Class.

121. TracFone knew, or should have known, of the risks inherent in collecting the confidential information of Plaintiffs and the Class Members and the importance of adequate security. On information and belief, TracFone received warnings that hackers routinely attempt to access and acquire confidential information without authorization. TracFone also knew or should have known about numerous, well-publicized data breaches involving other financial services companies. TracFone also knew or should have known of the risks of port-out fraud.

122. TracFone owed a duty of care to Plaintiffs and the Class Members whose confidential information was entrusted to it. TracFone's duties included, but are not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting confidential information in its possession;

b. To protect customers' confidential information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

d. To implement processes to prevent widespread port-out fraud against its customers.

123. By collecting confidential information, and using it for commercial gain, TracFone had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of the confidential information, and to safeguard the confidential information from theft.

124. Because TracFone knew, or should have known, that a breach of its systems would potentially damage thousands of customers, including Plaintiffs and the Class Members, it had a duty to adequately protect their confidential information.

125. TracFone owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

126. TracFone knew, or should have known, that its systems did not adequately safeguard the confidential information of Plaintiffs and the Class Members.

127. TracFone breached its duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the confidential information of Plaintiffs and the Class Members.

128. TracFone had a special relationship with Plaintiffs and the Class Members. Plaintiffs and the Class Members' willingness to entrust TracFone with their confidential information was predicated on the understanding that TracFone would take adequate security precautions. Moreover, only TracFone had the ability to protect its systems (and the confidential information that it stored on them) from attack.

129. TracFone's own conduct also created a foreseeable risk of harm to Plaintiffs' and the Class Members' confidential information. On information and belief, TracFone's misconduct included failing to:

a. Secure its customer support systems;

b. Secure access to its servers;

c. Comply with industry standard security practices;

d. Employ adequate network segmentation;

e. Implement adequate system and event monitoring;

f. Install updates and patches in a timely manner; and

g. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

130. TracFone also had independent duties under federal and state laws that required it to reasonably safeguard Plaintiffs and the Class Members' confidential information.

131. TracFone breached the duties it owed to Plaintiffs and the Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect confidential information both before and after learning of the Data Breach; and

c. By failing to comply with the minimum industry data security standards during the Data Breach.

132. But for TracFone's wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their confidential information either would not have been compromised or they would have been able to prevent some or all of their damages.

133. As a direct and proximate result of TracFone's negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

134. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was reasonably foreseeable.

135. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was the direct and proximate result of TracFone's negligent conduct.

136. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class)

137. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

138. Pursuant to Section 5 of the FTCA, 15 U.S.C. § 45, TracFone had a duty to provide fair and adequate computer systems and data security to safeguard the confidential information of Plaintiffs and the Class Members.

139. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as TracFone, of failing to use reasonable measures to protect confidential information. The FTC publications

and orders described above also form part of the basis of TracFone's duty in this regard. TracFone solicited, gathered, and stored confidential information, of its customers to provide financial services which affect commerce. TracFone violated the FTCA by failing to use reasonable measures to protect confidential information of Plaintiffs and the Class, and by not complying with applicable industry standards as described herein.

140. Pursuant to the FCA, 47 U.S.C. § 222(a), TracFone had a duty to protect the confidentiality of proprietary information of customers. TracFone violated this duty by failing to protect Plaintiffs and the Class Members from the Data Breach.

141. Pursuant to the FCA, 47 U.S.C. § 222(b), TracFone had a duty to prevent unauthorized access to customers' CPNI. TracFone violated this duty by failing to protect Plaintiffs and the Class Members CPNI from unauthorized access in the Data Breach.

142. TracFone's violation of the above-mentioned laws constitutes negligence *per se*.

143. Plaintiffs and the Class Members are within the class of persons that the above laws were intended to protect.

144. The harm that occurred as a result of the Data Breach is the type of harm the above laws were intended to guard against. For example, 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 suffered by Plaintiffs and the Class Members.

145. As a direct and proximate result of TracFone's negligence *per se*, Plaintiffs and the Class Members have suffered, and continue to suffer, injuries and damages from, *inter alia*, the loss of their data, their vulnerability to identity theft, and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

146. TracFone breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' confidential information.

147. TracFone's violation of the above-mentioned laws constitutes negligence *per se*.

148. But for TracFone's wrongful and negligent breach of its duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

149. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of TracFone's breach of its duties. TracFone knew or should have known that it was failing to meet its duties, and that TracFone's breach would cause Plaintiffs and the Class Members to experience the foreseeable harms associated with the exposure of their confidential information.

150. As a direct and proximate result of TracFone's negligent conduct, Plaintiffs and the Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

151. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

152. When Plaintiffs and the Class Members paid TracFone for mobile services, they entered into contracts by which TracFone agreed to, *inter alia*, (1) provide mobile service and (2) protect their confidential information in accordance with its Privacy Policy.

153. TracFone solicited and invited its customers, including Plaintiffs and the Class, to provide their confidential information.

154. An explicit part of the offer, as stated in its Privacy Policy, was that TracFone would safeguard the confidential information using reasonable or industry-standard means.

155. TracFone also affirmatively represented on its website and in its Privacy Policy that it protected the confidential information of Plaintiffs and the Class in several ways, as described above.

156. Based on TracFone's representations, Plaintiffs and the Class accepted the offers and provided TracFone with their confidential information when they opened their accounts with TracFone.

157. TracFone entered into binding contracts with Plaintiffs that included a contractual obligation to provide mobile service and to reasonably protect Plaintiffs' and the Class Members' confidential information through, among other things, its Privacy Policy.

158. In entering into such contracts, Plaintiffs and the Class Members reasonably believed and expected that TracFone would provide them mobile service and that TracFone's data security practices complied with relevant laws and regulations and were consistent with industry standards.

159. Plaintiffs and the Class Members would not have entered into such agreements and provided their confidential information to TracFone had they known that TracFone would not provide them mobile service nor safeguard their confidential information as promised.

160. Plaintiffs and the Class Members fully performed their obligations under the contracts with TracFone.

161. TracFone breached the contracts by failing to provide mobile service and by failing to safeguard Plaintiffs' and the Class Members' confidential information.

162. The losses and damages Plaintiffs and the Class Members sustained (as described above) were the direct and proximate result of TracFone's breaches of its contracts with them.

163. Plaintiffs and the Class Members also are entitled to injunctive relief requiring TracFone to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, provide credit monitoring and identity theft insurance to Plaintiffs and the Class Members, and, for those still without their mobile phone number, TracFone must immediately reinstate their mobile phone numbers.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

164. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

165. When Plaintiffs and the Class Members provided their confidential information to TracFone to create their accounts, they entered into contracts by which TracFone agreed to, *inter alia*, (1) provide mobile service and (2) protect their confidential information in accordance with its Privacy Policy.

166. TracFone solicited and invited its customers, including Plaintiffs and the Class, to provide their confidential information in order to open their TracFone accounts.

167. An implicit part of the offer was that TracFone would safeguard the confidential information using reasonable or industry-standard means.

168. TracFone also affirmatively represented in its Privacy Policy that it protected the confidential information of Plaintiffs and the Class in several ways, as described above.

169. Based on the implicit understanding and also on TracFone's representations, Plaintiffs and the Class Members accepted the offers and provided TracFone with their confidential information.

170. TracFone manifested its intent to enter into an implied contract that included a contractual obligation to provide mobile services and reasonably protect Plaintiffs' and the Class Members' confidential information through, among other things, its Privacy Policy.

171. In entering into such implied contracts, Plaintiffs and the Class Members reasonably believed and expected that TracFone's data security practices complied with relevant laws and regulations and were consistent with industry standards.

172. Plaintiffs and the Class Members would not have provided their confidential information to TracFone had they known that TracFone would not safeguard their confidential information as promised.

173. Plaintiffs and the Class Members fully performed their obligations under the implied contracts with TracFone.

174. TracFone breached the implied contracts by failing to provide mobile service and by failing to safeguard Plaintiffs' and the Class Members' confidential information.

175. The losses and damages Plaintiffs and the Class Members sustained (as described above) were the direct and proximate result of TracFone's breaches of its implied contracts with them.

176. Plaintiffs and the Class Members also are entitled to injunctive relief requiring TracFone to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

177. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

178. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

179. TracFone owes duties of care to Plaintiffs and the Class Members which required it to adequately secure confidential information.

180. TracFone still possesses confidential information regarding Plaintiffs and the Class Members.

181. Plaintiffs allege that TracFone's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their confidential information and remain at imminent risk that further compromises of their confidential information will occur in the future.

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

a. TracFone owes a legal duty to secure consumers' confidential information under the common law, the FTCA, and the FCA;

b. TracFone's existing security measures do not comply with its legal requirements nor its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' confidential information;

c. TracFone continues to breach this legal duty by failing to employ reasonable measures to secure consumers' confidential information;

d. TracFone must comply with its explicit or implicit contractual obligations and duties of care by implementing and maintaining reasonable security measures, including, but not limited to:

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

ii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. Auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of TracFone's systems;

v. Conducting regular database scanning and securing checks;

vi. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. Purchasing credit monitoring services for Plaintiffs and the Class Members for a period of ten years; and

viii. Meaningfully educating its users about the threats they face as a result of the loss of their confidential information to third parties, as well as the steps TracFone's customers must take to protect themselves.

183. This Court also should issue corresponding prospective injunctive relief requiring TracFone to employ adequate security protocols consistent with law and industry standards to protect consumers' confidential information.

184. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at TracFone. The risk of another such breach is real, immediate, and substantial. If another breach at TracFone occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

185. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to TracFone if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damages. On the other hand, the cost to TracFone of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and TracFone has a pre-existing legal obligation to employ such measures.

186. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at TracFone, thus eliminating the additional injuries that would result to Plaintiffs, the Class Members, and other consumers whose confidential information would be compromised.

COUNT VI
VIOLATIONS OF THE FEDERAL COMMUNICATIONS ACT, 47 U.S.C. §§ 201 ET SEQ.
(On behalf of Plaintiffs and the Nationwide Class)

187. Plaintiffs restate and reallege paragraphs 1-117 above as if fully set forth herein.

188. TracFone has violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of Plaintiffs and Class Members' confidential information.

189. TracFone has violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Plaintiffs and Class Members' CPNI without the notice, consent, and/or legal authorization required under the FCA. TracFone also caused and/or permitted third parties to use, disclose, and/or permit access to Plaintiffs and Class Members' CPNI without the notice, consent, and/or legal authorization required under the FCA.

190. TracFone has violated 47 U.S.C. § 201 by implementing practices that are unjust and unreasonable, as discussed above and below.

191. Plaintiff is informed and believes, and based on such information and belief alleges that in or before December 2021, TracFone permitted hackers to access Plaintiffs and Class Members' confidential information. Thereafter, the hackers used the information to request that TracFone port out Plaintiffs and Class Members' mobile phone numbers. But for TracFone's active approval of the hackers' port-out requests, the hackers could never have gained access to Plaintiffs and Class Members other accounts, including but not limited to email and financial accounts.

192. As fully alleged above, Plaintiffs and Class Members have suffered injuries to their person, property, health, and reputation as a consequence of TracFone's violations of the FCA. Additionally, Plaintiffs and Class Members have suffered emotional damages, including severe anxiety and depression, mental anguish, and suffering as a result of TracFone's acts and practices.

193. On behalf of themselves and Class Members, Plaintiffs seek the full amount of damages sustained as a consequence of TracFone's violations of the FCA, together with reasonable attorneys' fees, to be fixed by the Court and taxed and collected as part of the costs of the case. [26]

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the class members described above, seek the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class and Subclasses as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representative of the Class and Subclasses requested herein;
b. Judgment in favor of Plaintiffs and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class Members as requested herein;
d. An order instructing TracFone to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;
e. An order requiring TracFone to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
f. A judgment in favor of Plaintiffs and the Class Members awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
g. An award of such other and further relief as this Court may deem just and proper.

[26] 47 U.S.C. §§ 206, 207.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: November 15, 2024

Respectfully submitted,

/s/ Mason A. Barney

Mason A. Barney (SDNY Bar No. MB7225)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (646) 357-1732
E: mbarney@sirillp.com
E: tbean@sirillp.com

ClassAction.org
