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

| | | |
|---|---|---|
| TYLER BAKER on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>PARKMOBILE, LLC,<br><br>Defendant. | ) | Case No. _____ |

**CLASS ACTION COMPLAINT**

Plaintiff Tyler Baker ("Plaintiff"), brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class"), against Defendant**,** ParkMobile, LLC ("ParkMobile" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

**NATURE OF THE CASE**

1. Plaintiff brings this class action against ParkMobile for ParkMobile's failure to properly secure and safeguard highly-valuable, protected personally identifiable information, including without limitations, names, license plate numbers, email addresses, phone numbers, vehicle nicknames, passwords, and home addresses (collectively, "PII"), failure to comply with industry standards to protect information systems that contain PII, and failure to provide adequate notice to Plaintiff and other Class Members that their PII had been accessed and compromised. Plaintiff seeks, among other things, damages, orders requiring ParkMobile to fully and accurately disclose the nature of the PII and other information that has been compromised and to adopt

reasonably sufficient security practices and safeguards to protect Plaintiff's and the Class' PII and to prevent incidents like the disclosure in the future. Plaintiff further seeks an order requiring ParkMobile to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members are, and will continue to be at an increased risk of identity theft due to the disclosure of their PII as a result of the conduct of ParkMobile described herein.

2. ParkMobile owns and operates mobile applications that provide parking services to users throughout the United States. These services include, *inter alia*, allowing a user to pay the cost for parking at a parking meter from a mobile device, or reserving a parking spot for future use.

3. ParkMobile requires users to create an account in order to use their services through the mobile applications. During the registration process, Plaintiff and other users are required to provide their PII to ParkMobile.

4. On March 26, 2021, ParkMobile announced that it had been subject to a cybersecurity incident related to a vulnerability in a third-party software vendor that ParkMobile uses (the "Data Breach").

5. Since the Data Breach, ParkMobile has provided updates that indicate its investigation has revealed that the compromised information included its users' PII.

6. The Data Breach was a direct and proximate result of ParkMobile's failure to implement and follow basic security procedures. Plaintiff's and Class Members' PII is now in the hands of criminals and Plaintiff and Class Members now face a substantially increased risk of identity theft, both currently and for the indefinite future, at least in part because their PII will now be offered and sold to identity thieves in an aggregated format, lending itself, for example, for ease of use in widespread phishing email schemes, identity theft, and other harms caused by the

disclosure of their PII. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to ParkMobile's actions.

7. Plaintiff, on behalf of himself and all others similarly situated, brings claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including requiring ParkMobile to adopt reasonably sufficient practices to safeguard PII that remains in ParkMobile's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

## PARTIES

8. Plaintiff Tyler Baker is a citizen and resident of the State of Vermont. At all times relevant to this Complaint, Plaintiff was a customer of ParkMobile. Plaintiff's PII was disclosed without authorization to unknown third parties as a result of ParkMobile's Data Breach.

9. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time changing passwords and monitoring his various accounts in an effort to detect and prevent any misuses of his PII – time which he would not have had to expend but for the Data Breach.

10. Furthermore, Plaintiff has experienced abnormal activity related to his PayPal account which was linked to his ParkMobile Account. After he cancelled the account, Plaintiff has received and continues to receive fraudulent email messages claiming that funds in excess of $30,000 have been deposited into his inactive PayPal account. The suspicious messages then attempt to have the recipient submit additional personal information to receive the funds. Plaintiff has spent additional time reviewing and monitoring these suspicious and disturbing emails.

11. As a result of the Data Breach, Plaintiff has been and will continue to be at heightened risk for fraud and identity theft, continue to spend related time, and sustain attendant damages for years to come. Such risk is certainly impending and is not speculative, given that information from the Data Breach is already being offered for sale on the dark web.

12. Defendant ParkMobile, LLC is a Delaware Limited Liability Company with its principal place of business at 1100 Spring Street NW, Atlanta, Georgia. Defendant is a citizen of Georgia.

## JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. This Court has personal jurisdiction over Defendant because Defendant is a citizen of the State of Georgia.

15. Pursuant to 28 U.S.C. § 1391(b)(1), venue is proper in this District because Defendant resides in this District.

## FACTUAL BACKGROUND

***ParkMobile***

16. "ParkMobile Makes Parking a Breeze" by providing "one parking app to handle it all[.]"[1]

[1] https://parkmobile.io/how-it-works/

17. ParkMobile holds itself out to be "the leading provider of parking solutions in the U.S. and it's our mission to power smart mobility for every driver and vehicle, everywhere."[2]

18. ParkMobile allows users to pay the cost of parking at a parking meter, extend time on the meter, or reserve a parking space before the user arrives at their destination, all from ParkMobile's mobile applications.[3] "ParkMobile helps millions of people easily find and pay for parking on their mobile devices. People can use ParkMobile solutions to quickly pay for street and garage parking without having to use a meter or kiosk. Additionally, ParkMobile offers parking reservations for concerts, sporting events, airports, campuses and more."[4]

19. ParkMobile provides its users with details about parking in the area, such as whether there is EV charging for electric vehicles, covered parking, onsite security, valet parking, or handicapped parking.[5]

20. Users can also pay $0.99 per month to receive ParkMobile Pro, which provides users with additional benefits such as, *inter alia*, discounts on car washes, roadside assistance, and rental car discounts.[6]

21. ParkMobile allows users to store up to seven different payment methods in order to make payments for parking charges.[7]

22. ParkMobile is "[l]ocated in 8 of the top 10 U.S. cities, [and] helps millions of people park smarter every year."[8]

23. To use ParkMobile, users must create an online account with Defendant. As part of its relationship with users, ParkMobile routinely acquires and stores users' PII on its systems.

---

[2] https://parkmobile.io/company/
[3] https://parkmobile.io/how-it-works/
[4] https://parkmobile.io/company/
[5] https://parkmobile.io/how-it-works/
[6] *Id.*
[7] *Id.*
[8] https://parkmobile.io/company/

24. Users are entitled to security of their PII. As a vendor storing sensitive data, ParkMobile has a duty to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

***The ParkMobile Data Breach***

25. On March 26, 2021, ParkMobile announced that it "recently became aware of a cybersecurity incident linked to a vulnerability in a third-party software that we use."[9] ParkMobile stated that their "investigation indicates that no sensitive data or Payment Card Information, which we encrypt, was affected."[10]

26. On April 13, 2021, ParkMobile provided a security update, stating that their "investigation concluded that encrypted passwords, but not the encryption keys needed to read them, were accessed." Furthermore, ParkMobile's "investigation has confirmed that basic user information – license plate numbers and, if provided by the user, email addresses and/or phone numbers, and vehicle nicknames – was accessed. In a small percentage of cases, mailing addresses were affected."[11]

27. The PII obtained from ParkMobile has already been listed for sale on a Russian crime forum for $125,000.[12] This PII can then be used to commit cybercrimes against Plaintiff and the Class.

28. The information obtained in the Data Breach contains the PII of approximately 21 million individuals.[13]

[9] https://support.parkmobile.io/hc/en-us/articles/360058639032-Update-Security-Notification-March-2021
[10] *Id.*
[11] *Id.*
[12] https://krebsonsecurity.com/2021/04/parkmobile-breach-exposes-license-plate-data-mobile-numbers-of-21m-users/
[13] *Id.*

***ParkMobile Obtains, Collects, and Stores Plaintiff's and Class Members' PII***

29. In the ordinary course of doing business with ParkMobile's users, Plaintiff and Class Members are regularly required to provide their sensitive, personal and private protected information in order to register and use Defendant's services.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, ParkMobile assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

31. Plaintiff and Class Members reasonably expect that service providers such as Defendant will use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

32. Defendant acknowledges in its privacy policy its obligation to keep users' PII confidential, stating "[a]t ParkMobile, we are committed to respecting your privacy."[14]

33. Despite Defendant's commitment to protecting personal information, ParkMobile failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

34. Had ParkMobile remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, ParkMobile could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

[14] https://parkmobile.io/privacy-policy/

***The Value of Private Information and Effects of Unauthorized Disclosure***

35. ParkMobile was well aware that the protected PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

36. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers and when multiple types of information for a single user are combined. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical or financial fraud.[15] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

37. PII is valued on the dark web at approximately $1 per line of information.[16]

38. The ramifications of ParkMobile's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

39. Further, criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

40. ParkMobile knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. ParkMobile failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

[15] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[16] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20food%20joint.

***FTC Guidelines***

41. ParkMobile is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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 FTC Act.

42. The FTC has promulgated numerous guides for businesses that 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.[17]

43. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[18]

44. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[19]

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

[17] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[18] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf.
[19] *Id.*

unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. ParkMobile failed to properly implement basic data security practices. ParkMobile's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

47. ParkMobile was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. ParkMobile was also aware of the significant repercussions that would result from its failure to do so.

***Plaintiff and Class Members Suffered Damages***

48. The ramifications of ParkMobile's failure to keep user PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[20]

49. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.[21]

50. Besides the monetary damage sustained, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues.[22]

[20] https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics#:~:text=In%202019%2C%2014.4%20million%20consumers,about%201%20in%2015%20people&text=Identity%20theft%20is%20the%20most,data%20breaches%20increased%20by%2017%25

[21] *Id.*

[22] https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity-theft.html#:~:text=And%20ID%20theft%20recovery%20is,more%20resolving%20identity%20theft%20problems.

51. 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 PII.

52. Despite all of the publicly available knowledge of the continued compromises of PII, ParkMobile's approach to maintaining the privacy of PII was reckless, or in the very least, negligent.

**53.** As a result of ParkMobile's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

## CLASS ALLEGATIONS

54. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the ParkMobile Data Breach which occurred around March 2021.

55. Excluded from the Class is Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded

party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

56. Plaintiff reserves the right to modify or amend the definition of the proposed Class if necessary before this Court determines whether certification is appropriate.

57. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

58. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

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

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information unencrypted on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

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

h. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

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

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's 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.

59. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII.

60. Plaintiff and members of the Class were customers of ParkMobile, each having their PII obtained by an unauthorized third party.

61. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

***Georgia Law Should Apply to Plaintiff and the Class as a Whole***

62. The State of Georgia has a significant interest in regulating the conduct of businesses operating within its borders. Georgia, which seeks to protect the rights and interests of Georgia and all residents and citizens of the United States against a company headquartered and doing business in Georgia, has a greater interest in the claims of Plaintiff and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

63. The principal place of business and headquarters of ParkMobile, located at 1100 Spring Street NW in Atlanta, Georgia, is the "nerve center" of its business activities – the place

where its high-level officers direct, control, and coordinate ParkMobile's activities, including its data security functions and major policy, financial, and legal decisions.

64. ParkMobile's actions leading up to the Data Breach, and its response thereafter, and corporate decisions surrounding such response, were made from and in Georgia.

65. ParkMobile's breaches of duty to Plaintiff and Class members emanated from Georgia.

66. Application of Georgia law to the Class with respect to Plaintiff's and the Class' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Class.

67. Specifically, ParkMobile's Term of Service specifically state that the "laws of the State of Georgia, U.S.A., excluding Georgia's conflict of laws rules, will apply to any disputes arising out of or relating to these terms of the Services. All claims arising out of or relating to these terms of Services will be litigated exclusively in the federal or state courts of Fulton County, Georgia, USA, and you and ParkMobile consent to personal jurisdiction in those courts." *See* www.parkmobile.io.

68. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the nationwide common law claims of all Class members. Additionally, given Georgia's significant interest in regulating the conduct of businesses operating within its borders, and that Georgia has the most significant relationship to ParkMobile, as it is headquartered in Georgia, ParkMobile's computer systems are located in Georgia, and its executives and officers are located and made decisions which led to the Data Breach, there is no conflict in applying Georgia law to non-resident consumers such as Plaintiff and the Class.

**FIRST CAUSE OF ACTION**
**NEGLIGENCE**
**(On Behalf of Plaintiff and the Class)**

69. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

70. ParkMobile owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing ParkMobile's security systems to ensure that Plaintiff's and Class Members' PII in ParkMobile's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

71. ParkMobile's duty to use reasonable care arose from several sources, including but not limited to those described below.

72. ParkMobile had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, ParkMobile was obligated to act with reasonable care to protect against these foreseeable threats.

73. ParkMobile admits that it has the responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

74. ParkMobile breached the duties owed to Plaintiff and Class Members and thus was negligent. ParkMobile breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in ParkMobile's possession had been or was reasonably believed to have been, stolen or compromised.

75. But for ParkMobile's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

76. As a direct and proximate result of ParkMobile's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

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

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the ParkMobile Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to ParkMobile with the mutual understanding that ParkMobile would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in ParkMobile's possession and is subject to further breaches so long as ParkMobile fails to undertake appropriate and adequate measures to protected Plaintiff.

77. As a direct and proximate result of ParkMobile's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE PER SE**
**(On Behalf of Plaintiff and the Class)**

78. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

79. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as ParkMobile for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of ParkMobile's duty.

80. ParkMobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. ParkMobile's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

81. ParkMobile's violation of Section 5 of the FTC Act constitutes negligence *per se*.

82. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

83. Moreover, the harm that has occurred is the type of harm that the FTC Act 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.

84. Additionally, ParkMobile has a duty to act reasonably in handling consumer data and to use reasonable data security measures that arises under the Gramm–Leach–Bliley Act's implementing regulations, 16 C.F.R. § 314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions[.]" 16 C.F.R. § 314.1(a)-(b).

85. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution]." 16 C.F.R. § 314.1(b).

86. The Safeguards Rule requires financial institutions and entities who act on behalf of financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution's] size and complexity, the nature and scope of [the financial institution's] activities, and the sensitivity of any customer information at issue." 16 C.F.R. § 314.3(a).

87. Specifically, the Safeguards Rule requires entities to:

> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> * * *
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

88. As alleged herein, ParkMobile breached its duties under the Safeguards Rule.

89. ParkMobile also has a duty under the Georgia Constitution which contains a Right to Privacy clause, Chapter 1, Article 1, which states "no person shall be deprived of life, liberty,

or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

90. This duty has been recognized by the Georgia Supreme Court, adopting Restatement of the Law of Torts (Second) § 652A, which specifically recognized four common law invasion of privacy claims in Georgia, which include: 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

91. ParkMobile's failure to implement reasonable measures to secure consumers' PII violates the Georgia Constitution and the Restatement of the Law of Torts (Second).

92. As a direct and proximate result of ParkMobile's negligence, Plaintiff and Class Members have been injured as described herein and in Paragraph 68 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

## THIRD CAUSE OF ACTION
## DECLARATORY JUDGMENT
## (On Behalf of Plaintiff and the Class)

93. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

94. 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.

95. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether ParkMobile is currently maintaining data security

measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that ParkMobile's data security measures remain inadequate. ParkMobile publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

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

a. ParkMobile owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act; and

b. ParkMobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

97. This Court also should issue corresponding prospective injunctive relief requiring ParkMobile to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

98. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at ParkMobile. The risk of another such breach is real, immediate, and substantial. If another breach at ParkMobile occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

99. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to ParkMobile if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to ParkMobile of complying with an injunction by

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

100. 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 ParkMobile, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

## PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

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

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

## JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Respectfully submitted,

/s/ *MaryBeth V. Gibson*
MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Tel.: 404-320-9979
Fax: 404-320-9978
*mgibson@thefinleyfirm.com*

Bryan L. Bleichner (*pro hac vice forthcoming*)
CHESTNUT CAMBRONNE, PA
100 Washington Ave. S., Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
*bbleichner@chestnutcambronne.com*

Terence R. Coates (*pro hac vice forthcoming*)
MARKOVITS, STOCK & DE MARCO, LLC
3825 Edwards Rd., Suite 650
Cincinnati, Ohio 45209
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
*tcoates@msdlegal.com*

Joseph M. Lyon (*pro hac vice forthcoming*)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
*jlyon@thelyonfirm.com*

Brian C. Gudmundson (*pro hac vice forthcoming)*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
*brian.gudmundston@zimmreed.com*

*Counsel for Plaintiff and the Class*