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

TYLER BAKER, MARIAM GEORGE, EMMA JACKSON, SAIT KURMANGALIYEV, GREGORY MANSON, and HERIBERTO TRAVIESTO, on behalf of themselves and all others similarly situated, Plaintiffs, v. PARKMOBILE, LLC, Defendant.	)	Case No. **CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Tyler Baker, Miriam George, Emma Jackson, Sait Kurmangaliyev, Gregory Manson, and Heriberto Traviesto ("Plaintiffs"), by their undersigned counsel, file this Consolidated Class Action Complaint on behalf of themselves and a class of all similarly situated persons against Defendant ParkMobile, LLC ("ParkMobile" or "Defendant"). Plaintiffs base the forgoing allegations upon personal information and belief, the investigation of counsel, and state the following:

INTRODUCTION

1. ParkMobile developed and owns a parking application ("App") generally known by the same name, ParkMobile. ParkMobile launched its App in 2008 for smart phones and other handheld devices to purportedly help users find and

pay for parking using their cell phone, tablet, or computer. Additionally, ParkMobile's App, offers parking reservations in communities and for events, including concerts, sporting events, airport parking, and campus parking. ParkMobile claims it is "committed to creating tech-based solutions that power smart mobility and make parking hassles of the past obsolete."

2. ParkMobile operates in 42 states in 557 different cities and venues, including in 8 of the top 10 largest cities in the United States. These include, but are not limited to New York City, San Francisco, Washington D.C., Denver, Kansas City, Boston, Oakland, Nashville, Chicago, Milwaukee, Baltimore, and Atlanta.

3. To use ParkMobile's App, ParkMobile requires users to provide personal and sensitive data that ParkMobile unilaterally collects and stores. That personal and sensitive data includes: names, license plate numbers, email addresses, phone numbers, vehicle nicknames, passwords, credit card information, pay pal accounts and home addresses. This type of personal and sensitive data is highly targeted by hackers who seek to exploit this data for nefarious purposes. This type of personal information has inherent value and is routinely marketed and sold on the dark web. In the wrong hands, the personal and sensitive data that ParkMobile collects and stores may be utilized to cause significant harm to the users who provided the information.

4. The value of this information on the dark web is well recognized in the modern data economy. Additionally, the foreseeable risk to customers' identities as a result of a criminal hacking event is known and recognized by technology companies that gather and store data, including Defendant. Park Mobile is the type of tech company that gathers, stores, and uses its customers personal information to operate its business and provide its services and, in fact, requires all users to provide sensitive data to use ParkMobile's App. As such, ParkMobile has a duty to protect its users' data. ParkMobile assures users that it is highly sophisticated tech company and a technology innovator. ParkMobile previously has assured users that it can keep their information safe and that it uses industry standard data security measures to do so. Contrary to its representations and promises, however, ParkMobile utilized inadequate data security measures it knew, or should have known, put the personal and sensitive data it solicited, collected, and stored at significant risk of theft by or exposure to nefarious parties. Indeed, ParkMobile acknowledged in recent years that its data security was not "100% secure" and that it could not "guarantee the security of [user]information," despite the fact ParkMobile required users to provide it with personal and sensitive data, stored that data, utilized that data to provide its services, and was the only entity responsible for and capable of protecting that data. In essence, ParkMobile conceded that it did not prioritize data security or protect user data after it had collected such data from its users.

5. Consequently, and as a direct result of ParkMobile's knowingly operating its business with deficient security systems and security measures for handling and protecting its customers' data, sometime in or around March 2021, hackers breached ParkMobile's data environment and accessed personal and sensitive user data on tens of millions of individuals whose information ParkMobile had solicited, collected, utilized, and stored ("Data Breach").

6. Initially, ParkMobile represented to the public that no data had been stolen in the Data Breach. That was not true. On April 12, 2021, KrebsOnSecurity, an online security blog, reported that hackers were selling personal and sensitive data from 21 million ParkMobile customers for an "insanely high price." The data reportedly included customer email addresses, dates of birth, phone numbers, license plate numbers, hashed passwords, and mailing addresses. Gemini Advisory, a sophisticated threat intelligence firm confirmed KrebsOnSecurity's report.

7. On April 13, 2021—after KrebsOnSecurity reported the Data Breach had exposed personal and sensitive data that hackers were selling on the dark Web -- ParkMobile finally publicly acknowledged that personal and sensitive data had indeed been stolen in the Data Breach and recommended but, did not require, users to change their passwords. Instead, ParkMobile continued to downplay the Data Breach, claiming that only "basic" user data was stolen, no credit card data had been compromised and only encrypted passwords had been stolen. The reality,

however, is that the supposedly "basic" information stolen from ParkMobile is highly valuable and can be used to cause great financial harm to ParkMobile's users. Additionally, ParkMobile's purportedly protected passwords could easily be identified by reversing the encryption.

8. In April 2021, the news worsened for the more than 20 million individuals whose data ParkMobile failed to secure. The hackers released the data stolen from ParkMobile on the dark web for free in a .csv file (a type of excel-like spreadsheet). Thus, anyone with access to the internet could now find, download, and exploit ParkMobile users' data.

9. The Data Breach has already had serious consequences. Plaintiffs have each suffered harm responding and attempting to mitigate the consequences of the Data Breach by, among other things, monitoring their payment accounts, paying for monitoring services, freezing accounts and credit cards, researching the data stolen in the Data Breach, and/or changing impacted passwords. Additionally, some Plaintiffs have suffered from fraudulent activity directly and proximately linked to the Data Breach. Bad actors have already used the stolen data to, for instance, either log into or attempt to log into Plaintiffs' applications, accounts, and other websites, like PayPal, Comcast, Netflix, and Venmo, and have created fake accounts with Plaintiffs' names and other data stolen in the Data Breach. Plaintiffs have experienced actual damages by cancelling bank credit cards resulting in less access

to credit and paying interest on purchases rather than utilizing debit transactions. Plaintiffs have also paid out of pocket for increased identity theft protection. Plaintiffs have lost time changing passwords and monitoring theirs accounts and avoiding additional charges for late fees as a result of the fraudulent activity and risk to their identities that naturally flowed from Defendant's failure to protect their personal information.

10. Plaintiffs, therefore, bring this Consolidated Class Action Complaint seeking relief for their injuries and those of persons who were similarly impacted by the Data Breach and inadequate data security.

JURISDICTION

11. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Plaintiffs are diverse from Defendant because Plaintiffs resides in California, Florida, Pennsylvania, New York, Vermont, and Virginia and ParkMobile resides in Georgia, where it and its sole member are headquartered. Plaintiffs allege that, in the aggregate, the claims of all putative class members exceed $5,000,000, exclusive of interest and costs.

12. Defendant is a Delaware LLC with its principal place of business in Atlanta,

Georgia. Defendant is a citizen of Georgia. Its sole member, ParkMobile USA, Inc. is also a citizen of Georgia. Minimal diversity requirement under CAFA is met.

13. This Court has general personal jurisdiction over ParkMobile because ParkMobile and its sole member are citizens of the State of Georgia, are headquartered and operate their principal place of business in Atlanta, Georgia. ParkMobile has minimum contacts with Georgia because it is located there and conducts substantial business there, and Plaintiffs' claims arise from ParkMobile's conduct in Georgia.

14. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in Georgia and because ParkMobile conducts a substantial part of its business within this District.

PARTIES

15. **Plaintiff** Tyler Baker is a citizen and resident of the State of Vermont. At all relevant times, Plaintiff Baker was a customer of ParkMobile since approximately 2016. As required for use of the services, Plaintiff provided Park Mobile with his email address, password, credit card information, license plate. He also linked his Pay Pal account to the Park Mobile application. Plaintiff expected Park Mobile would secure and protect his personal information, and he never consented to its disclosure. Plaintiff Baker's personal and sensitive data was

exposed during the Data Breach. Following the Data Breach, Plaintiff received notice from Experian that his email and password were found on the Dark Web and "may indicate possible identity theft." As a result of this notice and the Data Breach, Plaintiff Baker took steps to mitigate his risk for identity theft. These steps included reviewing credit card accounts and statements, cancelling debit and credit cards, and purchasing additional identity theft protection. He also spent additional time changing his passwords on his banking, email, social media, utilities, and mortgage servicer which all utilized the same password which was compromised in the breach. In addition, since the announcement of the Data Breach, Plaintiff Baker has experienced abnormal activity related to his PayPal account, which was linked to his ParkMobile account, which resulted in Pay Pal cancelling his account. After the cancellation, Plaintiff Baker has received and continues to receive targeted and 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 Baker has spent additional time reviewing and monitoring these suspicious and disturbing emails. Plaintiff Baker also incurred a fraudulent charge on his debit card that remains unreimbursed. This debit card was linked to his Park Mobile account. As a result, Mr. Baker prudently cancelled his debit card which resulted in less access to cash and the use of credit cards to make transactions incurring

unwarranted interest. Mr. Baker also experienced a fraudulent application for additional services on his Comcast account. He spent additional time resolving this application for services which he did not order. Finally, Mr. Baker incurred costs and will continue to incur additional monthly costs for the purchase of more advanced identity theft protection. Prior to the Park Mobile Data Breach, Plaintiff Baker was not a victim of any other data breaches that he is aware of and has not experienced previous identity theft.

16. **Plaintiff** Miriam George is a citizen and resident of the State of Pennsylvania. At all relevant times, Plaintiff George was a customer of ParkMobile. Plaintiff George's personal and sensitive data was disclosed without authorization during the Data Breach. As a result of the Data Breach, her personal and sensitive information is now available on the dark web. Plaintiff George suffered harm as a result of the Data Breach. Specifically, since the announcement of the Data Breach, Plaintiff George spent time changing passwords and monitoring her accounts for fraud.

17. **Plaintiff** Emma Jackson is a citizen and resident of the State of California. At all relevant times, Plaintiff Jackson was a customer of ParkMobile. Plaintiff provided Park Mobile her personal information that included her email, password, phone number, license plate, billing address, and debit card. Plaintiff expected Park Mobile would secure and protect her personal information, and she

never consented to its disclosure. On or about April 23, 2021, Plaintiff Jackson received notice from ParkMobile of the Data Breach. The notice did not notify her that her specific information had been exposed but ParkMobile recommended that she change her password on the ParkMobile app and use different passwords on other accounts. Plaintiff then received notice from Capital One Credit Wise that on May 5, 2021, her email address and password were exposed on the Dark Web related to the Park Mobile breach. She also received notice from "Have I been Pwned" that her passwords and phone numbers were compromised in the ParkMobile breach. Since learning of the Data Breach and receiving notice that her personal information was on the Dark Web, Plaintiff Jackson took steps to mitigate her risk for identity theft. Specifically, she spent time reviewing her banking and credit card accounts. She also spent time changing her passwords which were the same passwords as her Park Mobile Password. She cancelled and created a new email account that required her to register for certain services, including healthcare notifications for her son. Ms. Jackson has also experienced identify theft with fraudulent Instagram and LinkedIn accounts created in her name. Ms. Jackson is an artist and sells her work online. The duplicate social media accounts have created online confusion to her person and harmed her online profile, which she utilizes for commercial purposes. Plaintiff Jackson has also experienced an increase in SPAM and targeted suspicious phone calls and emails that cost her additional annoyance and loss of time. Plaintiff

Jackson is unaware of being a victim of any previous data breach, and she has not experienced previous identity theft.

18. **Plaintiff** Sait Kurmangaliyev is a resident of Brooklyn, New York. At all relevant times, Plaintiff used ParkMobile's parking application for New York City, called ParkNYC. Plaintiff Kurmangaliyev received a notice that his information was exposed during the Data Breach. Plaintiff Kurmangaliyev's personal and sensitive information was included in the batch of information on 21 million ParkMobile users for sale on the dark web. Plaintiff Kurmangaliyev suffered harm as a result of the Data Breach. Specifically, since the announcement of the Data Breach, Plaintiff Kurmangaliyev spent time and effort monitoring accounts, freezing his credit, and has suffered a significant increase in spam calls and emails.

19. **Plaintiff** Gregory Manson is a citizen and resident of the State of Virginia. At all relevant times, Plaintiff Manson used ParkMobile's application for parking and was a customer of ParkMobile. As part of the terms for use, Plaintiff provided his personal and sensitive data to Park Mobile. This information included his email, password, phone number, license plates, and credit card information. Plaintiff expected Park Mobile would secure his personal information, and he never consented to its disclosure. On or about May 16, 2021 Plaintiff was notified by Chase Credit Journey that his email and password were compromised in the Park Mobile Data Breach and were a risk to his identity. Then on or about May 22, 2021,

Plaintiff received notice from Park Mobile that there was a Data Breach. The notice recommended that he change his password on the Park Mobile app and use different passwords on other accounts. Since learning of the Data Breach and receiving notice that his personal information was on the Dark Web, Plaintiff Manson took steps to mitigate his risk for identity theft. Specifically, he spent time reviewing his banking and credit card accounts and continues to monitor his financial accounts for fraudulent activity. He also spent time changing his passwords on numerous accounts, which were the same passwords as his Park Mobile Password, including his Chase Banking account. Mr. Manson also received notification from Microsoft that his account had suspicious login attempts from South Africa, which Mr. Manson did not make. He also experienced hacking attempts on his Instagram account. Plaintiff has also experienced an increase in SPAM and targeted suspicious phone calls and emails that have cost him additional annoyance and loss of time. Plaintiff Manson is unaware of being a victim of any previous data breach that involved the data at issue in this matter, and he has not experienced previous identity theft.

20. **Plaintiff** Heriberto Travieso is a citizen and resident of the State of Florida. At all relevant times, Plaintiff Travieso was a customer of ParkMobile. Plaintiff Travieso's personal and sensitive data was disclosed without authorization during the Data Breach. As a result of the Data Breach, Plaintiff Travieso's personal and sensitive data is now available on the dark web. Plaintiff Travieso suffered

harm. Specifically, since the announcement of the Data Breach, Plaintiff Travieso has experienced abnormal activity related to several of his accounts, including his credit card, PayPal, Venmo, email, and Netflix accounts. Since the Data Breach, unknown parties have accessed Plaintiff Travieso's email and Netflix accounts.

21. **Defendant** ParkMobile, LLC owns and operates the ParkMobile parking application for smart phones and devices. 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. The sole member of Defendant ParkMobile, LLC is ParkMobile USA, Inc. Member ParkMobile USA, Inc. is a Delaware corporation with its principal place of business at 1100 Spring Street NW, Atlanta, Georgia. ParkMobile USA, Inc. is a citizen of Georgia.

BACKGROUND

A. ParkMobile Collects Personal and sensitive Information from Users.

22. ParkMobile developed and owns an application ("App") for smart devices, cell phones, and computers that provides parking-related services. ParkMobile's App supposedly makes "Parking a Breeze" by providing "one parking app to handle it all[.]"[1]

[1] *How it Works*, ParkMobile.io (last visited, Aug. 13, 2021), https://parkmobile.io/how-it-works/.

23. ParkMobile represents that it "helps millions of people easily find and pay for parking on their mobile devices" and help users "to quickly pay for street and garage parking without having to use a meter or kiosk."[2] Parking locations include street parking, monthly permit or pass locations, and gated parking facility locations. ParkMobile's App also providers parking reservations for concerts, sporting events, airports, campuses and other venues, and lists some locations for EV charging.[3]

24. ParkMobile works by allowing 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.[4] Each time a user pays for parking, extends parking, or reserves a parking spot, the user pays a transaction fee included in the payment amount.[5] Users can also pay $0.99 per month to receive ParkMobile Pro, which allows users to receive additional benefits, including discounts on car washes, roadside assistance, and rental car discounts.[6]

---

[2] *About ParkMobile*, ParkMobile.io (last visited Aug. 13, 2021), https://parkmobile.io/company/

[3] *Id.*

[4] *How it Works*, *supra* note 1.

[5] Member Services, *What are the parking costs? What will I be charged?*, ParkMobile.io (Nov. 27, 2012) ("In addition to the fee you'll pay for parking, you may also be charged a transaction fee for using the ParkMobile pay by phone service to pay for your parking.").

[6] *How it Works*, *supar* note 1.

25. ParkMobile operates in at least 42 different states and provides parking-related services for over 550 venues, including 450 cities and metropolitan areas throughout the United States.[7] ParkMobile is available to use in some of the largest cities in the United States, including New York City, San Francisco, Washington D.C., Denver, Kansas City, Boston, Oakland, Nashville, Chicago, Milwaukee, Baltimore, Pittsburgh, Atlanta, and Minneapolis.[8]

26. Although most users use the "ParkMobile" App, some city-specific apps have different names but use ParkMobile's underlying software and systems. ParkMobile calls these "White-Label Apps," which allow cities and metropolitan areas to use ParkMobile's digital platform while retaining custom branding and management of inventory, availability, and rates.[9]

27. White-Labeled Apps include ParkNYC (parking in New York City), MPLS Parking (parking in Minneapolis, MN), MKE Park (parking in Milwaukee, WI), Go Mobile PGH (parking in Pittsburgh, PA), Park Columbus (parking in Columbus, OH), meterUP (parking in Philadelphia, PA), Park Houston (parking in

---

[7] *See Reserve Parking at 557 Venues in the United States with ParkMobile*, ParkMobile.io (last visited, Aug. 13, 2021), https://park.parkmobile.io/.

[8] *Company*, ParkMobile.io (last visited Aug. 13, 2021) (stating the ParkMobile is "[l]ocated in 8 of the top 10 U.S. cities [and] helps millions of people park smarter every year."), https://parkmobile.io/company/

[9] *White Label Reservation Parking Solution*, ParkMobile.io (last visited, Aug. 12, 2021), https://parkmobile.io/parking-solutions/white-labeling/

Houston, TX), ParkLouie (parking in St. Louis, MO), FW Park (parking in Fort Worth, TX), Park it Charlotte (parking in Charlotte, NC), 717Parking (parking in Tampa Bay, FL), Park915 (parking in El Paso, TX), and Premier Parking (parking in Nashville, TN).

28. ParkMobile has prolifically expanded its user base over the past several years. As of September 2020, ParkMobile reported that it "adds 1 million new users every 60 to 70 days" and that "[o]ver the past 12 years, the company has processed over 334,000,000 transactions totaling 57 billion minutes of parking time and over $1 billion of parking fees."[10] ParkMobile claims that it is "currently the #1 ranked parking app in the app store and ranks #3 in the navigation category, only behind Google Maps and Waze."[11]

29. For each of those millions of individuals who have downloaded and used ParkMobile's App, ParkMobile requires that they provide personal and sensitive user data. In fact, the App and its parking services cannot be used until users create an account and provide ParkMobile with the personal and sensitive information it requires. To use the App, ParkMobile collects user names, license

[10] Press Release, *ParkMobile App Hits the 20 Million User Milestone*, ParkMobile (Aug. 9, 202), https://parkmobile.io/newsroom/parkmobile-app-hits-20-million-user-milestone/

[11] Press Release, *ParkMobile App Hits the 20 Million User Milestone*, ParkMobile (Aug. 9, 202), https://parkmobile.io/newsroom/parkmobile-app-hits-20-million-user-milestone/

plate numbers, email addresses, phone numbers, vehicle nicknames, passwords, and home addresses. Additionally, ParkMobile collects and retains information on users' locations.

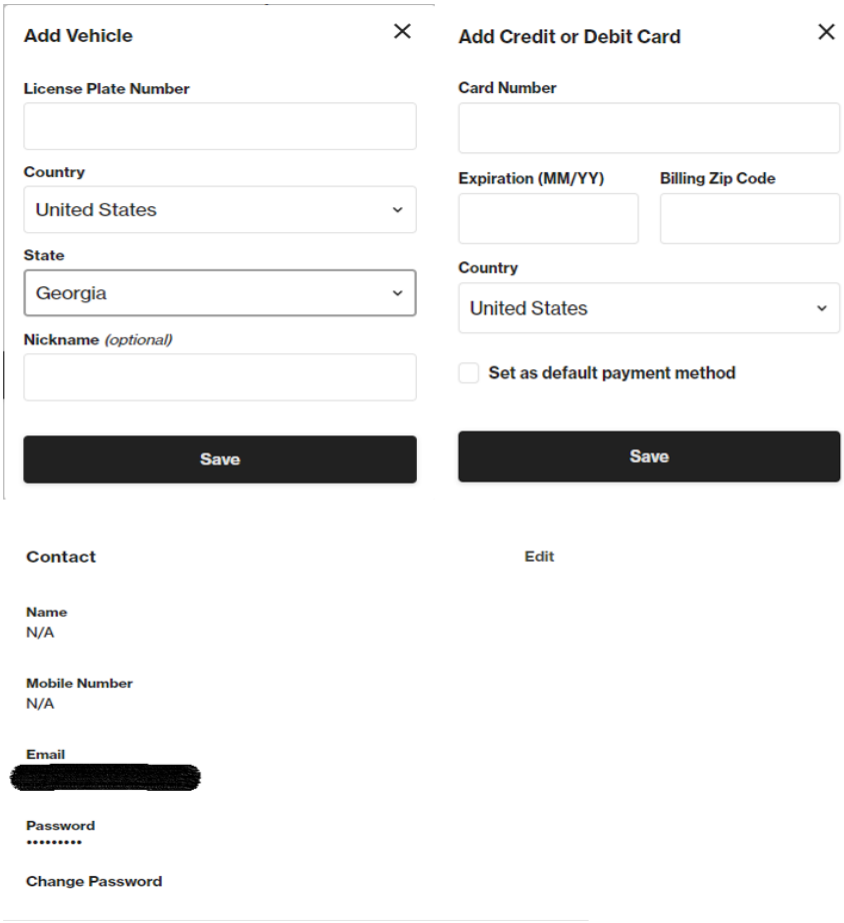


Image 1. Pictures of information users must provide ParkMobile's App when creating a user account.

30. Users of White-Labeled Apps, provide the same type of information. However, those users are given little indication that they are providing data to ParkMobile. None of the White-Labeled Apps have "ParkMobile" in their names, and users cannot reasonably identify ParkMobile as the digital platform underlying

the White-Labeled App. At best, some White-Labeled Apps are described as being "Powered by ParkMobile" in descriptions on Apple's and Google's stores (Apple's App Store or Google Play). Therefore, White-Labeled Apps users are given no indication that ParkMobile is managing and storing their data.

31. ParkMobile has publicly acknowledged the importance of protecting the personal and sensitive data it collects and stores. For instance, in 2012, it noted that "[t]here are numerous methods by which hackers may steal information" and that "the entry of personal data is at risk at any time depending on [one's] physical surroundings and the security of [one's] network or device."[12]

32. Early on, ParkMobile assured users that their personal and sensitive data was safe with ParkMobile. For example, ParkMobile's "Member Services" team promised users that "ParkMobile utilizes industry standard encryption methods to ensure cardholder details (name, credit card number, etc.) are stored using strong encryption algorithms."[13] ParkMobile further claims it "has been audited to ensure that [its] cardholder capture, handling, encryption, and storage are all compliant with

[12] Member Services, *Is my account and credit card information safe?*, ParkMobile.io (Feb. 21, 2012), https://support.parkmobile.io/hc/en-us/articles/203299650-Is-my-account-and-credit-card-information-safe-

[13] *Id.*

industry methods."[14] ParkMobile also represents that it uses "trusted methods to ensure cardholder data is protected[.]"[15]

33. Additionally, ParkMobile repeatedly represents itself as a trusted leader in technology and smart applications, calling itself a "Vanguard" of travel and technology. ParkMobile claims to use "tech-based solutions that power smart mobility and make parking hassles of the past obsolete."[16] It, furthermore, emphasizes its supposedly "innovative solutions" it uses to "eliminate friction while maximizing convenience and efficiency."[17]

34. On ParkMobile's "About Us" page, it highlights the broad range of technical, technology-focused, and software experience of its team members, which it claims allows ParkMobile to "better connect the practicalities of parking with tech-based solutions that make it hassle free."[18] Its employees and teams are supposedly made up of "Smart People" who "Build[] Smart Solutions."

35. ParkMobile also goes to great lengths to claim that its business and its products are user friendly and user-oriented. To that end, ParkMobile lists as a "core

---

[14] *Id.*

[15] *Id.*

[16] *About ParkMobile*, ParkMobile.io (last visited Jun. 28, 2021), https://parkmobile.io/company/

[17] *Id.*

[18] *Id.*

value" its "healthy obsession with the customer experience." ParkMobile represents that "[f]rom [its] app and online tools to [its] customer service team . . . [it] make[s] every interaction with ParkMobile and [its] products, perfect." It claims to hold itself to "a higher standard" and expresses that it "own[s] [its] commitments and are accountable."[19]

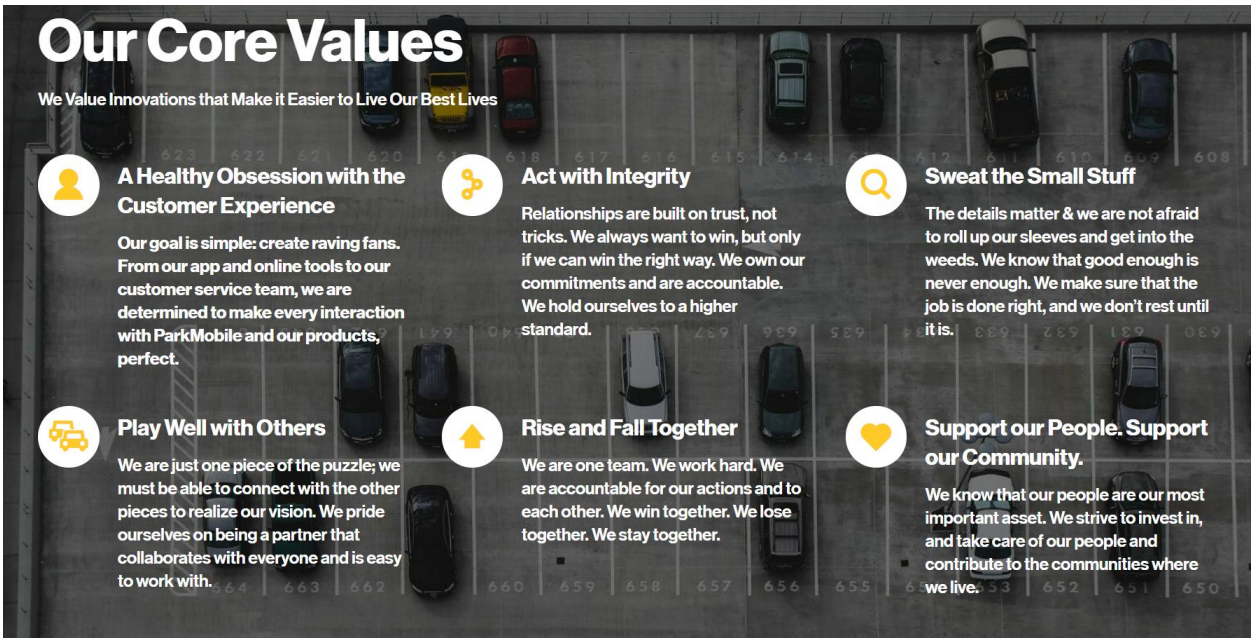


Image 2. A picture of ParkMobile's description of its "Core Values"

36. Given ParkMobile's self-described status as a "Vanguard" and technological innovator, its claimed consumer-friendly business model, and its prior representations that it would protect consumer information, users who provided their personal and sensitive data to ParkMobile when using its App or White-Label Apps

[19] *Id.*

were reasonable in believing their data was safe and secure and that ParkMobile was using reasonable security to protect their data. It was not.

37. Indeed, ParkMobile minimized any risks of its application by telling users that the only real risk of data theft was not from a breach at ParkMobile, but rather, from the users themselves: "While Parkmobile utilizes trusted methods to ensure cardholder data is protected, it is outside the scope of the Parkmobile security to ensure that a customer computer or mobile phone is not compromised."[20] After highlighting its supposedly sufficient data security measures, ParkMobile turned the issue toward its customers, warning that there are many ways in which users' data may be stolen from their own devices.

38. As it turns out, ParkMobile was wrong on both accounts. Its measures were not sufficient to protect against a data breach and, furthermore, the real risk to users' data was not from their own devices, but from ParkMobile itself. In March 2021, ParkMobile first disclosed it had been the subject of a "cybersecurity incident" and "launched an investigation" in response.[21]

[20] Member Services, *supra* note 12.

[21] *Update: Security Notification – March 2021*, ParkMobile.io (last visited Jun. 28, 2021), https://support.parkmobile.io/hc/en-us/articles/360058639032-Update-Security-Notification-March-2021

B. ParkMobile's Inadequate Data Security Measures Exposed Users' Personal and Sensitive Data

39. On March 26, 2021, ParkMobile admitted that it had "recently become aware of a cybersecurity incident linked to a vulnerability" that supposedly existed "in a third-party software that [it] use[d]." ParkMobile did not discover the breach or vulnerability itself, but rather, was put on notice by Gemini Advisory—a New York based threat intelligence firm that monitors cybercrime forums. Gemini Advisory identified a thread on a Russian-language crime forum that made available for purchase data stolen from ParkMobile.[22]

40. Initially, and despite the availability of information on the dark web, ParkMobile claimed that "no sensitive data or Payment Card Information . . . was affected."[23] As the investigation progressed, ParkMobile learned that personal and sensitive data had indeed been exposed. Less than three weeks after its initial notice, ParkMobile admitted that its "investigation has confirmed that basic user information—license plate numbers . . . email addresses and/or phone numbers, and

[22] Brian Krebs, *ParkMobile Breach Exposes License Plate Data, Mobile Numbers of 21M Users*, KrebsOnSecurity (Apr. 12, 2021), https://krebsonsecurity.com/2021/04/parkmobile-breach-exposes-license-plate-data-mobile-numbers-of-21m-users/

[23] *Security Notification*, *supra* note 21 (described in the section titled "Previous Notification from March 26, 2021").

vehicle nicknames—[were] accessed."[24] ParkMobile also disclosed that mailing addresses may have been affected.[25]

41. The Data Breach, furthermore, was not limited to users of ParkMobile's App, but included those using White-Labeled Apps. ParkMobile's Security Notification warned that "[t]his notice applies to users of the ParkMobile app and city/operator branded white-label apps" including "Go Mobile PHG, Park Columbus, meterUP, MPLS Parking, Park Houston, ParkLouie, MKE Park, FW Park, Park It Charlotte, ParkNYC, 717 Parking, Park 915, and Premier Parking."[26] The owner of many of the applications issued similar notices of the Data Breach, noting that ParkMobile, the developer of these White-Labeled Apps, had become aware of a cybersecurity incident linked to a vulnerability in a third-party software."[27]

42. Just prior to ParkMobile's second notification, KrebsOnSecurity—a website focused on providing information about ongoing data breaches—published

---

[24] *Id.* (described in the section titled "Previous Notification from April 13, 2021").

[25] Krebs, *supra* note 22 (claiming that "in a small percentage of cases, there may be mailing addresses [stolen].").

[26] *Security Notification*, *supra* note 21.

[27] *See, e.g.*, *ParkNYC Security Notice*, ParkNYC.zendesk.com (last visited Jun. 28, 2021), https://parknyc.zendesk.com/hc/en-us/articles/360060887852; Melissa Turtinen, *Minneapolis Parking App Experienced Data Breach in March*, BringMeTheNews.com (Apr. 28, 2021), https://bringmethenews.com/minnesota-news/minneapolis-parking-app-experienced-data-breach-in-march.

an article disclosing that a batch of data was for sale on the dark web that included information on 21 million ParkMobile's users.[28] KrebsOnSecurity reported that the data available for purchase included customer email addresses, dates of birth, phone numbers, license plate numbers, hashed passwords and mailing addresses.[29] Gemini Advisory confirmed KrebsOnSecurity's report that a batch of data was available for sale on a Russian-language dark website.[30]

43. The stolen data was available for sale on the dark web for an "insanely high starting price ($125,000)[.]"[31] However, other data security experts warned that, regardless of whether the data is purchased, it will become publicly available: "After a treat actor is unable to sell a stolen database or buyers begin to show little interest, it is common for the stolen data to be released on hacker forums for free as a way to increase reputation in the hacking community."[32] That is exactly what occurred here.

---

[28] Krebs, *supra* note 22.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Lawrence Abrams, *Your Stolen ParkMobile Data Is Now Free for Wannabe Scammrs*, Bleeping Computer (Apr. 30, 2021), https://www.bleepingcomputer.com/news/security/your-stolen-parkmobile-data-is-now-free-for-wannabe-scammers/.

44. After the stolen ParkMobile data had been available for purchase for some time, the hackers apparently provided links to the full database on a popular hacking forum.[33] Therefore, anyone with access to the forum could download free of charge a file containing 4.5 gigabytes of account information for 21,887,299 ParkMobile users.

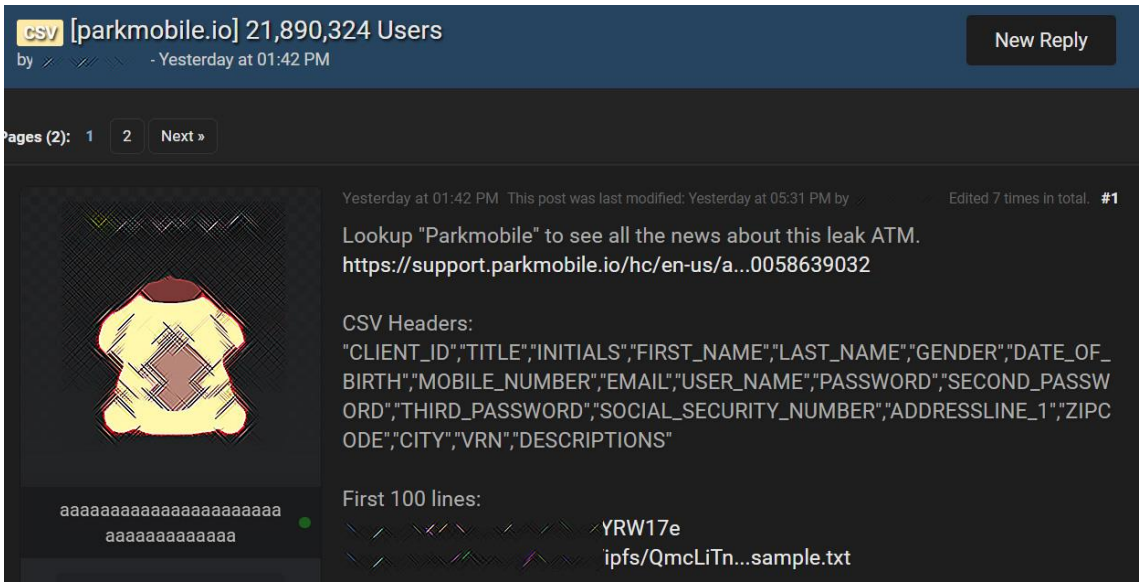
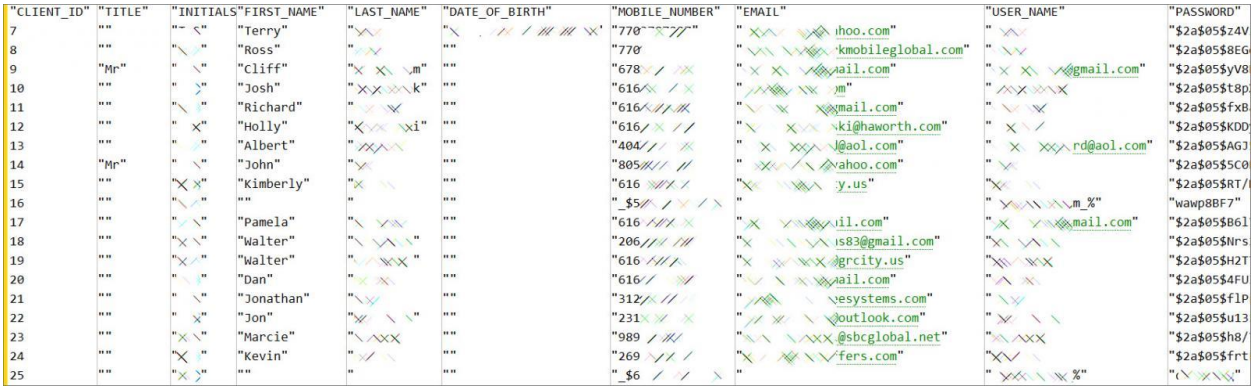


Image 3. A picture of the forum that posted links to the user data ParkMobile exposed during its Data Breach.

45. Bleeping Computer confirmed that the file contained customers' first and last names, initials, mobile numbers, email addresses, bcrypt hashed passwords, mailing address, license plate numbers, and vehicle information. Bleeping Computer also confirmed the leaked data is legitimate and actually represents information from ParkMobile users.

[33] *Id.*



"CLIENT_ID"	"TITLE"	"INITIALS"	"FIRST_NAME"	"LAST_NAME"	"DATE_OF_BIRTH"	"MOBILE_NUMBER"	"EMAIL"	"USER_NAME"	"PASSWORD"
7	""	"[illegible]"	"Terry"	"[illegible]"	"[illegible]"	"770[illegible]"	"[illegible]hoo.com"	"[illegible]"	"$2a$05$z4V
8	""	"[illegible]"	"Ross"	"[illegible]"	""	"770[illegible]"	"[illegible]kmobileglobal.com"	"[illegible]"	"$2a$05$8EG
9	"Mr"	"[illegible]"	"Cliff"	"[illegible]m"	""	"678[illegible]"	"[illegible]ail.com"	"[illegible]gmail.com"	"$2a$05$yV8
10	""	"[illegible]"	"Josh"	"[illegible]k"	""	"616[illegible]"	"[illegible]m"	"[illegible]"	"$2a$05$t8p
11	""	"[illegible]"	"Richard"	"[illegible]"	""	"616[illegible]"	"[illegible]mail.com"	"[illegible]"	"$2a$05$fxB
12	""	"[illegible]"	"Holly"	"[illegible]xi"	""	"616[illegible]"	"[illegible]ki@haworth.com"	"[illegible]"	"$2a$05$KDD
13	""	"[illegible]"	"Albert"	"[illegible]"	""	"404[illegible]"	"[illegible]l@aol.com"	"[illegible]rd@aol.com"	"$2a$05$AGJ
14	"Mr"	"[illegible]"	"John"	"[illegible]"	""	"805[illegible]"	"[illegible]ahoo.com"	"[illegible]"	"$2a$05$5C0
15	""	"[illegible]"	"Kimberly"	"[illegible]"	""	"616[illegible]"	"[illegible]y.us"	"[illegible]"	"$2a$05$RT/
16	""	"[illegible]"	""	""	""	"_$5[illegible]"	""	"[illegible]m_%"	"wawp8BF7"
17	""	"[illegible]"	"Pamela"	"[illegible]"	""	"616[illegible]"	"[illegible]il.com"	"[illegible]mail.com"	"$2a$05$B6l
18	""	"[illegible]"	"Walter"	"[illegible]"	""	"206[illegible]"	"[illegible]s83@gmail.com"	"[illegible]"	"$2a$05$Nrs
19	""	"[illegible]"	"Walter"	"[illegible]"	""	"616[illegible]"	"[illegible]grcity.us"	"[illegible]"	"$2a$05$H2T
20	""	"[illegible]"	"Dan"	"[illegible]"	""	"616[illegible]"	"[illegible]ail.com"	"[illegible]"	"$2a$05$4FU
21	""	"[illegible]"	"Jonathan"	"[illegible]"	""	"312[illegible]"	"[illegible]esystems.com"	"[illegible]"	"$2a$05$flP
22	""	"[illegible]"	"Jon"	"[illegible]"	""	"231[illegible]"	"[illegible]outlook.com"	"[illegible]"	"$2a$05$u13
23	""	"[illegible]"	"Marcie"	"[illegible]"	""	"989[illegible]"	"[illegible]@sbcglobal.net"	"[illegible]"	"$2a$05$h8/
24	""	"[illegible]"	"Kevin"	"[illegible]"	""	"269[illegible]"	"[illegible]fers.com"	"[illegible]"	"$2a$05$frt
25	""	"[illegible]"	""	""	""	"_$6[illegible]"	""	"[illegible]%"	"[illegible]"

Image 4. A picture of the .csv file containing the data ParkMobile exposed during the Data Breach.

46. Users, in fact, can now search the website, "Have I Been Pwned", which will disclose whether their data was exposed specifically as a result of the Data Breach, and receive a list of the exposed data.[34]

47. Although the stolen passwords were encrypted, almost all data security experts advised ParkMobile users to change their passwords immediately.[35] One expert warned that "[i]t is highly recommended that you change your password immediately" because "both the email and passwords were leaked, [and] they can be used by hackers to log in your online account[s]." The expert warned that having their passwords exposed in the Data Breach "is extremely risky, since many people

[34] *Id.*; HaveIBeenPwned.com (last visited, Aug. 12, 2021), https://haveibeenpwned.com/.

[35] Krebs, *supra* note 22; Abrams, *supra* note 32.

have the habit of using the same password across their online and social media accounts."[36]

48. Even though user passwords were encrypted—which is the basis of ParkMobile's claims that it took "extensive" measures to protect passwords—the fact of encryption does not prevent threat actors from obtaining the plain text passwords. Rather, due to the sheer volume of data stolen, threat actors have sufficient data to "crack" or reverse the encryption. One data security expert explained that bcrypt—the encryption tool used by ParkMobile—is not infallible.[37] Instead, "[b]ecause passwords created by humans are not chosen at random, then it does become computationally feasible (and often quite practical) to discover the original [password] based on the hash." Thus, while bycrpt "can slow down an attack from performing millions of computations per second, to just thousands[,]" that only means the attackers "need to do more work than they otherwise would to guess passwords stolen" in a data breach, and "it is not an 'infeasible' amount of work."[38]

---

[36] *ParkMobile Data Breach: Why You Should Be Concerned*, TrendMicro.com (last visited, Aug. 12, 2021), https://news.trendmicro.com/2021/05/28/parkmobile-data-breach-why-you-should-be-concerned/.

[37] Jeffery Goldberg, *Bcrypt is great, but is password cracking "infeasible"?*, 1password.com (Mar. 30, 2015), https://blog.1password.com/bcrypt-is-great-but-is-password-cracking-infeasible/.

[38] *Id.*

49. Another expert similarly explained that, with respect to the ParkMobile breach: "The ParkMobile passwords were hashed with an algorithm called bcrypt, which is difficult to convert into plaint text passwords. However, it's not impossible for the threat actor to do so over time. Once threat actors . . . gain your plaint text passwords, they will use your email address and password combination to log in to other websites using credential stuffing attacks."[39]

50. Furthermore, although it claimed to have taken "extensive measures to protect user passwords," ParkMobile only recommended, and did not require, that users change their passwords because only "encrypted passwords were accessed[.]"[40] KrebsOnSecurity noted, however, that it was unusual that ParkMobile was not requiring users to change their passwords given that those passwords had been stolen and the encryption would be reversible.[41] Therefore, KrebsonOnSecurity, like other experts, warned that "[i]f your data was exposed as part of this breach, the first thing you should do is immediately change your passwords at other sites using the same password as ParkMobile."[42]

---

[39] Abrams, *supra* note 32.

[40] *Security Notification*, *supra* note 21 (described in the section titled "Update: April 15, 2021").

[41] Krebs, *supra* note 22.

[42] *Id.*

51. Given the significant risk, Brian Krebs, and others, found ParkMobile's decision not to require new passwords to be dangerous and unusual.[43]

C. ParkMobile Disregarded Data Security Despite Knowing of the Need to Protect Users' Personal and Sensitive Data

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

53. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' personal and sensitive data, ParkMobile assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' personal and sensitive data from disclosure.

54. Plaintiffs and Class Members reasonably expected that service providers such as Defendant would 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.

55. ParkMobile knew of the need to protect users' personal and sensitive data. It acknowledged the need to protect users' privacy interests because it

[43] *Id.*

"collect[s], use[s], and share[s] information that [it] collect[s] through the ParkMobile website, mobile applications, and other services [it] operates."[44] Despite acknowledging the sensitive nature of the user data it collects, ParkMobile both implemented security measures that were woefully deficient and, additionally, failed to enact measures that were necessary to reasonably secure user data.

56. ParkMobile acknowledged that the Data Breach was a result of its disregard of data security. Even prior to the Data Breach, ParkMobile flatly admitted that it "[couldn't] guarantee that unauthorized third parties won't be able to defeat our security measures"[45] and, additionally, stated its "practices are [not] 100% secure, and we do not guarantee the security of your information."[46] Security best practices place the responsibility to secure sensitive data on the entity most capable of doing so. In this case, ParkMobile, as the entity that collected and stored user data was the *only* entity capable of reasonably securing Plaintiffs' and other users' data.

57. ParkMobile's passive attitude towards data security is not consistent with its obligations under the Payment Card Industry Data Security Standards ("PCI

---

[44] *Privacy Policy*, ParkMobile.io (last visited, Aug. 13, 2021), https://parkmobile.io/privacy-policy/

[45] *Terms of Use*, ParkMobile.io (last visited Aug. 12, 2021), https://parkmobile.io/terms-of-use/

[46] *Privacy Policy*, *supra* note 44.

DSS"), with data security best practices, or with the responsibilities incumbent on ParkMobile given that it has chosen to solicit (and in fact, require) users to provide sensitive data and store that data over time.

58. Indeed, "[w]ell-designed data storage security is . . . mandated by various compliance regulations such as the PCI-DSS" and is "an area that is of critical importance to enterprises because the majority of data breaches are ultimately caused by a failure in data storage security."[47] The international standard for storage security, ISO/ IEC 27040, calls for the use of physical, technical, and administrative controls to protect storage systems and infrastructure, and the data stored within. The Storage Networking Industry Association (SNIA) notes that compliance with ISO/IEC 27040 defines best practices that ultimately set the *minimum* expectations for storage security.

59. ParkMobile implemented data security practices that were not compliant with ISO/ IEC 27040, or the minimum expectations for reasonable data security. In fact, ParkMobile put the onus on *users* to keep their data safe. ParkMobile consistently warned users that the risk of a breach and theft of personal data derived from users' own inability to protect their devices. ParkMobile knew, or should have known, that its repository of over 20 million users' personal and

[47] Paul Rubens, *Data Storage Security: Best Practices for Security Teams*, ESecurity Planet (Jun. 6, 2019), https://www.esecurityplanet.com/cloud/data-storage-security-best-practices-for-security-teams/.

sensitive data (which, as ParkMobile acknowledged, was growing rapidly) would be a significant target to attackers.

60. Despite that knowledge, ParkMobile admitted that its actions had put users' data at risk by implementing inadequate data security measures. Specifically, after the Data Breach, ParkMobile acknowledged it needed to take measures to enhance its cybersecurity. For example, in its March 26, 2021 Data Breach notification, ParkMobile noted the need to take "additional precautionary steps since learning of the incident, including eliminating the third-party vulnerability, maintaining our security, and continuing to monitor our systems."[48] Nearly a month after the Data Breach, ParkMobile was apparently still working on resolving its deficient data security program, and noted that it was continuing its efforts to "maintain [its] security and monitor [its] systems."[49]

61. As a technology leader, ParkMobile knew, or should have known, that it needed to implement measures to adequately protect personal and sensitive data. ParkMobile consistently represented that it was technologically sophisticated, a leader in technological innovation, and a consumer-centric business with a "healthy obsession" for customer service.

---

[48] *Security Notification*, *supra* note 21 (described in the section titled "Previous Notification from March 26, 2021").

[49] *Id.* (described in the section titled "Previous Notification from April 15, 2021").

62. It also publicly acknowledged its obligation to comply with PCI DSS—bare minimum data security standards required for processors of payment cards. The PCI DSS, similar to other data security standards, requires certain protections over stored data.[50] In its notices on the Data Breach, ParkMobile similarly acknowledged it was required to implement certain, basic security measures to protect passwords and payment card data. In fact, as far back as 2012, ParkMobile wrote that it "is a PCI Level 1 Vendor" meaning it had to "ensure that our cardholder capture, handling, encryption and storage [were] all compliant with industry methods."[51] PCI DSS requires that ParkMobile take measures to prevent unauthorized access to stored payment card data.[52]

63. Other sources have also provided warnings to companies like ParkMobile of the need to protect sensitive data.

64. For example, the FTC has issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[53] According to

---

[50] *See, e.g.*, *PCI DSS Data Storage Do's and Don'ts*, PCI Security Standards Council (Oct. 2010)

[51] *See* Member Services, *supra* note 12.

[52] *Data Storage Do's and Don'ts*, *supra* note 50.

[53] Federal Trade Comm'n, *Start with Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015),

the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[54]

65. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

66. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW,*

---

https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[54] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

Inc., No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

67. These orders, which all proceeded ParkMobile's Data Breach, further clarify the measures businesses must take to meet their data security obligations and put ParkMobile on notice of the requirements to protect user data.

D. ParkMobile's Data Breach Harmed Plaintiffs and the Class

68. Plaintiffs' and the Class's data exposed in the Data Breach constitute the type of data specifically targeted by and valuable to hackers.

69. Indeed, hackers increasingly sell these personal and sensitive records on the black market to purchasers who seek to use the personally identifying

information to create fake IDs, make fraudulent transactions, obtain loans or commit other acts of identity theft.[55] With respect to the Data Breach, security experts warned that (1) "threat actors" would attempt to crack the encrypted passwords and "use your email address and password combination to log in to other websites uses credential stuffing attacks" and (2) ParkMobile users should expect "phishing emails and SMS tests that use the exposed data to try and steal even more sensitive information from you."[56] That risk is magnified here, because the ParkMobile data is now available online to all for free, meaning any threat actors can make free use of that data.

70. When data is exposed and available for free online, as it was here, the risk of identity theft is lasting. The U.S. Government Accountability Office's research into the effects of data breaches found 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 has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the

[55] *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/

[56] Abrams, *supra* note 32.

harm resulting from data breaches cannot rule out the significant risk of future harm."[57]

71. The type of personal and sensitive data exposed in the Data Breach is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers and includes data not found in other breaches (like license plate numbers). As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud, and can use stolen user names and passwords to steal additional personal and sensitive information from other applications and websites.[58] For that reason, a robust "cyber black market" exists in which criminals openly post stolen personally-identifying informaiton and other protected financial information on the dark web.

72. Because the stolen ParkMobile data has been posted publicly, it is now freely available for any threat actor to perpetrate scams, fraud, identity theft, or some combination of the three against Plaintiffs' and the Class. In other words, each Plaintiff and Class member are at a substantial and continued risk of future harm.

[57] Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (Jun. 2007), http://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 30, 2018).

[58] FTC Consumer Information, *What to Know about Identity Theft*, ftc.gov (last visited, Aug. 13, 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

As described further below, each Plaintiff has already suffered harm responding to and mitigating the risk of the Data Breach.

1. Tyler Baker

73. Baker downloaded and used ParkMobile starting in 2016 to pay for parking at meters. To use the App, ParkMobile required that he provide personal and sensitive information, including his name, license plate number, email address, mailing address, and other information. Baker provided all the information ParkMobile required.

74. Around March 2016, Baker received a notice from Experian that his information was involved in the Data Breach. Baker reviewed the website, "Have I Been Pwned"—a website that will inform users whether their email address or phone number was exposed in a data breach. "Have I Been Pwned" listed Baker's email, license plate numbers, passwords, and phone numbers as having been compromised due to the Data Breach.

75. The Data Breach has caused Baker harm. Baker spent time changing passwords on other accounts that used the same password as the one exposed in the Data Breach. Baker's PayPal account, which used the same password as the one exposed in the Data Breach, was compromised and closed due to suspicious activity. Baker also had fraudulent charges on his debit card, which is the same debit card he used to pay on ParkMobile. Finally, he also had a fraudulent account opened in his

name with Comcast. The timing and proximity of the fraudulent activity—right after the Data Breach—suggests the two are causally related. Due to the fraudulent activity, Baker purchased fraud monitoring services for $25 per month to prevent any further harm. Because his personal and sensitive information is now available for free to find on the dark web, he remains at a continued and heightened future risk of identity theft and fraud.

2. Miriam George

76. George used and provided information to ParkMobile for the purpose of using its App for parking. ParkMobile required George to provide personal and sensitive information to use the App, including his name, license plate number, email address, mailing address, and other information. George provided all the information ParkMobile required.

77. Upon learning of the Data Breach, George spent time monitoring accounts and changed the passwords on any account that used the same password as the one exposed in the Data Breach.

3. Emma Jackson

78. Jackson used and provided information to ParkMobile for the purpose of parking on his college campus in California. To use the App, ParkMobile required that Jackson provide personal and sensitive information, including her name, license

plate number, email address, mailing address, and other information. Jackson provided all the information ParkMobile required.

79. On May 5, 2021, Jackson received an email alert from Capital One ID Monitoring that her email, phone number, and password had been found on the dark web as a result of the Data Breach. Jackson also received an email from ParkMobile on April 23, 2021 alerting her of the Data Breach, but she only later discovered that email because it had been sent to spam.

80. Upon learning of the Data Breach, Jackson spent time changing all the passwords on other accounts that used the same password exposed during the Data Breach. She also noticed duplicate accounts being created in her name on Instagram and LinkedIn. Given the timing of the fraudulent accounts and the Data Breach, the two are likely causally related. Because her personal and sensitive information is now available for free to find on the dark web, she remains at a continued and heightened future risk of identity theft and fraud.

4. Plaintiff Sait Kurmangaliyev

81. Kurmangaliyev used and provided information to ParkNYC, ParkMobile's application for its users in New York City. ParkNYC solicited personal and sensitive information from Plaintiff, including his name, license plate number, email address, mailing address, and other information. Kurmangaliyev provided all the information ParkNYC required.

82. Around March 2021, Kurmangaliyev received a notice from Credit Karma stating: "In March 2021, ParkMobile's database was allegedly breached. Even if you don't use your ParkMobile account anymore, it's important to protect any info that was exposed." Credit Karma further warns that Plaintiff's data, including, but not limited to, his name, date of birth, email address, password and phone number, were exposed.

83. Kurmangaliyev already reported seeing a noticeable increase in spam shortly after the Data Breach, both spam sent directly to his phone and spam emails. After the Data Breach, he signed up for credit and identity theft monitoring, and froze his credit on several websites, including Equifax, Transunion, Experian, and LexisNexis. Kurmangaliyev also changed passwords on sensitive accounts that had previously used the same password as the one exposed in the Data Breach. Given the close proximity of the Data Breach and Kurmangaliyev's increased exposure to spam calls and emails, it is likely that the increase in spam is a direct result of the theft of Kurmangaliyev's data from ParkMobile. Because his personal and sensitive information is now available for free to find on the dark web, he remains at a continued and heightened future risk of identity theft and fraud.

5. Gregory Manson

84. Manson used and provided information to ParkMobile for the purpose of using the App for parking. He has owned and used the App for several years.

ParkMobile solicited personal and sensitive information from Manson, including his name, license plate number, email address, mailing address, and other information. Manson provided all the information ParkMobile required.

85. In April 2021, Manson received a warning from Chase Journey App—a fraud monitoring application for his phone—that the Data Breach may have exposed his email and password. On May 22, 2021, he received an email from ParkMobile warning him of the Data Breach.

86. Upon learning of the Data Breach, Manson spent time investigating the Data Breach and the information disclosed. He monitored his accounts for fraudulent activity, and changed his passwords on applications and websites that used the same password as the one exposed in Data Breach. On one account, he was notified that someone had attempted to use his username and password to login fraudulently. Because his personal and sensitive information is now available for free to find on the dark web, he remains at a continued and heightened future risk of identity theft and fraud.

6. Heriberto Travieso

87. Travieso used and provided information to ParkMobile for the purpose of using its App for parking. ParkMobile required Travieso to provide personal and sensitive information to use the App, including his name, license plate number, email

address, mailing address, and other information. Travieso provided all the information ParkMobile required.

88. Travieso was notified that his information was impacted in the Data Breach.

89. Upon learning of the Data Breach, Travieso spent time changing the passwords on accounts that used the same password exposed in the Data Breach. He also spent time freezing his credit cards and monitoring various accounts for fraudulent or suspicious activity. Travieso's Netflix, PayPal, Venmo, and credit card accounts appear to have been compromised due to the Data Breach. Specifically, Travieso experienced unauthorized logins to his Netflix accounts, and attempts to charge his credit card, PayPal and Venmo accounts. Given the close timing of those fraudulent activities and the Data Breach, they are likely causally connected.

CLASS ALLEGATIONS

90. Plaintiffs brings this action on behalf of themselves and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All individuals that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.

91. Excluded from the class is ParkMobile and its subsidiaries and affiliates; all employees of ParkMobile; all persons who make a timely election to

be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

92. In the alternative, Plaintiffs propose the following Subclasses:

> **California Subclass:** All residents of California that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.
>
> **Florida Subclass:** All residents of Florida that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.
>
> **Pennsylvania Subclass:** All residents of Pennsylvania that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.
>
> **New York Subclass:** All residents of New York that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.
>
> **Virginia Subclass:** All residents of Virginia that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.
>
> **Vermont Subclass:** All residents of Vermont that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.

93. Plaintiffs reserve the right to, after conducting discovery, modify, expand or amend the above Class and Subclass definitions or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

94. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiffs believe that there are millions of members of the Nationwide Class, and hundreds of thousands of members of each Subclass. The number of reportedly impacted individuals already exceeds 21 million U.S. users—and each users' information is readily available for free to download on hacking forums. The precise number of class members, however, is not yet known to Plaintiffs. Class members may be identified through objective means and, in fact, ParkMobile, has already provided notice to individuals affected by the Data Breach. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

95. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether ParkMobile knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether ParkMobile controlled and took responsibility for protecting Plaintiffs' and the Class's data when it solicited that data, collected it, and stored it on its servers;

c. Whether ParkMobile's security measures were reasonable in light of the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether ParkMobile acted in bad faith by abrogating its responsibility to protect user data from theft;

e. Whether ParkMobile owed Plaintiffs and the Class a duty to implement reasonable security measures;

f. Whether ParkMobile's failure to adequately secure Plaintiffs' and the Class's data constitutes a breach of its duty to institute reasonable security measures;

g. Whether ParkMobile's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiffs' and the Class's data;

h. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

i. Whether Plaintiffs and the Class were injured and suffered damages or other losses because of ParkMobile's failure to reasonably protect its data systems; and

j. Whether Plaintiffs and the Class are entitled to relief.

96. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs are typical members of the Class. Plaintiffs and the Class are each persons who provided data to ParkMobile, whose data resided on ParkMobile's servers, and whose personally identifying information was exposed in the Data Breach. Plaintiffs'

injuries are similar to other class members and Plaintiffs seek relief consistent with the relief due to the Class.

97. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against ParkMobile to obtain relief for themselves and for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs also have retained counsel competent and experienced in complex class action litigation of this type, having previously litigated numerous data breach cases on behalf of consumers and financial institutions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

98. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their

damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

99. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), ParkMobile, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CHOICE OF LAW

100. ParkMobile's terms and conditions state: "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 or the Services."

101. ParkMobile's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Georgia and the tortious and deceptive acts complained of occurred in, and radiated from, Georgia.

102. The key wrongdoing at issue in this litigation (ParkMobile's failure to employ adequate data security measures) emanated from its headquarters in Georgia.

103. ParkMobile's corporate IT personnel operate out of and are located at its headquarters in Georgia.

104. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. businesses against a company doing business in Georgia, has a greater

interest in the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

105. Application of Georgia law to a nationwide Class with respect to Plaintiffs' and the Class members' 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 the Plaintiff and the nationwide Class.

LEGAL CLAIMS

COUNT I
Negligence
(On behalf of the Nationwide Class)

106. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1 – 99 as if fully set forth herein.

107. ParkMobile owed a duty to Plaintiffs and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiffs and the Class, managed and stored. This duty arises from multiple sources.

108. ParkMobile owed a common law duty to Plaintiffs and the Class to implement reasonable data security measures because it was foreseeable that hackers would target ParkMobile's data systems and servers containing Plaintiffs' and the Class's sensitive data and that, should a breach occur, Plaintiffs and the Class would be harmed. ParkMobile alone controlled its technology, infrastructure, digital

platforms, and cybersecurity that were exposed during the Data Breach and allowed hackers to breach and steal ParkMobile's user database. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiffs and the Class. ParkMobile knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen, and that individual need would continue long after the Data Breach ended. Therefore, the Data Breach, and the harm it caused Plaintiffs and the Class, was the foreseeable consequence of ParkMobile's unsecured, unreasonable data security measures.

109. ParkMobile, furthermore, assumed a duty to protect user data by soliciting sensitive user data, collecting that data, and storing that data in its own databases. In fact, users were not allowed to utilize any portion of ParkMobile's App or services without first providing the sensitive nature that was stored by, and ultimately stolen from, ParkMobile. ParkMobile was the only entity capable of implementing reasonable measures to protect user data.

110. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required ParkMobile to take reasonable measures to protect Plaintiffs' and the Class's sensitive data and is a further source of ParkMobile's duty to Plaintiffs and the Class. Section 5 prohibits unfair practices in

or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like ParkMobile of failing to implement and use reasonable measures to protect sensitive data. ParkMobile, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of ParkMobile's duty to adequately protect sensitive information. By failing to implement and use reasonable data security measures, ParkMobile acted in violation of § 5 of the FTCA.

111. ParkMobile is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring ParkMobile to exercise reasonable care with respect to Plaintiffs and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, ParkMobile was the only entity of adequately protecting the data that it alone solicited, collected, and stored. ParkMobile, however, attempted to put the onus on users to protect their data by claiming, among other things, that the most likely risk to user data was from the theft and misuse of their devices, rather than a breach of ParkMobile's systems and databases.

112. ParkMobile breached its duty to Plaintiffs and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. As a self-proclaimed technology "Vanguard", ParkMobile knew or should have known that hackers might target sensitive data that ParkMobile solicited and collected on its users and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, ParkMobile acknowledged it was subject to certain standards to protect cardholder data and password information and utilize other industry standard data security measures. ParkMobile, furthermore, represented to users that their data was safe with ParkMobile.

113. ParkMobile was fully capable of preventing the Data Breach. ParkMobile, as a smart technology expert, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented and used, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. ParkMobile thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

114. As a direct and proximate result of ParkMobile's negligence, Plaintiffs and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*
(On behalf of the Nationwide Class)

115. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1–99 as if fully set forth herein.

116. ParkMobile's unreasonable data security measures and failure to timely notify Plaintiffs and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which ParkMobile failed to do.

117. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like ParkMobile of failing to implement and use reasonable measures to protect users' sensitive data. The FTC publications and orders described above also form the basis of ParkMobile's duty.

118. ParkMobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. ParkMobile's conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its users and the foreseeable consequences of a Data Breach should ParkMobile fail to secure its systems.

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

120. ParkMobile's unreasonable data security measures and failure to timely notify Plaintiffs and the Class of the Data Breach violates the Georgia Constitution ('the Constitution') which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution 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.

121. This duty has been recognized by the Georgia Supreme Court in the 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.

122. ParkMobile's implementation of inadequate data security measures, its failure to resolve known vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required users to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

123. Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes), the Georgia Constitution and the Restatement of the Law of Torts (Second), was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes), the Georgia Constitution and the Restatement of the Law of Torts (Second) were intended to guard against. 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 type of harm suffered by Plaintiffs and the Class. Moreover, courts in Georgia have recognized consumer's rights under the Georgia Constitution and the Restatement of the Law of Torts (Second), by allowing claims against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiffs and the Class.

124. As a direct and proximate result of ParkMobile's negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury.

COUNT III
Violation of O.C.G.A. § 13-6-11
(On behalf of the Nationwide Class)

125. Plaintiffs repeat and re-allege the foregoing allegations contained in paragraphs 1–99 as if fully set forth herein.

126. ParkMobile through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

127. 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 implement and use reasonable measures to protect PII. Various FTC publications and orders also form the basis of ParkMobile's duty.

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

129. ParkMobile also has a duty under the Georgia Constitution ('the Constitution') which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution 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.

130. This duty has been recognized by the Georgia Supreme Court in the 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.

131. ParkMobile's implementation of inadequate data security measures, its failure to resolve known vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required users to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

132. ParkMobile knew or should have known that it had a responsibility to protect the consumer data it required users to provide and stored, that it was entrusted with this data, and that it was the only entity capable of adequately protecting the data on its systems and databases.

133. Despite that knowledge, ParkMobile abdicated its duty to protect the data it solicited and stored, and instead put the onus on its users to protect their data. For example, ParkMobile represented to users that the only real risk of the theft of their data came from the users themselves, and the theft of data off of their smart phones, not supposedly "numerous methods by which hackers may steal information from [users'] computers and hand-held devices." Indeed, ParkMobile flatly

represented that its practices were not "100% secure" and that it would "not guarantee the security of your information." Thus, despite collecting and storing users' personal and sensitive data, ParkMobile did not intend to protect it. Rather, it hoped to avoid any responsibility and liability for stolen data by claiming it was impossible to fully protect it.

134. That, however, is not true. As numerous data security experts and data security standards make clear, even bare minimum measures can protect stored data from a data breach. ParkMobile, however, refused to do the bare minimum. Indeed, it wasn't until after the Data Breach that ParkMobile took efforts to improve its data security and remove vulnerabilities that existed within its digital platforms.

135. Unfortunately for Plaintiffs and the Class, ParkMobile's efforts came too late. As a direct and proximate result of ParkMobile's actions, Plaintiffs' and the Class' personal and sensitive data was stolen, put up for sale on the dark web, and eventually, posted in plain view on a dark web forum for anyone to view and steal. As further alleged above, the Data Breach was a direct consequence of ParkMobile's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the personal and sensitive data unsecured. Had ParkMobile adopted reasonable data security measures, it could have prevented the Data Breach.

136. As further described above, Plaintiffs and the Class have been injured and suffered losses directly attributable to the Data Breach.

137. Plaintiffs therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT IV
Violation of the California Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*
(On behalf of the California Subclass)

138. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1–99 as if fully set forth herein.

139. The Consumers Legal Remedies Act ("CLRA") is liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

140. ParkMobile is a "person" as defined by the CLRA, and it provided "services" as defined under the act. Cal. Civ. Code §§ 1761(b)-(c), 1770.

141. The CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." *Id.* at § 1770(a)(5).

142. Additionally, the CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another." *Id.* at § 1770(a)(7).

143. Plaintiff Jackson and the California Subclass members are "consumer[s]" as who were engaged in a "transaction" under the act. *Id.* at §§ 1761(d)-(e), 1770.

144. ParkMobile's acts and practices were intended to and did result in the sales of services to Plaintiffs and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Jackson's and the California Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jackson's and California Subclass members' sensitive data, including duties imposed by the Federal Trade

Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Jackson's and California Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jackson's and California Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

145. ParkMobile's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

146. Had ParkMobile disclosed, rather than concealing, to Plaintiffs and class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

147. Instead, ParkMobile received, maintained, and compiled Plaintiffs' and class members' sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiff Jackson and Class members that ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Jackson and the California Subclass members acted reasonably in relying on ParkMobile's omissions, the truth of which they could not have discovered.

148. Plaintiff Jackson and the California Subclass are contemporaneously providing notice in compliance with California Civil Code § 1782(a) and will amend their claims for damages to Defendants.

149. Pursuant to §1782(a) of the CLRA, on August 18, 2021, Plaintiff Jackson's counsel notified Defendants in writing by certified mail of the particular violations of §1770 of the CLRA and demanded that it rectify the problems associated with the actions detailed above and give notice to all affected consumers of Defendants' intent to act. If Defendants fail to respond to Plaintiffs' letter or agree to rectify the problems associated with the actions detailed above and give notice to all affected consumers within 30 days of the date of written notice, as proscribed by

§1782, Plaintiff Jackson will move to amend the Complaint to pursue claims for actual, punitive, and statutory damages on behalf of himself and the California Subclass, as appropriate against Defendants. As to this cause of action, at this time, Plaintiff Jackson seeks injunctive relief, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

150. Plaintiff Jackson and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT V
Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.20, *et seq.*
(On behalf of the Florida Subclass)

151. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1–99 as if fully set forth herein.

152. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") was enacted to "protect the consuming public and legitimate business enterprises form those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce" and "[t]o make state consumer practices and enforcement consistent with established policies of federal law relating to consumer protection." Fla. Stat. § 501.202(2)-(3).

153. Plaintiff Travieso and Florida Subclass members are "consumer[s]" as defined by § 501.203(7).

154. The FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" *Id*. § 501.204(1). ParkMobile advertised and offered services in Florida and engaged in commerce directly or indirectly affecting the people of Florida, including by offering serves to Plaintiff Travieso and the Florida Subclass in exchange for a transaction fee. *See id*. at § 401.203(8).

155. ParkMobile engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Travieso and the Florida Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Travieso and Florida Subclass members' sensitive data, including duties imposed by the Federal Trade

Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Travieso's and Florida Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Travieso's and Florida Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

156. ParkMobile's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

157. Had ParkMobile disclosed to Plaintiff Travieso and Florida Class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

158. Instead, ParkMobile received, maintained, and compiled Plaintiff Travieso's and class members' sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiffs and Class members that ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiffs and the Florida Subclass members acted reasonably in relying on ParkMobile's omissions, the truth of which they could not have discovered.

159. Plaintiffs Travieso and the Florida Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the FUDTPA.

COUNT VI
Violation of New York General Business Law § 349
(On behalf of the New York Subclass)

160. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-99 as if fully set forth herein.

161. ParkMobile engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services in New York, in

violation of N.Y. Gen. Bus. Law ("GBL") § 349. Specifically, ParkMobile performed the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Kurmangaliyev's and the New York Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kurmangaliyev's and New York Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Kurmangaliyev's and New York Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff Kurmangaliyev's and New York Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

162. These unfair and deceptive acts were consumer-oriented because they were geared towards the public and intended to encourage consumers to use ParkMobile's App without awareness as to the security deficiencies in ParkMobile's systems, digital platform, and data storage. Additionally, ParkMobile's omissions as to its data security were materially misleading because no reasonable consumer would have used ParkMobile had they known that ParkMobile did not prioritize data security, had implemented knowingly inadequate data security, and had failed to meet basic standards representing the bare minimum security measures necessary to protect data. Furthermore, Plaintiff Kurmangaliyev and the New York Subclass suffered harm as a result of ParkMobile's conduct, specifically, that their sensitive user data was exposed putting all Class members at risk and causing Class members to respond by taking appropriate action to prevent further harm.

163. ParkMobile's omissions were additionally material because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

164. Had ParkMobile disclosed to Plaintiff Kurmangaliyev and the New York Class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

165. Instead, ParkMobile received, maintained, and compiled Plaintiff Kurmangaliyev's and New York Subclass members' sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiffs and Class members that ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Kurmangaliyev and the New York Subclass members acted reasonably in relying on ParkMobile's omissions, the truth of which they could not have discovered.

166. Plaintiffs Kurmangaliyev and the New York Subclass seek all monetary and non-monetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the New York GBL.

COUNT VII
Violation of the Pennsylvania Unfair Trade Practices & Consumer Protection Law, 73 Penn. Stat. §§ 201-1, *et seq.*
(On behalf of the Pennsylvania Subclass)

167. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-99 as if fully set forth herein.

168. The Pennsylvania Unfair Trade Practices & Consumer Protection Law ("UTPCPL") prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade . . . ." Penn. Stat. § 201-3. Prohibited acts include:

a. Using deceptive representation or designations of geographic origin in connection with goods or services. *Id.* at § 201-2(4)(iv).

b. Representing that goods or services have sponsorship, approval, characteristics, ingredients, users, benefits, or quantities that they do not have or that a person has a sponsorship approval, status, affiliation, or connection that they do not have. *Id.* at § 201-2(4)(v).

c. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another. *Id.* at § 201-2(4)(vii).

d. Engaging in other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding. *Id.* at § 201-2(4)(xxi).

169. ParkMobile engaged in deceptive acts or practices in violation of the UTPCPL. Specifically, ParkMobile performed the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff George's and the Pennsylvania Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and the Pennsylvania Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff George and Pennsylvania Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff George's and Pennsylvania Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

170. Plaintiff George and the Pennsylvania Subclass members are "persons" under the act, *id.* at § 201-2(2), and used ParkMobile primarily for personal, family, or household purposes. *Id.* at § 201-9.2(a). Additionally, Plaintiffs George and the Pennsylvania Subclass suffered ascertainable loss of money because they paid transaction fees when using ParkMobile that, had they known of ParkMobile's representations, they would not have paid.

171. ParkMobile's omissions were material to Plaintiff George and the Pennsylvania Subclass because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

172. Had ParkMobile disclosed to Plaintiff George and the Pennsylvania Subclass members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

173. Instead, ParkMobile received, maintained, and compiled Plaintiff George's and the Pennsylvania Subclass's sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiffs and Class members that ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff George and the Pennsylvania Subclass members acted reasonably in relying on ParkMobile's omissions, the truth of which they could not have discovered.

174. Plaintiffs George and the Pennsylvania Subclass seek all monetary and non-monetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the UTPCPL.

COUNT VIII
Violation of the Virginia Consumer Protection Act, §§ 59.1-196, *et seq.*
(On behalf of the Virginia Subclass)

175. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-99 as if fully set forth herein.

176. The Virginia Consumer Protection Act ("VA CPA") is "applied as remedial legation to promote fair and ethical standards of dealings between suppliers

and the consumer public." V.S. § 59.1-197. The VA CPA prohibits "fraudulent acts or practices committed by a suppliers in connection with a consumer transaction[,]" including: "[m]isrepresenting that goods or services are of a particular standard, quality, grade, style, or model. *Id.* at § 59.1-200(6).

177. ParkMobile engaged in deceptive acts or practices in violation of the VA CPA. Specifically, ParkMobile performed the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Manson's and the Virginia Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Manson's and the Virginia Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Manson and Virginia Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Manson's and Virginia Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

178. ParkMobile is a "supplier" because it is a "seller . . . who advertises, solicits, or engages in consumer transactions . . . ." *Id.* at § 59.1-198.

179. ParkMobile's omissions were material to Plaintiff Manson and the Virginia Subclass because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

180. Had ParkMobile disclosed to Plaintiff Manson and the Virginia Subclass members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

181. Instead, ParkMobile received, maintained, and compiled Plaintiff Manson's and the Virginia Subclass's sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiffs and Class members that ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Manson and the Virginia Subclass members acted reasonably in relying on ParkMobile's omissions, the truth of which they could not have discovered.

182. Plaintiffs Manson and the Virginia Subclass seek all monetary and non-monetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the VCPA.

COUNT IX
Violation of the Vermont Consumer Protection Act, 9 V.S.A. § 2451, *et seq.*
(On behalf of the Vermont Subclass)

183. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-99 as if fully set forth herein.

184. The Vermont Consumer Protection Act ("VT CPA") is intended to "complement the enforcement of federal statutes and decisions governing unfair

methods of competition, unfair or deceptive acts or practices, and anti-competitive practices in order to protect the public and to encourage fair and honest competition." 9 V.S.A. § 2451.

185. The VT CPA declares "[u]nfair methods of competition in commerce and unfair or deceptive acts or practices in commerce . . . unlawful." *Id.* at § 2453(a). The VT CPA, furthermore, is intended to be similarly construed to the Section 5 of FTC Act. *Id.* at § 2453(b).

186. Plaintiff Baker and the members of the Vermont Subclass are "consumers" within the definition provided by the VT CPA. *Id.* at § 2451a(a).

187. ParkMobile committed "unfair or deceptive acts or practices in commerce" in violation of the VT CPA, including the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Baker's and the Vermont Subclasses' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Baker's and the Vermont Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Baker and Vermont Subclass members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Baker's and Vermont Subclass members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

188. ParkMobile's omissions were material to Plaintiff Baker and the Vermont Subclass because they were likely to and did deceive reasonable consumers about the adequacy of ParkMobile's data security and ability to protect the confidentiality of consumers' sensitive information that ParkMobile solicited, collected, and stored.

189. Had ParkMobile disclosed to Plaintiff Baker and the Vermont Subclass members that their cybersecurity, digital platforms, and data storage systems were

not secure and, thus, vulnerable to attack, ParkMobile would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

190. Instead, ParkMobile received, maintained, and compiled Plaintiff Baker's and the Vermont Subclass's sensitive data as part of the services ParkMobile provided and for which Plaintiffs and class members paid, in part, through transaction fees by omitting and concealing information from Plaintiffs and Class members that (1) ParkMobile's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' sensitive data and (2) that ParkMobile was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Baker and the Vermont Subclass members acted reasonably in relying on ParkMobile's omission, the truth of which they could not have discovered.

191. Plaintiffs Baker and the Vermont Subclass seek all monetary and non-monetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the VT CPA.

COUNT X
Declaratory and Injunctive Relief
(On behalf of the Nationwide Class)

192. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-99 as if fully set forth herein.

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

194. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiffs and the Class. Plaintiffs allege ParkMobile's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

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

a. ParkMobile owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically

including information it obtains from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. ParkMobile breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal information; and,

c. ParkMobile's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

196. The Court should also issue corresponding injunctive relief requiring ParkMobile to employ adequate security protocols consistent with industry standards to protect its users' (*i.e.* Plaintiffs' and the Class's) data.

197. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of ParkMobile's data systems. If another breach of ParkMobile's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover

the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

198. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to ParkMobile if an injunction is issued.

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

PRAYER FOR RELIEF

200. Wherefore, Plaintiffs, on behalf of themselves and the Class, request that this Court award relief as follows:

a. An order certifying the class and designating Plaintiffs as the Class Representatives and their counsel as Class Counsel;

b. An award to Plaintiffs and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiffs and the Class;

d. Injunctive relief to Plaintiffs and the Class;

e. An award of attorneys' fees and costs pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

201. Plaintiffs hereby demand a jury trial for all the claims so triable.

Respectfully submitted,

/s/ *MaryBeth V. Gibson*
MaryBeth V. Gibson
N. Nicholas Jackson
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
njackson@thefinleyfirm.com

Arthur M. Murray
Caroline Thomas White
MURRAY LAW FIRM
701 Poydras Street
New Orleans, LA 70139
Telephone: (504) 525-8100
amurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Joseph P. Guglielmo
Sean Russell
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com

srussell@soctt-scott.com

Gary F. Lynch
Nicolas Colella (*Pro Hac Forthcoming)*
CARLSON LYNCH, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com
ncolella@carlsonlynch.com

Brian C. Gudmudson
Michael J. Laird (*Pro Hac 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
Michael.laird@zimmreed.com

James J. Pizzirusso
Steven M. Nathan
Swathi Bojedla (*Pro Hac Forthcoming)*
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, DC 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com
snathan@hausfeld.com
sbojedla@hausfeld.com

Karen H. Riebel (*Pro Hac Forthcoming)*
Kate M. Baxter-Kauf *(Pro Hac Forthcoming)*
LOCKRIDGE GRINDAL NAUEN, PLLP
100 Washington Avenue S., Suite 2200

Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile; (612) 339-0981
khriebel@locklaw.com
Kmbaxter-kauf@locklaw.com

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

Terence R. Coates
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
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Counsel for Plaintiffs and the Class