E FIN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

	)	
TYLER BAKER, MARIAM GEORGE, EMMA JACKSON, SAIT KURMANGALIYEV, GREGORY MANSON, HERIBERTO TRAVIESTO and JACK WEAVER, on behalf of themselves and all others similarly situated,	)	Case No. 1:21-CV-02182-SCJ
	)	
Plaintiffs,	)	
v.	)	
	)	
PARKMOBILE, LLC,	)	
	)	
Defendant.	)	
	)	

<u>MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION</u>

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.,
2009 WL 5184352 (W.D. Ky. Dec. 22, 2009) 20

In re Disposable Contact Lens Antitrust,
329 F.R.D. 336 (M.D. Fla. 2018) .... *passim*

In re Equifax, Inc. Customer Data Sec. Breach Litig.,
362 F. Supp. 3d 1295 (N.D. Ga. 2019) 25

In re Equifax, Inc. Customer Data Sec. Breach Litig.,
2020 WL 256132 (N.D. Ga. Mar. 17, 2020) 26

In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.,
341 F.R.D. 128 (D. Md. 2022) .... *passim*

In re Sonic Corp. Customer Data Sec. Breach Litig.
2020 WL 6701992 (N.D. Ohio Nov. 13, 2020) 17, 22, 23

In re Sonic Corp., No. 20-0305,
2021 WL 6694843 (6th Cir. Aug. 24, 2021) 17, 24, 25

In re Tri-State Crematory Litig.,
215 F.R.D. 660 (N.D. Ga. 2003) 23

Karhu v. Vital Pharms., Inc.,
621 F. App'x 945 (11th Cir. 2015) 14

Klay v. Humana, Inc.,
382 F.3d 1241 (11th Cir. 2004) 22, 23, 28

Kornberg v. Carnival Cruise Lines, Inc.,
741 F.2d 1332 (11th Cir. 1984) 19

Little v. T-Mobile USA, Inc.,
691 F.3d 1302 (11th Cir. 2012) 14

Luse v. Sentinel Offender Servs., LLC,
2017 WL 11629203 (N.D. Ga. Aug 21, 2017) 24

Statutes

I. INTRODUCTION

On March 8, 2021, Defendant ParkMobile LLC ("ParkMobile") experienced a data breach that impacted over twenty million of its customers in the United States. The data breach was the result of ParkMobile's inadequate data security, including, among others, its conscious decision not to patch a vulnerability which was known to them for nearly a year (contrary to its own policy to patch such vulnerabilities within 45 days), and its failure to use adequate system logging and monitoring. ParkMobile only learned of the breach after the threat actor told them about it. This data was ultimately posted on the dark web, and subsets are still being posted nearly three years later.

Plaintiffs brought a consolidated class action against ParkMobile for the breach of its obligations to adequately protect their personal information. Plaintiffs now move to certify two classes under Rule 23(b)(3), a Nationwide Class for the purposes of Plaintiffs' negligence and negligence *per se* claims; and a California Subclass for purposes of the California Plaintiffs' claim under the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150. The two classes are defined as:

1. **Nationwide Class:** All residents of the United States and its territories who received or were sent notice of ParkMobile's data breach, or whose information was otherwise included in the dark web posting of information stolen from

ParkMobile (the "Class").

2. California Subclass: All residents of California who received or were sent notice of ParkMobile's data breach, or whose information was otherwise included in the dark web posting of information stolen from ParkMobile (the "Subclass").

As described further below, the Court should certify the Class and Subclass because they satisfy both the Eleventh Circuit's and Rule 23's requirements for class certification. The members of the Class and Subclass each may be determined by objective records—ParkMobile's records identifying recipients of its data breach notice and records listing the name and contact information of those whose data was stolen and posted on the dark web. The members of the Class and Subclass also have standing under the Eleventh Circuit's analysis of standing in the data breach context. Specifically, because Class and Subclass members had their information posted on the dark web, their personal information was "misused", establishing a present injury and a risk of future injury. Additionally, consistent with Rule 23(a), both classes meet the criteria of numerosity, commonality, typicality, and adequacy.

Both the Class and Subclass also meet the requirements of Rule 23(b)(3), which requires that common issues predominate over individual ones and that the class action is the superior method of adjudication. Concerning predominance, common issues in the Class's claims predominate for several reasons, including: (1)

Plaintiffs' and the Class's claims are all governed under a single state's laws, Georgia's, due to a choice of law provision in ParkMobile's user agreement; (2) the elements of Plaintiffs' claims depend almost exclusively on generalized proof of ParkMobile's misconduct, including whether it acted reasonably and whether its actions created a foreseeable risk of harm; and (3) in addition to common classwide injuries, Plaintiffs have developed a method of measuring individual damages that may be applied to each Class and Subclass member. As this Court held in its order on ParkMobile's Rule 12(c) motion, the Subclass's CCPA claim depends entirely on whether that statute protects the type of data at issue or whether hashing passwords prevents that claim. That issue predominates over individual ones for the Subclass.

Finally, the class action is a superior method of adjudicating both the Class and the Subclass's claims. For these reasons and below, the Court should grant Plaintiffs' motion.

II. BACKGROUND

Defendant ParkMobile operates a mobile device application that provides parking-related services to its users (its "App"). Through the ParkMobile App, users are able to pay for street and garage parking and make parking reservations. In order to utilize ParkMobile's parking-related services, users must provide certain personal information, including at a minimum their email address and a password (to sign up for ParkMobile), along with vehicle license plate information and payment card data (to arrange for parking). Ex. A, Peters Report, Fig. 1. Users also sign a user agreement that, among other things, requires that any disputes between the user and ParkMobile be governed under Georgia law. Ex. 1, PM00035489, at -93.

A. ParkMobile's Systems Were Breached, and Data Was Exfiltrated.

On or around March 8, 2021, a threat actor breached ParkMobile's network and accessed user data stored on ParkMobile's servers (the "Data Breach"). The threat actor took advantage of a known vulnerability in ParkMobile's servers. Specifically, a report commissioned by ParkMobile's outside counsel stated that [redacted] Ex. 2, PM00001468, at -73 ("Ankura Report").[1] The Ankura Report noted that the [redacted] *Id.* [redacted] *Id.*[2] In plain terms, per ParkMobile's

[1] [redacted] is a vendor that provided components of web applications used by ParkMobile. Ex. 3, Hodges Dep. 67:15-68:11.

[2] CVE stands for "Common Vulnerablity and Exploitation." Ex. 4, VerSprite 30(b)(6) 92:15-21. CVEs are assigned numbers and documented on public website libraries. A CVE will detail "what the implications are of a specific vulnerability on

VP, [redacted] Ex. 3, Hodges Dep. 75:9-11.

[redacted]. Ex. 2, PM00001468, at -73. Ankura, the forensic investigator, determined that [redacted] *Id.* at -74. Those servers stored [redacted] Ex. 3, Hodges Dep. 149:16-150:4; Ex. 6, ParkMobile 30(b)(6) Dep. 270:5-11. From there, [redacted] Ex. 2, PM00001468, at -74. Ankura noted that it reviewed the server audit logs for evidence of threat actor activity but [redacted] *Id.* at 75. Ankura noted [redacted]

a software service or a piece of hardware.” Ex. 5, Ankura 30(b)(6) 59:9-60:7. The CVE at issue here—[redacted]—made clear that the outdated version of [redacted] that ParkMobile was running was vulnerable to a third party executing malicious code on its servers. *Id.*

[redacted] *Id.* ParkMobile determined that [redacted] Ex. 6, ParkMobile 30(b)(6) Dep. 209:13-22.

On or about March 16, 2021, [redacted] Ex. 7, PM00003836. [redacted] *Id.* [redacted]. *Id.* [redacted] Ex. 3, Hodges Dep. 119:3-6.

B. Class Member Data Was Posted Online After the Breach.

On March 26, 2021, ParkMobile informed the public of the Data Breach. ParkMobile reassured the public that "no sensitive data or Payment Card Information" was affected in the breach. Ex. A, Peters Report, Fig. 3. ParkMobile did not warn users to change their passwords or take any steps to safeguard their information. On April 12, 2021, KrebsOnSecurity, an online cyber security blog, announced that hackers were selling personal information from 21 million

ParkMobile customers online.[3] On April 29, 2021, the threat actor published a 4.5 gigabyte file containing the account information for 21.8 million ParkMobile customers on a hacker forum for free. *Id.* ¶ 46. The data included customers' first and last names, bcrypt hashed passwords, license plate numbers and in some cases email address, mobile phone number, dates of birth, and other vehicle identification. *Id.* ¶ 47.

After the KrebsOnSecurity article, ParkMobile sent a follow-up communication, telling the public that "encrypted passwords" were accessed, and for the first time told users that, "as an added precaution, users may consider changing their passwords . . . ." *Id.* Fig. 4. ParkMobile also stated that "[n]o credit cards… were accessed" and that it did not collect dates of birth. *Id.*

The record evidence contradicts these statements. First, ParkMobile does not encrypt passwords; instead, it uses what's called "bcrypt hashing." Hashed passwords can be cracked without the need for an encryption key, which distinguishes them from encrypted passwords. *Id.* ¶ 43. Experts have called ParkMobile's statement "extremely misleading" for referring to the breached passwords as encrypted. *Id.* ¶ 43 & Fig. 5. Indeed, online communities have successfully cracked at least 35% of the roughly 21 million passwords exposed in

[3] *Update: Security Notification – March 2021*, PARKMOBILE (last updated Apr. 16, 2021, 14:10), https://support.parkmobile.io/hc/en-us/articles/360058639032-Security-Notification-March-2021.

the Data Breach. *Id.* ¶ 57. Cracked passwords were posted on the dark web in combination with email addresses, so that other bad actors may access existing ParkMobile accounts where payment information is saved, and receive "Paid Parking for Free." Ex. B, Brinkworth Report at 23-24. Plaintiffs' own expert was able to decode over 60,000 ParkMobile passwords over the course of a few days, using a free online tool. Ex. A, Peters Report ¶ 62. This was no secret to ParkMobile—Ankura identified cracked passwords for sale shortly after the Data Breach. Ex. 8, ANK-00083002.

Second, while ParkMobile claimed in its public statements that it did not collect dates of birth, [redacted]. Ex. 3, Hodges Dep. 118:13-119:3-6. Similarly, the Data Breach dataset made available on the internet includes dates of birth. Ex. A, Peters Report Fig. 8.

Third, there is no factual basis to support ParkMobile's statement that credit card data was not accessed in the breach. Indeed, the record evidence establishes that Ankura stated that [redacted] Ex. 2, PM00001468, at -75. ParkMobile's own 30(b)(6) witness admitted that [redacted]

[redacted]. Ex. 6, ParkMobile 30(b)(6) Dep. 276:7-15. *See also* Ex. B, Brinkworth Report at 19 ([redacted]). Indeed, [redacted]. *E.g.* Ex. 9, PM00041145; Ex. 10, Brown Dep. 235:2-7 (Brown admitting that [redacted] could be evidence that payment cards had been accessed and misused).

C. ParkMobile Knew of the [redacted] Vulnerability for Nearly a Year Prior to the Data Breach and Failed to Act.

As early as May 2020, ten months before the Data Breach, ParkMobile was made aware *in writing* of the [redacted] that was ultimately responsible for the Data Breach. As part of its regular cybersecurity procedures, ParkMobile engaged a third-party vendor, VerSprite, to assist in risk management, "penetration testing, monthly scanning and helping teams resolve issues." Ex. 6, ParkMobile 30(b)(6) 48:15-49:2.[4] VerSprite served as ParkMobile's virtual Chief Information

[4] Penetration testing allows companies to test their systems for security issues. As Mr. Hodges explained, during penetration testing, the tester "attempt[s] to break into our system" and "us[es] various different techniques and tools to see how they can bypass our security measures and what they are able to do within the systems." Ex. 3, Hodges Dep. 34:4-12.

Security Officer ("CISO"); ParkMobile did not have its own internal CISO. *Id.* 50:6-9. On May 3, 2020, VerSprite delivered a report to ParkMobile entitled "Annual Penetration Test, Web Phase I", in which [redacted]. Ex. 11, PM00001077. [redacted]. *Id.* at -080.

[redacted]. *Id.* at -101. VerSprite wrote: [redacted] *Id.* VerSprite went on to inform ParkMobile that [redacted] *Id.* at -102. VerSprite warned ParkMobile that, [redacted] Ex. 4, VerSprite 30(b)(6) Dep. 94:17-95:5. VerSprite advised that ParkMobile should [redacted] Ex. 11, PM00001077 at -101.[5] ParkMobile admitted that [redacted] Ex. 6, ParkMobile 30(b)(6) Dep. 219:14-17.

Despite having this information, and the specific threat of unauthorized activity on its servers, [redacted]. Ex. 6, ParkMobile 30(b)(6) Dep. 220:20-22 [redacted]. In failing to do so, ParkMobile not only ignored VerSprite's written recommendation, but also flouted its internal policy that stated that all medium vulnerabilities should be remediated within 45 days. Ex. 3, Hodges Dep. 39:2-17 ([redacted]). ParkMobile testified that [redacted]. Ex. 6, ParkMobile 30(b)(6) Dep. 225:4-7. ParkMobile did not [redacted] Ex. 3, Hodges Dep. 78:16-21.

After the [redacted] was exploited in the Data Breach, ParkMobile

[5] A software "patch" is an update from the software company "intended to address specific security vulnerabilities within those applications or those systems." Ex. 3, Hodges Dep. 53:5-20.

finally [redacted]. According to ParkMobile's Incident Response Team timeline, [redacted]. Ex. 12, PM00001372, at -77. Afterwards, Mr. Hodges wrote that [redacted] Ex. 13, PM00002279, at -80. Had ParkMobile taken that "surprisingly minimal" effort when it first learned of the vulnerability according to its own policies, the Data Breach would have been thwarted.

D. ParkMobile's Failure to Implement Reasonable Security Measures Contributed to the Data Breach.

Beyond its failure to heed direct warnings about the vulnerability that led to the Data Breach, ParkMobile misused security tools that, if properly implemented, could have prevented the breach. For example, ParkMobile claims to have had a Security, Information and Event Management ("SIEM") tool in place that, if properly functioning, should have identified and flagged suspicious activity. Ex. B, Brinkworth Report at 16-17. But Ankura found that [redacted] Ex. 2, PM00001468, at -74. Had ParkMobile properly employed its SIEM tool, and trained it to look for anomalous activity, they would have been alerted of the breach attempt and could have taken steps to stop it. That they did not detect the suspicious activity indicated that "the tools may not have been configured correctly, the right data was not being collected, alerts were not configured or data and alerts were not being reviewed," creating a foreseeable risk of harm. Ex. B, Brinkworth Report at 17. Further, the threat actor appeared to [redacted]. Ex. 2, PM00001468, at -73; Ex. 6, ParkMobile 30(b)(6) 283:18-284:2, 284:14-20. Had ParkMobile employed geo-IP filters, which prohibit access to servers from IP addresses located in certain foreign countries, many of the threat actor's attempts to breach its systems could have been blocked. Ex. B, Brinkworth Report at 16. [redacted]. Ex. 6, ParkMobile 30(b)(6) 285:3-7. ParkMobile's data security, therefore, lacked the basic measures necessary to identify and prevent a data breach.

III. ARGUMENT

A. The Court Should Certify the Class.

To certify a Rule 23(b)(3) damages class, Plaintiffs must show that they meet the criteria of Rule 23(a)—numerosity, commonality, typicality, and adequacy—and of Rule 23(b)(3)—predominance and superiority. Fed. R. Civ. P. 23(a), (b)(3). The Eleventh Circuit also considers whether the class is sufficiently defined, such that class membership is ascertainable and class members have standing. *See, e.g.*, *Cherry v. Dometic Corp.*, 986 F.3d 1296, 1304 (11th Cir. 2021); *Green-Cooper v.*

Brinker Int'l, Inc., 73 F.4th 883, 891 (11th Cir. 2023) ("*Green-Cooper*"). Where, as here, a class has suffered injuries arising out of a defendant's uniform course of conduct (here, ParkMobile's actions or omissions giving rise to the Data Breach) and a single state's laws govern the entire class's claims (here, Georgia's), plaintiffs and the class are usually sufficiently cohesive to warrant adjudication by representation. *See, e.g.*, *In re Disposable Contact Lens Antitrust*, 329 F.R.D. 336, 413 (M.D. Fla. 2018) ("*Contact Lens*").

1. The Class Is Adequately Defined

"[A] plaintiff seeking to represent a proposed class must establish that the proposed class is adequately defined and clearly ascertainable." *Contact Lens*, 329 F.R.D. at 403 (citing *Little v. T-Mobile USA, Inc.*, 691 F.3d 1302, 1304 (11th Cir. 2012)). To be ascertainable, class membership must be determinable by "objective criteria" such that "identifying class members is a manageable process that does not require much, if any, individual inquiry." *Id.*; *see also Bussey v. Macon Cnty. Greyhound Park, Inc.*, 562 F. App'x 782, 787 (11th Cir. 2014). These objective criteria can include reference to the defendant's business records. *Karhu v. Vital Pharms., Inc.*, 621 F. App'x 945, 948 (11th Cir. 2015). Here, Class membership can be determined by ParkMobile's records, including: (1) the list of recipients of ParkMobile's notice of the Data Breach; (2) the records posted on the dark web which include the identity (and even contact information) of ParkMobile's affected users (*i.e.* the Nationwide Class). The Class is, thus, ascertainable.

2. Class Members Each Have an Article III Injury

In assessing class certification, courts in the Eleventh Circuit consider the ease of determining whether class members have standing. *See, e.g.*, *Cordoba v. DirectTV, LLC*, 942 F.3d 1259, 1272–73 (11th Cir. 2019). In *Green-Cooper*, the Eleventh Circuit examined the standing of the members of a certified class in the context of a data breach. *See* 73 F.4th at 889–90. There, the Court held that data breach victims have standing where the stolen data has been "misuse[d]" because misuse establishes "both a 'present' injury and a 'substantial risk' of harm in the future." *Id.* at 889. The Court found that posting data online satisfies the misuse requirement:

> All three plaintiffs maintain that their credit card and personal information was exposed for theft and sale on the dark web. That allegation is critical. The fact that hackers took credit card data and corresponding personal information from the [defendant's] restaurant systems and affirmatively posted that information for sale on [the dark web] is the misuse for standing purposes . . . . [I]t establishes . . . a present injury—credit card data and personal information floating around on the dark web—and a substantial risk of future injury[.]

Id. at 889–90.

Like *Green-Cooper*, Plaintiffs here have had their data "misused" because the entire Class's personal information stolen from ParkMobile was affirmatively posted to the dark web for *free* to download. Ex. A, Peters Report ¶ 46. Cracked passwords and email combinations are still actively being posted as of late 2023. Ex. B, Brinkworth Report at 23-24. Cracked passwords put all Class members at imminent risk for "credential stuff", where threat actors use the breached information to access other accounts, including credit cards and other financial accounts. *Id.* at 24. That "misuse" establishes a present injury for standing purposes classwide.

3. Plaintiffs Satisfy the Elements of Rule 23(a)

Fed. R. Civ. P. 23(a) sets forth four requirements that any class must meet before certification: numerosity, commonality, typicality, and adequacy. Here, Plaintiffs and the Class meet those requirements.

a) The Class of Over Twenty Million is Sufficiently Numerous

Numerosity is satisfied where "the class is so numerous that joinder of all members is impracticable." Fed. R. Civ. P. 23(a)(1). Numerosity is a "generally low hurdle[.]" *Contact Lens*, 329 F.R.D at 336. "[T]he general rule of thumb in the Eleventh Circuit is that 'less than twenty-one is inadequate, more than forty adequate, with numbers between varying according to other factors.'" *Manno v. Healthcare Revenue Recovery Grp., LLC*, 289 F.R.D. 674, 684 (S.D. Fla. 2013). Here, the Class includes over twenty million ParkMobile users, as evidenced both by ParkMobile's notices to the Class of the Data Breach and the information posted on the dark web. The Class satisfies numerosity.

b) Common Issues of Law and Fact Arise from the Data Breach

Rule 23(a)(2) requires "questions of law or fact common to the class." Fed. R. Civ. P. 23(a)(2). "The 'commonality' requirement carries a 'light burden,' demanding 'only that there be questions of law or fact common to the class.'" *Contact Lens*, 329 F.R.D. at 405. "[C]ommonality can be satisfied even with some factual variations among class members" as long as "'there [is] at least one issue whose resolution will affect all or a significant number of the putative class members.'" *Id.* (quoting *Williams v. Mohawk Indus., Inc.*, 568 F.3d 1350 (11th Cir. 2009)).

In data breach actions like this one, commonality is generally satisfied because the defendant's uniform course of conduct (its inadequate data security) caused classwide harm from the theft of the personal data. *See In re Sonic Corp. Customer Data Sec. Breach Litig.* ("*Sonic I*"), No. 1:17-md-2807, 2020 WL 6701992, at *3 (N.D. Ohio Nov. 13, 2020)[6] (finding "all potential class members shared a common injury due to the same set of circumstances—[defendant's] actions leading to and after the data breach."); *see also In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 148 (D. Md. 2022) ("*Marriott*") ("The common answers to the common questions of fact . . . will ultimately generate yet more common answers to common questions of law—i.e., whether [d]efendants failed to adequately protect customers' PII [personal identifiable information] such

[6] The Sixth Circuit denied the *Sonic* defendant's Rule 23(f) petition to appeal the class certification order. *In re Sonic Corp.*, No. 20-0305, 2021 WL 6694843 (6th Cir. Aug. 24, 2021) ("*Sonic II*").

that they breached a duty . . . ."); *In re Brinker Data Incident Litig.*, 3:18-cv-0686, 2021 WL 1405508, at *8 (M.D. Fla. Apr. 14, 2021) (finding "several questions that are common to the class" including "whether [defendant] had a duty to protect customer data, whether [defendant] knew or should have known its data systems were susceptible, and whether [defendant] failed to implement adequate data security measures . . . ."), *vacated in part sub nom. Green-Cooper*, 73 F.4th 883 (11th Cir. 2023)[7].

As in those cases, commonality is met here. The central issue of ParkMobile's liability includes common factual and legal questions, including whether: (1) ParkMobile knowingly created a risk of harm to the Class by, among other things, using an outdated version of [redacted], inadequate logging and monitoring tools, and insufficient geo-fencing; (2) ParkMobile's inadequate data security caused the data breach; (3) the Data Breach and the resulting harm to the Class was foreseeable; (4) ParkMobile owed Plaintiffs and the Class a duty; (5) ParkMobile breached its duty; (6) ParkMobile's conduct was "unfair or deceptive" in violation of § 5 of the FTC Act; and (7) ParkMobile's representation that passwords, dates of birth, and credit card information were not at risk was negligent or knowingly false and put the Class

[7] In *Green-Cooper*, the Eleventh Circuit held that the class was ascertainable and class members had standing but remanded to allow the district court to "refine the class definition" and "clarify its predominance finding." *See* 73 F.4th at 892.

at further risk of harm. Common issues of law and fact also concern injury, causation and damages, and would require similar proof of facts. This includes evidence that the Class's PII was posted on the dark web and the hashed passwords were inadequately protected. This requirement is satisfied here.

c) Plaintiffs' Claims are Typical of the Class

Typicality is satisfied if "the claims or defenses of the representative parties are typical of the claims or defenses of the class." Fed. R. Civ. P. 23(a)(3). Unlike commonality, which considers the relatedness of all claims throughout the class and named plaintiffs, typicality "refers to the individual characteristics of the named plaintiff[s] in relation to the class." *Piazza v. Ebsco Indus., Inc.*, 273 F.3d 1341, 1346 (11th Cir. 2001). In assessing typicality, the Eleventh Circuit considers "whether a sufficient nexus exists between the claims of the named representative and those of the class at large." *Hines v. Widnall*, 334 F.3d 1253, 1256 (11th Cir. 2003) (quotations and citations omitted). "A sufficient nexus is established if the claims or defenses of the class and the class representative arise from the same event or pattern or practice and are based on the same legal theory." *Kornberg v. Carnival Cruise Lines, Inc.*, 741 F.2d 1332, 1337 (11th Cir. 1984). Factual variations only undermine typicality where "the representative's position differs markedly from other class members." *In re Checking Account Overdraft Litig. v. RBC Bank (USA)*, No. 20-13367, 2022 WL 472057, at *3 (11th Cir. Feb. 16, 2022) (quotation and citation omitted).

Here, Plaintiffs' claims are typical of the Class's because they arise out of the same event, concerning the same type of harm, and seek the same relief. Here, Plaintiffs and the Class all interacted with ParkMobile in largely the same manner, that is, providing information to ParkMobile in exchange for using its parking app. Ex. A, Peters Report, Fig. 1. The same misconduct (ParkMobile's inadequate data security procedure and systems) and the same event (the Data Breach) caused Plaintiffs and the Class to suffer similar harm from the theft and misuse of their personal data. *See In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, 3:08-md-1998, 2009 WL 5184352 (W.D. Ky. Dec. 22, 2009) (holding typicality was met where "all class members had their private information compromised, and their claims arise from the same course of uniform conduct of [the defendant]."). Plaintiffs' claims share a nexus with the Class's—the cause and fallout of the Data Breach—satisfying typicality here.

d) Plaintiffs Will Continue to Adequately Represent the Class

Rule 23(a)(4) requires that plaintiffs "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). In determining the adequacy of the named plaintiffs, courts consider two questions "(1) whether any substantial conflicts of interest exist between the representatives and the class; and (2) whether the representatives will adequately prosecute the action." *Valley Drug Co. v. Geneva Pharms., Inc.*, 350 F.3d 1181, 1189 (11th Cir. 2003) (internal quotations omitted).

Here, Plaintiffs have no interests that are antagonistic to the Class. Rather, they have the same interests—each was a customer of ParkMobile who had their personal and sensitive user data stolen from ParkMobile and posted on the dark web, causing them harm and a threat of future harm. Plaintiffs have and will continue to vigorously and capably press the claims of the Class. Their counsel, additionally, has extensive experience managing and litigating complex cases, including data breach class actions. ECF No. 35-1, at 9–22 (describing the experience of interim Co-Lead Class Counsel and the Plaintiffs' Steering Committee). Accordingly, the requirement of adequate representation is established here.

4. Plaintiffs Satisfy the Elements of Rule 23(b)(3)

In addition to the Rule 23(a) requirements, certification of a Rule 23(b)(3) class requires the court to determine whether: (1) "questions of law or fact common to class members predominate over any questions affecting only individual members", the predominance inquiry; and (2) "a class action is superior to other available methods for fairly and efficiently adjudicating the controversy", the superiority inquiry. Fed. R. Civ. P. 23(b)(3). Both requirements are met here.

a) Common Issues of Law and Fact Predominate.

"The predominance inquiry asks whether the common, aggregation-enabling, issues in the case are more prevalent or important than the non-common, aggregation-defeating, individual issues." *Contact Lens*, 329 F.R.D. at 411-12 (citing *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016)). "[I]n assessing whether a plaintiff has demonstrated that common questions predominate, a court should distinguish between individual questions, for which evidence varies from member to member" and "common questions, for which 'the same evidence will suffice for each member[.]'" *Rivera v. Equifax Info. Servs., LLC*, 341 F.R.D. 328, 336 (N.D. Ga. 2022). "Common issues of fact and law predominate if they have a direct impact on every class member's effort to establish liability and . . . entitlement to injunctive and monetary relief." *Pizarro v. Home Depot*, No. 1:18-cv-1566, 2020 WL 6939810, at *15 (N.D. Ga. Sept. 21, 2020) ("*Pizarro*").

Here, common issues predominate for three reasons: (1) Georgia law applies uniformly to the Class's claims; (2) ParkMobile's liability is subject to generalized proof; and (3) Plaintiffs have a common method of measuring individual damages.

i. A Contractual Choice of Law Provision Applies Georgia Law to the Class's Claims.

Where a class claim "is based on a principle of law that is uniform among the states, class certification is a realistic possibility." *Klay v. Humana, Inc.*, 382 F.3d 1241, 1262 (11th Cir. 2004) ("*Klay*"); *see also Brinker Data Incident*, 2021 WL 1405508, at *10 (explaining that class have been certified in "the data breach context . . . have not suffered from choice of law issues."); *Sonic I*, 2020 WL 6701992, at *6 ("[A] single state's law will be used to determine liability" and thus, "[c]ommon issues of fact and law predominate.").

Here, Georgia law applies to the Class's claims pursuant to the user agreement. Each Class member entered into an agreement with ParkMobile that, at the time of the Data Breach, stated: "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 Services." Ex. 1, PM00035489, at -493. In its discovery responses, ParkMobile acknowledged the application of this provision. Ex. 14, RFP Response 67. Pursuant to that mutually agreed-upon contract, Georgia law governs the Class's claims.[8] With one state's laws governing the claims, the legal issues predominate. *Klay*, 382 F.3d at 1262; *see also Tri-State*, 215 F.R.D. at 696 ("Because of Georgia's choice of law rules, this case has little variation in state law for the Court to consider . . . Variations in state law therefore do not overwhelm the common issues in the case at bar.").

[8] Separately from the agreement, Georgia law would apply under Georgia's choice of law rules because in Georgia: "'the application of another jurisdiction's laws is limited to statutes and decisions construing those statutes'" and "'[w]hen no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law.'" *In re Tri-State Crematory Litig.*, 215 F.R.D. 660, 677 (N.D. Ga. 2003) ("*Tri-State*"); *Coon v. Med. Ctr., Inc.*, 797 S.E.2d 828, 833–35 (Ga. 2017). Under this standard, Georgia would apply its law to Plaintiffs' common law tort claims, including negligence and negligence *per se*. *See, e.g.*, *Elder v. Reliance Worldwide Corp.*, 563 F. Supp. 3d 1221, 1231 (N.D. Ga. 2021); *Monopoli v. Mercedes-Benz USA, LLC*, No. 1:21-cv-1353, 2022 WL 409484, at *4 (N.D. Ga. Feb. 10, 2022).

ii. Liability is Subject to Generalized Proof.

Just as one law will govern Plaintiffs' claims, the same set of facts will be required to prove virtually every element of Plaintiffs' and the Class's negligence-based claims, further establishing predominance here. *See, e.g.*, *Contact Lens*, 329 F.R.D. at 413 (certifying a class where "the claims of the proposed putative class members all arise out of the same alleged illegal conduct by [d]efendants."); *Luse v. Sentinel Offender Servs., LLC*, No. 2:16-cv-0030, 2017 WL 11629203, at *4 (N.D. Ga. Aug 21, 2017) ("If every Class Member brought an individual action, each would attempt to prove essentially the same set of facts" making the class "sufficiently cohesive to warrant adjudication by representation.").

To establish negligence in Georgia, Plaintiffs and the Class must show: (1) defendant owed them a duty; (2) defendant breached that duty; (3) the breach caused an injury; and (4) the amount of resulting damages. *Ramirez v. v. Paradies Shops*, 69 F.4th 1213, 1218 (11th Cir. 2023) ("*Ramirez*"). Negligence *per se* requires establishing that a defendant violated a statute intended to protect the plaintiff against the type of harm experienced, in this case, § 5 of the FTC Act and caused a classwide injury. *In re Equifax, Inc. Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019). As other courts have found in data breach actions, the issues of duty and breach are subject to generalized proof because they concern defendant's misconduct. *See, e.g.*, *Sonic II*, 2021 WL 6694843, at *3 (holding that the "elements of a negligence claim—duty, breach, and causation" all depend on whether "[the defendant's] internal data security measures and its remote access policy caused the data breach[.]"); *Marriott*, 341 F.R.D. at 170 (in certifying an issue class under Fed. R. Civ. P. 23(c)(4), holding that "efficiency gains stemming from certification of the duty and breach issues outweigh" any individual issues).

That is no different here. In *Ramirez*, for example, the Eleventh Circuit held that the existence of a duty depends on whether the defendant created a risk of harm and whether that risk was foreseeable. *See* 69 F.4th at 1219 (holding that "the creator of a potentially dangerous situation has a duty to do something about it so as to prevent injury to others" and that duty is limited by the "reasonably foreseeable risks of harm."). This Court and others have also held that whether the foreseeability of the harm in a data breach case triggers a duty depends on the type of data the defendant stored. ECF No. 89, at 16 (citing *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360 (N.D. Ga. 2021)). Whether ParkMobile owed a duty, thus, depends on whether *its* actions created a risk of harm and whether that risk was foreseeable given the information at hand, which are issues subject to generalized proof.

Similarly, whether ParkMobile breached its duty depends exclusively on its own knowledge and misconduct. Here, Plaintiffs and the Class would commonly seek to establish that ParkMobile: (1) was warned of the vulnerability that led to the breach long beforehand but never patched it; (2) lacked basic security measures like adequately logging, monitoring, and geo-fencing; and (3) inadequately investigated the scope of the Data Breach, causing it to issue premature and false claims that users' credit card information, dates of birth, and passwords were not a risk.[9] That evidence of ParkMobile's negligence is common to the Class.

Finally, the Class also shares common questions concerning their injuries due to the Data Breach. Here, every Class member suffered an injury in having their sensitive information posted to the dark web due expressly to the Data Breach. As *Green-Cooper* held, the posting of private information on the dark web constitutes "misuse" of the data and creates an injury. *See* 73 F.4th at 889–90. Every Class member here had data stolen from ParkMobile and posted on the dark web. Plaintiffs' experts describe the harm caused and impairment of the usefulness and value of data when sensitive information is posted on the dark web, supporting via common evidence a Classwide injury.[10] Ex. C, Mangum Report ¶¶ 94-107.

Consequently, every element of Plaintiffs' claims relies on generalized proof and, as described below, although the amount of damages differs, Plaintiffs have

[9] Plaintiffs' negligence *per se* claim will rely on similar evidence to show ParkMobile violated the FTC Act by using unreasonable data security.

[10] Even if those injuries cannot be easily calculated, Plaintiffs and the Class may still recover nominal damages, which supports predominance of causation and injury. O.C.G.A § 51-12-4; *Equifax*, 2020 WL 256132, at *13; *see also Marriott*, 341 F.R.D. at 164 ("One may recover nominal damages" and "by their nature, nominal damages do not require individualized calculation and, thus, they are consistent with a predominance finding on that score.").

proposed a common methodology for measuring those differences.

iii. Plaintiffs' Have a Common Method of Measuring Individual Damages

"It is axiomatic that individualized damages calculations are generally insufficient to foreclose class certification, and particularly so where the central liability question is common to each class member." *Monroe Cnty. Emps. Ret. Sys. v. S. Co.*, 332 F.R.D. 370, 397 (N.D. Ga. 2019); *Carriuolo v. Gen. Motors Co.*, 823 F.3d 977, 988 (11th Cir. 2016) ("[I]ndividualized damages calculations are insufficient to foreclose the possibility of class certification, especially when, as here, the central liability question is so clearly common to" the class); *Pizarro*, 2020 WL 6939810, at *17.

Here, as described above, Plaintiffs and the Class suffered some common injuries, namely, the posting of their private information on the dark web and the loss in value of their data, which, if proven, entitles them to at least nominal damages. In addition to nominal damages, Dr. Mangum has identified the loss in value of Plaintiffs' and Class Members' PII through a market valuation of the various data elements impacted in the Data Breach. Additionally, Dr. Mangum applies the results of Dr. Swain's conjoint survey to determine how much Plaintiffs and Class Members overpaid ParkMobile based on their reasonable expectation that their PII would be kept safe. Had Plaintiffs and Class Members known of ParkMobile's inadequate data security practices, they would have paid ParkMobile significantly less to use its services. Dr. Mangum can calculate damages for both models on a classwide basis, or as to any individual Plaintiff or class member. Ex. C, Mangum Report ¶¶ 94-107; Ex. D, Swain Report ¶¶ 95-96, 98.

Although the extent to which Plaintiffs experienced those harms varies, Plaintiffs proposed a common methodology for measuring those damages. While the inputs depend on the individual circumstances of each Class member, once that data is obtained, Plaintiffs can determine damages through a uniform method. These types of models support predominance in data breach class actions. *See Marriott*, 341 F.R.D. at 162; *Green-Cooper*, 73 F.4th at 893. The common legal and factual issues here predominate.

b) A Class Action is a Superior Method of Adjudication.

"The superiority requirement of Rule 23(b)(3) focuses 'not on the convenience or burden of a class action suit *per se*, but on the relative advantages of a class action suit over whatever other forms of litigation might be realistically available to the plaintiffs.'" *Contact Lens*, 329 F.R.D. at 425 (citing *Klay*, 382 F.3d at 1269). Consequently, "the predominance analysis . . . has a tremendous impact on the superiority analysis . . . for the simple reason that, the more common issues predominate over individual issues, the more desirable a class action lawsuit will be[.]" *Klay*, 382 F.3d at 1269. Superiority of the class action device is often met where it would be economically infeasible to litigate an action individually due to the relatively small amount of damages. *Contact Lens*, 329 F.R.D. at 425; *Deposit Guar. Nat'l Bank of Jackson, Miss. v. Roper*, 445 U.S. 326, 339 (1980) ("Where it is not economically feasible to obtain relief within the traditional framework of a multiplicity of small individual suits for damages, aggrieved persons may be without any effective redress unless they may employ the class-action device.").

Here, all the cases against ParkMobile for its Data Breach are consolidated before the Court. Without the availability of a class action, the small individual damages values would likely preclude individual litigation, supporting superiority. *Contact Lens*, 329 F.R.D. at 426. Moreover, litigating the Class's claims collectively would be far more efficient and far less costly than individual actions, particularly because of the overwhelmingly common issues of law and facts. *Id.* at 425. Consequently, Plaintiffs have established superiority here.

B. The Court Should Certify Plaintiffs' Subclass.

Plaintiffs Weaver and Jackson also request the Court certify a Rule 23(b)(3) Subclass of California residents for Plaintiffs' California Consumer Protection Act ("CCPA") claim. For much of the same reasons as that proposed Class, the Subclass meets the requirements of Rule 23(a): (1) the Class is sufficiently numerous because it includes hundreds of thousands of individuals; (2) the Class shares common issues of law and fact, particularly whether, under the CCPA, the Data Breach occurred due to ParkMobile's "violation of the duty to implement and maintain reasonably security procedures and practices . . .", Cal. Civ. Code § 1798.150(a)(1); (3) Plaintiffs' claims are typical of the Subclass because they all arise out of the same event (ParkMobile's Data Breach) and concern the same harm.; and (4) Plaintiffs have no conflict with the members of the Subclass, as each are pursuing the same statutory damages. *Id.* at § 1798.150(a)(1)(A).

Common issues also predominate. The Court has already highlighted the common legal and factual questions that governs the CCPA claim: whether the theft of Plaintiffs' username and passwords constitute the type of information protected by the CCPA and whether the type of encryption precludes a private right of action. *See* ECF No. 211, at 12–14. The result of those issues affects each Subclass members' claim: if Plaintiffs' position prevails, the entire Class's CCPA claim will succeed; and if ParkMobile's position prevails, the entire Subclass's CCPA claim will fail. *Amgen Inc. v. Conn. Ret. Plans & Trust Funds*, 568 U.S. 455, 460 (2013) ("[T]he class is entirely cohesive: It will prevail or fail in unison.").

Given the overwhelmingly predominating issue on the Subclass's CCPA claim and the small measure of individual damages, a class action is the superior means of adjudicating this claim. The Court should, thus, certify the California Subclass.

IV. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court grant the Motion to certify the proposed Class and Subclass.

Dated: February 12, 2024

Respectfully submitted,

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Gibson Consumer Law Group, LLC
4729 Roswell Road
Suite 208-108
Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.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
Nicholas A. Colella
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
nickc@lcllp.com

Brian C. Gudmundson
Michael J. Laird
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
Michael.laird@zimmreed.com

Swathi Bojedla
James J. Pizzirusso
Steven M. Nathan
HAUSFELD LLP
888 16th Street NW, Suite 300
Washington, DC 20006
Telephone: (202) 540-7200
sbojedla@hausfeld.com
jpizzirusso@hausfeld.com
snathan@sfeld.com

Karen H. Riebel
Kate M. Baxter-Kauf
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

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: February 12, 2024

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson

CERTIFICATE OF SERVICE

I hereby certify that on February 12, 2024, I caused the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail Notice List.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson