KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff
Jennifer Hansen

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JENNIFER HANSEN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GRAVY ANALYTICS, A SUBSIDIARY OF UNACAST, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*;
2. NEGLIGENCE;
3. BREACH OF IMPLIED CONTRACT; and
4. UNJUST ENRICHMENT

JURY TRIAL DEMANDED

//

//

//

//

//

//

Plaintiff Jennifer Hansen ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class Members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, brings this class action against Gravy Analytics, a subsidiary of Unacast, Inc. ("Defendant" or "Gravy Analytics") and alleges as follows:

NATURE OF THE CASE

1. Defendant reported to the Norwegian Data Protection Authority that "On January 4, 2025, Gravy Analytics, a subsidiary of Unacast, Inc, identified unauthorized access to its AWS cloud storage environment."[1] Defendant further reported that the unauthorized person gained access to the Gravy Analytics AWS environment through a misappropriated access key and that preliminary findings indicated that an unauthorized person obtained certain files, which could contain personal data that is likely associated with users of third-party services that supply this data to Gravy Analytics.

2. On or around January 8, 2025, the Russian cybercrime forum called XSS posted screenshots and uploaded 17 terabytes of information stolen from Defendant's inadequately protected computer systems, including customer lists, information on the broader location data tracking industry, and, perhaps most concerningly, location data harvested from individuals' smartphones which show peoples' precise movements. As a result, thousands of individuals, including Plaintiff and the Class Members (as defined below), have had their personal identifiable information ("PII") as well as their location data (collectively "Private Information") exposed without their consent to unauthorized third parties (the "Data Breach").

[1] https://www.reuters.com/technology/cybersecurity/location-tracking-company-unacast-tells-norway-its-data-was-hacked-broadcaster-2025-01-11/

3. The hacked Gravy Analytics data included *tens of millions of mobile phone coordinates of devices inside the U.S.*, Russia, and Europe, obtained through individuals' use of major mobile applications such as Tinder, Grindr, Candy Crush, Subway Surfers, Moovit, My Period Calendar & Tracker, MyFitnessPal, Tumblr, Microsoft's 365 office application, Yahoo's email client, religious-focused apps such as Muslim prayer and Christian Bible apps, various pregnancy trackers, and many VPN apps, which users generally download, ironically, in an attempt to protect their privacy.[2]

4. Gravy is a subsidiary of Unacast, Inc., and a global location intelligence company that tracks individual's locations and movements using machine learning and artificial intelligence.

5. In December 2024, the Federal Trade Commission ("FTC") accused Gravy and its subsidiary, Venntel, of illegally collecting and selling Americans' location data without their knowledge or obtaining proper legal consent. The FTC action culminated in a unanimous, finalized order on January 15, 2025, prohibiting Gravy Analytics and its subsidiary Venntel from selling, disclosing, or using sensitive location data except in limited circumstances involving national security or law enforcement.

6. Gravy Analytics, Unacast, and Venntel have been some of the largest and most important companies in the location data industry for years, collating smartphone location data from around the world, in some instances, to sell to the U.S. government.

7. In addition to selling location data to customers for this use, Gravy Analytics itself also analyzes the data to create additional data products to sell to its customers. For example, Gravy Analytics uses the data it collects to create "audience

[2] Joseph Cox, *Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location*, WIRED (January 9, 2025), https://www.wired.com/story/gravy-location-data-app- leak-rtb/

segments," or subsets of consumers who share interests or characteristics, including audience segments based on sensitive interests or characteristics. These groupings are formed based on the locations and events visited by mobile devices, combined with other information gathered about consumers, and allow Gravy Analytics' customers to identify and target consumers based on identified sensitive and personal interests or characteristics. This location data is extremely valuable as demonstrated by the large and growing market for location data.

8. In carrying out their business, Defendant obtain, collect, use, and derive a benefit from the Private Information of Plaintiff and the Class Members. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and disclosure.

9. As a result of Defendant's negligence and inadequate data security, negligence, cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals, including Plaintiff and the Class Members.

10. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' Private Information to be accessed, exfiltrated, and disclosed to unauthorized third parties in the Data Breach. This action seeks to address and remedy these failings. Plaintiff brings this action on behalf of themself individually and all other similarly situated victims of the Data Breach.

11. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for themself and the Class members, injunctive relief, including public injunctive relief, and actual damages.

//

//

//

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

13. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in the State of California and within this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in or was directed to this District.

PARTIES

15. Plaintiff is a resident and citizen of Oakland, California.

16. Plaintiff owns a smart phone that she regularly uses and (or has used) to access and utilize a number of mobile applications. Upon information and belief, Plaintiff's Private Information, including her location data, has been collected by Defendant as a result of her use of this and other mobile applications and was subsequently compromised by the Data Breach.

17. Defendant Gravy Analytics is a subsidiary of Unacast, Inc., which is a Delaware corporation with its headquarters or principal place of business located in Cos Cob, Connecticut.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of Defendant's owners, predecessors, successors, subsidiaries, agents and/or assigns.

//

//

//

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

19. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[3] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

20. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

21. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[5] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

22. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[6]

23. As a result of its real value and the recent large-scale data breaches,

---

[3] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[4] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[5] *See* Soma, *Corporate Privacy Trend, supra*.

[6] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

24. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[7] This business has created a new market for the sale and purchase of this valuable data.[8]

25. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[9]

---

[7] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[8] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[9] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

26. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[10]

27. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of Private Information Has Grave and Lasting Consequences for Victims

28. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

29. Theft or breach of Private Information is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[11]

30. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use Private Information to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[12] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[10] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[11] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[12] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

31. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[13]

32. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[14] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[15]

33. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[16] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[17] And in 2019, Javelin Strategy & Research compiled consumer

---

[13] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[14] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[15] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[16] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[17] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[18]

34. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

35. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[19]

36. It is within this context that Plaintiff and thousands of other individuals subjected to the Data Breach must now live with the knowledge that their Private Information was disclosed and stolen unauthorized persons, is likely forever in cyberspace and likely available for sale on the dark web or black market.

The Data Breach

37. Defendant reported that "[o]n January 4, 2025, Gravy Analytics, a subsidiary of Unacast, Inc, identified unauthorized access to its AWS cloud storage environment."[20] Defendant further reported that the unauthorized person gained access to the Gravy Analytics AWS environment through a misappropriated access key and that preliminary findings indicated that an unauthorized person obtained certain files, which could contain personal data that is likely associated with users of third-party

---

[18] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[19] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[20] https://www.reuters.com/technology/cybersecurity/location-tracking-company-unacast-tells-norway-its-data-was-hacked-broadcaster-2025-01-11/

services that supply this data to Gravy Analytics.

38. On or around January 8, 2025, the Russian cybercrime forum called XSS posted screenshots and uploaded 17 terabytes of information stolen from Defendant's inadequately protected computer systems. The information stolen and posted on the Dark Web includes Plaintiff's and the Class Members' Private Information, such as their email addresses and private location information that Defendant illegally collected and intended to sell or did sell.

39. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of American citizens like Plaintiff and Class Members.

40. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

41. The unencrypted Private Information of Plaintiff and Class Members has already been posted on the Dark Web.[21]

42. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information for Plaintiff and Class Members.

43. Because Defendant had a duty to protect Plaintiff's and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

[21] https://www.nbcnews.com/tech/security/location-data-broker-gravy-analytics-was-seemingly-hacked-experts-say-rcna187038

44. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights;

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

k. Failing to protect against reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information;

l. Failing to train all members of its workforces effectively on the policies and procedures regarding Private Information as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of Private Information;

m. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Private Information;

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

o. Failing to adhere to industry standards for cybersecurity as discussed above; and

p. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

45. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained Plaintiff's and Class Members' unsecured and unencrypted Private Information.

46. As a result of the Data Breach, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Defendant Knew or Should Have Known PII Are High Risk Targets

47. Defendant knew or should have known that Private Information like that at issue here, are high risk targets for identity thieves.

48. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 million records in 2018.[22] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

49. Prior to the Data Breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in December 2018, Marriott International announced a data breach that affected up to 500 million individuals. The data breach allowed hackers to access customer names, physical addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, loyalty program account information, and payment card information.[23]

50. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks,

---

[22] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[23] *See* https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach#:~:text=Marriott%20International%20says%20that%20a,up%20to%20500%20million%20people.&text=The%20hotel%20chain%20says%20the,10%2C%202018%20could%20be%20affected

ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[24]

51. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[25]

52. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[26]

53. As such, Defendant was aware, or should have known, that Plaintiff's and Class Members' Private Information is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' Private Information against data breaches and unauthorized disclosures that Defendant should have anticipated and guarded against.

54. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

---

[24] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at https://www.ic3.gov/Media/Y2019/PSA191002

[25] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000- sec-filings-over-the-past-year/

[26] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

55. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[27]

56. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:[28]

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless

[27] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[28] *Id.*

absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/ decompression programs, including the "AppData/LocalAppData" folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

57. Given that Defendant was storing the Private Information of other individuals, Defendant could and should have implemented the above measures to detect and prevent ransomware attacks.

58. The occurrence of the Data Breach indicates that Defendant failed to

adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

59. Defendant could have prevented the Data Breach by properly securing and encrypting the folders, files, and or data fields storing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored Plaintiff and the Class Members' data in an Internet-accessible environment when there was a reasonable need to do so.

60. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

61. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

62. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

63. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2)

failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents

64. The ramifications of Defendant's failure to safeguard Plaintiff's and Class Members' Private Information are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years and indefinitely.

Damages Suffered by Plaintiff and the Class Members

65. Plaintiff and Class Members have suffered injury from the misuse of their location data and Private Information that can be directly traced to Defendant.

66. Plaintiff currently uses (or has used in the recent past) several mobile applications that provide location data to Defendant. As a condition of using these mobile applications, Plaintiff was required to provide and entrust her location data and Private Information to Defendant. Plaintiff would not have entrusted her location data and Private Information to Defendant had she known of Defendant's inadequate data security practices and procedures.

67. Upon information and belief, at the time of the Data Breach, Defendant had obtained, stored, and maintained Plaintiff's Private Information including location data in its systems.

68. Upon information and belief, Plaintiff's Private Information including location data was targeted, accessed, and acquired in the Data Breach.

69. Plaintiff has undertaken reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and Plaintiff has spent significant time which would have otherwise been spent on other activities, including work or recreation, which has been lost and cannot be regained.

70. As a result of the Data Breach, Plaintiff has suffered fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of the details and scope of the Data Breach. Plaintiff has also experienced an increase in unusual messages on her phone from unknown and unidentified individuals who appear to know her location information.

71. Plaintiff anticipates spending additional time and money to continue mitigating the harms caused by the Data Breach.

72. Plaintiff has a continuing interest in ensuring that her location data, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future data breaches.

73. Defendant negligently disclosed Plaintiff and Class Members' Private Information for criminals to use in the conduct of criminal activity. Specifically, Defendant allowed unauthorized access, disclosure, and exfiltration the Private Information of Plaintiff and the Class Members to unauthorized third parties engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity theft or fraud), using stolen Private Information.

74. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially thousands of individuals' detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

76. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

77. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiff and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an imminent and indefinite increased risk of suffering identity theft, fraud, misuse of their PII, diminution of value of PII, out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

78. Upon information and believe, the unencrypted Private Information of Plaintiff and Class Members is already published and/or available for sale on the dark web.

79. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[29] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they

[29] *What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

wish to visit in advance. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

80. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information accessed and exfiltrated in the Data Breach. The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information. As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[30]

81. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime. For example, armed with just a name and Social Security number, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or financial account information. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

---

[30] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

82. Moreover, the existence and prevalence of "Fullz" packages means that the PII/PHI stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

83. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[31]

84. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

85. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old

---

[31] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

86. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[33]

87. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[34]

88. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[35]

---

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft

[33] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[34] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).

[35] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

CLASS ALLEGATIONS

89. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and intend to certify the Nationwide Class and the California Subclass as follows:

Nationwide Class:

All individuals whose PII or Private Information, including location data, was compromised in the Data Breach.

California Subclass:

All individuals residing in California whose PII or Private Information, including location data, was compromised in the Data Breach.

90. The Nationwide Class and the California Subclass shall collectively be referred to as "the Class."

91. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

92. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

93. The Class members are so numerous and geographically dispersed throughout the United States and California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and the Class size is anticipated to be in the millions. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

94. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had Private Information including location data compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

95. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information, including location data, it collected from Plaintiff and Class Members;

(b) Whether Defendant breached its duty to protect the Private Information, including location data, of Plaintiff and Class members; and

(c) Whether Plaintiff and Class Members are entitled to damages and other equitable relief.

96. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that they has no interests adverse to or that conflicts with the Class they seek to represent. Plaintiff have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

97. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would

make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

98. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of Plaintiff and California Class Members)

99. Plaintiff re-alleges and incorporate by reference all proceeding paragraphs as if fully set forth herein.

100. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

101. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes,

controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' Private Information, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

102. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect Private Information and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

103. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of statutory and common law in that a portion of the money Plaintiff and Class members paid, or that Defendant received, for Defendant's products and services went to fulfill the obligations, including maintaining

the security of their Private Information, and Defendant's legal obligations, and Defendant failed to fulfill those obligations.

104. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

105. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their Private Information but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security in conformance with its legal obligations. Had Plaintiff and Class members known about Defendant's substandard data security practices they would not have entrusted their Private Information to Defendant or purchased Defendant's products or services or would have paid less for them. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's Private Information.

106. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing heightened increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Private Information, (iv) statutory damages under the CCPA, (v) deprivation of the value of their Private Information for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and

mitigating damages.

107. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of themselves, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

SECOND CAUSE OF ACTION

Negligence

108. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

109. Defendant owed various duties to Plaintiff and the Class, including pursuant to the CCPA, as alleged in detail above. Defendant owed duties to Plaintiff and the Class with regard to their manner of collection, transmission, sharing, and maintenance of Plaintiff's and the Class members' Private Information, including location data, and were required to maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class members personal information.

110. Defendant's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable care in protecting such information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either affirmatively acquires, maintains, or stores. Industry standards require Defendant to exercise reasonable care with respect to Plaintiff and Class Members by

implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity that could adequately protect the data that that it solicited, collected, and stored.

111. Defendant breached its respective duties by engaging in the conduct and omissions alleged above and in violation other statutes and regulations, including the CCPA, UCL, and FTC Act.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

113. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

114. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

116. Defendant is both the actual and legal cause of Plaintiff's and the Class Members' damages.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is

used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and Class Members; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

118. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

119. Due to the egregious violations alleged herein, Plaintiff asserts that Defendant breached its duties in an oppressive, malicious, despicable, gross, and wantonly negligent manner. Defendant's conscious disregard for Plaintiff's privacy right entitles Plaintiff and the Class to recover punitive damages.

THIRD CAUSE OF ACTION

Breach of Implied Contract

120. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

121. Defendant collected, stored, and maintained the Private Information, including location data, of Plaintiff and the Class.

122. Plaintiff and Class Members provided their Private Information including location data to Defendant, either directly or indirectly, in the ordinary course of Defendant's business as a requirement to access and use the mobile applications on their cell phones or other smart devices.

123. Plaintiff and Class Members were required to provide their location data as part of Defendant's regular business practices; and in order to fully use their mobile applications, Plaintiff and Class Members accepted provided their Private Information including location data to Defendant.

125. Plaintiff and Class Members entrusted Defendant, directly or indirectly, with their Private Information, including location data, with the reasonable and mutual understanding that Defendant would safeguard their information.

126. Defendant received and accepted possession of Plaintiff's and Class Members' Private Information including location data for the purpose of collecting, storing, selling, and ultimately profiting from the Private Information and location data of Plaintiff and Class Members as part of Defendant's business practices.

127. When Plaintiff and Class Members provided, and Defendant accepted, their Private Information including location data in the course of using certain mobile applications on their smart phones or other mobile devices, Plaintiff and Class Members entered into implied contracts with Defendant.

128. Through this exchange and these implied contracts, Defendant agreed to safeguard and protect their location data, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached, compromised, or stolen.

129. Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

130. Implicit in the agreements between Plaintiff and Class Members and Defendant, was Defendant's obligation to: (a) use such Private Information including location data for valid business purposes only; (b) take reasonable steps to safeguard that location data; (c) prevent unauthorized access to and/or disclosures of the location data; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their location data; (e) reasonably safeguard and protect the location data of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the location data only under conditions that kept such information secure and confidential.

131. Plaintiff and Class Members would not have entrusted their Private Information including location data to Defendant without the implied assurance that Defendant would keep their location data secure from unauthorized access, disclosure, or exfiltration.

132. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

125. Defendant breached the implied contracts made with Plaintiff and the Class Members by failing to safeguard and protect their Private Information including location data.

126. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information including location data;

(iii) lost or diminished value of their location data; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach) (v) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their location data, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's continued possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect their Private Information including location data.

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

128. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring and identity theft protection services to all Class Members.

FOURTH CAUSE OF ACTION

Unjust Enrichment

124. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

125. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their Private Information including location data to derive profit and facilitate its business.

126. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

127. Defendant enriched itself selling and marketing Plaintiff's and the Class Members Private Information including location data without their consent.

128. Under principles of equity and good conscience, Defendant should not

be permitted to retain the value of Plaintiff's and Class Members' Private Information including location because Defendant unlawfully collected and sold the Private Information including location.

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

130. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be appointed a representative of the Class, and (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, on behalf of themselves and members of the Class further requests that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit;

(vii) pre-judgment and post-judgment interest; and

(vii) such other and further relief the Court deems just and proper.

//

//

//

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a jury trial on all issues so triable.

Dated: February 5, 2025

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Abbas Kazerounian*

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff