KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
Mona Amini, Esq. (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
David Keifer

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF CONTRA COSTA – COMPLEX CIVIL

DAVID KEIFER, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

SLT LENDING SPV, INC. d/b/a SUR LA TABLE,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*;
3. BREACH OF CONTRACT; and
4. NEGLIGENCE

DEMAND FOR JURY TRIAL

//

//

//

//

//

//

//

Plaintiff David Keifer ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class members"), by and through his attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, brings this class action against Defendant SLT Lending SPV, Inc. d/b/a Sur La Table ("Defendant" or "Sur La Table"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against Defendant and its related entities, subsidiaries, and agents for failing to secure and safeguard the personally identifiable information ("PII") that Defendant collected and maintained and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been stolen. Sur La Table is a retailer of a variety of upscale cooking & dining supplies, plus home décor and cooking classes. For its business purposes, Defendant collects, receives, and maintains a substantial amount of PII from individuals, like Plaintiff, in its servers and/or networks.

2. On or around May 24, 2023, Defendant disseminated a "Notice of Data Breach" letter announcing that Defendant recently had an incident that involved some of the information Plaintiff and entrusted in Defendant's care, and that Defendant had become aware of unusual activity on its network and "[t]he evidence showed that an unauthorized actor accessed certain folders on [Defendant's] devices between March 15, 2023 and March 25, 2023" (the "Data Breach"). Defendant's investigation and review of the files that were accessed determined Plaintiff's and other similarly situated individuals' PII, including names, Social Security numbers, driver's license numbers or state identification number, and/or medical or health information were included in the personal information or PII accessed and/or obtained in the Data Breach.

3. Although the Data Breach was identified in March 2023, placing Plaintiff's and other similarly situated persons' sensitive information in the hands of malicious actors as a result of Defendant's failure to safeguard Plaintiff's and others' PII, Defendant waited months later until on or around May 24, 2023 to provide the above-referenced Notice of Data Breach to Plaintiff and other similarly situated Class members. This notice was still lacking in information necessary for Plaintiff and Class members to understand the scope and severity of the Data Breach. Due to this

lapse in time between the Data Breach and Defendant's notice to Plaintiff and affected Class members, unauthorized third parties have already been able to acquire and sell Plaintiff's and the Class members' PII (including Social Security Numbers) on the black market or dark web, or otherwise fraudulently misuse it for their personal gain.

4. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from individuals and maintained for business purposes and stored on its networks.

5. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access, disclosure, and exfiltration of Plaintiff's and Class members' personal information on inadequately protected servers and/or networks.

6. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' PII to be accessed, viewed, stolen and/or disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on behalf of himself individually and on behalf of all other similarly situated California residents affected by the Data Breach.

7. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for himself and the Class, equitable relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

9. This Court has personal jurisdiction over Defendant because Defendant's regularly conducts business in California and with California consumers.

10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant regularly conducts business in this county, and unlawful acts or omissions have occurred in this county.

PARTIES

11. At all relevant times, Plaintiff resided in Contra Costa County, California. Plaintiff is an individual who had his personal information and PII collected and maintained by Defendant, and received notice that he was a victim of the Data Breach.

12. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII was accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

13. Defendant is a corporation formed under the laws of the State of Delaware with its principal place of business and/or headquarters located in Merrillville, Indiana.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

14. The California Constitution guarantees every Californian a right to privacy and PII is a recognized valuable property right.[1] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

15. 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.[2]

16. 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

[1] *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).

[2] 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.

traditional financial assets."[3] 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.

17. 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.[4]

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

19. 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.[5] This business has created a new market for the sale and purchase of this valuable data.[6]

20. Consumers place a high value not only on their PII, 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

---

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

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

[5] 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.

[6] *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.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

21. 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.[8]

22. 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 PII Has Grave and Lasting Consequences for Victims

23. 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.

24. Theft or breach of PII 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."[9]

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[10] 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.

---

[7] 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#

[8] 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).

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

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

26. 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.[11]

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12] 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.[13]

28. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of 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

---

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

[12] 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*.

[13] *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/.

> your Social Security number and assuming your identity can cause a lot of problems.[14]

29. 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.[15] 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.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

30. 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."

31. 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.[18]

32. It is within this context that Plaintiff and thousands of similar Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

---

[14] 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.

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

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

[17] 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).

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

Defendant's Collection of Individuals' PII

33. Defendant collects the PII of individuals like Plaintiff and the Class members. This PII includes, *inter alia*, Plaintiff and the Class members' names, contact information, Social Security numbers, driver's license or state identification numbers, and medical or health information.

34. Defendant represents in it its Privacy Policy, which is incorporated into its Terms & Conditions use by reference,[19] that they " have implemented measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to us is stored on our secure servers behind firewalls. Any payment transactions will be encrypted using SSL technology."[20]

35. Defendant had the duty to keep Plaintiff's and the Class members' sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers like Plaintiff and the Class members, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, particularly when Social Security numbers are involved.

36. Defendant's Privacy Policy states that it has collected several categories of PII, including:

- Personal and online identifiers (such as first and last name, email address, phone number, usernames or unique online identifiers, IDFA, AAID);
- Financial Account Information (such as credit card numbers, bank account information, PayPal account information);
- Customer Profile Information (such as race, gender, age range, income range, ad demographics);
- Transactional Information;
- Online Activity Information (such as browsing history, search history, interactions with a website, email, application, or advertisement);

---

19 *See* https://www.surlatable.com/terms_and_conditions.html
20 *See* https://www.surlatable.com/privacy-policy.html

- Non-Precise Geolocation Information (such as zip or area code, state, country);
- Precise Geolocation Information (such as home or billing address or latitude and longitude);
- Inferences drawn from the above information about your predicted characteristics and preferences; and
- Other information about you that is linked to the Personal Information above

The Data Breach

37. On or around May 24, 2023, Defendant issued an official Notice of Data Breach to Plaintiff and other Class members who were victims of the Data Breach, stating that Defendant recently had an incident that involved some of the information Plaintiff and entrusted in Defendant's care.

38. According to Defendant, its investigation determined that "an unauthorized actor accessed certain folders on [Defendant's] devices between March 15, 2023 and March 25, 2023." As part of Defendant's investigation, Defendant reviewed the files that were accessed by the unauthorized person and determined that Plaintiff's and other similarly situated individuals' PII, including names, Social Security numbers, driver's license numbers or state identification number, and/or medical or health information were included in the personal information or PII accessed and/or obtained in the Data Breach.

39. Defendant's Notice of Data Breach letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding why it waited months since learning of the data breach and identifying Plaintiff and affected Class members to send them notice or how many people were affected by the Data Breach.

40. As a result of the Data Breach, Plaintiff has suffered an invasion and loss of Plaintiff's privacy, Plaintiff has spent time monitoring their personal financial accounts and credit reports, which was time that Plaintiff otherwise would have spent performing other activities or leisurely events for the enjoyment of life rather than mitigating the impact of the Data Breach.

41. As a result of the Data Breach, Plaintiff is, and will continue to be, at heightened and imminent risk for financial fraud and/or identity theft, and the associated damages resulting from it, for years to come.

Defendant Knew or Should Have Known PII Are High Risk Targets

42. Defendant knew or should have known that PII like that at issue here, is a high-risk target for identity thieves.

43. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[21]

44. 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 May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services have the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[22]

45. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data

---

[21] 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.

[22] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[23]

46. As such, Defendant was aware that PII 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' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS ACTION ALLEGATIONS

47. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intend to seek certification of a class (the "Class") defined as:

All California residents whose PII was subjected to the Data Breach.

48. Excluded from the Class are: (1) Defendant and its officers, directors, 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.

49. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their 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.

50. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of thousands of persons whose personal information was compromised in Data Breach, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

[23] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

51. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII 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.

52. 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 PII it collected, stored, and maintained from Plaintiff and Class members;

(b) Whether Defendant breached its duty to protect the PII of Plaintiff and each Class member; and

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

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

54. 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.

55. 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 Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

56. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

57. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[24]

58. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

[24] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

59. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

60. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

61. Plaintiff and the Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

62. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in and is headquartered in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

63. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and other Class members' unencrypted names and Social Security numbers, among other personal information.

64. Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure because Plaintiff's PII, including name, Social Security number, driver's license numbers or state identification number, and/or medical or health information, *at minimum*, were wrongfully accessed, viewed, and/or taken by unauthorized persons in the Data Breach.

65. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an invasion of its network and stored files by unauthorized individuals and to prevent unauthorized access of Plaintiff's and Class members' PII as a result of the Data Breach.

66. On or about June 9, 2023, Plaintiff sent Defendant written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. If Defendant does not cure the violation within 30 days, Plaintiff will amend this complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

67. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff, on behalf of himself individually and the Class, seeks actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

68. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

69. 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.

70. 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' PII, 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*.), Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5, and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. 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.

71. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to better safeguard and protect their PII and identities.

72. 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 PII 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.

73. 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.

74. 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 (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 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 PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII 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 caused by the Data Breach.

75. 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 himself, the 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 PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Breach of Contract

76. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

77. Plaintiff and Class members were required to provide their PII to Defendant in connection with their communications and/or transactions with Defendant.

78. As part of these communications and/or transactions, Plaintiff and Class members entered into implied and/or express contracts with Defendant as set forth in its Terms & Conditions and Privacy Policy that included Defendant's promise to safeguard personal information given to Defendant or that Defendant gathered on their own, from disclosure, as set forth in Defendant's Privacy Policy, which was posted on its website and incorporated into its Terms & Conditions. In providing their PII to Defendant, it was implicit that Defendant would use Plaintiff's and the Class members' PII for approved business purposes only and would not make unauthorized disclosures of such information or allow unauthorized access to their PII.

79. Plaintiff and Class members entered into implied contracts with Defendant with the reasonable expectation that Defendant's data security practices and policies were adequate and consistent with industry standards. Plaintiff and Class members believed that Defendant would provide adequate and reasonable data security practices to protect their PII and would provide accurate and timely notice if such information was compromised, lost, or stolen.

80. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their communications and/or transactions involving products or services from Defendant.

81. By allowing unauthorized users to gain access to Plaintiff's and Class members' PII through the Data Breach, Defendant breached these contractual obligations. As a result, Defendant failed to comply with its own policies, including its Privacy Policy, as well as applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII. Defendant's breach of contract also violated California Business and Professions Code § 22576,

which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy.

82. By failing to fulfill its contractual obligations under its Terms & Conditions and Privacy Policy, Defendant failed to confer on Plaintiff and Class members the benefit of the bargain, causing them economic injury.

83. As a direct and proximate result of the Data Breach and Defendant's breach of its contractual obligations, Plaintiff and Class members have been harmed and have suffered actual losses and damages as described herein and above, and will continue to suffer, imminent and continued damages and injuries for years to come.

FOURTH CAUSE OF ACTION

Negligence

84. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

85. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

86. Defendant and the Class members' PII was entrusted to Defendant with the understanding that Defendant would safeguard their personal information.

87. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII were wrongfully disclosed or accessed by unauthorized persons, including in the event of a data breach.

88. By collecting and storing the personal information, or PII, of Plaintiff and the Class members, Defendant had a duty to use reasonable means to secure and safeguard its computer systems and networks—and Class members' PII held within it— to prevent disclosure of the information, and to safeguard the information from unauthorized access or disclosure, to promptly detect a breach of its security systems, and to give prompt notice to those affected in the event of a data breach.

89. Defendant's duty to use reasonable care in protecting confidential data 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 PII.

90. Defendant was negligent and breached its duties by failing to use reasonable security practices and procedures to safeguard Plaintiff's and the Class members' PII.

91. It was foreseeable that Defendant's failure to use reasonable security practices and procedures to safeguard Plaintiff's and the Class members' PII would result in injury to Plaintiff and the Class. Further, the Data Breach was reasonably foreseeable given the known danger and frequency of cyberattacks, phishing and ransomware attacks, and data breaches in the industry.

92. Defendant is both the actual and legal cause of Plaintiff and the Class members' damages.

93. Plaintiff alleges upon information and belief that as a proximate result of Defendant's negligence, Plaintiff and the Class have suffered actual damages and significant emotional distress as described herein and above because of the Data Breach.

94. As a result of Defendant's negligence, Plaintiff and the Class members have suffered and will continue to suffer damages and injury including, but not limited to out-of- pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

95. Plaintiff and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach, as well as injunctive relief and declaratory relief.

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

PRAYER FOR RELIEF

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

- general, compensatory, and/or consequential damages
- actual and punitive damages to be determined by the trier of fact;
- equitable relief, including restitution;
- appropriate injunctive relief;
- declaratory relief;
- attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;
- costs of suit;
- pre-judgment and post-judgment interest at the highest legal rates applicable; and
- any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Dated: June 9, 2023

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: _____

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

Attorneys for Plaintiff