

1 MAYER BROWN LLP  
JOHN NADOLENCO (SBN 181128)  
2 jnadolenco@mayerbrown.com  
DOUGLAS A. SMITH (SBN 290598)  
3 dougsmith@mayerbrown.com  
350 S. Grand Ave., 25th Floor  
4 Los Angeles, CA 90071-1503  
Telephone: (213) 229-9500  
5 Facsimile: (213) 625-0248

6 DAVID SIMON (*pro hac vice* to be filed)  
dsimon@mayerbrown.com  
7 1999 K Street, NW  
Washington, DC 20006-1101  
8 Telephone: (202) 263-3388  
Facsimile: (202) 264-3300

9 SAMANTHA A. MACHOCK (SBN 298852)  
smachock@mayerbrown.com  
10 Two Palo Alto Square  
11 3000 El Camino Real  
Palo Alto, CA 94306-2112  
12 Telephone: (650) 331-2087  
Facsimile: (650) 331-2060  
13

14 *Attorneys for Defendants*  
15 *Smile Brands Inc. and Sahawneh Dental*  
*Corporation*

16  
17 **UNITED STATES DISTRICT COURT**  
18 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**  
19

20 ANGELICA PONCE, individually, and  
21 on behalf of all others similarly situated,

22 Plaintiff,

23 v.

24 SMILE BRANDS INC.; SAHAWNEH  
DENTAL CORPORATION; and DOES  
25 1-50, inclusive,

26 Defendants.  
27  
28

Case No. 8:21-cv-2115

**NOTICE OF REMOVAL  
PURSUANT TO 28 U.S.C. §§ 1441(a)  
AND 1453 BY DEFENDANTS  
SMILE BRANDS INC. AND  
SAHAWNEH DENTAL  
CORPORATION**

[Removed from California Superior  
Court, County of Orange, Case No. 30-  
2021-01232683-CU-NP-CXC]

**TO THE UNITED STATES DISTRICT COURT FOR THE CENTRAL  
DISTRICT OF CALIFORNIA AND TO PLAINTIFF AND HER COUNSEL  
OF RECORD:**

**PLEASE TAKE NOTICE THAT**, Defendants Smile Brands Inc. (“SBI”), and Sahawneh Dental Corporation (collectively, “Defendants”) hereby remove *Ponce v. Smile Brands, Inc.*, Case No. 30-2021-01232683-CU-NP-CXC, from the Superior Court of California, County of Orange, to the United States District Court for the Central District of California pursuant to 28 U.S.C. § 1441(a) governing the removal of civil actions and § 1453 governing the removal of class actions. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d)(2)(a), as well as federal question jurisdiction under 28 U.S.C. § 1331 and corresponding supplemental jurisdiction under 28 U.S.C. § 1367(a). Pursuant to 28 U.S.C. § 1446(a), all process, pleadings, and orders served on Defendants in the action to date are attached as Exhibit 1 to the Declaration of Douglas A. Smith (“Smith Decl.”), and Defendants provide the following “short and plain statement of the grounds for removal.”<sup>1</sup>

---

<sup>1</sup> As the Supreme Court has held, § 1446(a) requires only that Defendants plausibly allege the requirements for federal jurisdiction; Defendants “need not [offer] evidentiary submissions” with the notice of removal. *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 84 (2014). “Evidence establishing [jurisdiction] is required by § 1446(c)(2)(B) only when the plaintiff contests, or the court questions, the defendant’s allegation.” *Id.* at 89; *accord Arias v. Residence Inn by Marriott*, 936 F.3d 920, 924–25 (9th Cir. 2019) (“[A] removing defendant’s notice of removal ‘need not contain evidentiary submissions’ but only plausible allegations of the jurisdictional elements. . . . [E]vidence showing [that the jurisdictional requirements are met] is required ‘only when the plaintiff contests, or the court questions, the defendant’s allegation.’” (citations omitted)).

## INTRODUCTION

1  
2 1. In April 2021, Defendants allegedly fell victim to a ransomware attack,  
3 which affected certain computer systems containing Personally Identifiable  
4 Information (“PII”), and Protected Health Information (“PHI”), as defined under the  
5 federal Health Insurance Portability and Accountability Act (“HIPAA”) and 45  
6 C.F.R. § 160.103. (Compl. ¶¶ 27, 121.)

7 2. On November 18, 2021, Plaintiff Angelica Ponce filed a putative  
8 nationwide class action against Defendants in the Superior Court of the State of  
9 California, County of Orange, alleging harm from having both her PII and PHI  
10 “accessed, exfiltrated, and disclosed to unauthorized persons.” (Compl. ¶¶ 4, 15, 77,  
11 99.)

12 3. Against all Defendants, Plaintiff alleges four claims: (1) a violation of  
13 the California Consumer Privacy Act (“CCPA”), Cal. Civ. Code §§ 1798.100 to  
14 1799.100; (2) violations of the California Confidentiality of Medical Information Act  
15 (“CCMIA”), Cal. Civ. Code §§ 56 to 56.37; (3) violations of the unlawful, unfair,  
16 and fraudulent prongs of the California Unfair Competition Law (“UCL”), Cal. Bus.  
17 & Prof. Code §§ 17200 to 17210, including on the basis that Defendants violated  
18 Section 5 of the FTC Act, the CCMIA, the CCPA, HIPAA, and Article I, Section I  
19 of the California Constitution (Compl. ¶¶ 120–29); and (4) breach of contract.

20 4. The purported nationwide class that Plaintiff seeks to represent is  
21 defined as:

22 All individuals whose PII and/or PHI was compromised in the Data  
23 Breach disclosed by Defendants in their notice of Data Breach letter(s)  
24 (the “Class”) (Compl. ¶ 82.)

25 5. Among other remedies, Plaintiff, on behalf of herself and all members  
26 of the Class, seeks an award of actual, statutory, nominal, and punitive damages, and  
27 attorneys’ fees and costs. (*See* Compl., Prayer for Relief ¶¶ i–viii, ¶ 118.)  
28

1           6.       The Court has jurisdiction over this action pursuant to the Class Action  
2 Fairness Act (“CAFA”), 28 U.S.C. § 1332(d)(2)(a). In addition, federal question  
3 jurisdiction exists over Plaintiff’s UCL claim under 28 U.S.C. § 1331 because those  
4 claims raise “significant federal issues,” and corresponding supplemental jurisdiction  
5 exists over Plaintiff’s remaining claims under 28 U.S.C. § 1367 because those claims  
6 purportedly arise from “part of the same case or controversy” as the claims raising  
7 “significant federal issues.” Accordingly, this action may be properly removed to this  
8 Court under 28 U.S.C. §§ 1441 and 1453 for multiple reasons.

9                               **REMOVAL IS PROPER UNDER CAFA**

10           7.        “[A]ny civil action brought in a State court of which the district courts  
11 of the United States have original jurisdiction, may be removed by the . . . defendants,  
12 to the district court for the district and division embracing the place where such action  
13 is pending.” 28 U.S.C. § 1441(a); *see also id.* § 1453(b).

14           8.       CAFA vests district courts with original jurisdiction over putative class  
15 actions with 100 or more class members, where the aggregate amount in controversy  
16 exceeds \$5 million exclusive of interest and costs, and where “any member of [the]  
17 class of plaintiffs is a citizen of a state different from any defendant.” 28 U.S.C.  
18 § 1332(d)(1)–(2). This action satisfies each of CAFA’s requirements, as evidenced  
19 by the fact that other plaintiffs who have filed suit against SBI because of the  
20 ransomware attack have asserted that federal court jurisdiction exists under CAFA.  
21 *See Complaint, Hellyer v. Smile Brands, Inc.*, Case No. 8:21-cv-01886-DOC-ADS,  
22 at ¶ 22 (C.D. Cal. Nov. 18, 2021) (“This Court has diversity jurisdiction over this  
23 action under the Class Action Fairness Act (CAFA), 28 U.S.C. §1332(d)”) [ECF No.  
24 1].

25           9.       **Covered Class Action.** This action meets CAFA’s definition of a class  
26 action, which is “any civil action” filed under a “State statute or rule of judicial  
27 procedure” that, “similar” to Federal Rule of Civil Procedure 23, authorizes “an  
28 action to be brought by 1 or more representative persons as a class action.” 28 U.S.C.

1 § 1332(d)(1)(B); *see* 28 U.S.C. § 1453(a). Plaintiff seeks certification of a nationwide  
 2 class under California Code of Civil Procedure § 382 and § 1781 (Compl. ¶¶ 82–  
 3 90)—which are California’s analogues to Federal Rule of Civil Procedure 23. *See*  
 4 *Williams v. Superior Court*, 221 Cal. App. 4th 1353 (2013) (stating that California  
 5 Code of Civil Procedure § 382 is analogous to Federal Rule of Civil Procedure 23(a));  
 6 *Vasquez v. Superior Ct.*, 4 Cal. 3d 800, 821 (1971) (discussing that trial courts may  
 7 look to Rule 23 when analyzing difficult issues regarding class certification under  
 8 § 1781). Accordingly, Plaintiff filed a “class action” within the meaning of CAFA.

9       **10. Class Action Consisting of More Than 100 Members.** Plaintiff seek  
 10 to represent a class of “[a]ll individuals whose PII and/or PHI was compromised in  
 11 the Data Breach,” (Compl. ¶ 82) which Plaintiff’s complaint suggests number in the  
 12 “hundreds of thousands” (Compl. ¶ 40). Further, Plaintiff alleges that Defendants  
 13 “[r]eported to the U.S. Department of Health and Human Services that Defendants’  
 14 Data Breach involved the unsecured protected health information of at least 199,683  
 15 individuals.” (Compl. ¶ 40, n. 27). Accordingly, by Plaintiff’s own admission, there  
 16 are at least 100 persons in the putative class, as required by 28 U.S.C.  
 17 § 1332(d)(5)(B). *See Kuxhausen v. BMW Fin. Servs. NA LLC*, 707 F.3d 1136, 1140  
 18 (9th Cir. 2013) (“Complaint . . . seeking to ‘provide remedies for hundreds of affected  
 19 consumers’” was sufficient to establish at least 100 class members).

20       **11. The Parties Are Minimally Diverse.** CAFA requires minimal  
 21 diversity—which means that at least one putative class member must be “a citizen of  
 22 a State different from any defendant.” 28 U.S.C. § 1332(d)(2)(A). A class member is  
 23 any person “who falls[] within the definition” of the proposed class. *Id.*  
 24 § 1332(d)(1)(D). And corporations are deemed to be citizens of the states where they  
 25 are incorporated or organized, and where they have their principal places of business.  
 26 28 U.S.C. § 1332(c)(1), (d)(10).

27       12. Defendant SBI is a Washington corporation with its principal place of  
 28 business in California. (Compl. ¶ 11.) Defendant Sahawneh Dental is a California

1 Corporation with its principal place of business in California. (Compl. ¶ 12.)  
 2 Although Plaintiff, an individual, is a citizen of California, minimal diversity exists  
 3 because she brings suit on behalf of a nationwide class consisting of “hundreds of  
 4 thousands” of individuals associated with Defendants’ “700 affiliated dental offices,”  
 5 and Defendant SBI provides business support services to “[h]undreds of other dental  
 6 office[s].” (Compl. ¶¶ 1, 40, 41.) And the Complaint alleges that the “Class members  
 7 are . . . geographically dispersed throughout the United States,” thereby admitting  
 8 that putative absent class members are citizens of states other than California. *Id.* ¶  
 9 85.

10 13. **The Amount In Controversy Exceeds \$5 Million.** Under CAFA, the  
 11 claims of class members are aggregated to determine if the amount in controversy  
 12 exceeds the required “sum or value of \$5,000,000, exclusive of interests and costs.”  
 13 28 U.S.C. § 1332(d)(2), (d)(6). A “defendant’s notice of removal need include only  
 14 a *plausible allegation* that the amount in controversy exceeds the jurisdictional  
 15 threshold” of \$5 million. *Dart Cherokee Basin Operating Co. v. Owens*, 574 U.S. 81,  
 16 89 (2014) (emphasis added).

17 14. Although Defendants deny all allegations of wrongdoing and state that  
 18 Plaintiff’s claims are meritless, Plaintiff’s complaint seeks, among other things,  
 19 compensatory, statutory, and punitive damages, attorneys’ fees, and a laundry list of  
 20 injunctive relief that leaves no question that the amount in controversy far exceeds  
 21 \$5 million.<sup>2</sup>

22 15. Plaintiff alleges a nationwide class of “hundreds of thousands.” (Compl.  
 23 ¶ 40.) Plaintiff references the publicly available data on the U.S. Department of  
 24 Health and Human Service’s “Breach Portal,” which shows that the ransomware

25 \_\_\_\_\_  
 26 <sup>2</sup> See generally *Ibarra v. Manheim Invs., Inc.*, 775 F.3d 1193, 1198 n.1 (9th Cir.  
 27 2015) (“Even when defendants have persuaded a court upon a CAFA removal that  
 28 the amount in controversy exceeds \$5 million, they are still free to challenge the  
 actual amount of damages in subsequent proceedings and at trial. This is so because  
 they are not stipulating to damages suffered, but only estimating the damages that  
 are in controversy.”).

1 attack affected at least 199,683 individuals. *See id.* n.27.<sup>3</sup> On behalf of that putative  
 2 class, Plaintiff seeks to recover compensatory and consequential damages for, among  
 3 other things:

- 4 (i) the imminent and continued risk of identity theft;
- 5 (ii) the delayed ability to take necessary precautions to protect against  
 6 identity theft and other fraud;
- 7 (iii) unauthorized person(s) accessing, viewing, and acquiring Plaintiff  
 8 and the Class' data;
- 9 (iv) out-of-pocket expenses associated with the prevention, detection,  
 10 and recovery from identity theft, tax fraud, or unauthorized use of their  
 11 PII and PHI;
- 12 (v) invasion of privacy;
- 13 (vi) breach of the confidentiality of Plaintiff and the Class' PII/PHI;
- 14 (vii) deprivation of the value of Plaintiff and the Class' PII/PHI;
- 15 (viii) financial and temporal cost of monitoring credit, financial  
 16 accounts, and mitigating damages; and
- 17 (ix) insufficient identity theft protection. (Compl. ¶¶ 63-65, 77, 99, 101,  
 18 117, 118, 125, 135; Prayer for Relief ¶¶ i-viii.).

19 It is more than plausible that all of this relief—some of which is intended to  
 20 compensate class members for purported harm they will face for “years to come”  
 21 (Compl. ¶ 64)—would total \$26 per class member *at a minimum*. Multiplied by a  
 22 class of at least 199,683, the requested compensatory and consequential damages  
 23 *alone* exceed the amount in controversy threshold of \$5 million (199,683 x \$26 =  
 24 \$5.2 million).

25 16. Likewise, the amount of statutory damages Plaintiff has placed at issue  
 26 independently satisfies the \$5 million amount in controversy requirement. (*See*

27 \_\_\_\_\_  
 28 <sup>3</sup> *See also* U.S. Dep't of Health & Human Services, Office of Civil Rights, Breach  
 Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health  
 Information, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).



1 Compl. ¶¶ 91–102, 103–118.) For example, the California Confidentiality of Medical  
 2 Information Act (“CCMIA”) authorizes \$1,000 in statutory damages per individual.  
 3 Cal. Civ. Code § 56.36(b)(1). For a class of at least 199,683, California residents  
 4 would need to comprise only 2.6% of the class for the amount in controversy based  
 5 on CCMIA statutory damages *alone* to exceed \$5 million (\$1,000 x (199,683 x 2.6%)  
 6 = \$5.2 million). And that is not even factoring in Plaintiff’s request for punitive  
 7 damages of \$3,000 per affected California patient under the CCMIA,<sup>4</sup> or the \$100 to  
 8 \$750 per affected California resident Plaintiff seeks as statutory damages under the  
 9 CCPA.<sup>5</sup> The amount of requested statutory damages therefore provides an alternative  
 10 and independently sufficient reason why this case involves more than \$5 million in  
 11 controversy.

12 17. Further adding to the amount in controversy, the Court may consider  
 13 that Plaintiff has requested attorneys’ fees under California Civil Code § 56.35 of up  
 14 to \$1,000 per affected California subclass member (*see* Compl. ¶ 118), which could  
 15 be sizeable given that even Plaintiffs themselves recognize that the case is “complex”  
 16 (Compl. at 1). *See Fritsch v. Swift Transp. Co. of Ariz., LLC*, 899 F.3d 785, 794 (9th  
 17 Cir. 2018) (vacating a district court’s remand order because “a court *must* include  
 18 future attorneys’ fees recoverable by statute . . . when assessing whether the amount-  
 19 in-controversy requirement [under CAFA] is met.” (emphasis added)).

20 18. In addition, the Court may consider the value of Plaintiff’s requested  
 21 injunctive relief. *See Hunt v. Wash. State Apple Advert. Comm’n*, 432 U.S. 333, 347  
 22 (1977) (“In actions seeking declaratory or injunctive relief, it is well established that  
 23 the amount in controversy is measured by the value of the object of the litigation.”).  
 24 Plaintiff seeks injunctive relief requiring, among other things, that Defendants  
 25 (i) “modify its corporate culture and design,” and (ii) “design, adopt, implement,

26  
 27 <sup>4</sup> Compl. ¶ 118 (citing Cal. Civ. Code § 56.35); *Greene v. Harley-Davidson, Inc.*,  
 28 965 F.3d 767, 772 (9th Cir. 2020) (allowing defendant to rely on potential punitive  
 damages to satisfy CAFA’s amount-in-controversy requirement).

<sup>5</sup> Compl. ¶ 101; Cal. Civ. Code § 1798.150(a)(1)(A) & (b).



1 control, direct, oversee, manage, monitor and audit appropriate data security  
 2 processes, controls, policies, procedures, protocols, and software and hardware  
 3 systems to safeguard and protect the PII/PHI entrusted to it.” (Compl. ¶ 129.)  
 4 Implementing all of Plaintiff’s requested injunctive relief—together with Plaintiff’s  
 5 request for out-of-pocket expenses associated with credit monitoring (Compl. ¶¶ 117,  
 6 128)—would easily run in the millions.

7 19. In sum, because the amount in controversy exceeds \$5 million and all  
 8 the other factors for CAFA jurisdiction are met, this case “belongs in federal court.”  
 9 *See Lewis v. Verizon Commc’ns, Inc.*, 627 F.3d 395, 399 (9th Cir.2010).

### 10 FEDERAL QUESTION JURISDICTION

#### 11 PROVIDES AN ADDITIONAL BASIS FOR REMOVAL

12 20. The Supreme Court has recognized that “in certain cases federal-  
 13 question jurisdiction will lie over state-law claims that implicate significant federal  
 14 issues.” *Grable & Sons Metal Prods., Inc. v. Darue Eng’g & Mfg.*, 545 U.S. 308, 312  
 15 (2005). “The doctrine captures the commonsense notion that a federal court ought to  
 16 be able to hear claims recognized under state law that nonetheless turn on substantial  
 17 questions of federal law, and thus justify resort to the experience, solicitude, and hope  
 18 of uniformity that a federal forum offers on federal issues.” *Id.*

19 21. Federal jurisdiction over a state-law claim will lie if a federal issue is:  
 20 (1) necessarily raised, (2) actually disputed, (3) substantial, and (4) capable of  
 21 resolution in federal court without disrupting the federal-state balance approved by  
 22 Congress. *Gunn v. Minton*, 568 U.S. 251, 258 (2013).

23 22. Plaintiff’s UCL claim raises “significant federal issues.” *First*, this  
 24 claim explicitly raises federal issues. Plaintiff’s UCL claim is predicated on a  
 25 violation of Section 5 of the FTC Act and HIPAA. (Compl. ¶¶ 121, 124.) Moreover,  
 26 Plaintiff’s UCL claim is predicated on an allegedly imminent risk of “identity theft”  
 27 (Compl. ¶¶ 40, 63, 117, 128)—and Plaintiff defines that risk by express reference to  
 28 the regulatory definition of “identify theft” in the Code of Federal Regulations, *see*

1 16 C.F.R. § 603.2 (cited at Compl. ¶ 32 n.15). Accordingly, despite asserting only  
 2 state-law claims, a full resolution of Plaintiff's claim, as alleged, would require the  
 3 Court to resolve significant federal issues in connection with her UCL claim. *See*  
 4 *Rosenman v. Facebook Inc.*, 2021 WL 3829549, at \*7 (N.D. Cal. Aug. 27, 2021).

5 23. *Second*, the aforementioned federal issues are actually disputed because  
 6 Defendants deny all the claims asserted against them. *See Gunn*, 568 U.S. at 259  
 7 (holding that the federal issue was actually disputed where the defendants denied the  
 8 plaintiff's allegations on the federal issue).

9 24. *Third*, the federal issues raised in Plaintiff's complaint are substantial in  
 10 the sense that the issues are important to the "federal system as a whole." *Gunn*, 568  
 11 U.S. at 260. Plaintiff's UCL claim turns on whether Defendants violated Section 5 of  
 12 the FTC Act, HIPAA, or both, when they suffered a ransomware attack. Ransomware  
 13 attacks on national corporations, such as Smile Brands, that result in alleged  
 14 disclosure of data protected under federal law (*i.e.*, "Protected Health Information")  
 15 do not raise a state or local issue, but rather a federal one. As President Biden's  
 16 "Executive Order on Improving the Nation's Cybersecurity" made clear,  
 17 "remediation of cyber incidents is a top priority [of the federal government] and  
 18 essential to national and economic security."<sup>6</sup> The federal interest in enforcing  
 19 cybersecurity measures in the context of ransomware attacks is therefore  
 20 unquestionably substantial. *See Rosenman*, 2021 WL 3829549, at \*6.

21 25. *Fourth*, the federal issues are capable of resolution in federal court  
 22 without disrupting the federal-state balance approved by Congress. This requirement  
 23 focuses "principally on the nature of the claim, the traditional forum for such a claim,  
 24 and the volume of cases that would be affected." *New York ex rel. Jacobson v. Wells*  
 25 *Fargo Nat'l Bank, N.A.*, 824 F.3d 308, 316 (2d Cir. 2016). Neither Section 5 of the  
 26

27  
 28 <sup>6</sup> Executive Order on Improving the Nation's Cybersecurity (May 12, 2021),  
[https://www.whitehouse.gov/briefing-room/presidential-](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)  
[actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

1 FTC nor HIPAA provides for a private right of action<sup>7</sup> and were intended by  
 2 Congress to be enforced exclusively by the FTC and Health and Human Services  
 3 respectively<sup>8</sup>—which means that Plaintiff’s UCL claim cannot be brought based on  
 4 a violation of these federal statutes. As the California Supreme Court’s reasoning in  
 5 *Loeffler v. Target Corp.*, 58 Cal. 4th 1081 (2014), makes clear, it would be  
 6 “inconsistent” to allow Plaintiff to assert a UCL unlawful prong claim predicated on  
 7 an underlying violation of a federal statute that Congress gave federal agencies  
 8 exclusive authority to enforce, in part to ensure nationwide uniformity in application.  
 9 Plaintiff’s UCL claim therefore belongs in this Court given the substantial federal  
 10 issues it raises—because California law does *not* provide a right of action in state  
 11 court for it.

12 26. Accordingly, the Court has federal question jurisdiction over Plaintiff’s  
 13 UCL claim because it necessarily turns on disputed and substantial questions of  
 14 federal law important to the federal system, and because resolution would not disrupt  
 15 the federal-state balance. *See In re: Nat’l Football League’s Sunday Ticket Antitrust*  
 16 *Litig.*, 2016 WL 1192642, at \*4–6 (C.D. Cal. Mar. 28, 2016) (denying motion to  
 17 remand because claims were federal in nature and relief depended on the resolution  
 18 of substantial questions of federal law); *California ex rel. Lockyer v. Mirant Corp.*,  
 19 375 F.3d 831, 841–43 (9th Cir. 2004), *opinion amended on denial of reh’g*, 387 F.3d  
 20 966 (9th Cir. 2004) (same); *Rosenman*, 2021 WL 3829549, at \*7 (“This Court thus  
 21 exercises federal question jurisdiction over Plaintiff’s UCL unfair prong claim.”);  
 22

23 <sup>7</sup> *See United States v. Streich*, 560 F.3d 926, 935 (9th Cir. 2009) (“HIPAA does not  
 24 provide any private right of action.”); *Carlson v. Coca-Cola Co.*, 483 F.2d 279, 281  
 25 (9th Cir. 1973) (holding that Section 5 of the FTC Act lacks a private right of  
 action).

26 <sup>8</sup> *United States v. St. Regis Paper Co.*, 355 F.2d 688, 693 (2d Cir. 1966) (stating the  
 27 Congress “granted the FTC exclusive authority to enforce the proscription against  
 28 unfair methods of competition and deceptive acts or practices in commerce and,  
 also, granted the FTC exclusive authority to issue orders to cease and desist from  
 such practices.”); *Logan v. Dep’t of Veterans Affairs*, 357 F. Supp. 2d 149, 155  
 (D.D.C. 2004) (holding that HIPAA provides HHS the exclusive authority to  
 enforce its provisions).

1 *Cent. Valley Med. Grp., Inc. v. Indep. Physician Assoc. Med. Grp.*, 2019 WL  
 2 2491328, at \*3 (E.D. Cal. June 14, 2019) (denying motion to remand and concluding  
 3 that UCL unfair prong claim necessarily raised a federal issue); *Cordon v. Wachovia*  
 4 *Mortg., a Div. of Wells Fargo Bank, N.A.*, 776 F. Supp. 2d 1029, 1036 (N.D. Cal.  
 5 2011) (“Because the success or failure of Plaintiff’s UCL claims is contingent upon  
 6 violations of federal law, the Court finds that subject matter jurisdiction is present  
 7 with respect to the FAC.”).

8 27. Because the Court has federal question jurisdiction over Plaintiff’s UCL  
 9 claim, it has supplemental jurisdiction under 28 U.S.C. § 1367(a) over Plaintiff’s  
 10 remaining state-law causes of action because they arise from “the same case or  
 11 controversy,” namely the ransomware attack Defendants suffered. (*Compare* ¶¶ 98,  
 12 206, *with* ¶¶ 133, 139, 151, 163, 173, 198); *see, e.g., Rosenman*, 2021 WL 3829549,  
 13 at \*7 (“[T]his Court exercises supplemental jurisdiction over Plaintiff’s claims under  
 14 the fraudulent prong of the UCL and for unjust enrichment because these claims,  
 15 which also concern [Defendant’s] alleged conduct . . . arise from ‘the same case or  
 16 controversy’ as Plaintiff’s UCL unfair prong claim.”).

### 17 COMPLIANCE WITH OTHER REMOVAL REQUIREMENTS

18 28. **Removal Is Timely.** This Notice of Removal is timely because the  
 19 Defendants filed it within 30 days of being served with the summons and initial  
 20 complaint on November 24, 2021. *See* 28 U.S.C. § 1446(b)(1) (requiring, as relevant  
 21 here, that a notice of removal of a civil action be filed within 30 days after the  
 22 defendant receives, “through service or otherwise,” a copy of the summons and  
 23 complaint); *see also Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc.*, 526 U.S.  
 24 344, 354 (1999).

25 29. **Venue Is Proper.** Plaintiff filed this action in the Superior Court of the  
 26 State of California, County of Orange. Therefore, venue is proper in the United States  
 27 District Court for the Central District of California, Southern Division, because it is  
 28

1 the “district and division embracing the place where such action is pending.” 28  
2 U.S.C. § 1441(a); *see also id.* § 84(c)(3).

3       30.   **Notice To Plaintiff And State Court.** Promptly after the filing of this  
4 Notice, written notice of the filing will be given to Plaintiff, and a copy of the Notice,  
5 including exhibits, will be filed in the Superior Court of the State of California,  
6 County of Orange, as required by 28 U.S.C. § 1446(d).

7  
8 Dated: December 23, 2021

Respectfully submitted,  
MAYER BROWN LLP

11 By: /s/ John Nadolenco  
John Nadolenco

12  
13 *Attorneys for Defendants*  
14 *Smile Brands, Inc. and Sahawneh Dental*  
15 *Corporation*  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 MAYER BROWN LLP  
2 JOHN NADOLENCO (SBN 181128)  
3 jnadolenco@mayerbrown.com  
4 DOUGLAS A. SMITH (SBN 290598)  
5 dougsmith@mayerbrown.com  
350 S. Grand Ave., 25th Floor  
Los Angeles, CA 90071-1503  
Telephone: (213) 229-9500  
Facsimile: (213) 625-0248

6 DAVID SIMON (*pro hac vice* to be filed)  
7 dsimon@mayerbrown.com  
1999 K Street, NW  
Washington, DC 20006-1101  
8 Telephone: (202) 263-3388  
9 Facsimile: (202) 264-3300

10 SAMANTHA A. MACHOCK (SBN 298852)  
11 smachock@mayerbrown.com  
Two Palo Alto Square  
3000 El Camino Real  
Palo Alto, CA 94306-2112  
12 Telephone: (650) 331-2087  
13 Facsimile: (650) 331-2060

*Attorneys for Defendants  
Smile Brands Inc. and Sahawneh Dental  
Corporation*

16 **UNITED STATES DISTRICT COURT**  
17 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

19 ANGELICA PONCE, individually, and  
20 on behalf of all others similarly situated,

21 Plaintiff,

22 v.

23 SMILE BRANDS INC.; SAHAWNEH  
24 DENTAL CORPORATION; and DOES  
1-50, inclusive,

25 Defendants.

Case No. 8:21-cv-2115

**DECLARATION OF DOUGLAS A.  
SMITH IN SUPPORT OF ALL  
DEFENDANTS' NOTICE OF  
REMOVAL UNDER 28 U.S.C.  
§§ 1441(a) AND 1453**



**DECLARATION OF DOUGLAS A SMITH**


I, Douglas A. Smith, declare as follows:

1. I am licensed to practice law in the State of California. I am Counsel in the law firm of Mayer Brown LLP and counsel of record for Defendants Smile Brands Inc. (“SBI”) and Sahawneh Dental Corporation (“Defendants”). I submit this declaration in support of Defendants’ Notice of Removal Pursuant to 28 U.S.C. §§ 1441(a) and 1453. I have knowledge of the facts set forth herein, and if called to testify as a witness thereto, I could and would completely do so under oath.

2. Attached as **Exhibit 1** is a true and correct copy of all process, pleadings, and orders served to date on Defendants in *Ponce v. Smile Brands, Inc.*, Case No. 30-2021-01232683-CU-NP-CXC, pending in the California Superior Court for the County of Orange.

I declare under penalty of perjury under the laws of the United States of America that the forgoing is true and correct.

Executed on December 23, 2021, in Los Angeles, California.

  
\_\_\_\_\_  
Douglas A Smith

# Exhibit 1

## Case Summary:

Case Id:	30-2021-01232683-CU-NP-CXC
Case Title:	ANGELICA PONCE VS. SMILE BRANDS INC.
Case Type:	NON-PI/PD/WD TORT - OTHER
Filing Date:	11/18/2021
Category:	CIVIL - UNLIMITED

## Register Of Actions:

ROA	Docket	Filing Date	Filing Party	Document	Select
1	E-FILING TRANSACTION 31088362 RECEIVED ON 11/18/2021 10:31:54 PM.	11/23/2021		NV	
2	COMPLAINT FILED BY PONCE, ANGELICA ON 11/18/2021	11/18/2021		30 pages	<input type="checkbox"/>
3	CIVIL CASE COVER SHEET FILED BY PONCE, ANGELICA ON 11/18/2021	11/18/2021		2 pages	<input type="checkbox"/>
4	SUMMONS ISSUED AND FILED FILED BY PONCE, ANGELICA ON 11/18/2021	11/18/2021		1 pages	<input type="checkbox"/>
5	PAYMENT RECEIVED BY ONELEGAL FOR 194 - COMPLAINT OR OTHER 1ST PAPER, 34 - COMPLEX CASE FEE - PLAINTIFF IN THE AMOUNT OF 1,435.00, TRANSACTION NUMBER 12974341 AND RECEIPT NUMBER 12802258.	11/23/2021		1 pages	<input type="checkbox"/>
6	CASE ASSIGNED TO JUDICIAL OFFICER SHERMAN, RANDALL ON 11/18/2021.	11/18/2021		NV	
7	CASE MANAGEMENT CONFERENCE SCHEDULED FOR 04/22/2022 AT 09:00:00 AM IN CX105 AT CIVIL COMPLEX CENTER.	12/21/2021		NV	
8	THE CASE MANAGEMENT CONFERENCE IS SCHEDULED FOR 04/22/2022 AT 09:00 AM IN DEPARTMENT CX105.	12/21/2021		NV	
9	MINUTES FINALIZED FOR CHAMBERS WORK 12/21/2021 11:29:00 AM.	12/21/2021		1 pages	<input type="checkbox"/>
10	CLERK'S CERTIFICATE OF MAILING/ELECTRONIC SERVICE	12/21/2021		2 pages	<input type="checkbox"/>

## Participants:

Name	Type	Assoc	Start Date	End Date
ANGELICA PONCE	PLAINTIFF		11/23/2021	
KAZEROUNI LAW GROUP, APC	ATTORNEY		11/23/2021	
SAHAWNEH DENTAL CORPORATION	DEFENDANT		11/23/2021	
SMILE BRANDS INC.	DEFENDANT		11/23/2021	

## Hearings:

Description	Date	Time	Department	Judge
CASE MANAGEMENT CONFERENCE	04/22/2022	09:00	CX105	SHERMAN

Print this page

SUM-100

# SUMMONS

## (CITACION JUDICIAL)

FOR COURT USE ONLY  
(SOLO PARA USO DE LA CORTE)

### NOTICE TO DEFENDANT: (AVISO AL DEMANDADO):

SMILE BRANDS INC.; SAHAWNEH DENTAL CORPORATION; and DOES 1-50, inclusive

### YOU ARE BEING SUED BY PLAINTIFF: (LO ESTÁ DEMANDANDO EL DEMANDANTE):

ANGELICA PONCE, individually, and on behalf of all others similarly situated

**NOTICE!** You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), or by contacting your local court or county bar association. NOTE: The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case. ¡AVISO! Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), en el Centro de Ayuda de las Cortes de California, ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de \$10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:

(El nombre y dirección de la corte es):

Superior Court of California, County of Orange - Civil Complex Center  
751 W. Santa Ana Blvd., Santa Ana, CA 92701

CASE NUMBER: (Número del Caso):

30-2021-01232683-CU-NP-CXC

Judge Randall J. Sherman

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is: (El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):

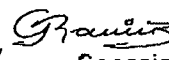
Abbas Kazerounian - KAZEROUNI LAW GROUP, APC - 245 Fischer Ave., D1, Costa Mesa, CA 92626 - Tel: (800) 400-6808

DATE: 11/18/2021

DAVID H. YAMASAKI, Clerk of the Court

Clerk, by

(Secretario,



Deputy

(Adjunto)

Georgina Ramirez

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)

(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons, (POS-010)).

[SEAL]

**NOTICE TO THE PERSON SERVED: You are served**

1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of (specify):
3. ☐ on behalf of (specify):  
under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)  
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)  
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)  
☐ other (specify):
4. ☐ by personal delivery on (date):

Page 1 of 1

**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

Assigned for all Purposes  
 Judge Randall J. Sherman  
 CX-105

*Attorneys for Plaintiff,  
 Angelica Ponce and the proposed Class*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
 FOR THE COUNTY OF ORANGE – CIVIL COMPLEX**

ANGELICA PONCE, individually, and on behalf  
 of all others similarly situated,

Plaintiff,

vs.

SMILE BRANDS INC.; SAHAWNEH DENTAL  
 CORPORATION; and DOES 1-50, inclusive,

Defendants.

Case No.: 30-2021-01232683-CU-NP-CXC

CLASS ACTION COMPLAINT FOR  
 VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY  
 ACT OF 2018, CAL. CIV. CODE §§  
 1798.100, *et seq.*;
2. CALIFORNIA CONFIDENTIALITY OF  
 MEDICAL INFORMATION ACT, CAL.  
 CIV. CODE §§ 56, *et seq.*;
3. CALIFORNIA UNFAIR COMPETITION  
 LAW, CAL. BUS. & PROF. CODE  
 §§ 17200, *et seq.*; and
4. BREACH OF CONTRACT

JURY TRIAL DEMANDED

Plaintiff ANGELICA PONCE (“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, bring this class action against Defendants SMILE BRANDS INC. (“Smile Brands”), SAHAWNEH DENTAL CORPORATION (“Sahawneh Dental”), and DOES 1-50, inclusive (collectively “Defendants”), and alleges as follows:

**NATURE OF THE CASE**

1. This is a data breach class action arising out of Defendants' failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information. Smile Brands is one of the largest dental service organizations in the United States and Defendant Sahawneh Dental is one its affiliate dental offices. Smile Brands has over 700 affiliated dental offices and provides comprehensive business support services through exclusive long term agreements with affiliate dental groups like Sahawneh Dental and hundreds of other dental offices.<sup>1</sup> For its business purposes, Defendants obtain, store, and transmit personally identifiable information ("PII") and protected health information ("PHI") from individuals like Plaintiff, including but not limited to names, addresses, dates of birth, Social Security numbers, personal financial information, government-issued identification numbers, and personal health information.

2. On April 24, 2021, Defendants became of aware of a ransomware attack, which led to unauthorized access of Defendants' systems containing PII and PHI (the "Data Breach"). Defendants determined that the information involved included Plaintiff and other similarly situated Class members' names, addresses, telephone numbers, dates of birth, Social Security numbers, personal financial information, government-issued identification number and/or personal health information. However, Defendants only provided notice to Plaintiff and its other Class members of the Data Breach on or around September 28, 2021.

3. Although Defendants knew about the Data Breach and that sensitive information was in the hands of malicious actors, it waited until September 28, 2021, to send certain individuals letters regarding the Data Breach. Defendants' notice to individuals like Plaintiff and the Class members was misleading and inadequate as the notice did not explain the two-month delay between discovering the breach and notifying affected individuals.

4. The Data Breach happened as a result of Defendants' inadequate cybersecurity, which caused Plaintiff and the Class members' PII/PHI to be accessed, exfiltrated, and disclosed to

<sup>1</sup> <https://smilebrands.com/about-us/>



1 unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on behalf  
2 of herself and all affected California and U.S. residents.

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

5 **VENUE AND JURISDICTION**

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

9 7. This Court has personal jurisdiction over Defendants because Defendants regularly  
10 conducts business in California and are headquartered in the City of Irvine in Orange County,  
11 California.

12 8. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5  
13 because Defendants regularly conducts business in the State of California, Defendants are both  
14 headquartered in the City of Irvine in Orange County, California; and the unlawful acts or omissions  
15 giving rise to this action also occurred or arose in this county.

16 **PARTIES**

17 9. At all relevant times, Plaintiff Angelica Ponce resided in the State of California.

18 10. At all relevant times, Defendants conducted business in the State of California and  
19 maintained offices within the City of Irvine in Orange County, California.

20 11. Defendant Smile Brands is a corporation formed under the laws of the State of  
21 Washington and is headquartered at 100 Spectrum Center Drive, Suite 1500, Irvine, CA 92618.

22 12. Defendant Sahawneh Dental is a corporation formed under the laws of the State of  
23 California and is headquartered at 100 Spectrum Center Drive, Suite 1500, Irvine, CA 92618.

24 13. Plaintiff provided her PII/PHI to Defendants as part of financing their dental services,  
25 including Plaintiff's name, addresses, telephone numbers, date of birth, Social Security number,  
26 personal financial information, government-issued identification number and personal health  
27 information. In September 2021, Plaintiff was notified that her PII/PHI was accessed and acquired by  
28 unauthorized individuals through the Data Breach.



1           14. Defendants sent Plaintiff a letter dated September 28, 2021 with the title, "Notice of  
2 Data Breach." The letter notified Plaintiff and similarly situated Class members that as a result of a  
3 "cybersecurity incident" a malicious actor had gained unauthorized access to Defendants' systems  
4 containing personal information and certain PII/PHI data was acquired by an unauthorized third party.  
5 Specifically, the data accessed and acquired by the unauthorized third party included Plaintiff and  
6 other similarly situated Class members' names, addresses, telephone numbers, dates of birth, Social  
7 Security numbers, personal financial information, government-issued identification number and/or  
8 personal health information. No details were provided regarding who stole the information or why  
9 there was a delay in notifying affected individuals.

10           15. As a result of Defendants' failure to implement and maintain reasonable security  
11 procedures and practices appropriate to the nature of the personal information it collected, maintained,  
12 and stored on its servers, network, and/or email system, Plaintiff and the Class members' PII/PHI was  
13 accessed, viewed, exfiltrated, stolen, acquired and/or otherwise disclosed to unauthorized persons in  
14 the Data Breach.

15           16. Plaintiff is unaware of the true names and capacities of the Defendant(s) sued herein  
16 as DOES 1 through 50, inclusive, and therefore sue these Defendants by such fictitious names  
17 pursuant to Cal. Civ. Proc. Code § 474. Plaintiff is informed and believes, and based thereon, alleges  
18 that Defendants designated herein are legally responsible in some manner for the unlawful acts and  
19 occurrences complained of herein, whether such acts were committed intentionally, negligently,  
20 recklessly, or otherwise, and Defendants thereby proximately caused the injuries and damages to  
21 Plaintiff and the Class members as herein alleged. Plaintiff will seek leave of Court to amend this  
22 complaint to reflect the true names and capacities of Defendant(s) when they have been ascertained  
23 and become known through further investigation and completion of discovery.

24           17. The agents, servants and/or employees of Defendants and each of them acting on  
25 behalf of Defendants acted within the course and scope of his, her or its authority as the agent, servant  
26 and/or employee of Defendants, and personally participated in the conduct alleged herein on behalf  
27 of Defendants with respect to the conduct alleged herein. Consequently, the acts of each Defendant  
28 are legally attributable to the other Defendants and all Defendants are jointly and severally liable to

1 Plaintiff and other similarly situated individuals, for the loss sustained as a proximate result of the  
2 conduct of the Defendants' agents, affiliates, servants, and/or employees.

### 3 FACTUAL ALLEGATIONS

#### 4 *PII/PHI Is a Valuable Property Right that Must Be Protected*

5 18. The California Constitution guarantees every Californian a right to privacy. PII/PHI is  
6 a recognized valuable property right.<sup>2</sup> California has repeatedly recognized this property right, most  
7 recently with the passage of the California Consumer Privacy Act of 2018.

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

10 Most consumers cannot begin to comprehend the types and amount of  
11 information collected by businesses, or why their information may be  
12 commercially valuable. Data is currency. The larger the data set, the greater  
13 potential for analysis – and profit.<sup>3</sup>

14 20. The value of PII as a commodity is measurable. "PII, which companies obtain at little  
15 cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional  
16 financial assets."<sup>4</sup> It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals  
17 often trade it on the "cyber black-market" for several years.

18 21. Companies recognize PII as an extremely valuable commodity akin to a form of  
19 personal property. For example, Symantec Corporation's Norton brand has created a software  
20 application that values a person's identity on the black market.<sup>5</sup>

21 22. As a result of its real value and the recent large-scale data breaches, identity thieves  
22 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive  
23 information directly on various illicit Internet websites making the information publicly available for  
24 other criminals to take and use. This information from various breaches, including the information

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

<sup>3</sup> 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>.

<sup>4</sup> See Soma, *Corporate Privacy Trend*, *supra*.

<sup>5</sup> Risk Assessment Tool, Norton 2010,  
[www.everyclickmatters.com/victim/assessmenttool.html](http://www.everyclickmatters.com/victim/assessmenttool.html).



1 exposed in the Data Breach, can be aggregated and become more valuable to thieves and more  
 2 damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and  
 3 other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard  
 4 filtering mechanism – the "Safe Browsing list."

5 23. PHI is particularly valuable. All-inclusive health insurance dossiers containing  
 6 sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social  
 7 Security numbers and bank account information, complete with account and routing numbers, can  
 8 fetch up to \$1,200 to \$1,300 each on the black market.<sup>6</sup> According to a report released by the Federal  
 9 Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times  
 10 the price of a stolen Social Security or credit card number.<sup>7</sup>

11 24. Recognizing the high value that consumers place on their PII/PHI, some companies  
 12 now offer consumers an opportunity to sell this information to advertisers and other third parties. The  
 13 idea is to give consumers more power and control over the type of information they share – and who  
 14 ultimately receives that information. By making the transaction transparent, consumers will make a  
 15 profit from the surrender of their PII/PHI.<sup>8</sup> This business has created a new market for the sale and  
 16 purchase of this valuable data.<sup>9</sup>

17 25. Consumers place a high value not only on their PII/PHI, but also on the privacy of that  
 18 data. Researchers shed light on how much consumers value their data privacy – and the amount is  
 19 considerable. Indeed, studies confirm that "when privacy information is made more salient and  
 20  
 21  
 22

23 <sup>6</sup> Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black*  
 24 *Market* (July 16, 2013), available at <https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/>.

25 <sup>7</sup> Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for*  
 26 *Increased Cyber Intrusions for Financial Gain* (April 8, 2014) available at  
<https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

27 <sup>8</sup> 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>.

28 <sup>9</sup> 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>.



1 accessible, some consumers are willing to pay a premium to purchase from privacy protective  
2 websites.”<sup>10</sup>

3 26. One study on website privacy determined that U.S. consumers valued the restriction  
4 of improper access to their PII between \$11.33 and \$16.58 per website.<sup>11</sup>

5 27. Given these facts, any company such as Defendants that transacts business with a  
6 consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer  
7 of the full monetary value of the consumer’s transaction with the company.

8 ***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

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

13 29. Theft or breach of PII/PHI is serious. The California Attorney General recognizes that  
14 “[f]oundational” to every Californian’s constitutional right to privacy is “information security: if  
15 companies collect consumers’ personal data, they have a duty to secure it. An organization cannot  
16 protect people’s privacy without being able to secure their data from unauthorized access.”<sup>12</sup>

17 30. The United States Government Accountability Office noted in a June 2007 report on  
18 Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts,  
19 open new financial accounts, receive government benefits and incur charges and credit in a person’s  
20 name.<sup>13</sup> As the GAO Report states, this type of identity theft is so harmful because it may take time  
21 for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

22 31. In addition, the GAO Report states that victims of identity theft will face “substantial  
23 costs and inconveniences repairing damage to their credit records ... [and their] good name.”

24  
25 <sup>10</sup> Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An*  
26 *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](https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents).

27 <sup>11</sup> 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>.

28 <sup>12</sup> California Data Breach Report, Kamala D. Harris, Attorney General, California Department  
of Justice, February 2016.

<sup>13</sup> See GAO, GAO Report 9 (2007), available at <http://www.gao.gov/new.items/d07737.pdf>.

1 According to the FTC, identity theft victims must spend countless hours and large amounts of money  
2 repairing the impact to their good name and credit record.<sup>14</sup>

3 32. Identity thieves use personal information for a variety of crimes, including credit card  
4 fraud, phone or utilities fraud, and bank/finance fraud.<sup>15</sup> According to Experian, “[t]he research shows  
5 that personal information is valuable to identity thieves, and if they can get access to it, they will use  
6 it” to among other things: open a new credit card or loan; change a billing address so the victim no  
7 longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad  
8 checks; use a debit card number to withdraw funds; obtain a new driver license or ID; use the victim’s  
9 information in the event of arrest or court action.<sup>16</sup>

10 33. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report,  
11 the average cost of a data breach per consumer was \$150 per record.<sup>17</sup> Other estimates have placed  
12 the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity  
13 theft – a common result of data breaches – was \$298 dollars.<sup>18</sup> And in 2019, Javelin Strategy &  
14 Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket  
15 cost to consumers for identity theft was \$375.<sup>19</sup>

16 34. The consequences can be even more serious when the hack includes taking PHI. Data  
17 breaches involving medical information “typically leave[] a trail of falsified information in medical  
18

19  
20 <sup>14</sup> See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

21 <sup>15</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying  
22 information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying  
23 information” as “any name or number that may be used, alone or in conjunction with any other  
24 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.*

25 <sup>16</sup> See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How  
Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at  
26 [https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-](https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/)  
information-and-how-can-you-protect-yourself/.

27 <sup>17</sup> Brook, *What’s the Cost of a Data Breach in 2019*, *supra*.

28 <sup>18</sup> Norton By Symantec, 2013 Norton Report 8 (2013), available at  
[https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf).

<sup>19</sup> 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).



records that can plague victims' medical and financial lives for years."<sup>20</sup> It "is also more difficult to detect, taking almost twice as long as normal identity theft."<sup>21</sup> "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."<sup>22</sup>

35. Further, medical data is more valuable than other commonly available personal data. "While a stolen credit card number might be sold for just a few cents, medical files can be worth as much as \$1,000 each" or more.<sup>23</sup>

36. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just \$1 in 2016 – the same as a Facebook account.<sup>24</sup> That pales in comparison with the asking price for medical data, which was selling for \$50 and up.<sup>25</sup>

37. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

<sup>20</sup> Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), [https://www.ftc.gov/system/files/documents/public\\_comments/2018/01/00037-142815.pdf](https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf).

<sup>21</sup> See FBI CYBER DIVISION, (U) HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN 2 (2014), available at <https://publicintelligence.net/fbi-health-care-cyber-intrusions/> (FBI, April 8, 2014).

<sup>22</sup> See Federal Trade Commission, *Medical Identity Theft*, available at <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft>.

<sup>23</sup> Brian O'Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, Experian (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

<sup>24</sup> See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), available at: <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/> (last visited June 2, 2021).

<sup>25</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), available at: <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last visited June 2, 2021).



- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

38. A person whose PII/PHI 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.

39. 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.<sup>26</sup>

40. It is within this context that Plaintiff and hundreds of thousands<sup>27</sup> of individuals and/or patients who provided their PII/PHI to Defendants face imminent risk of identity theft and must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken, accessed, and viewed by unauthorized persons willing and able to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web or the black market.

<sup>26</sup> See Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), available at <https://blog.linkedin.com/2016/05/18/protecting-our-members>.

<sup>27</sup> Defendant Smile Brands reported to the U.S. Department of Health and Human Services that Defendants' Data Breach involved the unsecured protected health information of at least 199,683 individuals.

***Defendants' Businesses***

41. Defendant Smile Brands is one of the largest dental service organizations in the United States and Defendant Sahawneh Dental is one its affiliate dental offices. Smile Brands has over 700 affiliated dental offices and provides comprehensive business support services through exclusive long term agreements with affiliate dental groups like Sahawneh Dental and hundreds of other dental office

42. For its business and dental services purposes, Defendants obtain, store, and transmit PII/PHI from individuals like Plaintiff, including but not limited to individuals and patients' names, addresses, dates of birth, Social Security numbers, personal financial information, government-issued identification numbers, and personal health information of individuals and/or patients. When Plaintiff and similarly situated individuals provided PII/PHI to Defendants, Plaintiff reasonably believed that Defendants would keep their PII/PHI secure.

***Defendants' Collection of Individuals' PII/PHI***

43. Defendants acknowledge that they obtains, stores and transmits a substantial amount of personal, financial, and medical information from individuals and/or patients. The type of information is detailed in their Privacy Policy,<sup>28</sup> which states that Defendants collects the following categories of personal information and identifiers from individuals and/or patients:

- contact information (such as name, email address, mailing address, phone number), a username and password for our website, IP address (and general location), date of birth, and information in financing applications and patient forms (such as social security number, tax ID number, driver's license number, and signature), and other similar identifying information.

44. Defendants' Privacy Policy indicates the above personal information is collected from individuals such as Plaintiff and Class members "when [they] apply for financing, contact [Defendants], register and create a profile, use web chats to schedule an appointment, submit patient forms, use [Defendants'] websites, view [Defendants'] advertising or content on other websites (including social media sites), sign up for an email list, or apply for a job. [Defendants] also receive

<sup>28</sup> <https://smilebrands.com/terms-conditions/#privacy>



1 this information from vendors who collect it on [Defendants'] behalf. [Defendants] may receive this  
 2 information from a patient who lists [them] as an emergency contact or spouse in their pre-visit  
 3 paperwork or refers [Defendants] to [them], and [Defendants] occasionally purchase mailing lists  
 4 from other businesses."<sup>29</sup>

5 45. Defendants' Privacy Policy states "[t]his Privacy Policy applies to all patients and  
 6 users of Smile Brands and all of our affiliated practices," and Sahawneh Dental is one of over the 700  
 7 such affiliated dental practices.

8 46. Defendants' Privacy Policy further indicates the purpose of collecting this information  
 9 is to "operate our business and our website; help you locate an office or practice near you; review  
 10 credit applications; intake new patients; provide customer service; improve our services; perform  
 11 research and business analytics; verify requests made pursuant to this Privacy Policy; protect our  
 12 business and our patients against illegal activity; and to tailor and send you marketing  
 13 communications for ourselves and for selected third parties. We may use this information for other  
 14 similar purposes related to the operation of our business, or as we may notify you from time to time."<sup>30</sup>

15 47. For Californians, Defendants' Privacy Policy identifies the rights of California  
 16 residents regarding their personal information pursuant to the California Consumer Privacy Act  
 17 ("CCPA"). These rights include requesting disclosure of the information collected, the purpose for  
 18 collecting the information, and any third parties with whom the information is sold or disclosed.  
 19 Additionally, the rights under the CCPA identified by Defendants' Privacy Policy include requesting  
 20 deletion of the personal information, and opting out of have personal information sold to third parties.

21 ***Defendants' Promises to Safeguard PII/PHI***

22 48. Defendants promise that they "recognize [Plaintiff and the Class members'] right to  
 23 confidentiality and is committed to protecting [their] privacy."<sup>31</sup>

24 49. Defendants claim that they "are dedicated to doing our best to protect [Plaintiff and  
 25 the Class members'] personal information."<sup>32</sup>

26  
 27 <sup>29</sup> <https://smilebrands.com/terms-conditions/#privacy>

28 <sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*



50. Defendants warns that “the Internet is not 100% secure, and technology is no substitute for common sense” and encourages users to “keep their login names and passwords secret” and “communicate over secure channels wherever possible, disable the automatic login features found in some browsers, and empty their browser caches regularly.”<sup>33</sup>

51. Defendants’ Terms and Conditions expressly references and incorporates Defendants’ Privacy Policy.

***The Data Breach and Defendants’ Notice of Data Breach***

52. On or around September 28, 2021, Defendants sent Plaintiff and other similarly situated Class members a letter with the title, “Notice of Data Breach.” The letter states that Defendants “write to inform you of a cybersecurity incident that may have involved your personal information” and “to explain the circumstances of the incident, the types of information involved, what we are doing and have done in response to the breach, and steps that can be taken to help protect your information.”

53. The letter goes on to state that on April 24, 2021, Defendants “became aware of a ransomware attack, which led to unauthorized access to certain systems containing personal information.” Further, the letter states that on “certain data appears to have been acquired by an unauthorized third party.”

54. According to Defendants, the information involved in the Data Breach included Plaintiff’s “name, address, telephone number, date of birth, Social Security number, personal financial information, government-issued identification number, and/or personal health information.”

55. Defendants also claimed to have promptly launched an investigation, notified law enforcement, and engaged leading cybersecurity firms to help assess the scope of the incident. However, no details regarding the timing or completion of the investigation or the scope of the Data Breach were provided.

56. Defendants offered Plaintiff and the Class members complimentary identity theft protection through Experian IdentityWorks<sup>SM</sup> for one (1) year.

---

<sup>33</sup> *Id.*



57. For California residents, the letter does not identify the rights of consumers under CCPA and instead says to “[v]isit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.”

58. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must be sent to residents of California “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person” due to a “breach of the security of the system[.]” Thus, Defendants reported the Data Breach to the U.S. Department of Health and Human Services and filed and disseminated its breach notification letter because Plaintiff and the Class members’ unencrypted PII/PHI was accessed and viewed by an unauthorized person or persons as a result of the Data Breach.

59. Plaintiff and the Class members’ PII/PHI is “personal information” as defined by California Civ. Code § 1798.82(h).

60. California Civ. Code § 1798.82(g) defines “breach of the security of the system” as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”

61. The Data Breach was a “breach of the security of the system” as defined by California Civ. Code § 1798.82(g).

62. Defendants’ Notice of the Data Breach letter sent to Plaintiff and other putative Class members is inadequate and fails to provide sufficient detail. Defendants state only that it had “became aware of a ransomware attack, which led to unauthorized access to certain systems containing personal information” on April 24, 2021 and “certain data appears to have been acquired by an unauthorized third party.”

63. Defendants’ vague description of the Data Breach leaves Plaintiff and Class members at continuing risk. By failing to adequately inform Plaintiff and Class members of the details surrounding the breach Plaintiff and Class members are unable to adequately protect themselves against the imminent and continued risk of identity theft and other damages.

64. Further, Defendants offered Plaintiff and Class members little to assist them with any fall-out from the Data Breach or to advise them of the extent of the potential threat they face as a



1 result of their sensitive PII/PHI being in the hands of criminals. Defendants' offer of a one (1) year  
 2 subscription to the Experian IdentityWorks<sup>SM</sup> identity theft protection program is insufficient where  
 3 Plaintiff and Class members are now at increased risk of identity theft for years to come as a result of  
 4 the Data Breach.

5 65. Defendants also fail to explain why they waited over five (5) months to notify Plaintiff  
 6 and Class members about the Data Breach. This delayed Plaintiff and Class members' ability to take  
 7 necessary precautions to protect themselves from identity theft and other fraud.

8 ***Defendants Knew or Should Have Known PII/PHI Are High Risk Targets***

9 66. Defendants knew or should have known that PII and PHI like the information obtained,  
 10 maintained and stored on Defendants' systems are a high risk target for identity thieves.

11 67. The Identity Theft Resource Center reported that the business sector had the largest  
 12 number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing  
 13 at least 415,233,143 million records in 2018.<sup>34</sup> Further, the ITRC identified "hacking" as the most  
 14 common form of data breach in 2018, accounting for 39% of data breaches.

15 68. Over the past years, phishing and ransomware have become the most rampant form of  
 16 cybercrime and an exponentially increasing threat to organizations such as Defendants. The vast  
 17 majority of organizations have been targeted by phishing or ransomware. Ransomware, a form of  
 18 malware designed for the sole purpose of extorting money from victims; and phishing, the delivery  
 19 mechanism of choice for ransomware and other malware, are critical problems and an evolving threat  
 20 that every organization must be prepared to face and address.

21 69. Companies are increasingly being targeted with phishing attacks. A phishing attack is  
 22 a method of infiltrating for the purpose of removing data for the purpose of viewing and using it to  
 23 commit acts such as identity theft and otherwise wrongfully obtaining money or other things of value.  
 24 Sometimes the person who engaged in phishing uses the data obtained to commit cyber fraud and

25  
 26  
 27  
 28 <sup>34</sup> 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](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf).



1 sometimes the person sells the data to other identity thieves. Either way, the information must be  
2 viewed to be of any use or to confirm the contents of the data before being sold.

3 70. Phishing is a cybercrime in which a target or targets are contacted by email, telephone  
4 or text message by someone posing as a legitimate person or entity so that the recipient provides  
5 sensitive data. The hacker cannot do it by him or herself. A phishing incident requires the email  
6 system to allow the phishing email to reach the email recipient, for the email recipient to click on a  
7 link, provide login credentials, download a file, or take similar affirmative action to allow the hacker  
8 to compromise the email recipient's system. The information is then used to access important  
9 accounts such as Plaintiff and Class members' PII/PHI.

10 71. Phishing does not just happen. To be successful, phishing relies on a series of  
11 affirmative acts by a company and its employees. This is because computers must be told what to do;  
12 they do not make independent decisions. Rather, they rely on instructions and actions from users and  
13 programmers. A successful phishing attack also requires an intentional affirmative act on the part of,  
14 for example, a company employee, such as clicking a link, downloading a file, or providing sensitive  
15 information.

16 72. Phishing attempts are extremely common. According to the Anti-Phishing Working  
17 Group's ("APWG") Phishing Activity Trends Report for Q2 2020, the first half of the year saw  
18 146,994 reported phishing attacks.<sup>35</sup> Verizon's 2020 Data Breach Investigation Report found that  
19 phishing is one of the top data breach threats, with 22 percent of data breaches involving phishing.

20 73. Phishing is one way identity thieves, scammers and fraudsters steal information.  
21 Comparitech explains the goal of phishing is to trick victims into divulging confidential or personal  
22 information that can then be used for fraudulent purposes, like identity theft.<sup>36</sup> The HIPAA Journal  
23 explains that phishing attacks on the healthcare industry typically have one of two objectives – to  
24 obtain access to PHI or to deliver ransomware. PHI is a valuable commodity on the black market  
25 because it can be used to create false identities, obtain free medical treatment, and commit insurance  
26

27 <sup>35</sup> [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q2\\_2020.pdf](https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf).

28 <sup>36</sup> <https://www.comparitech.com/blog/information-security/common-phishing-scams-how-to-avoid/>.



1 fraud. Thus, the goal of phishing is to obtain and use compromised data so that it may be used to  
2 commit fraud.<sup>37</sup>

3 74. The APWG describes phishing as a crime employing both social engineering and  
4 technical subterfuge to steal personal identity data and account credentials. Social engineering  
5 schemes prey on unwary victims by fooling them into believing they are dealing with a trusted,  
6 legitimate party, such as by using deceptive email addresses and email messages. Phishing schemes  
7 are designed to lead victims to counterfeit websites that trick recipients into divulging personal data  
8 such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to  
9 steal credentials directly, often using systems that intercept victims' account usernames and  
10 passwords or misdirect victims to counterfeit websites.

11 75. The HIPAA Journal describes that most phishing attacks on the healthcare industry  
12 are deployed by email. The communications generally look authentic and instruct employees to  
13 follow a link to a web page – where they will be asked to complete some action that will trigger a  
14 malware download or enter their username and password to continue. In addition to ransomware, the  
15 malware may be in the form of surveillance software such as adware and keystroke loggers that can  
16 be downloaded to follow an employee's online activities and record their usernames and passwords.  
17 Other types of malicious software can be downloaded to create gateways for hackers to enter an  
18 organization's network remotely. If the phishing attempt has been successful in obtaining a username  
19 and password, the hacker will likely be able to access PHI almost immediately.<sup>38</sup>

20 76. Phishing attacks are successful when a company has not employed adequate security  
21 procedures such as (1) training employees on how to recognize and report phishing attacks and  
22 conducting mock phishing scenarios; (2) deploying spam filters that can be enabled to recognize and  
23 prevent emails from suspicious sources from ever reaching the inbox of employees; (3) keeping all  
24 systems current with the latest security patches and updates; (4) installing antivirus solutions and  
25 monitoring the antivirus status on all equipment; (5) developing a security policy that includes  
26 password expiration and complexity and using two factor authentication to prevent hackers who have

27  
28 <sup>37</sup> <https://www.hipaajournal.com/protect-healthcare-data-from-phishing/>.  
<sup>38</sup> *Id.*



1 compromised a user's credentials from ever gaining access; (6) encrypting all sensitive company  
 2 information; (7) using only well-configured devices and employing good end point defenses that can  
 3 stop malware from installing, even if a phishing email is clicked; and (8) implementing policies and  
 4 procedures for responding quickly to incidents.

5 77. Defendants negligently left their computer systems open to attack. Thus, once the  
 6 unauthorized user gained access to Defendants' systems, the contents of those systems (including  
 7 Plaintiff and Class members' PHI/PII) were available for the unauthorized person(s) to access, view,  
 8 acquire and exfiltrate for their nefarious use.

9 78. Prior to the Data Breach, there were many reports of high-profile data breaches that  
 10 should have put a company like Defendants on high alert and forced it to closely examine its own  
 11 security procedures, as well as those of third parties with which it did business and gave access to  
 12 their subscriber PII/PHI.

13 79. In 2019, a record 1,473 data breaches occurred, resulting in approximately  
 14 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data  
 15 breaches, 525 of them, or 35.64%, were in the medical or healthcare industry. The 525 reported  
 16 breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only  
 17 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

18 80. In light of recent high profile data breaches at other healthcare partner and provider  
 19 companies, including, American Medical Collection Agency (25 million patients, March 2019)  
 20 University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute  
 21 (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018),  
 22 Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians  
 23 (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System  
 24 (286,876 patients, March 2020), Defendants knew or should have known that its electronic records  
 25 would be targeted by cybercriminals.

26 81. As such, Defendants were and should have been aware that PII/PHI is at high risk of  
 27 theft, and consequently should have but did not take appropriate and standard measures to protect  
 28

1 Plaintiff and Class members' PII/PHI against cyber-security attacks that Defendants should have  
2 anticipated and guarded against, including phishing or ransomware.

3 **CLASS DEFINITION AND ALLEGATIONS**

4 82. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seek to  
5 represent and intend to certify the following class:

6 All individuals whose PII and/or PHI was compromised in the Data Breach  
7 disclosed by Defendants in their Notice of Data Breach letter(s) (the  
8 "Class").

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

14 84. Certification of Plaintiff's claims for classwide treatment is appropriate because  
15 Plaintiff can prove the elements of Plaintiff's claims on a classwide basis using the same evidence as  
16 would be used to prove those elements in individual actions alleging the same claims.

17 85. The Class members are so numerous and geographically dispersed throughout the  
18 United States and California that joinder of all Class members would be impracticable. While the  
19 exact number of class members is unknown, Defendants acknowledges the Data Breach, and reports  
20 estimate the breach to include nearly 200,000 individuals, including Plaintiff and Class members.  
21 Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

22 86. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed  
23 members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members  
24 were injured by the same wrongful acts, practices, and omissions committed by Defendants, as  
25 described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that  
26 give rise to the claims of all Class members.  
27  
28



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

- 4           (a) Whether Defendants had a duty to implement and maintain reasonable security  
5 procedures and practices appropriate to the nature of the PII/PHI it collected  
6 from Plaintiff and Class members;  
7           (b) Whether Defendants breached their duty to protect the PII/PHI of Plaintiff and  
8 each Class members;  
9           (c) Whether Defendants violated the statutes alleged herein; and  
10           (d) Whether Plaintiff and each Class member are entitled to damages and other  
11 equitable relief.

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

16           89. A class action is superior to any other available method for the fair and efficient  
17 adjudication of this controversy since individual joinder of all Class members is impractical.  
18 Furthermore, the expenses and burden of individual litigation would make it difficult or impossible  
19 for the individual members of the Class to redress the wrongs done to them, especially given that the  
20 damages or injuries suffered by each individual member of the Class are outweighed by the costs of  
21 suit. Even if the Class members could afford individualized litigation, the cost to the court system  
22 would be substantial and individual actions would also present the potential for inconsistent or  
23 contradictory judgments. By contrast, a class action presents fewer management difficulties and  
24 provides the benefits of single adjudication and comprehensive supervision by a single court.

25           90. Defendants have acted or refused to act on grounds generally applicable to the entire  
26 Class, thereby making it appropriate for this Court to grant final injunctive, including public  
27 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.*)**

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

92. 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 and disclosure. The California Legislature explained: “The unauthorized disclosure of personal information and the loss of privacy can have devastating 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.”<sup>39</sup>

93. 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. Defendants failed to implement such procedures which resulted in the Data Breach.

94. 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.” Cal. Civ. Code § 1798.81.5(c).

95. 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

---

<sup>39</sup> California Consumer Privacy Act (CCPA) Compliance, <https://buyergenomics.com/ccpa-compliance/>.



1 and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and  
 2 maintain reasonable security procedures and practices appropriate to the nature of the information to  
 3 protect the personal information may institute a civil action for" statutory or actual damages,  
 4 injunctive or declaratory relief, and any other relief the court deems proper.

5 96. Plaintiff and the Class members are "consumer[s]" as defined by Civ. Code  
 6 § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in  
 7 Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1,  
 8 2017."

9 97. Defendants are a "business" as defined by Civ. Code § 1798.140(c) because  
 10 Defendants are:

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

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

17 c. do business in California; and

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

23 98. The PII/PHI taken in the Data Breach is personal information as defined by Civil Code  
 24 § 1798.81.5(d)(1)(A) because it contains Plaintiff and the Class members' unencrypted names, Social  
 25 Security numbers, personal financial information, government-issued identification number, and  
 26 personal healthcare information, among other information.

27 99. Plaintiff and the putative Class members' PII was subject to unauthorized access and  
 28 exfiltration, theft, or disclosure because their PII/PHI, including names, Social Security numbers,



1 personal financial information, government-issued identification number, and personal healthcare  
2 information, among other information were wrongfully taken, accessed, viewed, and acquired by  
3 unauthorized third parties.

4 100. The Data Breach occurred as a result of Defendants' failure to implement and maintain  
5 reasonable security procedures and practices appropriate to the nature of the information to protect  
6 Plaintiff and the Class members' PII/PHI. Defendants failed to implement reasonable security  
7 procedures to prevent an attack on its server or network, including its email system, by hackers and  
8 to prevent unauthorized access of Plaintiff and the Class members' PII/PHI as a result of this attack.

9 101. On November 18, 2021, Plaintiff provided Defendants with written notice of their  
10 violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1) which she alleges Defendants have  
11 violated. In the event Defendants have not cured the violation within 30 days thereof, Plaintiff intends  
12 to amend the complaint to also pursue the greater of statutory damages in an amount not less than one  
13 hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident,  
14 or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

15 102. As a result of Defendants' failure to implement and maintain reasonable security  
16 procedures and practices that resulted in the Data Breach, Plaintiff seeks, injunctive relief, including  
17 public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

18 **SECOND CAUSE OF ACTION**  
19 **Violation of the California Confidentiality of Medical Information Act ("CMIA")**  
20 **(Cal. Civ. Code §§ 56, *et seq.*)**

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

23 104. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care,  
24 health care service plan, or contractor shall not disclose medical information regarding a patient of  
25 the provider of health care or an enrollee or subscriber of a health care service plan without first  
26 obtaining an authorization[.]"

27 105. Defendants are a "contractor" within the meaning of Civil Code § 56.05(d) and/or a  
28 "provider of healthcare" within the meaning of Civil Code § 56.06 and/or a "business organized for  
the purpose of maintaining medical information" and/or a "business that offers software or hardware



1 to consumers . . . that is designed to maintain medical information” within the meaning of Civil Code  
 2 § 56.06(a) and (b), and maintained and continues to maintain “medical information,” within the  
 3 meaning of Civil Code § 56.05(j), for “patients” of Defendant, within the meaning of Civil Code  
 4 § 56.05(k).

5 106. Plaintiff and all members of the Class are “patients” within the meaning of Civil Code  
 6 § 56.05(k) and are “endanger[ed]” within the meaning of Civil Code § 56.05(e) because Plaintiff and  
 7 the Class fear that disclosure of their medical information could subject them to harassment or abuse.

8 107. Plaintiff and the respective Class members, as patients, had their individually  
 9 identifiable “medical information,” within the meaning of Civil Code § 56.05(j), created, maintained,  
 10 preserved, and stored on Defendants’ systems at the time of the Data Breach.

11 108. Defendants, through inadequate security, allowed unauthorized third-party access to  
 12 Plaintiff and the Class members’ medical information, without the prior written authorization of  
 13 Plaintiff and the Class members, as required by Civil Code § 56.10 of the CMIA.

14 109. In violation of Civil Code § 56.10(a), Defendants disclosed Plaintiff and the Class  
 15 members’ medical information without first obtaining an authorization. Plaintiff and the Class  
 16 members’ medical information was accessed, viewed, and acquired by unauthorized individuals as a  
 17 direct and proximate result of Defendants’ violations of Civil Code § 56.10(a).

18 110. Defendants violated Civil Code § 56.101 of the CMIA through its failure to maintain  
 19 and preserve the confidentiality of the medical information of Plaintiff and the Class members.

20 111. In violation of Civil Code § 56.101(a), Defendants created, maintained, preserved,  
 21 stored, abandoned, destroyed, or disposed of Plaintiff and the Class members’ medical information  
 22 in a manner that failed to preserve and breached the confidentiality of the information contained  
 23 therein. Plaintiff and the Class members’ medical information was viewed by unauthorized  
 24 individuals as a direct and proximate result of Defendants’ violation of Civil Code § 56.101(a).

25 112. In violation of Civil Code § 56.101(a), Defendants negligently created, maintained,  
 26 preserved, stored, abandoned, destroyed, or disposed of Plaintiff and the Class members’ medical  
 27 information. Plaintiff and the Class members’ medical information was viewed by unauthorized  
 28 individuals as a direct and proximate result of Defendants’ violations of Civil Code § 56.101(a).



113. Plaintiff and the Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

114. In violation of Civil Code § 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violations of Civil Code § 56.101(b)(1)(A).

115. Defendants violated Civil Code § 56.36 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class members.

116. As a result of Defendants' above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

117. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the 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, identity fraud and medical 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/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

118. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages

of up to \$3,000 per Plaintiff and each Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

**THIRD CAUSE OF ACTION**  
**Violation of the California Unfair Competition Law ("UCL")**  
**(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)**

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

120. 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, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

121. In the course of conducting its business, Defendants 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 and Class members' PII/PHI, and by violating the statutory and common law alleged herein, including, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56.10(a), (e); 56.101(a), 56.101(b)(1)(A); 56.36), the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.150(a)(1)), the Health Insurance Portability and Accountability Act of 1996, (42 U.S.C. § 1302d; 45 C.F.R. §§ 164.306(a), (d), (e); 164.308(a); 164.312(a), (d), (e); 164.316(a), (b)), Civil Code § 1798.81.5, and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

122. Defendants also violated the UCL's unlawful prong by breaching contractual obligations created by its Privacy Policy and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial



1 website operator from “knowingly and willfully” or “negligently and materially” failing to comply  
2 with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact  
3 and lost money or property as a result of Defendants’ violations of its Privacy Policy.

4 123. Defendants also violated the UCL by failing to adequately and timely notify Plaintiff  
5 and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and  
6 disclosure of their PII/PHI. If Plaintiff and Class members had been adequately and timely notified  
7 in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI  
8 and identities.

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

20 125. Plaintiff and Class members suffered injury in fact and lost money or property as a  
21 result of Defendants’ violations of its Privacy Policy and statutory and common law in that a portion  
22 of the money Plaintiff and Class members paid for Defendants’ services went to fulfill the contractual  
23 obligations set forth in its Privacy Policy, including maintaining the security of their PII/PHI, and  
24 Defendants’ legal obligations and Defendants failed to fulfill those obligations.

25 126. The UCL also prohibits any “fraudulent business act or practice.” Defendants’ above-  
26 described claims, nondisclosures and misleading statements were false, misleading and likely to  
27 deceive the consuming public in violation of the UCL.



127. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendants' unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII/PHI but receiving a lower level, paying more for Defendants' products and services than they otherwise would have had they known Defendants were not providing the reasonable security represented in its Privacy Policy and as in conformance with its legal obligations. Defendants' security practices have economic value in that reasonable security practices reduce the risk of theft of PII/PHI collected, maintained, and stored by Defendants.

128. 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 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/PHI, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII/PHI 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.

129. Unless restrained and enjoined, Defendants 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 seek restitution and an injunction, including public injunctive relief prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants 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/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

//

//

//



**FOURTH CAUSE OF ACTION**

**Breach of Contract**

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

131. Plaintiff and Class members entered into express contracts with Defendants as set forth in its Terms and Conditions and Privacy Policy that included Defendants' promise to protect personal information given to Defendants or that Defendants gathered on their own, from disclosure, as set forth in Defendants' Privacy Policy, which was posted on its website.

132. Plaintiff and Class members performed their obligations under the contracts when they provided their PII/PHI to Defendants in relation to their purchase of insurance products or services from Defendant.

133. By allowing unauthorized users to gain access to Plaintiff and Class members' PII/PHI through the Data Breach, Defendants breached these contractual obligations. As a result, Defendants failed to comply with its own policies, including its Privacy Policy, and applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII/PHI. Defendants' 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.

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

135. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of herself individually and all members of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the certified class(es), and (iii) Plaintiff's undersigned counsel be appointed as Class

Counsel. Plaintiff, on behalf of herself and members of the Class further requests that upon final trial or hearing, judgment be awarded against each and all of the Defendants for:

- (i) actual and punitive damages to be determined by the trier of fact;
- (ii) statutory damages;
- (iii) equitable relief, including restitution;
- (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- and post-judgment interest at the highest legal rates applicable; and
- (viii) any such other and further relief the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of herself individually and the putative Class, hereby demands a jury trial on all issues so triable.

Dated: November 18, 2021

Respectfully submitted,

**KAZEROUNI LAW GROUP, APC**

By: 

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

*Attorneys for Plaintiff and the putative Class*

Electronically Filed by Superior Court of California, County of Orange, 11/18/2021 10:31:54 PM  
 30-2021-01232683-CU-NP-CXC (RON # 3 - DAVID H. AMASAKI, Clerk of the Court By Georgina Ramirez, Deputy Clerk.)

ABBAS KAZEROUNI, Esq. (249203); Mona Amini, Esq. (296829)  
 KAZEROUNI LAW GROUP, APC - 255 Fischer Ave., D1, Costa Mesa, CA 92626

TELEPHONE NO.: (800) 400-6808 FAX NO. (Optional): (800) 520-5523  
 E-MAIL ADDRESS: ak@kazlg.com; mona@kazlg.com  
 ATTORNEY FOR (Name): Plaintiff, Angelica Ponce

**SUPERIOR COURT OF CALIFORNIA, COUNTY OF ORANGE COUNTY**  
 STREET ADDRESS: 751 W. Santa Ana Blvd.  
 MAILING ADDRESS:  
 CITY AND ZIP CODE: Santa Ana, CA 92701  
 BRANCH NAME: Civil Complex Center

CASE NAME:  
 Angelica Ponce v. Smile Brands Inc., et al.

<b>CIVIL CASE COVER SHEET</b> <input checked="" type="checkbox"/> <b>Unlimited</b> (Amount demanded exceeds \$25,000) <input type="checkbox"/> <b>Limited</b> (Amount demanded is \$25,000 or less)		<b>Complex Case Designation</b> <input type="checkbox"/> Counter <input type="checkbox"/> Joinder Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)	CASE NUMBER: <b>30-2021-01232683-CU-NP-CXC</b> JUDGE: <b>Judge Randall J. Sherman</b> DEPT.:
---	--	--	---

Items 1-6 below must be completed (see instructions on page 2).

CX-105

1. Check **one** box below for the case type that best describes this case:

<b>Auto Tort</b> <input type="checkbox"/> Auto (22) <input type="checkbox"/> Uninsured motorist (46) <b>Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort</b> <input type="checkbox"/> Asbestos (04) <input type="checkbox"/> Product liability (24) <input type="checkbox"/> Medical malpractice (45) <input type="checkbox"/> Other PI/PD/WD (23) <b>Non-PI/PD/WD (Other) Tort</b> <input type="checkbox"/> Business tort/unfair business practice (07) <input type="checkbox"/> Civil rights (08) <input type="checkbox"/> Defamation (13) <input type="checkbox"/> Fraud (16) <input type="checkbox"/> Intellectual property (19) <input type="checkbox"/> Professional negligence (25) <input checked="" type="checkbox"/> Other non-PI/PD/WD tort (35) <b>Employment</b> <input type="checkbox"/> Wrongful termination (36) <input type="checkbox"/> Other employment (15)	<b>Contract</b> <input type="checkbox"/> Breach of contract/warranty (06) <input type="checkbox"/> Rule 3.740 collections (09) <input type="checkbox"/> Other collections (09) <input type="checkbox"/> Insurance coverage (18) <input type="checkbox"/> Other contract (37) <b>Real Property</b> <input type="checkbox"/> Eminent domain/Inverse condemnation (14) <input type="checkbox"/> Wrongful eviction (33) <input type="checkbox"/> Other real property (26) <b>Unlawful Detainer</b> <input type="checkbox"/> Commercial (31) <input type="checkbox"/> Residential (32) <input type="checkbox"/> Drugs (38) <b>Judicial Review</b> <input type="checkbox"/> Asset forfeiture (05) <input type="checkbox"/> Petition re: arbitration award (11) <input type="checkbox"/> Writ of mandate (02) <input type="checkbox"/> Other judicial review (39)	<b>Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400-3.403)</b> <input type="checkbox"/> Antitrust/Trade regulation (03) <input type="checkbox"/> Construction defect (10) <input type="checkbox"/> Mass tort (40) <input type="checkbox"/> Securities litigation (28) <input type="checkbox"/> Environmental/Toxic tort (30) <input type="checkbox"/> Insurance coverage claims arising from the above listed provisionally complex case types (41) <b>Enforcement of Judgment</b> <input type="checkbox"/> Enforcement of judgment (20) <b>Miscellaneous Civil Complaint</b> <input type="checkbox"/> RICO (27) <input type="checkbox"/> Other complaint (not specified above) (42) <b>Miscellaneous Civil Petition</b> <input type="checkbox"/> Partnership and corporate governance (21) <input type="checkbox"/> Other petition (not specified above) (43)
---	--	--

2. This case ☒ is ☐ is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:

a. <input type="checkbox"/> Large number of separately represented parties	d. <input type="checkbox"/> Large number of witnesses
b. <input checked="" type="checkbox"/> Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve	e. <input type="checkbox"/> Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
c. <input checked="" type="checkbox"/> Substantial amount of documentary evidence	f. <input type="checkbox"/> Substantial postjudgment judicial supervision

3. Remedies sought (check all that apply): a. ☒ monetary b. ☒ nonmonetary; declaratory or injunctive relief c. ☒ punitive

4. Number of causes of action (specify): 4 - violations of Cal Civ. Code 1798.100, Cal. Civ. Code § 56, Cal. Bus. & Prof. § 17200, and Breach of Contract

5. This case ☒ is ☐ is not a class action suit.

6. If there are any known related cases, file and serve a notice of related case. (You may use form CM-815.)

Date: 11/18/2021  
 Abbas Kazeroounian

(TYPE OR PRINT NAME) (SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

**NOTICE**

- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on all other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

Page 1 of 2

**INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET****CM-010**

**To Plaintiffs and Others Filing First Papers.** If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the Civil Case Cover Sheet contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must complete items 1 through 6 on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 2.30 and 3.220 of the California Rules of Court.

**To Parties in Rule 3.740 Collections Cases.** A "collections case" under rule 3.740 is defined as an action for recovery of money owed in a sum stated to be certain that is not more than \$25,000, exclusive of interest and attorney's fees, arising from a transaction in which property, services, or money was acquired on credit. A collections case does not include an action seeking the following: (1) tort damages, (2) punitive damages, (3) recovery of real property, (4) recovery of personal property, or (5) a prejudgment writ of attachment. The identification of a case as a rule 3.740 collections case on this form means that it will be exempt from the general time-for-service requirements and case management rules, unless a defendant files a responsive pleading. A rule 3.740 collections case will be subject to the requirements for service and obtaining a judgment in rule 3.740.

**To Parties in Complex Cases.** In complex cases only, parties must also use the Civil Case Cover Sheet to designate whether the case is complex. If a plaintiff believes the case is complex under rule 3.400 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

**CASE TYPES AND EXAMPLES****Auto Tort**

Auto (22)–Personal Injury/Property Damage/Wrongful Death  
Uninsured Motorist (46) (*if the case involves an uninsured motorist claim subject to arbitration, check this item instead of Auto*)

**Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort**

Asbestos (04)  
Asbestos Property Damage  
Asbestos Personal Injury/Wrongful Death  
Product Liability (*not asbestos or toxic/environmental*) (24)  
Medical Malpractice (45)  
Medical Malpractice–Physicians & Surgeons  
Other Professional Health Care Malpractice  
Other PI/PD/WD (23)  
Premises Liability (e.g., slip and fall)  
Intentional Bodily Injury/PD/WD (e.g., assault, vandalism)  
Intentional Infliction of Emotional Distress  
Negligent Infliction of Emotional Distress  
Other PI/PD/WD

**Non-PI/PD/WD (Other) Tort**

Business Tort/Unfair Business Practice (07)  
Civil Rights (e.g., discrimination, false arrest) (*not civil harassment*) (08)  
Defamation (e.g., slander, libel) (13)  
Fraud (16)  
Intellectual Property (19)  
Professional Negligence (25)  
Legal Malpractice  
Other Professional Malpractice (*not medical or legal*)  
Other Non-PI/PD/WD Tort (35)

**Employment**

Wrongful Termination (36)  
Other Employment (15)

**Contract**

Breach of Contract/Warranty (06)  
Breach of Rental/Lease  
Contract (*not unlawful detainer or wrongful eviction*)  
Contract/Warranty Breach–Seller Plaintiff (*not fraud or negligence*)  
Negligent Breach of Contract/Warranty  
Other Breach of Contract/Warranty  
Collections (e.g., money owed, open book accounts) (09)  
Collection Case–Seller Plaintiff  
Other Promissory Note/Collections Case  
Insurance Coverage (*not provisionally complex*) (18)  
Auto Subrogation  
Other Coverage  
Other Contract (37)  
Contractual Fraud  
Other Contract Dispute

**Real Property**

Eminent Domain/Inverse Condemnation (14)  
Wrongful Eviction (33)  
Other Real Property (e.g., quiet title) (26)  
Writ of Possession of Real Property  
Mortgage Foreclosure  
Quiet Title  
Other Real Property (*not eminent domain, landlord/tenant, or foreclosure*)

**Unlawful Detainer**

Commercial (31)  
Residential (32)  
Drugs (38) (*if the case involves illegal drugs, check this item; otherwise, report as Commercial or Residential*)

**Judicial Review**

Asset Forfeiture (05)  
Petition Re: Arbitration Award (11)  
Writ of Mandate (02)  
Writ–Administrative Mandamus  
Writ–Mandamus on Limited Court Case Matter  
Writ–Other Limited Court Case Review  
Other Judicial Review (39)  
Review of Health Officer Order  
Notice of Appeal–Labor Commissioner Appeals

**Provisionally Complex Civil Litigation (Cal. Rules of Court Rules 3.400–3.403)**

Antitrust/Trade Regulation (03)  
Construction Defect (10)  
Claims Involving Mass Tort (40)  
Securities Litigation (28)  
Environmental/Toxic Tort (30)  
Insurance Coverage Claims (*arising from provisionally complex case type listed above*) (41)

**Enforcement of Judgment**

Enforcement of Judgment (20)  
Abstract of Judgment (Out of County)  
Confession of Judgment (*non-domestic relations*)  
Sister State Judgment  
Administrative Agency Award (*not unpaid taxes*)  
Petition/Certification of Entry of Judgment on Unpaid Taxes  
Other Enforcement of Judgment Case

**Miscellaneous Civil Complaint**

RICO (27)  
Other Complaint (*not specified above*) (42)  
Declaratory Relief Only  
Injunctive Relief Only (*non-harassment*)  
Mechanics Lien  
Other Commercial Complaint Case (*non-tort/non-complex*)  
Other Civil Complaint (*non-tort/non-complex*)

**Miscellaneous Civil Petition**

Partnership and Corporate Governance (21)  
Other Petition (*not specified above*) (43)  
Civil Harassment  
Workplace Violence  
Elder/Dependent Adult Abuse  
Election Contest  
Petition for Name Change  
Petition for Relief From Late Claim  
Other Civil Petition

**SUPERIOR COURT OF CALIFORNIA,  
COUNTY OF ORANGE  
CIVIL COMPLEX CENTER**

**MINUTE ORDER**

DATE: 12/21/2021

TIME: 11:29:00 AM

DEPT: CX105

JUDICIAL OFFICER PRESIDING: Randall J. Sherman

CLERK: Jason Phu

REPORTER/ERM: None

BAILIFF/COURT ATTENDANT:

CASE NO: **30-2021-01232683-CU-NP-CXC** CASE INIT.DATE: 11/18/2021

CASE TITLE: **Ponce vs. Smile Brands Inc.**

CASE CATEGORY: Civil - Unlimited CASE TYPE: Non-PI/PD/WD tort - Other

---

EVENT ID/DOCUMENT ID: 73667465

**EVENT TYPE:** Chambers Work

---

**APPEARANCES**

There are no appearances by any party.

The Court finds that this case is exempt from the case disposition time goals imposed by California Rule of Court, rule 3.714 due to exceptional circumstances and estimates that the maximum time required to dispose of this case will exceed twenty-four months due to the following case evaluation factors of California Rules of Court, rules 3.715 and 3.400: Case is Complex.

Each party who has not paid the Complex fee of \$ 1,000.00 as required by Government Code section 70616 shall pay the fee to the Clerk of the Court within 10 calendar days from date of this minute order. Failure to pay required fees may result in the dismissal of complaint/cross-complaint or the striking of responsive pleadings and entry of default.

**The Initial Case Management Conference is scheduled for 04/22/2022 at 09:00 AM in Department CX105.**

Plaintiff shall, at least five court days before the hearing, file with the Court and serve on all parties of record or known to Plaintiff a Case Management Statement that covers the applicable subjects set forth in CRC Rule 3.727. The parties are encouraged to meet and confer and file a Joint Case Management Statement. Counsel should begin the Case Management Statement with a brief, objective summary of the case, its procedural status, the contentions of the parties, and any special considerations of which the Court should be aware. Do NOT use Judicial Council Form CM-110, the Case Management Statement form used for non-complex cases.

This case is subject to mandatory electronic filing pursuant to Superior Court Rules, County of Orange, Rule 352. Plaintiff shall give notice of the Status Conference and the electronic filing requirement to all parties of record or known to plaintiff, and shall attach a copy of this minute order.

Clerk to give notice to plaintiff and plaintiff to give notice to all other parties.

**SUPERIOR COURT OF CALIFORNIA, COUNTY OF ORANGE**

Civil Complex Center  
 751 W. Santa Ana Blvd  
 Santa Ana, CA 92701

**SHORT TITLE:** Ponce vs. Smile Brands Inc.

**CLERK'S CERTIFICATE OF MAILING/ELECTRONIC  
 SERVICE**

**CASE NUMBER:**  
**30-2021-01232683-CU-NP-CXC**

I certify that I am not a party to this cause. I certify that the following document(s), Minute Order dated 12/21/21, have been transmitted electronically by Orange County Superior Court at Santa Ana, CA. The transmission originated from Orange County Superior Court email address on December 21, 2021, at 2:50:27 PM PST. The electronically transmitted document(s) is in accordance with rule 2.251 of the California Rules of Court, addressed as shown above. The list of electronically served recipients are listed below:

KAZEROUNI LAW GROUP, APC  
 AK@KAZLG.COM

Clerk of the Court, by:



, Deputy

---

**CLERK'S CERTIFICATE OF MAILING/ELECTRONIC SERVICE**



**SUPERIOR COURT OF CALIFORNIA,  
COUNTY OF ORANGE  
CIVIL COMPLEX CENTER**

**MINUTE ORDER**

DATE: 12/21/2021

TIME: 11:29:00 AM

DEPT: CX105

JUDICIAL OFFICER PRESIDING: Randall J. Sherman

CLERK: Jason Phu

REPORTER/ERM: None

BAILIFF/COURT ATTENDANT:

CASE NO: **30-2021-01232683-CU-NP-CXC** CASE INIT.DATE: 11/18/2021

CASE TITLE: **Ponce vs. Smile Brands Inc.**

CASE CATEGORY: Civil - Unlimited CASE TYPE: Non-PI/PD/WD tort - Other

---

EVENT ID/DOCUMENT ID: 73667465

**EVENT TYPE:** Chambers Work

---

**APPEARANCES**

There are no appearances by any party.

The Court finds that this case is exempt from the case disposition time goals imposed by California Rule of Court, rule 3.714 due to exceptional circumstances and estimates that the maximum time required to dispose of this case will exceed twenty-four months due to the following case evaluation factors of California Rules of Court, rules 3.715 and 3.400: Case is Complex.

Each party who has not paid the Complex fee of \$ 1,000.00 as required by Government Code section 70616 shall pay the fee to the Clerk of the Court within 10 calendar days from date of this minute order. Failure to pay required fees may result in the dismissal of complaint/cross-complaint or the striking of responsive pleadings and entry of default.

**The Initial Case Management Conference is scheduled for 04/22/2022 at 09:00 AM in Department CX105.**

Plaintiff shall, at least five court days before the hearing, file with the Court and serve on all parties of record or known to Plaintiff a Case Management Statement that covers the applicable subjects set forth in CRC Rule 3.727. The parties are encouraged to meet and confer and file a Joint Case Management Statement. Counsel should begin the Case Management Statement with a brief, objective summary of the case, its procedural status, the contentions of the parties, and any special considerations of which the Court should be aware. Do NOT use Judicial Council Form CM-110, the Case Management Statement form used for non-complex cases.

This case is subject to mandatory electronic filing pursuant to Superior Court Rules, County of Orange, Rule 352. Plaintiff shall give notice of the Status Conference and the electronic filing requirement to all parties of record or known to plaintiff, and shall attach a copy of this minute order.

Clerk to give notice to plaintiff and plaintiff to give notice to all other parties.



# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Smile Brands, Sahawneh Dental Hit with Class Action Over April 2021 Data Breach](#)

---