

Vassi Iliadis, SBN 296382
Brhan A. Ahmed, SBN 328157
HOGAN LOVELLS US LLP
1999 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: 310.785.4600
Facsimile: 310.785.4601
vassi.iliadis@hoganlovells.com
brhan.ahmed@hoganlovells.com

Michelle A. Kisloff
(*pro hac vice application to be submitted*)
HOGAN LOVELLS US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, D.C. 20004
Telephone: 202.637.5600
Facsimile: 202.637.5910
michelle.kisloff@hoganlovells.com

Attorneys for Defendant
DAVACO, Inc.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA – EASTERN DIVISION

CHARLES CHACON, individually
and on behalf of all others similarly
situated,

Plaintiff,

v.

DAVACO, INC.,

Defendant.

Case No. 5:21-cv-1589

**NOTICE OF REMOVAL OF
ACTION TO FEDERAL
COURT UNDER 28 U.S.C.
SECTIONS 1332, 1441, 1446,
AND 1453**

(Riverside County Superior Court Case
No. CVRI2103666)

1 **TO PLAINTIFF AND HIS ATTORNEYS OF RECORD:**

2 **PLEASE TAKE NOTICE** that Defendant DAVACO, Inc. (“Defendant”)
3 hereby invokes this Court’s removal jurisdiction pursuant to the Class Action
4 Fairness Act (“CAFA”), Pub. L. 109-2, codified at 28 U.S.C. § 1332(d).

5 **I. THE REMOVED ACTION IS A PUTATIVE CLASS ACTION**
6 **AGAINST DEFENDANT ARISING OUT OF A DATA SECURITY**
7 **INCIDENT.**

8 1. This is a civil action over which this Court has jurisdiction pursuant to
9 28 U.S.C. §§ 1441, 1446, 1453, and CAFA.

10 2. Defendant is a multi-site project management and resource deployment
11 firm that provides support to clients with the development, transformation, and
12 maintenance of physical sites.

13 3. On August 13, 2021, Plaintiff Charles Chacon (“Plaintiff”) filed this
14 action in the Superior Court of California for the County of Riverside (Case No.
15 CVRI2103666). Plaintiff asserts claims against Defendant arising out of a data
16 security incident individually and on behalf of a class. *See* Complaint (“Compl.”) ¶¶
17 10, 74.

18 4. Plaintiff alleges that Defendant collects and stores confidential
19 employee information as part of its business. *Id.* ¶ 2. Plaintiff further alleges that on
20 or around June 11, 2021, “unauthorized and unknown persons” “accessed and
21 viewed” Plaintiff’s and the putative class’s “sensitive information” on Defendant’s
22 computer network. *Id.* ¶ 5.

23 5. On or about July 2, 2021, Defendant “provided notice of a security
24 breach involving the unauthorized access to Defendant’s network,” which stated that
25 “employees[’] name, Social Security number, and Driver’s license or government
26 issued identification were compromised in the Data Breach.” *Id.* ¶¶ 6, 19-21, 23.

27 6. Pursuant to 28 U.S.C. § 1446(a), Defendant attaches a true and correct
28 copy of the as-filed Complaint, summons, civil case cover sheet, certificate of

1 counsel, alternative dispute resolution information package, filing payment, notice
2 of department assignment, and notice of case management conference served on
3 Defendant as **Exhibit A**.

4 **II. DEFENDANT HAS SATISFIED THE PROCEDURAL**
5 **REQUIREMENTS FOR REMOVAL.**

6 7. Removal to this Court is proper under 28 U.S.C. § 1446. First, this
7 Court is the “district court of the United States for the district and division within
8 which [this] action is pending” 28 U.S.C. § 1446(a). Assignment to the
9 Eastern Division is proper because this action was pending in the Superior Court of
10 California for the County of Riverside, which is embraced by the United States
11 District Court for the Central District of California, Eastern Division.

12 8. Defendant’s Notice of Removal is timely under 28 U.S.C. § 1446(b)
13 because Plaintiff’s Complaint was served on Defendant on August 20, 2021. *See*
14 **Exhibit B**. Accordingly, this Notice of Removal is filed within thirty (30) days of
15 service.

16 9. Defendant will provide copies of this Notice of Removal to counsel of
17 record for Plaintiff, and will also file a copy with the Clerk of the Superior Court of
18 California for the County of Riverside, as required by 28 U.S.C. § 1446(d).

19 **III. THIS COURT HAS REMOVAL JURISDICTION UNDER CAFA.**

20 10. Defendant alleges that this Court has diversity jurisdiction over this
21 action pursuant to CAFA. Congress passed CAFA, in part, “to restore the intent of
22 the framers of the United States Constitution by providing for Federal court
23 consideration of interstate cases of national importance under diversity jurisdiction.”
24 Pub. L. No. 109-2, 2(b)(2), 119 Stat. 4 (codified as a note to 28 U.S.C. § 1711); *see*
25 *Luther v. Countrywide Home Loans Servicing LP*, 533 F.3d 1031, 1034 (9th Cir.
26 2008). Indeed, Congress enacted CAFA “to facilitate adjudication of certain class
27 actions in federal court” and “no antiremoval presumption attends cases invoking
28 CAFA.” *Dart Cherokee Basin Operating Co., LLC v. Owens*, 135 S. Ct. 547, 554
(2014).

11. Accordingly, CAFA expanded federal jurisdiction to permit removal of putative class actions pending in state court when three basic elements are met: (1) the members of the proposed class are not less than 100; (2) any member of the alleged plaintiff class is a citizen of a state different from any defendant; and (3) the aggregate amount in controversy exceeds \$5,000,000. *See* 28 U.S.C. §§ 1332(d), 1453(b).

12. The Supreme Court has held that removal is appropriate when the defendant plausibly pleads these three elements because “a defendant’s notice of removal need include only a plausible allegation” of CAFA jurisdiction. *Dart Cherokee*, 135 S. Ct. at 554; *see also id.* at 553 (noting that, by design, 28 U.S.C. § 1446(a) “tracks the general pleading requirement stated in Rule 8(a)”). Defendant readily meets CAFA’s requirements here.

13. **Numerosity**. The putative class exceeds 100 members. Plaintiff purports to represent a class defined as “[a]ll residents of the State of California whose Sensitive Information stored or possessed by Davaco, Inc. was subject to the Data Breach announced by Davaco, Inc. on or about July 2, 2021.” Compl. ¶ 74. Plaintiff alleges that the putative class is “so numerous that joinder of all members is impracticable.” *Id.* ¶ 77.

14. Defendant submits, based on information and belief, that between approximately 1,400 and 1,500 California residents may have had information accessed by unauthorized persons in this data security incident. Therefore, CAFA’s numerosity requirement is satisfied.

15. **Minimal Diversity**. CAFA’s minimal diversity requirement is satisfied when “any member of a class of plaintiffs is a citizen of a State different from any defendant.” 28 U.S.C. § 1332(d)(2)(A).

16. Plaintiff and the putative class are residents of the State of California. Compl. ¶¶ 11, 74.

17. For purposes of federal jurisdiction, corporations are deemed to be

1 citizens of the States in which they were incorporated and the States in which they
 2 have their principal place of business. 28 U.S.C. § 1332(c)(1), (d)(10). Defendant is
 3 incorporated in the State of Delaware, and its principal place of business is in the
 4 State of Texas. Compl. ¶ 13.

5 18. Accordingly, for diversity purposes under CAFA, Defendant is a citizen
 6 of Delaware and Texas and Plaintiff and the California putative class members are
 7 citizens of California. CAFA's minimal diversity requirement is met because at
 8 least one putative class member is diverse with respect to Defendant.

9 19. **Amount in Controversy.** The amount in controversy in this putative
 10 class action based on the allegations of the Complaint exceeds \$5,000,000.¹
 11 According to the Complaint, as a result of the data security incident, Plaintiff and
 12 putative class members allegedly face "imminent, immediate, and continuing
 13 increased risk of harm from identity theft and fraud" Compl. ¶ 64. Further,
 14 Plaintiff and class members seek compensation for the "time and resources . . . to
 15 mitigate the actual and potential impact of the Data Breach on their lives," including
 16 but not limited to "[o]ut-of-pocket costs associated with the prevention, detection,
 17 recovery, and remediation from identity theft or fraud"; "[l]ost opportunity costs and
 18 lost wages associated with efforts . . . to mitigate actual and future consequences of
 19 the Data Breach"; and "[c]urrent and future costs in terms of time, effort, and money
 20

21 ¹ The relevant inquiry for removal concerns the amount in controversy based on the
 22 allegations contained in the Complaint, in which Plaintiff seeks damages exceeding
 23 CAFA's jurisdictional threshold. *Lokey v. CVS Pharmacy, Inc.*, No. 20-cv-04782-
 24 LB, 2020 WL 5569705, at *6 (N.D. Cal. Sep. 17, 2020). Defendant does not admit
 25 that any injury occurred or that there is any liability under any of the claims asserted
 26 in this action and does not waive any challenges to any of the claims asserted. The
 27 law is clear that "[e]ven when defendants have persuaded a court upon a CAFA
 28 removal that the amount in controversy exceeds \$5 million, they are still free to
 challenge the actual amount of damages in subsequent proceedings and at trial." *Ibarra v. Manheim Invts., Inc.*, 775 F.3d 1193, 1198 n.1 (9th Cir. 2015).

1 that will be expended to prevent, detect, contest, remediate, and repair the impact of
2 the Data Breach for the remainder of the lives of Plaintiff and Class Members.” *Id.*
3 ¶¶ 64, 67.

4 20. Based on these allegations, the Complaint asserts nine causes of action
5 against Defendant for: (1) Negligence, (2) Invasion of Privacy, (3) Breach of
6 Implied Contract, (4) Unjust Enrichment, (5) Breach of Fiduciary Duty, (6) Breach
7 of Confidence, (7) Violation of California’s Unfair Competition Law for Unfair
8 Business Practices; (8) Violation of California’s Information Practices Act of 1977,
9 and (9) Violation of California Consumer Records Act. *Id.* ¶ 10.s

10 21. Plaintiff, individually and on behalf of the putative class, seeks
11 compensatory and statutory damages, injunctive relief, restitution and disgorgement
12 of an unidentified sum of revenues, attorneys’ fees and costs, and “other and further
13 relief as this Court may deem just and proper.” *See* Compl. Prayer for Relief, at 41-
14 44.

15 22. Upon information and belief, Plaintiff and a putative class comprised of
16 between approximately 1,400 and 1,500 individuals in California allegedly impacted
17 by the data security incident at issue are now seeking damages related to the
18 incident.

19 23. To take just one cause of action, Plaintiff’s ninth cause of action seeks
20 to recover “all remedies available under Cal. Civ. Code § 1798.84” in connection
21 with Defendant’s purported “fail[ure] to disclose to Plaintiff and Class members,
22 without unreasonable delay and in the most expedient time possible, the breach of
23 security” Compl. ¶¶ 175-76, 181. Section 1798.84 provides for damages and
24 for civil penalties of up to \$3,000 for each “willful, intentional, or reckless”
25 violation, and up to \$500 for other violations. Although Defendant submits that
26 Plaintiff does not allege facts that would support a finding of “willful, intentional,
27 or reckless” violations under § 1798.84 or § 1798.83 (upon which the civil penalties
28 in § 1798.84 are based), Plaintiff seeks “all remedies” available under the statute,

1 and asserts that the lack of prompt notification occurred despite Defendant's
2 knowledge of the data security incident at issue for some unspecified period of time,
3 ostensibly in order to "conceal the Data Breach from the public to ensure continued
4 revenue." *Id.* ¶¶ 175-77 & 181.

5 24. Plaintiff additionally demands injunctive relief that would require
6 Defendant to encrypt "all data collected through the course of business," "implement
7 and maintain a comprehensive Information Security Program" of unspecified
8 proportionality, "engage independent third-party security auditors/penetration testers
9 as well as internal security personnel to conduct testing" and "promptly correct any
10 problems or issues detected," "engage independent third-party security auditors and
11 internal personnel to run automated security monitoring" as well as "regular
12 database scanning and securing checks," "establish an information security training
13 program" with general and tailored trainings, and "provide ongoing credit
14 monitoring and identity theft repair services to Class members." *See* Compl. Prayer
15 for Relief, at 41-44. Each of these requested forms of relief would be costly and
16 increase the amount in controversy. *See Lokey*, No. 20-cv-04782-LB, 2020 WL
17 5569705, at *9 n.38 ("CAFA allows courts to aggregate the value of the claims, and
18 that aggregation rule applies to the value of the injunctive relief.").

19 25. Although the Complaint does not plead the specific amount at issue, it
20 does not disclaim damages over any amount. That, and the size of the purported
21 class, Plaintiff's requests for compensatory and statutory damages, civil penalties,
22
23
24
25
26
27
28

attorneys' fees,² and the value of sought injunctive relief and other equitable relief for restitution and disgorgement, mean that CAFA's jurisdictional minimum is clearly satisfied here. *See Lokey*, No. 20-cv-04782-LB, 2020 WL 5569705, at *8-10 (holding that Defendant "sufficiently established the CAFA amount in controversy" by combining amounts for "restitution," "attorney's fees," and "injunction costs"); *see also Bayol v. Zipcar, Inc.*, No. 14-cv-02483-TEH, 2015 WL 4931756, at *10 (N.D. Cal. Aug. 18, 2015). As a result, the amount in controversy plausibly exceeds \$5,000,000.

26. This action thus satisfies each of CAFA's jurisdictional requirements, and removal to this Court is proper.

27. Nothing in this Notice of Removal constitutes a waiver or admission of any allegation, defense, argument, or principle of equity available to Defendant.

IV. CONCLUSION.

For each of these reasons and pursuant to 28 U.S.C. §§ 1332, 1441, 1446, and 1453, the above described action now pending against Defendant in the Superior Court of California for the County of Riverside is properly removed to the United States District Court for the Central District of California.

² The Ninth Circuit calculates attorneys' fees added to the amount in controversy as a percentage of the class's common fund—with the Ninth Circuit "benchmark" set at "25% of the common fund"—or by using the lodestar method. *See Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1029 (9th Cir. 1998). When opting for the class-action percentage method in the removal context, courts in the Ninth Circuit have "relied on the benchmark [25% of the common fund] amount as an estimate for the amount in controversy analysis" *Bayol*, No. 14-cv-02483-TEH, 2015 WL 4931756, at *17 (internal citations omitted). Regardless of which method is used here, the attorneys' fees for a case involving the size of the purported class, coupled with Plaintiff's requests for compensatory and statutory damages, civil penalties, and the value of sought injunctive relief and other equitable relief for restitution and disgorgement, satisfy CAFA's jurisdictional minimum.

1 Dated: September 17, 2021 **HOGAN LOVELLS US LLP**

2 By: /s/ Vassi Iliadis

3 Vassi Iliadis, SBN 296382
4 Brhan Ahmed, SBN 328157
5 **HOGAN LOVELLS US LLP**
6 1999 Avenue of the Stars, Suite 1400
7 Los Angeles, CA 90067
8 Tel: 310.785.4600
9 Fax: 310.785.4601
10 vassi.iliadis@hoganlovells.com
11 brhan.ahmed@hoganlovells.com

12 Michelle A. Kisloff
13 *(pro hac vice application to be submitted)*
14 **HOGAN LOVELLS US LLP**
15 Columbia Square
16 555 Thirteenth Street, NW
17 Washington, D.C. 20004
18 Tel: 202.637.5600
19 Fax: 202.637.5910
20 michelle.kisloff@hoganlovells.com

21 *Attorneys for Defendant*
22 *DAVACO, Inc.*
23
24
25
26
27
28

PROOF OF SERVICE

I am a citizen of the United States and employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Hogan Lovells US LLP, 1999 Avenue of the Stars, Suite 1400, Los Angeles, California 90067.

On September 17, 2021, I served a copy of the within document(s):

NOTICE OF REMOVAL OF ACTION TO FEDERAL COURT UNDER 28, U.S.C. SECTIONS 1332, 1441, 1446, AND 1453;

- ☐ by transmitting via facsimile the document(s) listed above to the fax number(s) set forth below on this date before 5:00 p.m.
- ☒ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, the United States mail at Los Angeles, California addressed as set forth below.
- ☐ by placing the document(s) listed above in a sealed Federal Express envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a Federal Express agent for delivery.
- ☐ by personally delivering the document(s) listed above to the person(s) at the address(es) set forth below.
- ☒ by transmitting via e-mail or electronic transmission the document(s) listed above to the person(s) at the e-mail address(es) set forth below.

SWIGART LAW GROUP, APC
Joshua B. Swigart
Rahil Swigart
Evan Thamamahong
2221 Camino Del Rio S., Suite 308
San Diego, California 92108
josh@swigartlawgroup.com
rahil@swigartlawgroup.com
evan@swigartlawgroup.com

Attorneys for Plaintiff

Casey Gerry Schenk Francavilla Blatt & Penfield LLP
Gayle M. Blatt
110 Laurel St.
San Diego, CA 92101
gmb@cglaw.com

Attorneys for Plaintiff

I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

1 I declare that I am employed in the office of a member of the bar of this court at whose
2 direction the service was made.

3 Executed on September 17, 2021, at Los Angeles, California.
4

5 _____
6 Mae F. Chester
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A

1 Joshua B. Swigart, SBN 225557
josh@swigartlawgroup.com
2 **SWIGART LAW GROUP, APC**
2221 Camino Del Rio S., Suite 308
3 San Diego, CA 92108
4 Tel: (866) 219-3343; Fax: (866) 219-8344

5 *Counsel for Plaintiff Chacon, and the Putative Class*

6
7
8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
COUNTY OF RIVERSIDE

9 CHARLES CHACON, individually
10 and on behalf of all others similarly
11 situated,

12 Plaintiff,

13 v.

14 DAVACO, INC.,

15 Defendant.

Case No. **CVRI2103666**

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

COMPLEX

16
17
18
19
20
21
22
23
24
25
26
27
28

CLASS ACTION COMPLAINT

1 Plaintiff CHARLES CHACON ("Plaintiff") bring this Class Action Complaint
2 against Davaco, Inc. ("Defendant") in their individual capacities and on behalf of all
3 others similarly situated (the "Class," defined below), and allege, upon personal
4 knowledge as to their own actions and their counsels' investigations, and upon
5 information and belief as to all other matters, as follows:

6 INTRODUCTION

7 1. Defendant Davaco, Inc. is a multi-site project management and
8 deployment company that supports retail, restaurant, and hospitality services with the
9 development, transformation, and maintenance of their sites.

10 2. A part of Defendant's business involves collecting and storing
11 confidential employee information.

12 3. Under California law, including California common law, the California
13 Unfair Competition Law, ("UCL"), Plaintiff and all other persons similarly situated had
14 a right to keep their Personal Identifying Information ("PII") provided to Defendant
15 confidential (PII collectively "Sensitive Information"). Plaintiff and other members of
16 the Class relied on Defendant to keep their sensitive PII confidential as required by the
17 applicable laws.

18 4. Defendant violated this right. It failed to implement or follow reasonable
19 data security procedures as required by law and failed to protect Plaintiff and the
20 proposed Class Employees' Sensitive Information from unauthorized access.

21 5. As a result of Defendant's inadequate data security and inadequate or
22 negligent training of its employees, on or around June 11, 2021, Defendant was alerted
23 to suspicious activity on Defendant's computer network. Plaintiff and Class
24 Employees' Sensitive Information was accessed and viewed by unauthorized and
25 unknown persons through Defendant's employee email accounts. On or about June 15,
26 2021, Defendant confirmed this unauthorized access.

27 6. On information and belief, on or around July 2, 2021, Defendant provided
28 notice of a security breach involving the unauthorized access to Defendant's network.

1 The attacker viewed and removed data stored in Defendant's system which contained
2 sensitive and confidential Sensitive Information. The notice stated that the information
3 included employees name, Social Security number, and Driver's license or government
4 issued identification were compromised in the Data Breach.

5 7. The Data Breach was a direct result of Defendant's failure to implement
6 adequate and reasonable cybersecurity procedures and protocols necessary to protect
7 its employees' Sensitive Information.

8 8. Defendant disregarded the rights of Plaintiff and Class members by,
9 among other things, recklessly or negligently failing to take adequate and reasonable
10 measures to ensure its data systems were protected against unauthorized intrusions;
11 failing to disclose that it did not have reasonable or adequately robust computer
12 systems and security practices to safeguard its employees' Sensitive Information;
13 failing to take standard and reasonably available steps to prevent the Data Breach;
14 failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff
15 and Class members prompt and accurate notice of the Data Breach.

16 9. As a result of Defendant's failure to implement and follow reasonable
17 security procedures, Class employees' Sensitive Information is now in the hands of
18 thieves. Plaintiff and Class members have spent, and will continue to spend, significant
19 amounts of time and money trying to protect themselves from the adverse
20 ramifications of the Data Breach and dealing with actual fraud and will forever be at a
21 heightened risk of identity theft and fraud.

22 10. Plaintiff, on behalf of all others similarly situated, allege claims for
23 (1) negligence; (2) invasion of privacy; (3) breach of implied contract; (4) unjust
24 enrichment; (5) breach of fiduciary duty; (6) breach of confidence; (7) violation of the
25 California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq.*);
26 (8) violation of the California Information Practices Act of 1977 (Cal. Civ. Code § 1798,
27 *et seq.*); and (9) violation of the California Consumer Records Act ("CCRA") (Cal. Civ.
28 Code § 1798.80, *et seq.*). Plaintiff and the Class members seek damages, including but

1 not limited to nominal damages from Defendant, and to compel Defendant to adopt
2 reasonably sufficient security practices to safeguard its Employees' Sensitive
3 Information that remains in Defendant's custody to prevent incidents like the Data
4 Breach from reoccurring in the future.

5 **PARTIES**

6 11. Plaintiff Charles Chacon is a resident of the State of California and was an
7 employee of Defendant. On or about July 2, 2021, Plaintiff Chacon received notice from
8 Defendant that his Sensitive Information had been improperly exposed to
9 unauthorized third parties.

10 12. The notices received by Plaintiff are substantially similar to the exemplar
11 Notice of Data Breach letter submitted to the State of California. On information and
12 belief, Defendant has not posted a notice of the Data Breach on Defendant's website.

13 13. Defendant conducts business in the state of California. Defendant's
14 headquarters are located at 6688 North Central Expwy Suite 100 Dallas, Texas.

15 **JURISDICTION AND VENUE**

16 14. This Court has jurisdiction over this action because Defendant is a citizen
17 of California and conducts business in California.

18 15. Venue in this Court is proper pursuant to California Code of Civil
19 Procedure § 395, *et seq.*, because – on information and belief – the acts complained of
20 herein took place within the county of San Joaquin, California; and Defendant conducts
21 business in San Joaquin County, California.

22 **FACTUAL ALLEGATIONS**

23 **A. Background.**

24 16. Defendant develops business solutions such as graphic installations,
25 project management, hard line and soft line merchandising, marketing surveys, and
26 logistics for retail, restaurant, and hospitality businesses throughout the United States.

1 17. Common practice for employers, Defendant must keep its employees'
2 Sensitive Information in its system. Defendant accomplishes this by keeping the
3 Sensitive Information electronically – even in its email systems.

4 18. As an employer, Defendant is required to ensure that such sensitive,
5 personal information is not disclosed or disseminated to unauthorized third parties
6 without Employees' express, written consent, as further detailed below.

7 **B. The Data Breach.**

8 19. On or around July 2, 2021, Defendant issued a Notice of Data Event,
9 notifying employees of an incident involving potential unauthorized access to personal
10 information. Defendant provided this Data Breach Notification to an undisclosed
11 number of members ("July 2021 Data Breach Notice").¹ The July 2021 Data Breach
12 Notice informed the affected members that:

13 On June 11, 2021, Davaco was alerted to suspicious activity on our
14 computer network. We hired cybersecurity experts and computer
15 forensic investigators to help us investigate the incident, ensure the
16 safety of our environment, and confirm whether anyone's personal
17 information was impacted. While the investigation is ongoing, we can
18 confirm that we were the victim of a ransomware attack, and an
19 unauthorized individual gained access to our network. Based on the
20 investigation, the attacker viewed and removed some data stored in
21 the system. On June 15, 2021, we confirmed that the data viewed or
22 taken by the attacker included employees' personal information.

23 The potentially impacted information includes your name, Social
24 Security number, and Driver's license or government issued
25 identification number.

26 20. On information and belief, Defendant has not posted any Notice of Data
27 Breach on its website. Defendant provided members the July 2021 Data Breach Notice
28 which informed the affected members that:

 We are writing to provide you with information about a recent data
security incident that may have involved your personal information.
At Davaco, we take the privacy and security of our employees'

¹ <https://oag.ca.gov/ecrime/databreach/reports/sb24-543040> (last accessed August 9, 2021).

1 information very seriously. That is why we are sending you this letter
2 to tell you about the incident, offering you credit monitoring and
3 identity monitoring services, and providing you with information,
4 resources and steps you can take to help protect your personal
5 information.

6 On June 11, 2021, Davaco was alerted to suspicious activity on our
7 computer network. We hired cybersecurity experts and computer
8 forensic investigators to help us investigate the incident, ensure the
9 safety of our environment, and confirm whether anyone's personal
10 information was impacted. While the investigation is ongoing, we can
11 confirm that we were the victim of a ransomware attack, and an
12 unauthorized individual gained access to our network. Based on the
13 investigation, the attacker viewed and removed some data stored in
14 the system. On June 15, 2021, we confirmed that the data viewed or
15 taken by the attacker included employees' personal information.

16 As soon as we discovered the incident, we took the steps described
17 above. We also notified the FBI and will fully cooperate with any law
18 enforcement investigation. In addition, although we have no
19 evidence that your personal information has been misused, we are
20 offering you identity theft protection services through IDX®, the data
21 breach and recovery services expert, these services include:
22 <<12/24>>months of credit monitoring, a \$1,000,000 insurance
23 reimbursement policy, and fully managed identity theft recovery
24 services. With this protection, IDX will help you resolve issues if your
25 identity is compromised. If you complete the sign-up steps specified
26 in this letter, the product we are offering you will provide protection
27 from the misuse of any personal information that may have been
28 impacted by this incident. We encourage you to contact IDX with any
questions and to enroll in the free services we are offering by calling
833-909-3912 or going to <https://response.idx.us/davaco> and using
the Enrollment Code provided above. IDX experts are available
Monday through Friday from 9 am - 9 pm Eastern Time. Please note
the deadline to enroll is October 2, 2021. It is important to contact IDX
with questions. DAVACO has hired IDX as a full-service provider to
its employees; as such, DAVACO management does not have details
of these services.

At this time, we are unaware of the misuse of any of your information.
However, we encourage you to take full advantage of this service
offering. IDX representatives can answer questions or concerns you
may have regarding protection of your personal information.

1 21. The July 2021 Data Breach Notice identified the following data points:
2 employee name, Social Security number, and Driver's license or government issued
3 identification number.

4 22. Defendant failed to put in place proper security protocols to protect
5 against the unauthorized release of patient information and failed to properly train its
6 employees on such protocols, resulting in the unauthorized release of private data. As a
7 result of Defendants failures, Plaintiff and the Class Employees' Sensitive Information
8 was accessed and viewed by unknown and unauthorized third parties and is, or likely
9 will be, for sale on the dark web. This means that the Data Breach was successful:
10 unauthorized individuals accessed Plaintiff and the Class employees' unencrypted,
11 unredacted information set forth above.

12 23. Plaintiff received data breach notification letters from Defendant on or
13 about July 2, 2021, informing them of the Data Breach and that their Sensitive
14 Information was present in the affected Daveco, Inc. email accounts. The Data Breach
15 notification indicated the following information may have been compromised
16 employee name, Social Security number, and Driver's license or government issued
17 identification number.

18 24. This kind of Sensitive Information is highly valued by criminals, as
19 evidenced by the prices they will pay through the dark web. Numerous sources cite
20 dark web pricing for stolen identity credentials. For example, personal information can
21 be sold at a price ranging from \$40 to \$200. Social Security numbers and Driver's
22 license or government issued identification numbers are especially valuable to identity
23 thieves.

24 25. The theft of this kind of information leads to a known increased risk of
25 identity theft. As stated by the Federal Trade Commission:

26 A thief may use your name or health insurance numbers to see a
27 doctor, get prescription drugs, file claims with your insurance
28 provider, or get other care. If the thief's health information is mixed

1 with yours, your treatment, insurance and payment records, and
2 credit report may be affected.²

3 **C. Plaintiff's Exposure and Mitigation Efforts**

4 **Plaintiff Chacon**

5 26. As a direct result of the Data Breach, Plaintiff Chacon has engaged in
6 mitigation efforts and expended time and resources. Plaintiff Chacon now checks his
7 credit reports as well as his banking statements and credit card statements on a daily
8 basis. This is time Plaintiff Chacon otherwise would have spent performing other
9 activities, such as his job or leisure activities.

10 27. Following the Data Breach, on or around July 10, 2021, Plaintiff Chacon
11 was notified by his bank, BBVA that there were multiple transactions posted to his
12 account and an unauthorized third party withdrew funds from his bank account.

13 28. As a direct result of the Data Breach, Plaintiff Chacon requested a new
14 account number and Debit card from his bank BBVA. Subsequently, on or around July
15 26, 2021, Plaintiff Chacon was notified by his bank, BBVA that there were new
16 fraudulent transactions posted to his account and an unauthorized third party
17 withdrew funds from his bank account. Plaintiff Chacon requested a new account
18 number and debit card from BBVA.

19 29. On or around August 6, 2021, Plaintiff Chacon attempted to use his debit
20 card and it was blocked by his bank, BBVA. Plaintiff Chacon contacted his bank and
21 was forced to receive a third new account number and debit card.

22 30. Following the Data Breach, Plaintiff Chacon was notified of an
23 unauthorized attempt to open multiple credit cards in his name. During this time,
24 Plaintiff Chacon had no other payment method to pay for bills. Plaintiff Chacon had to
25
26

27 ² Federal Trade Commission, Medical Identity Theft,
28 <https://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Feb.
11, 2021).

1 go to the BBVA branch, pull cash out of his account and purchase Prepaid Visa cash
2 cards in order to pay his bills.

3 31. Knowing that thieves stole his Sensitive Information and knowing that
4 his Sensitive Information may now or in the future be available for sale on the dark
5 web has caused Plaintiff Chacon great anxiety. He is now very concerned about his
6 healthcare coverage and identity theft in general. This Data Breach has given Plaintiff
7 Adams hesitation about using electronic services and reservations about conducting
8 other online activities requiring his personal information.

9 32. Plaintiff Chacon suffered actual injury from having his Sensitive
10 Information exposed as a result of the Data Breach including, but not limited to: (a)
11 actual instances of identity fraud; (b) continued employment by Defendant had
12 Defendant disclosed that it lacked data security practices adequate to safeguard
13 consumers' Sensitive Information from theft; (c) damages to and diminution in the
14 value of his Sensitive Information – a form of intangible property that Plaintiff Chacon
15 entrusted to Defendant as a condition for employment; (d) loss of his privacy; (e)
16 imminent and impending injury arising from the increased risk of fraud and identity
17 theft; and (f) the time and expense of his mitigation efforts as a result of the Data
18 Breach.

19 33. As a result of the Data Breach, Plaintiff Chacon will continue to be at
20 heightened risk for financial fraud, medical fraud and identity theft, and the attendant
21 damages, for years to come.

22 **D. Defendant's Information Security Statement and Privacy Policies.**

23 34. Defendant's policies detail its promises and legal obligations to maintain
24 and protect employees' Sensitive Information.

25 //

26 //

35. Defendant's Privacy Policy³ provides, in part:

Security

DAVACO uses industry-standard efforts to safeguard the confidentiality of your personal information such as firewalls and authentication protection. However, we do not guarantee complete security, as it does not exist on the Internet Defendant's Notice of Privacy Practices⁴ provides, in part:

36. Defendant also describes how it may use and disclose health information for each category of uses or disclosures – none of which provide it a right to expose employees' Sensitive Information to unauthorized third parties, such as was done in the Data Breach.

E. Defendant Knew or Should Have Known of the Risk Because large employers are Particularly Susceptible to Cyber Attacks.

37. The number of U.S. data breaches surpassed 1,000 in 2016 – a record high and a 40 percent increase in the number of data breaches from the previous year.⁵ In 2017, 1,579 breaches were reported – a new record high and a 44.7 percent increase in just one year.⁶ That trend continues.

38. Defendant knew and understood unprotected or exposed Sensitive Information in the custody of employers, such as Defendant, is valuable and highly

³ Davaco's Privacy Policy, available at <https://www.davacoinc.com/privacy-policy/> (last accessed August 9, 2021).

⁴ Davaco's Notice of Privacy Practices, available at: <https://www.davacoinc.com/privacy-policy/> (last accessed August 9, 2021).

⁵ Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), available at: <https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html> (last accessed June 7, 2021).

⁶ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, available at: <https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf> (last accessed June 7, 2021).

1 sought after by nefarious third parties seeking to illegally monetize that Sensitive
2 Information through unauthorized access. Indeed, when compromised, highly
3 confidential related data is among the most sensitive and personally consequential.
4 Forty percent of the customers were never able to resolve their identity theft at all. Data
5 breaches and identity theft have a crippling effect on individuals, and detrimentally
6 impacts the economy as a whole.⁷

7 39. Data breaches continue to rapidly increase. From social security and
8 insurance policies, to next of kin and credit cards, no other organization, including
9 credit bureaus, have so much monetizable information stored in their data centers.”⁸

10 40. As an employer provider, Defendant knew, or should have known, the
11 importance of safeguarding Sensitive Information entrusted to it by Plaintiff and Class
12 members, and of the foreseeable consequences if its data security systems were
13 breached. This includes the significant costs imposed on Plaintiff and Class members as
14 a result of a breach. Defendant failed, however, to take adequate cybersecurity
15 measures to prevent the Data Breach.

16 **F. Defendant Acquires, Collects, and Stores Plaintiff and Class Employees’ PII.**

17 41. Defendant acquires, collects, and stores a massive amount of its
18 Employees’ protected confidential information and other personally identifiable data.

19 42. As a condition of engaging in employment, Defendant requires its
20 employees to entrust them with highly confidential Sensitive Information.

21 43. By requiring, obtaining, collecting, using, and deriving a benefit from
22 Plaintiff’s and Class Employees’ Sensitive Information, Defendant assumed legal and
23 equitable duties, and knew or should have known it was responsible for protecting
24 Plaintiff’s and Class Employees’ Sensitive Information from disclosure.

25
26
27 ⁷ *Id.*
28

44. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff and Class members relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, to only allow authorized disclosures of this information, and prevent unauthorized disclosure of the information.

G. The Value of PII and the Effects of Unauthorized Disclosure.

45. Defendant was well aware of the highly private nature of the Sensitive Information it collects and its significant value to those who would use it for wrongful purposes.

46. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.⁹ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

47. While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much as \$363, according to the Infosec Institute. This is because an individual’s health history (e.g., ailments, diagnosis, surgeries, etc.) cannot be changed.¹⁰

48. The ramifications of Defendant’s failure to keep Plaintiff’ and Class Employees’ Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable

⁹ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last accessed June 7, 2021).

¹⁰ Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at: <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last accessed June 7, 2021).

consequences if its data security systems were breached, including the significant costs that would be imposed on its members as a result of a breach.

H. Defendant Failed to Comply with FTC Guidelines.

50. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹¹

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.¹² The guidelines note that businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

52. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.¹³

53. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these

¹¹ Federal Trade Commission, *Start With Security*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed June 7, 2021).

¹² Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 7, 2021).

¹³ FTC, *Start With Security*, *supra* note 16.

1 actions further clarify the measures businesses must take to meet their data security
2 obligations.

3 54. Defendant failed to properly implement basic data security practices.
4 Defendant's failure to employ reasonable and appropriate measures to protect against
5 unauthorized access to Employees' Sensitive Information constitutes an unfair act or
6 practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

7 55. Defendant was at all times fully aware of its obligation to protect Plaintiff'
8 and Class Employees' Sensitive Information because of Defendant's position as a
9 trusted healthcare provider. Defendant was also aware of the significant repercussions
10 that would result from its failure to do so.

11 **I. Defendant Failed to Comply with Industry Standards.**

12 56. Defendant failed to implement several basic cybersecurity safeguards that
13 can be implemented to improve cyber resilience and require a relatively small financial
14 investment yet can have a major impact on an organization's cybersecurity posture
15 including: (a) the proper encryption of PII; (b) educating and training employees on
16 how to protect PII; and (c) correcting the configuration of software and network
17 devices.

18 57. Private cybersecurity firms have also identified the healthcare sector as
19 being particularly vulnerable to cyber-attacks, both because of the value of the PII they
20 maintain and because as an industry they have been slow to adapt and respond to
21 cybersecurity threats.¹⁴ These private cybersecurity firms have also promulgated
22 similar best practices for bolstering cybersecurity and protecting against the
23 unauthorized disclosure of PII.

24 58. Despite the abundance and availability of information regarding the
25 threats and cybersecurity best practices to defend against those threats, Defendant
26 chose to ignore them. These best practices were known, or should have been known by
27

1 Defendant, whose failure to heed and properly implement industry standards directly
2 led to the Data Breach and the unlawful exposure of Sensitive Information.

3 **J. Plaintiff and Class members Suffered Damages.**

4 59. The ramifications of Defendant's failure to keep Plaintiff's and Class
5 Employees' Sensitive Information secure are long lasting and severe. Once that kind of
6 Sensitive Information is stolen, fraudulent use of that information and damage to
7 victims may continue for years. Consumer victims of data breaches are more likely to
8 become victims of identity fraud.¹⁵

9 60. The Sensitive Information belonging to Plaintiff and Class members is
10 private, sensitive in nature, and left inadequately protected by Defendant—who did
11 not obtain Plaintiff's or Class Employees' consent to disclose such Sensitive
12 Information to any other person as required by applicable law and industry standards.

13 61. The Data Breach was a direct and proximate result of Defendant's failure
14 to: (a) properly safeguard and protect Plaintiff's and Class Employees' Sensitive
15 Information from unauthorized access, use, and disclosure, as required by various state
16 and federal regulations, industry practices, and common law; (b) establish and
17 implement appropriate administrative, technical, and physical safeguards to ensure the
18 security and confidentiality of Plaintiff's and Class Employees' Sensitive Information;
19 and (c) protect against reasonably foreseeable threats to the security or integrity of such
20 information.

21 62. Defendant had the resources necessary to prevent the Data Breach, but
22 neglected to adequately implement data security measures, despite its obligation to
23 protect member data.

24 63. Defendant could have prevented the intrusions into its systems and,
25 ultimately, the theft of Sensitive Information if Defendant had remedied the
26

27
28 ¹⁵ 2014 LexisNexis True Cost of Fraud Study, available at:
<https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last
accessed June 7, 2021).

1 deficiencies in its data security systems and adopted security measures recommended
2 by experts in the field.

3 64. As a direct and proximate result of Defendant's wrongful actions and
4 inactions, Plaintiff and Class members are now in imminent, immediate, and
5 continuing increased risk of harm from identity theft and fraud, requiring them to
6 dedicate time and resources which they otherwise would have dedicated to other life
7 demands, such as work and family, to mitigate the actual and potential impact of the
8 Data Breach on their lives.

9 65. The U.S. Department of Justice's Bureau of Justice Statistics found that
10 "among victims who had personal information used for fraudulent purposes, 29%
11 spent a month or more resolving problems," and that "resolving the problems caused
12 by identity theft [could] take more than a year for some victims."¹⁶

13 66. In the breach notification letter, Defendant made an offer of 12-months of
14 identity monitoring services to its members that had their social security numbers
15 breached but did not offer this to other people whose information was breached. This is
16 wholly inadequate to compensate Plaintiff and Class members as it fails to provide for
17 the fact victims of data breaches and other unauthorized disclosures commonly face
18 multiple years of ongoing identity theft, medical and financial fraud, and it entirely
19 fails to provide sufficient compensation for the unauthorized release and disclosure of
20 Plaintiff's and Class Employees' Sensitive Information.

21 67. As a direct result of the Defendant's failures to prevent the Data Breach,
22 Plaintiff and Class members have suffered, will suffer, and are at increased risk of
23 suffering:

- 24 a. The compromise, publication, theft and/or unauthorized use of their
25 Sensitive Information;

26
27 ¹⁶ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics,
28 *Victims of Identity Theft*, 2012, December 2013, available at:
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed June 7, 2021).

- b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;
- d. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information in its possession; and
- e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

68. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

K. Defendant's Delay in Identifying & Reporting the Breach Caused Additional Harm.

69. It is axiomatic that:

The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.¹⁷

¹⁷ *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, available at: <https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million> (last accessed June 7, 2021).

1 70. Indeed, once a data breach has occurred:

2 [o]ne thing that does matter is hearing about a data breach quickly.
3 That alerts consumers to keep a tight watch on credit card bills,
4 insurance invoices, and suspicious emails. It can prompt them to
5 change passwords and freeze credit reports. And notifying
6 officials can help them catch cybercriminals and warn other
7 businesses of emerging dangers. If consumers don't know about a
8 breach because it wasn't reported, they can't take action to protect
9 themselves (internal citations omitted).¹⁸

10 71. Although their Sensitive Information was improperly exposed on or
11 around June 11, 2021, Plaintiff and Class members were not notified of the Data Breach
12 until on or around July 2, 2021, and in many cases, including Plaintiff Chacon, over
13 seven months later, depriving Plaintiff and Class members of the ability to promptly
14 mitigate potential adverse consequences resulting from the Data Breach.

15 72. As a result of Defendant's delay in detecting and notifying consumers of
16 the Data Breach, there is an increased risk of fraud for Plaintiff and Class members.

17 CLASS ACTION ALLEGATIONS

18 73. This action has been brought and may be maintained as a class action
19 pursuant to California Code of Civil Procedure section § 382 because there is a well-
20 defined community of interest among the persons who comprise the readily
21 ascertainable class defined below and because the Plaintiff are unaware of any
22 difficulties likely to be encounter in managing this case as a class action.

23 74. The Plaintiff bring this class action on behalf of themselves and the
24 following proposed class initially defined as:

25 All residents of the State of California whose Sensitive Information
26 stored or possessed by Davaco, Inc. was subject to the Data Breach
27 announced by Davaco, Inc. on or about July 2, 2021. (the "Class").

28 ¹⁸ Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, available at: <https://www.consumerreports.org/data-theft/the-data-breach-next-door/> (last accessed June 7, 2021).

1 75. Excluded from the Class are the following individuals and/or entities:
2 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,
3 current or former employees, and any entity in which Defendant has a controlling
4 interest; all individuals who make a timely election to be excluded from this
5 proceeding using the correct protocol for opting out; any and all federal, state or local
6 governments, including but not limited to their departments, agencies, divisions,
7 bureaus, boards, sections, groups, counsels and/or subdivisions; Class Counsel; and all
8 judges assigned to hear any aspect of this litigation, as well as their staff and immediate
9 family members.

10 76. Pursuant to Rule of Court 3.765(b), Plaintiff reserve the right to modify or
11 amend the definition of the proposed Class before the Court determines whether
12 certification is appropriate.

13 77. **Numerosity:** The Class is so numerous that joinder of all members is
14 impracticable. Defendant has identified hundreds of thousands of members whose
15 Sensitive Information may have been improperly accessed in the Data Breach, and the
16 Class is apparently identifiable within Defendant's records. A precise number of class
17 members can be ascertained through appropriate discovery and from records
18 maintained by Defendant.

19 78. **Commonality and Predominance:** Questions of law and fact common to
20 the Class exist and predominate over any questions affecting only individual Class
21 members. These include but are not limited to, the following:

- 22 a. Whether Plaintiff's and the Class Employees' Sensitive Information
23 was accessed and/or viewed by one or more unauthorized persons in
24 the Data Breach alleged above;
25 b. Whether Defendant's publishing Plaintiff's and Class Employees'
26 Sensitive Information to unauthorized persons was permissible
27 without the prior written authorization of the Plaintiff or the Class
28 members;
 c. When and how Defendant should have learned and actually learned of

- 1 the Data Breach;
- 2 d. Whether Defendant's response to the Data Breach was adequate;
- 3 e. Whether Defendant owed a duty to the Class to exercise due care in
- 4 collecting, storing, safeguarding and/or obtaining their Sensitive
- 5 Information;
- 6 f. Whether Defendant breached that duty;
- 7 g. Whether Defendant implemented and maintained reasonable security
- 8 procedures and practices appropriate to the nature of storing Plaintiff's
- 9 and Class Employees' Sensitive Information;
- 10 h. Whether Defendant acted negligently in connection with the
- 11 monitoring and/or protecting of Plaintiff's and Class Employees'
- 12 Sensitive Information;
- 13 i. Whether Defendant knew or should have known that they did not
- 14 employ reasonable measures to keep Plaintiff's and Class Employees'
- 15 Sensitive Information secure and prevent loss or misuse of that
- 16 Sensitive Information;
- 17 j. Whether Defendant adequately addressed and fixed the vulnerabilities
- 18 which permitted the Data Breach to occur;
- 19 k. Whether Defendant caused Plaintiff and Class members damages;
- 20 l. Whether Defendant violated the law by failing to promptly notify
- 21 Class members their Sensitive Information was compromised;
- 22 m. Whether Plaintiff's and Class Employees' Sensitive Information were
- 23 recorded onto Defendant's internet portal on or before March 3, 2020;
- 24 n. Whether Plaintiff and Class members are entitled to actual damages,
- 25 nominal and/or statutory damages, credit monitoring, other monetary
- 26 relief, and/or equitable relief;
- 27 o. Whether Defendant violated the California Unfair Competition Law
- 28 (Business & Professions Code § 17200, *et seq.*)
- p. Whether Defendant violated the California Consumer Privacy Act
- (Cal. Civ. Code § 1798.100, *et seq.* (§ 1798.150(a)); and
- q. Information Act (Cal. Civ. Code § 56, *et seq.*).

1 79. There are no defenses of a unique nature that may be asserted against the
2 Plaintiff individually, as distinguished from the other members of the class, and the
3 relief sought is common to the class.

4 80. **Typicality**: Plaintiff's claims are typical of those of other Class members
5 because all had their Sensitive Information compromised because of the Data Breach,
6 due to Defendant's virtually identical conduct.

7 81. **Adequacy of Representation**: Plaintiff will fairly and adequately
8 represent and protect the interests of the Class members in that Plaintiff's interests are
9 aligned with the class. Plaintiff have no disabling conflicts of interest that would be
10 antagonistic to those of the other members of the Class. Plaintiff seek no relief adverse
11 to Class members. In addition, Plaintiff retained counsel experienced in data breach
12 and complex consumer class action litigation. Neither Plaintiff nor their counsel have
13 any interests which might cause them not to vigorously pursue this claim.

14 82. **Superiority**: Class action treatment is superior to all other available
15 methods for the fair and efficient adjudication of the controversy alleged herein; it will
16 permit a large number of class members to prosecute their common claims in a single
17 forum simultaneously, efficiently, and without the unnecessary duplication of
18 evidence, effort, and expense that hundreds of individual actions would require. Class
19 action treatment will permit the adjudication of relatively modest claims by certain
20 class members, who could not individually afford to litigate a complex claim against
21 large corporations, like Defendant. Further, even for those class members who could
22 afford to litigate such a claim, it would still be economically impractical and impose a
23 burden on the courts.

24 83. The prosecution of separate actions by individual members of the class
25 would create a risk of inconsistent or varying adjudications with respect to individual
26 members of the class, and a risk that any adjudications with respect to individual
27 members of the class would, as a practical matter, either be dispositive of the interests
28

1 of other members of the class not party to the adjudication or substantially impair or
2 impede their ability to protect their interests.

3 84. Class certification is also warranted for purposes of injunctive and
4 declaratory relief because the defendant has acted, or refused to act, on grounds
5 generally applicable to the class, so that final injunctive and declaratory relief are
6 appropriate with respect to the class as a whole.

7 **CAUSES OF ACTION**

8 **First Cause of Action**

9 **Negligence**

10 **(On Behalf of Plaintiff and the Class)**

11 85. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
12 herein.

13 86. Defendant's own negligent conduct created a foreseeable risk of harm to
14 Plaintiff and Class members. Defendant's negligence included, but was not limited to,
15 its failure to take the steps and opportunities to prevent the Data Breach as set forth
16 herein. Defendant's negligence also included its decision not to comply with
17 (1) industry standards, and/or best practices for the safekeeping and encrypted
18 authorized disclosure of the Sensitive Information of Plaintiff and Class members; or
19 (2) Section 5 of the FTC Act.

20 87. First, Defendant had a duty to exercise reasonable care in safeguarding,
21 securing and protecting such information from being compromised, lost, stolen,
22 misused, and/or disclosed to unauthorized parties. This duty includes, among other
23 things, designing, maintaining and testing its security protocols to ensure Sensitive
24 Information in Defendant's possession was adequately secured and protected, and that
25 employees tasked with maintaining such information were adequately trained on
26 relevant cybersecurity measures. Defendant also had a duty to put proper procedures
27 in place to prevent the unauthorized dissemination of Plaintiff's and Class Employees'
28 Sensitive Information.

1 88. As a condition of receiving services, Plaintiff and Class members were
2 obligated to provide Defendant directly, or through their respective healthcare
3 providers, with their Sensitive Information. As such, Plaintiff and the Class members
4 entrusted their Sensitive Information to Defendant with the understanding Defendant
5 would safeguard their information.

6 89. Defendant was in a position to protect against the harm suffered by
7 Plaintiff and Class members as a result of the Data Breach. However, Plaintiff and Class
8 members had no ability to protect their Sensitive Information in Defendant's
9 possession.

10 90. Defendant had full knowledge of the sensitivity of the Sensitive
11 Information, and the types of harm Plaintiff and Class members could, would, and will
12 suffer if the Sensitive Information were wrongfully disclosed.

13 91. Defendant admitted that certain email accounts containing Plaintiff's and
14 Class Employees' Sensitive Information were wrongfully compromised and accessed
15 by unauthorized third persons, and that the Data Breach occurred due to Defendant's
16 actions and/or omissions.

17 92. Plaintiff and Class members were the foreseeable and probable victims of
18 Defendant's negligent and inadequate security practices and procedures that led to the
19 Data Breach. Defendant knew or should have known of the inherent risks in collecting
20 and storing the highly valuable Sensitive Information of Plaintiff and Class members,
21 the critical importance of providing adequate security of that Sensitive Information, the
22 current cyber security risks being perpetrated, and that Defendant had inadequate
23 employee training, monitoring and education and IT security protocols in place to
24 secure the Sensitive Information of Plaintiff and Class members.

25 93. Defendant negligently, through its actions and/or omissions, and
26 unlawfully breached its duty to Plaintiff and Class members by failing to exercise
27 reasonable care in protecting and safeguarding Plaintiff's and Class Employees'
28 Sensitive Information while the data was within Defendant's possession and/or control

1 by failing to comply with and/or deviating from standard industry rules, regulations,
2 and practices at the time of the Data Breach.

3 94. The harm the Data Breach caused is the type of harm HIPAA privacy
4 laws were intended to guard against. And Plaintiff and Class members are within the
5 class of persons California privacy laws were intended to protect.

6 95. Defendant negligently failed to comply with privacy laws by failing to
7 protect against and prevent the dissemination of Plaintiff's and Class Employees'
8 Sensitive Information to unauthorized third parties.

9 96. Third, Defendant's violations of Section 5 of the FTC Act constitute
10 negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting
11 commerce," including, as interpreted and enforced by the FTC, the unfair act or
12 practice by businesses, such as Defendant, of failing to use reasonable measures to
13 protect Sensitive Information. The FTC publications and orders described above also
14 form part of the basis of Defendant's duty in this regard.

15 97. Defendant violated Section 5 of the FTC Act by failing to use reasonable
16 measures to protect Plaintiff's and Class Employees' Sensitive Information and not
17 complying with applicable industry standards, as described in detail herein.
18 Defendant's conduct was particularly unreasonable given the nature and amount of
19 Sensitive Information it required, obtained, and stored, and the foreseeable
20 consequences of a data breach including, specifically, the damages that would result to
21 Plaintiff and Class members.

22 98. Plaintiff and Class members are within the class of persons the FTC Act
23 was intended to protect.

24 99. The harm the Data Breach caused, and continues to cause, is the type of
25 harm the FTC Act was intended to guard against. The FTC pursues enforcement
26 actions against businesses, which, as a result of their failure to employ reasonable data
27 security measures and avoid unfair and deceptive practices, caused the same harm as
28 that suffered by Plaintiff and Class members.

1 100. Defendant, through its actions and/or omissions, unlawfully breached its
2 duty to Plaintiff and Class members by failing to have appropriate procedures in place
3 to detect and prevent unauthorized dissemination of Plaintiff's and Class Employees'
4 Sensitive Information.

5 101. Defendant, through its actions and/or omissions, unlawfully breached its
6 duty to adequately disclose to Plaintiff and Class members the existence and scope of
7 the Data Breach.

8 102. But for Defendant's wrongful and negligent breach of duties owed to
9 Plaintiff and Class members, Plaintiff's and Class Employees' Sensitive Information
10 would not have been compromised.

11 103. There is a temporal and close causal connection between Defendant's
12 failure to implement security measures to protect the Sensitive Information and the
13 harm suffered, and/or risk of imminent harm suffered, by Plaintiff and Class members.

14 104. As a direct and proximate result of Defendant's negligence, Plaintiff and
15 Class members have suffered, and continue to suffer, injuries and damages arising
16 from the Data Breach, including, but not limited to: damages from lost time and efforts
17 to mitigate the actual and potential impact of the Data Breach on their lives, including,
18 *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting
19 their financial institutions, closing or modifying financial and medical accounts, closely
20 reviewing and monitoring their credit reports and various accounts for unauthorized
21 activity, filing police reports, and damages from identity theft, which may take
22 months—if not years—to discover, detect, and remedy.

23 105. Additionally, as a direct and proximate result of Defendant's negligence,
24 Plaintiff and Class members have suffered, and will continue to suffer, the continued
25 risks of exposure of their Sensitive Information, which remains in Defendant's
26 possession and is subject to further unauthorized disclosures so long as Defendant fails
27 to undertake appropriate and adequate measures to protect the Sensitive Information
28 in its continued possession.

Second Cause of Action
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

106. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

107. Plaintiff and Class members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

108. Defendant owed a duty to its members, including Plaintiff and Class members, to keep their Sensitive Information confidential.

109. The unauthorized release of Sensitive Information, especially the type related to personal health information, is highly offensive to a reasonable person.

110. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Sensitive Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

111. The Data Breach constitutes an intentional interference with Plaintiff's and Class Employees' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

112. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

113. Acting with knowledge, Defendant had notice and knew its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

1 114. As a proximate result of Defendant's acts and omissions, Plaintiff and
2 Class Employees' Sensitive Information was disclosed to, and used by, third parties
3 without authorization, causing Plaintiff and Class members to suffer damages.

4 115. Unless and until enjoined and restrained by order of this Court,
5 Defendant's wrongful conduct will continue to cause great and irreparable injury to
6 Plaintiff and Class members in that the Sensitive Information maintained by Defendant
7 may be breached again — leading to further viewing, distributing, and use of updated
8 and additional Sensitive Information by unauthorized persons.

9 116. Plaintiff and Class members have no adequate remedy at law for the
10 injuries in that a judgment for monetary damages will not end the invasion of privacy
11 for Plaintiff and Class members.

12 **Third Cause of Action**
13 **Breach of Implied Contract**
14 **(On Behalf of Plaintiff and the Class)**

15 117. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
16 herein.

17 118. Plaintiff and Class members were required to provide their Sensitive
18 Information, including their names, Social Security numbers, addresses, medical record
19 numbers, dates of birth, telephone numbers, email addresses, and various health
20 related information to Defendant as a condition of their use of Defendant's services.

21 119. Plaintiff and Class members paid money, or money was paid on their
22 behalf, to Defendant in exchange for services, along with Defendant's promise to
23 protect their health information and other Sensitive Information from unauthorized
24 disclosure.

25 120. In their written privacy policies, Defendant expressly promised Plaintiff
26 and Class members that it would only disclose protected health information and other
27 Sensitive Information under certain circumstances, none of which relate to the Data
28 Breach.

1 121. Defendant promised to comply with HIPAA standards, and to make sure
2 Plaintiff's and Class Employees' health information and other Sensitive Information
3 would remain protected.

4 122. Implicit in the agreement between Plaintiff and Class members on the one
5 hand, and the Defendant on the other, regarding providing protected health
6 information and other Sensitive Information, was Defendant's obligation to: (a) use
7 such Sensitive Information for business purposes only; (b) take reasonable steps to
8 safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the
9 Sensitive Information; (d) provide Plaintiff and Class members with prompt and
10 sufficient notice of any and all unauthorized access and/or theft of their Sensitive
11 Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiff
12 and Class members from unauthorized disclosure or uses; and (f) retain the Sensitive
13 Information only under conditions that kept such information secure and confidential.

14 123. Without such implied contracts, Plaintiff and Class members would not
15 have provided their Sensitive Information to Defendant.

16 124. Plaintiff and Class members fully performed their obligations under the
17 implied contract with Defendant. However, Defendant did not.

18 125. Defendant breached the implied contracts with Plaintiff and Class
19 members by failing to:

- 20 a. Reasonably safeguard and protect Plaintiff's and Class Employees'
21 Sensitive Information, which was compromised as a result of the Data
22 Breach;
- 23 b. Ensure the confidentiality and integrity of electronic protected health
24 information Defendant created, received, maintained, and transmitted, in
25 violation of 45 C.F.R 164.306(a)(1);
- 26 c. Implement technical policies and procedures for electronic information
27 systems that maintain electronic protected health information to allow
28

1 access only to those persons or software programs that have been granted
2 access rights, in violation of 45 C.F.R 164.312(a)(1);

3 d. Implement policies and procedures to prevent, detect, contain, and
4 correct security violations, in violation of 45 C.F.R 164.308(a)(1);

5 e. Identify and respond to suspected or known security incidents;

6 f. Mitigate, to the extent practicable, harmful effects of security incidents
7 that are known to the covered entity, in violation of 45 C.F.R
8 164.308(a)(6)(ii); and

9 g. Protect against any reasonably anticipated threats or hazards to the
10 security or integrity of electronic protected health information, in
11 violation of 45 C.F.R 164.306(a)(2).

12 126. As a direct and proximate result of Defendant's breach of the implied
13 contracts, Plaintiff and Class members have suffered, and continue to suffer, injuries
14 and damages arising from the Data Breach including, but not limited to: damages from
15 lost time and effort to mitigate the actual and potential impact of the Data Breach on
16 their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting
17 agencies, contacting their financial institutions, closing or modifying financial and
18 medical accounts, closely reviewing and monitoring their credit reports and various
19 accounts for unauthorized activity, filing police reports, and damages from identity
20 theft, which may take months if not years to discover, detect, and remedy.

21 **Fourth Cause of Action**
22 **Unjust Enrichment**
23 **(On Behalf of Plaintiff and the Class)**

24 127. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
25 herein.

26 128. Plaintiff and Class members conferred a monetary benefit on Defendant.
27 Specifically, they paid money, or money was paid on their behalf, for goods and
28 services from Defendant and in so doing were required to provide Defendant with
their Sensitive Information. In exchange, Plaintiff and Class members should have

1 received from Defendant the goods and services that were the subject of the transaction
2 and have their Sensitive Information protected with adequate data security.

3 129. Defendant knew Plaintiff and Class members conferred a benefit which
4 Defendant accepted. Defendant profited from these transactions and used the Sensitive
5 Information of Plaintiff and Class members for business purposes.

6 130. The amounts Plaintiff and Class members paid for goods and services
7 were used, in part, to pay for use of Defendant's network and the administrative costs
8 of data management and security.

9 131. Under the principles of equity and good conscience, Defendant should
10 not be permitted to retain the money belonging to Plaintiff and Class members, because
11 Defendant failed to implement appropriate data management and security measures
12 mandated by industry standards.

13 132. Defendant failed to secure Plaintiff's and Class Employees' Sensitive
14 Information and, therefore, did not provide full compensation for the benefit Plaintiff
15 and Class members provided.

16 133. Defendant acquired the Sensitive Information through inequitable means
17 in that it failed to disclose its inadequate security practices, as previously alleged.

18 134. If Plaintiff and Class members knew Defendant had not reasonably
19 secured their Sensitive Information, they would not have agreed to Defendant's
20 services.

21 135. Plaintiff and Class members have no adequate remedy at law.

22 136. As a direct and proximate result of Defendant's conduct, Plaintiff and
23 Class members have suffered, and will suffer, injury, including but not limited to:
24 (a) actual identity theft; (b) the loss of the opportunity to control how their Sensitive
25 Information is used; (c) the compromise, publication, and/or theft of their Sensitive
26 Information; (d) out-of-pocket expenses associated with the prevention, detection, and
27 recovery from identity theft, and/or unauthorized use of their Sensitive Information;
28 (e) lost opportunity costs associated with efforts expended and the loss of productivity

1 addressing and attempting to mitigate the actual and future consequences of the Data
2 Breach, including but not limited to efforts spent researching how to prevent, detect,
3 contest, and recover from identity theft; (f) the continued risk to their Sensitive
4 Information, which remains in Defendant's possession and is subject to further
5 unauthorized disclosures so long as Defendant fails to undertake appropriate and
6 adequate measures to protect Sensitive Information in their continued possession; and
7 (g) future costs in terms of time, effort, and money that will be expended to prevent,
8 detect, contest, and repair the impact of the Sensitive Information compromised as a
9 result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

10 137. As a direct and proximate result of Defendant's conduct, Plaintiff and
11 Class members have suffered, and will continue to suffer, other forms of injury and/or
12 harm.

13 138. Defendant should be compelled to disgorge into a common fund or
14 constructive trust, for the benefit of Plaintiff and Class members, proceeds it unjustly
15 received from Plaintiff and Class members.

16 **Fifth Cause of Action**
17 **Breach of Fiduciary Duty**
18 **(On Behalf of Plaintiff and the Class)**

19 139. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
20 herein.

21 140. In light of their special relationship, Defendant became the guardian of
22 Plaintiff's and Class Employees' Sensitive Information. Defendant became a fiduciary,
23 created by its undertaking and guardianship of Plaintiff's and Class Employees'
24 Sensitive Information, to act primarily for the benefit of Plaintiff and Class members.
25 This duty included the obligation to safeguard Plaintiff's and Class Employees'
26 Sensitive Information, and to timely notify them in the event of a data breach.

27 141. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class
28 members upon matters within the scope of its relationship. Defendant breached its
fiduciary duties owed to Plaintiff and Class members by failing to:

- a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Employees' protected confidential information and other Sensitive Information;
- b. Timely notify and/or warn Plaintiff and Class members of the Data Breach;
- c. Ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R 164.306(a)(1);
- d. Implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);
- e. Implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R 164.308(a)(1);
- f. Identify and respond to suspected or known security incidents;
- g. Mitigate, to the extent practicable, harmful effects of security incidents known to the covered entity, in violation of 45 C.F.R 164.308(a)(6)(ii);
- h. Protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R 164.306(a)(2);
- i. Protect against any reasonably anticipated uses or disclosures of electronic protected health information not permitted under the privacy rules regarding individually identifiable confidential information, in violation of 45 C.F.R 164.306(a)(3);
- j. Effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of

1 protected confidential information, in violation of 45 C.F.R 164.530(b) and
2 45 C.F.R 164.308(a)(5);

- 3 k. Design, implement, and enforce policies and procedures establishing
4 physical and administrative safeguards to reasonably safeguard protected
5 confidential information, in compliance with 45 C.F.R 164.530(c); and
6 l. Otherwise failing to safeguard Plaintiff's and Class Employees' Sensitive
7 Information.

8 142. As a direct and proximate result of Defendant's breaches of its fiduciary
9 duties, Plaintiff and Class members have suffered, and will suffer, injury, including but
10 not limited to: (a) actual identity theft; (b) the loss of the opportunity to control how
11 their Sensitive Information is used; (c) the compromise, publication, and/or theft of
12 their Sensitive Information; (d) out-of-pocket expenses associated with the prevention,
13 detection, and recovery from identity theft and/or unauthorized use of their Sensitive
14 Information; (e) lost opportunity costs associated with the effort expended and the loss
15 of productivity addressing and attempting to mitigate the actual and future
16 consequences of the Data Breach, including but not limited to efforts spent researching
17 how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to
18 their Sensitive Information, which remain in Defendant's possession and is subject to
19 further unauthorized disclosures so long as Defendant fails to undertake appropriate
20 and adequate measures to protect its Employees' Sensitive Information in continued
21 possession; and (g) future costs in terms of time, effort, and money that will be
22 expended to prevent, detect, contest, and repair the impact of the Sensitive Information
23 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff
24 and Class members.

25 143. As a direct and proximate result of Defendant's breach of its fiduciary
26 duty, Plaintiff and Class members have suffered, and will continue to suffer, other
27 forms of injury and/or harm, and other economic and non-economic losses.
28

Sixth Cause of Action
Breach of Confidence
(On Behalf of Plaintiff and the Class)

144. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

145. At all times during Plaintiff's and Class Employees' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Employees' Sensitive Information that Plaintiff and Class members provided to Defendant.

146. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class Employees' Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

147. Plaintiff and Class members provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

148. Plaintiff and Class members also provided their Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including Defendant's employees' email accounts.

149. Defendant required and voluntarily received, in confidence, Plaintiff's and Class Employees' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

150. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Employees' Sensitive Information, Plaintiff's and Class Employees'

1 Sensitive Information was disclosed to, and misappropriated by, unauthorized third
2 parties beyond Plaintiff's and Class Employees' confidence, and without their express
3 permission.

4 151. As a direct and proximate cause of Defendant's actions and/or omissions,
5 Plaintiff and Class members have suffered, and will continue to suffer damages.

6 152. But for Defendant's disclosure of Plaintiff's and Class Employees'
7 Sensitive Information in violation of the parties' understanding of confidence,
8 Plaintiff's and Class Employees' Sensitive Information would not have been
9 compromised, stolen, viewed, accessed, and used by unauthorized third parties.

10 Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and
11 Class Employees' Sensitive Information, as well as the resulting damages.

12 153. The injury and harm Plaintiff and Class members suffered, and continue
13 to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure
14 of Plaintiff's and Class Employees' Sensitive Information. Defendant knew its
15 computer systems and technologies for accepting and securing Plaintiff's and Class
16 Employees' Sensitive Information had numerous security and other vulnerabilities
17 placing Plaintiff's and Class Employees' Sensitive Information in jeopardy.

18 154. As a direct and proximate result of Defendant's breaches of confidence,
19 Plaintiff and Class members have suffered and will suffer injury, including but not
20 limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of
21 their Sensitive Information; (c) out-of-pocket expenses associated with the prevention,
22 detection, and recovery from identity theft and/or unauthorized use of their Sensitive
23 Information; (d) lost opportunity costs associated with effort expended and the loss of
24 productivity addressing and attempting to mitigate the actual and future consequences
25 of the Data Breach, including but not limited to efforts spent researching how to
26 prevent, detect, contest, and recover from identity theft; (e) the continued risk to their
27 Sensitive Information, which remains in Defendant's possession and is subject to
28 further unauthorized disclosures so long as Defendant fails to undertake appropriate

1 and adequate measures to protect the Sensitive Information in its continued possession;
2 (f) future costs in terms of time, effort, and money that will be expended as result of the
3 Data Breach for the remainder of the lives of Plaintiff and Class members; and (g) the
4 diminished value of Defendant's services they received.

5 155. As a direct and proximate result of Defendant's breaches of its fiduciary
6 duties, Plaintiff and Class members have suffered and will continue to suffer other
7 forms of injury and/or harm, and other economic and non-economic losses.

8 **Seventh Cause of Action**
9 **Violation of the California Unfair Competition Law,**
10 **Cal. Bus. & Prof. Code § 17200, *et seq.*--Unfair Business Practices**
11 **(On Behalf of Plaintiff and the Class)**

12 156. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
13 herein.

14 157. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq.*, by engaging in
15 unlawful, unfair, or fraudulent business acts and practices, and unfair, deceptive,
16 untrue, or misleading advertising that constitute acts of "unfair competition" as
17 defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to
18 Plaintiff and Class members.

19 158. Defendant engaged in unlawful acts and practices with respect to the
20 services by establishing the sub-standard security practices and procedures described
21 herein; by soliciting and collecting Plaintiff's and Class Employees' Sensitive
22 Information with knowledge the information would not be adequately protected; and
23 by storing Plaintiff's and Class Employees' Sensitive Information in an unsecure
24 electronic environment in violation of California's data breach statute, Cal. Civ. Code §
25 1798.81.5, which require Defendant to take reasonable methods of safeguarding the
26 Sensitive Information of Plaintiff and Class members.

27 159. In addition, Defendant engaged in unlawful acts and practices by failing
28 to disclose the Data Breach in a timely and accurate manner, contrary to the duties
imposed by Cal. Civ. Code § 1798.82.

1 160. As a direct and proximate result of Defendant's unlawful practices and
 2 acts, Plaintiff and Class members were injured and lost money or property, including
 3 but not limited to the price received by Defendant for the services, the loss of Plaintiff's
 4 and Class Employees' legally protected interest in the confidentiality and privacy of
 5 their Sensitive Information, nominal damages, and additional losses as described
 6 herein.

7 161. Defendant knew or should have known Defendant's computer systems
 8 and data security practices were inadequate to safeguard Plaintiff's and Class
 9 Employees' Sensitive Information and that the risk of a data breach or theft was highly
 10 likely. Defendant's actions in engaging in the above-named unlawful practices and acts
 11 were negligent, knowing, and willful, and/or wanton and reckless with respect to the
 12 rights of Plaintiff and Class members.

13 162. Plaintiff, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code
 14 § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class members
 15 of money or property Defendant may have acquired by means of Defendant's
 16 unlawful, and unfair business practices, restitutionary disgorgement of all monies that
 17 accrued to Defendant because of Defendant's unlawful and unfair business practices,
 18 declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5),
 19 and injunctive or other equitable relief.

20 **Eighth Cause of Action**
 21 **Violation of California's Information Practices Act of 1977**
 22 **Cal. Civ. Code § 1798, *et seq.***
 (On Behalf of Plaintiff and the Class)

23 163. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
 24 herein.

25 164. Defendant was legally obligated to "establish appropriate and reasonable
 26 administrative, technical, and physical safeguards to ensure compliance with the
 27 [Information Practices Act of 1977], to ensure the security and confidentiality of
 28

1 records, and to protect against anticipated threats or hazards to their security or
2 integrity which could result in any injury.” (Cal. Civ. Code § 1798.21.)

3 165. Defendant failed to establish appropriate and reasonable administrative,
4 technical, and physical safeguards to ensure compliance with the Information Practices
5 Act of 1977 regarding Plaintiff’s and Class Employees’ Sensitive Information.

6 166. Defendant failed to ensure the security and confidentiality of records
7 containing Plaintiff’s and Class Employees’ Sensitive Information.

8 167. Defendant failed to protect against anticipated threats and hazards to the
9 security and integrity of records containing Plaintiff’s and Class Employees’ Sensitive
10 Information.

11 168. As a result of these failures, Plaintiff and Class members have suffered,
12 and will continue to suffer, economic damages and other injury and actual harm in the
13 form of, inter alia, (i) an imminent, immediate and continuing increased risk of identity
14 theft, identify fraud, and medical fraud risks justifying expenditures for protective and
15 remedial services for which they are entitled to compensation, (ii) invasion of privacy,
16 (iii) breach of the confidentiality of their Sensitive Information, (iv) deprivation of the
17 value of their private and Sensitive Information, for which there is a well-established
18 national and international market, and/or (v) the financial and temporal cost of
19 monitoring their credit, monitoring their financial accounts, and mitigating their
20 damages.

21 169. Plaintiff and Class members are also entitled to injunctive relief under
22 California Civil Code § 1798.47.

23 **Ninth Cause of Action**
24 **Violation of California Consumer Records Act (“CCRA”)**
25 **Cal. Civ. Code § 1798.80, *et seq.***
26 **(On Behalf of Plaintiff and the Class)**

27 170. Plaintiff incorporate by reference the prior paragraphs as if fully set forth
28 herein.

1 171. Section 1798.2 of the California Civil Code requires any “person or
2 business that conducts business in California, and that owns or licenses computerized
3 data that includes personal information” to “disclose any breach of the security of the
4 system following discovery or notification of the breach in the security of the data to
5 any resident of California whose unencrypted personal information was, or is
6 reasonably believed to have been, acquired by an unauthorized person.” Under section
7 1798.82, the disclosure “shall be made in the most expedient time possible and without
8 unreasonable delay.”

9 172. The CCRA further provides: “Any person or business that maintains
10 computerized data that includes personal information that the person or business does
11 not own shall notify the owner or licensee of the information of any breach of the
12 security of the data immediately following discovery, if the personal information was,
13 or is reasonably believed to have been, acquired by an unauthorized person.” (Cal. Civ.
14 Code § 1798.82(b).)

15 173. Any person or business required to issue a security breach notification
16 under the CCRA shall meet the following requirements:

- 17 a. The security breach notification shall be written in plain language;
- 18 b. The security breach notification shall include, at a minimum, the
19 following information:
 - 20 i. The name and contact information of the reporting person or
21 business subject to this section;
 - 22 ii. A list of the types of personal information that were or are
23 reasonably believed to have been the subject of a breach;
 - 24 iii. If the information is possible to determine at the time the notice
25 is provided, then any of the following:
 - 26 1. The date of the breach;
 - 27 2. The estimated date of the breach; or
 - 28 3. The date range within which the breach occurred. The
notification shall also include the date of the notice.

- iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

174. The Data Breach described herein constituted a "breach of the security system" of Defendant.

175. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class members about the Data Breach, affecting their Personal and Medical Information, after Defendant knew the Data Breach had occurred.

176. Defendant failed to disclose to Plaintiff and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendant knew or reasonably believed such information had been compromised.

177. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

178. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and Class members would impede its investigation.

179. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members were deprived of prompt notice of the Data Breach, and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of

1 the damages suffered by Plaintiff and Class members because their stolen information
2 would have had less value to identity thieves.

3 180. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff
4 and Class members suffered incrementally increased damages separate and distinct
5 from those simply caused by the Data Breach itself.

6 181. Plaintiff and Class members seek all remedies available under Cal. Civ.
7 Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and
8 Class members as alleged above and equitable relief.

9 **PRAYER FOR RELIEF**

10 **WHEREFORE**, Plaintiff, on behalf of themselves and all Class members, request
11 judgment against the Defendant, and that the Court grant the following:

- 12 A. An order certifying the Class as defined herein, and appointing
13 Plaintiff and their Counsel to represent the Class;
- 14 B. Granting injunctive relief requested by Plaintiff, including but not
15 limited to, injunctive and other equitable relief as is necessary to
16 protect the interests of Plaintiff and Class members, including but not
17 limited to an order:
- 18 i. prohibiting Defendant from engaging in the wrongful and unlawful
19 acts described herein,
- 20 ii. requiring Defendant to protect, including through encryption, all data
21 collected through the course of its business in accordance with all
22 applicable regulations, industry standards, and federal, state or local
23 laws,
- 24 iii. requiring Defendant to delete, destroy, and purge the personal
25 information of Plaintiff and Class members unless Defendant can
26 provide to the Court reasonable justification for the retention and use
27 of such information when weighed against the privacy interests of
28 Plaintiff and Class members,

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiff and Class Employees' personal information,
- v. prohibiting Defendant from maintaining Plaintiff's and Class Employees' personal information on a cloud-based database,
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,
- ix. requiring Defendant to conduct regular database scanning and securing checks,
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiff and Class members,
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal information,
 - xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,
 - xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,
 - xv. requiring Defendant to design, maintain, and test its computer systems to ensure that PI in its possession is adequately secured and protected,
 - xvi. requiring Defendant disclose any future data disclosures in a timely and accurate manner; and
 - xvii. requiring Defendant to provide ongoing credit monitoring and identity theft repair services to Class members.
- C. An award of compensatory, statutory, and nominal in an amount to be determined;
 - D. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
 - E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

1 F. Such other and further relief as this Court may deem just and proper.

2 **DEMAND FOR JURY TRIAL**

3 Plaintiff hereby demand a trial by jury.

4
5
6 Date: August 9, 2021

Respectfully submitted,
SWIGART LAW GROUP, APC

7
8
9

Joshua B. Swigart

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Joshua B. Swigart (SBN 225557) Swigart Law Group, APC. 2221 Camino Del Rio S. Ste. 308, San Diego, CA 92108		FOR COURT USE ONLY
TELEPHONE NO.: 866-219-3343	FAX NO. (Optional):	
ATTORNEY FOR (Name): Charles Chacon, et al.		
SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE STREET ADDRESS: 4050 Main Street MAILING ADDRESS: CITY AND ZIP CODE: Riverside, CA 92501 BRANCH NAME:		
CASE NAME: Chacon, et al. v. Davaco, Inc.		
CIVIL CASE COVER SHEET <input checked="" type="checkbox"/> Unlimited (Amount demanded exceeds \$25,000) <input type="checkbox"/> Limited (Amount demanded is \$25,000)		Complex Case Designation <input type="checkbox"/> Counter <input type="checkbox"/> Joinder Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)
		CASE NUMBER: CVRI2103666
		JUDGE: DEPT.:

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

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

Auto Tort <input type="checkbox"/> Auto (22) <input type="checkbox"/> Uninsured motorist (46) Other P/DP/WD (Personal Injury/Property Damage/Wrongful Death) Tort <input type="checkbox"/> Asbestos (04) <input type="checkbox"/> Product liability (24) <input type="checkbox"/> Medical malpractice (45) <input type="checkbox"/> Other P/DP/WD (23) Non-P/DP/WD (Other) Tort <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 type="checkbox"/> Other non-P/DP/WD tort (35) Employment <input type="checkbox"/> Wrongful termination (36) <input type="checkbox"/> Other employment (15)	Contract <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) Real Property <input type="checkbox"/> Eminent domain/Inverse condemnation (14) <input type="checkbox"/> Wrongful eviction (33) <input type="checkbox"/> Other real property (26) Unlawful Detainer <input type="checkbox"/> Commercial (31) <input type="checkbox"/> Residential (32) <input type="checkbox"/> Drugs (38) Judicial Review <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)	Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400-3.403) <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) Enforcement of Judgment <input type="checkbox"/> Enforcement of judgment (20) Miscellaneous Civil Complaint <input type="checkbox"/> RICO (27) <input checked="" type="checkbox"/> Other complaint (not specified above) (42) Miscellaneous Civil Petition <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. ☐ Large number of separately represented parties d. ☒ Large number of witnesses
- b. ☐ Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve e. ☐ Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
- c. ☒ Substantial amount of documentary evidence f. ☐ 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):
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-015.)

Date: August 13, 2021

Joshua B. Swigart

(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 (32)
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

SUM-100

SUMMONS (CITACION JUDICIAL)

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

NOTICE TO DEFENDANT: (AVISO AL DEMANDADO):

Davaco, Inc.

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

Charles Chacon, 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), 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), the California Courts Online Self-Help Center (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), 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), en el Centro de Ayuda de las Cortes de California, (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 o 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):

Riverside Superior Court; 4050 Main Street, Riverside, CA 92501

CASE NUMBER: (Número del Caso):

CVRI 21 03666

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):

Joshua B. Swigart, 2221 Camino Del Rio S. Ste. 308, San Diego, CA 92108

DATE:
(Fecha) 8/13/2021

Clerk, by
(Secretario)

, Deputy
(Adjunto)

(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

- RI-CI032

Page 1 of 1
Local Rule 3117
riverside.courts.ca.gov/localrules/localrules.shtml



SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE
www.riverside.courts.ca.gov

Self-represented parties: <https://www.riverside.courts.ca.gov/SelfHelp/self-help.php>

**ALTERNATIVE DISPUTE RESOLUTION (ADR) –
INFORMATION PACKAGE**

***** THE PLAINTIFF MUST SERVE THIS INFORMATION PACKAGE
ON EACH PARTY WITH THE COMPLAINT. *****

What is ADR?

Alternative Dispute Resolution (ADR) is a way of solving legal disputes without going to trial. The main types are mediation, arbitration, and settlement conferences.

Advantages of ADR:

- ✓ Faster: ADR can be done in a 1-day session within months after filing the complaint.
- ✓ Less expensive: Parties can save court costs and attorneys' and witness fees.
- ✓ More control: Parties choose their ADR process and provider.
- ✓ Less stressful: ADR is done informally in private offices, not public courtrooms.

Disadvantages of ADR:

- ✓ No public trial: Parties do not get a decision by a judge or jury.
- ✓ Costs: Parties may have to pay for both ADR and litigation.

Main Types of ADR:

Mediation: In mediation, the mediator listens to each person's concerns, helps them evaluate the strengths and weaknesses of their case, and works with them to create a settlement agreement that is acceptable to everyone. If the parties do not wish to settle the case, they go to trial.

Mediation may be appropriate when the parties:

- ✓ want to work out a solution but need help from a neutral person; or
- ✓ have communication problems or strong emotions that interfere with resolution; or
- ✓ have a continuing business or personal relationship.

Mediation is not appropriate when the parties:

- ✓ want their public "day in court" or a judicial determination on points of law or fact;
- ✓ lack equal bargaining power or have a history of physical/emotional abuse.

Arbitration: Arbitration is less formal than trial, but like trial, the parties present evidence and arguments to the person who decides the outcome. In "binding" arbitration the arbitrator's decision is final; there is no right to trial. In "non-binding" arbitration, any party can request a trial after the arbitrator's decision. The court's mandatory Judicial Arbitration program is non-binding.

Arbitration may be appropriate when the parties:

- ⚡ want to avoid trial, but still want a neutral person to decide the outcome of the case.

Arbitration is not appropriate when the parties:

- ⚡ do not want to risk going through both arbitration and trial (Judicial Arbitration)
- ⚡ do not want to give up their right to trial (binding arbitration)

Settlement Conferences: Settlement conferences are similar to mediation, but the settlement officer usually tries to negotiate an agreement by giving strong opinions about the strengths and weaknesses of the case, its monetary value, and the probable outcome at trial. Settlement conferences often involve attorneys more than the parties and often take place close to the trial date.

RIVERSIDE COUNTY SUPERIOR COURT ADR REQUIREMENTS

ADR Information and forms are posted on the ADR website:
<https://www.riverside.courts.ca.gov/Divisions/ADR/ADR.php>

General Policy:

Parties in most general civil cases are expected to participate in an ADR process before requesting a trial date and to participate in a settlement conference before trial. (Local Rule 3200)

Court-Ordered ADR:

Certain cases valued at under \$50,000 may be ordered to judicial arbitration or mediation. This order is usually made at the Case Management Conference. See the "Court-Ordered Mediation Information Sheet" on the ADR website for more information.

Private ADR (for cases not ordered to arbitration or mediation):

Parties schedule and pay for their ADR process without Court involvement. Parties may schedule private ADR at any time; there is no need to wait until the Case Management Conference. See the "Private Mediation Information Sheet" on the ADR website for more information.

BEFORE THE CASE MANAGEMENT CONFERENCE (CMC), ALL PARTIES MUST:

1. Discuss ADR with all parties at least 30 days before the CMC. Discuss:
 - ⚡ Your preferences for mediation or arbitration.
 - ⚡ Your schedule for discovery (getting the information you need) to make good decisions about settling the case at mediation or presenting your case at an arbitration.
2. File the attached "Stipulation for ADR" along with the Case Management Statement, if all parties can agree.
3. Be prepared to tell the judge your preference for mediation or arbitration and the date when you could complete it.

(Local Rule 3218)

RIVERSIDE COUNTY ADR PROVIDERS INCLUDE:

- ⚡ The Court's Civil Mediation Panel (available for both Court-Ordered Mediation and Private Mediation). See <https://adr.riverside.courts.ca.gov/Home/CivilMedPanel> or ask for the list in the civil clerk's office, attorney window.
- ⚡ Riverside County ADR providers funded by DRPA (Dispute Resolution Program Act):
 - Dispute Resolution Service (DRS) Riverside County Bar Association: (951) 682-1015
 - Dispute Resolution Center, Community Action Partnership (CAP): (951) 955-4900
 - Chapman University School of Law Mediation Clinic (services only available at the court)

SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE

☐ **BLYTHE** 265 N. Broadway, Blythe, CA 92225 ☐ **MURRIETA** 30755-D Auld Rd., Murrieta, CA 92563
☐ **CORONA** 505 S. Buena Vista, Rm. 201, Corona, CA 92882 ☐ **PALM SPRINGS** 3255 Tahquitz Canyon Way, Palm Springs, CA 92262
☐ **MORENO VALLEY** 13800 Heacock St. #D201, Moreno Valley, CA 92553 ☐ **RIVERSIDE** 4050 Main St., Riverside, CA 92501

RI-ADR001

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar Number and Address)	FOR COURT USE ONLY
TELEPHONE NO: _____ FAX NO. (Optional): _____ E-MAIL ADDRESS (Optional): _____ ATTORNEY FOR (Name): _____	CASE NUMBER: _____ CASE MANAGEMENT CONFERENCE DATE(S): _____
PLAINTIFF/PETITIONER: _____	
DEFENDANT/RESPONDENT: _____	
STIPULATION FOR ALTERNATIVE DISPUTE RESOLUTION (ADR) (CRC 3.2221; Local Rule, Title 3, Division 2)	

Court-Ordered ADR:

Eligibility for Court-Ordered Mediation or Judicial Arbitration will be determined at the Case Management Conference. If eligible, the parties agree to participate in:

☐ Mediation ☐ Judicial Arbitration (non-binding)

Private ADR:

If the case is not eligible for Court-Ordered Mediation or Judicial Arbitration, the parties agree to participate in the following ADR process, which they will arrange and pay for without court involvement:

☐ Mediation ☐ Judicial Arbitration (non-binding)

☐ Binding Arbitration ☐ Other (describe): _____

Proposed date to complete ADR: _____

SUBMIT THIS FORM ALONG WITH THE CASE MANAGEMENT STATEMENT.

_____ (PRINT NAME OF PARTY OR ATTORNEY) <input type="checkbox"/> Plaintiff <input type="checkbox"/> Defendant	_____ (SIGNATURE OF PARTY OR ATTORNEY)	_____ (DATE)
_____ (PRINT NAME OF PARTY OR ATTORNEY) <input type="checkbox"/> Plaintiff <input type="checkbox"/> Defendant	_____ (SIGNATURE OF PARTY OR ATTORNEY)	_____ (DATE)
_____ (PRINT NAME OF PARTY OR ATTORNEY) <input type="checkbox"/> Plaintiff <input type="checkbox"/> Defendant	_____ (SIGNATURE OF PARTY OR ATTORNEY)	_____ (DATE)
_____ (PRINT NAME OF PARTY OR ATTORNEY) <input type="checkbox"/> Plaintiff <input type="checkbox"/> Defendant	_____ (SIGNATURE OF PARTY OR ATTORNEY)	_____ (DATE)

SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE**Branch Name:** Historic Court House**Mailing Address:** 4050 Main Street**City, State and Zip Code:** Riverside CA 92501**SHORT TITLE:** CHACON vs DAVACO, INC.**CASE NUMBER:**

CVRI2103666

NOTICE OF CONFIRMATION OF ELECTRONIC FILING

The Electronic Filing described by the below summary data was reviewed and accepted by the Superior Court of California, County of RIVERSIDE. In order to process the filing, the fee shown was assessed.

Electronic Filing Summary Data

Electronically Submitted By: Green Filing RV

Reference Number: 5436923_1

Submission Number: 21RSCR00018304

Court Received Date: 08/13/2021

Court Received Time: 3:56 pm

Case Number: CVRI2103666

Case Title: CHACON vs DAVACO, INC.

Location: Historic Court House

Case Type: Civil

Case Category: Unlimited Civil Other Complaint

Jurisdictional Amount: Amount over \$25,000

Notice Generated Date: 08/17/2021

Notice Generated Time: 4:08 pm

Documents Electronically Filed/Received**Status**

Complaint for Other Complaint (Over \$25,000)

Accepted

Summons Issued and Filed

Accepted

Civil Case Cover Sheet (Complex) (CM-010)

Accepted

Certificate of Counsel.

Accepted

ADR Packet

Accepted

NOTICE OF CONFIRMATION OF FILING

Comments

Submitter's Comments:

Clerk's Comments:

Electronic Filing Service Provider Information

Service Provider: Green Filing RV

Contact: Green Filing RV

Phone: (801) 448-7268



Superior Court of California
 County of Riverside
 4050 Main Street
 RIVERSIDE, CA 92501

Receipt EFM20210817-00656.1

Cashier RSC

Payor:

Date: 08/17/2021

Time 4:08 PM

CASE # CVRI2102848

CHACON vs DAVACO, INC.

Line Item: Unlimited complaint or other first paper in unlimited civil case amount over \$25,000 including UD over \$25K, petition for writ of review, mandate, or prohibition; petition for a decree of change of name or gender (GC70611)	450.00
---	--------

Line Item: Additional fee for case designated as complex - Plaintiff (GC70616A)	1,000.00
---	----------

Case	1,450.00
-------------	----------

Total	1,450.00
--------------	----------

Change:	0.00
----------------	------

Cashier Comment: 21RSCR00018304

Current Balance:	0.00
-------------------------	------

KEEP THIS RECEIPT FOR YOUR RECORDS

Receipt must be provided as proof of payment in case of a dispute

SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE

Historic Court House
4050 Main Street, Riverside, CA 92501

Case Number: CVRI2103666

Case Name: CHACON vs DAVACO, INC.

NOTICE OF DEPARTMENT ASSIGNMENT



The above entitled case is assigned to the Honorable Sunshine Sykes in Department 6 for All Purposes.

Any disqualification pursuant to CCP section 170.6 shall be filed in accordance with that section.

The court follows California Rules of Court, Rule 3.1308(a)(1) for tentative rulings (see Riverside Superior Court Local Rule 3316). Tentative Rulings for each law and motion matter are posted on the internet by 3:00 p.m. on the court day immediately before the hearing at <http://riverside.courts.ca.gov/tentativerulings.shtml>. If you do not have internet access, you may obtain the tentative ruling by telephone at (760) 904-5722.

To request oral argument, you must (1) notify the judicial secretary at (760) 904-5722 and (2) inform all other parties, no later than 4:30 p.m. the court day before the hearing. If no request for oral argument is made by 4:30 p.m., the tentative ruling will become the final ruling on the matter effective the date of the hearing.

The filing party shall serve a copy of this notice on all parties.

	Interpreter services are available upon request. If you need an interpreter, please complete and submit the online Interpreter Request Form (https://riverside.courts.ca.gov/Divisions/InterpreterInfo/ri-in007.pdf) or contact the clerk's office and verbally request an interpreter. All requests must be made in advance with as much notice as possible, and prior to the hearing date in order to secure an interpreter.
	Assistive listening systems, computer-assisted real time captioning, or sign language interpreter services are available upon request if at least 5 days notice is provided. Contact the Office of the ADA Coordinator by calling (951) 777-3023 or TDD (951) 777-3769 between 8:00 am and 4:30 pm or by emailing ADA@riverside.courts.ca.gov to request an accommodation. A <i>Request for Accommodations by Persons With Disabilities and Order</i> (form MC-410) must be submitted when requesting an accommodation. (Civil Code section 54.8.)

Dated: 08/17/2021

W. SAMUEL HAMRICK JR.,
Court Executive Officer/Clerk of Court

by:



D. Brown, Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE

Historic Court House
4050 Main Street, Riverside, CA 92501

Case Number: CVRI2103666

Case Name: CHACON vs DAVACO, INC.

DAVACO, INC.

NOTICE OF CASE MANAGEMENT CONFERENCE



The Case Management Conference is scheduled as follows:

Hearing Date	Hearing Time	Department
10/18/2021	8:30 AM	Department 6
Location of Hearing: 4050 Main Street, Riverside, CA 92501		

No later than 15 calendar days before the date set for the case management conference or review, each party must file a case management statement and serve it on all other parties in the case. CRC, Rule 3.725.

The plaintiff/cross-complainant shall serve a copy of this notice on all defendants/cross-defendants who are named or added to the complaint and file proof of service.

Any disqualification pursuant to CCP Section 170.6 shall be filed in accordance with that section.

	Interpreter services are available upon request. If you need an interpreter, please complete and submit the online Interpreter Request Form (https://riverside.courts.ca.gov/Divisions/InterpreterInfo/ri-in007.pdf) or contact the clerk's office and verbally request an interpreter. All requests must be made in advance with as much notice as possible, and prior to the hearing date in order to secure an interpreter.
	Assistive listening systems, computer-assisted real time captioning, or sign language interpreter services are available upon request if at least 5 days notice is provided. Contact the Office of the ADA Coordinator by calling (951) 777-3023 or TDD (951) 777-3769 between 8:00 am and 4:30 pm or by emailing ADA@riverside.courts.ca.gov to request an accommodation. A <i>Request for Accommodations by Persons With Disabilities and Order</i> (form MC-410) must be submitted when requesting an accommodation. (Civil Code section 54.8.)

CERTIFICATE OF MAILING

I certify that I am currently employed by the Superior Court of California, County of Riverside, and that I am not a party to this action or proceeding. In my capacity, I am familiar with the practices and procedures used in connection with the mailing of correspondence. Such correspondence is deposited in the outgoing mail of the Superior Court. Outgoing mail is delivered to and mailed by the United States Postal Service, postage prepaid, the same day in the ordinary course of business. I certify that I served a copy of the Notice of Case Management Conference on this date, by depositing said copy as stated above.

Dated: 08/17/2021

W. SAMUEL HAMRICK JR.,
Court Executive Officer/Clerk of Court

by: NO SIGNATURE ON FILE
J. EFM, Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF RIVERSIDE

Historic Court House
4050 Main Street, Riverside, CA 92501

Case Number: CVRI2103666

Case Name: CHACON vs DAVACO, INC.

CHARLES CHACON

NOTICE OF CASE MANAGEMENT CONFERENCE



The Case Management Conference is scheduled as follows:

Hearing Date	Hearing Time	Department
10/18/2021	8:30 AM	Department 6
Location of Hearing: 4050 Main Street, Riverside, CA 92501		

No later than 15 calendar days before the date set for the case management conference or review, each party must file a case management statement and serve it on all other parties in the case. CRC, Rule 3.725.

The plaintiff/cross-complainant shall serve a copy of this notice on all defendants/cross-defendants who are named or added to the complaint and file proof of service.

Any disqualification pursuant to CCP Section 170.6 shall be filed in accordance with that section.

	Interpreter services are available upon request. If you need an interpreter, please complete and submit the online Interpreter Request Form (https://riverside.courts.ca.gov/Divisions/InterpreterInfo/ri-in007.pdf) or contact the clerk's office and verbally request an interpreter. All requests must be made in advance with as much notice as possible, and prior to the hearing date in order to secure an interpreter.
	Assistive listening systems, computer-assisted real time captioning, or sign language interpreter services are available upon request if at least 5 days notice is provided. Contact the Office of the ADA Coordinator by calling (951) 777-3023 or TDD (951) 777-3769 between 8:00 am and 4:30 pm or by emailing ADA@riverside.courts.ca.gov to request an accommodation. A <i>Request for Accommodations by Persons With Disabilities and Order</i> (form MC-410) must be submitted when requesting an accommodation. (Civil Code section 54.8.)

CERTIFICATE OF MAILING

I certify that I am currently employed by the Superior Court of California, County of Riverside, and that I am not a party to this action or proceeding. In my capacity, I am familiar with the practices and procedures used in connection with the mailing of correspondence. Such correspondence is deposited in the outgoing mail of the Superior Court. Outgoing mail is delivered to and mailed by the United States Postal Service, postage prepaid, the same day in the ordinary course of business. I certify that I served a copy of the Notice of Case Management Conference on this date, by depositing said copy as stated above.

Dated: 08/17/2021

W. SAMUEL HAMRICK JR.,
Court Executive Officer/Clerk of Court

by: NO SIGNATURE ON FILE
J. EFM, Deputy Clerk

Notice has been printed for the following Firm/Attorneys or Parties: CVRI2103666

DAVACO, INC.

CHACON, CHARLES

EXHIBIT B

Joshua B. Swigart (SBN 225557)
Josh@SwigartLawGroup.com
SWIGART LAW GROUP, APC
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
P: 866-219-3343
F: 866-219-8344

Attorneys for Plaintiff and Putative Class

**SUPERIOR COURT FOR THE STATE OF CALIFORNIA
COUNTY OF RIVERSIDE**

CHARLES CHACON, individually and)
on behalf of all others similarly situated,)
Claimant,)
vs.)
DAVACO, INC.,)
Respondent.)

Case No: CVRI2103666

**PROOF OF SERVICE OF
SUMMONS AND COMPLAINT**

AFFIDAVIT OF SERVICE

Case: CVR12103666	Court: SUPERIOR COURT OF THE STATE OF CALIFORNIA	County: RIVERSIDE , CA	Job: 6024531 (081821-1)
Plaintiff / Petitioner: CHARLES CHACON, individually and on behalf of all others similarly situated		Defendant / Respondent: DAVACO, INC	
Received by: DALLAS CIVIL PROCESS AND LEGAL SUPPORT SERVICE		For: Swigart Law Group, APC	
To be served upon: DAVACO, INC			

I, BILL BOYETT, being duly sworn, depose and say: I am over the age of 18 years and not a party to this action, and that within the boundaries of the state where service was effected, I was authorized by law to make service of the documents and informed said person of the contents herein

Recipient Name / Address: DAVACO, INC, 4050 Valley View Ln 150, IRVING, TX 75038

Manner of Service: Authorized, Aug 20, 2021, 1:15 pm CDT

Documents: ALTERNATIVE DISPUTE RESOLUTION (ADR), STIPULATION FOR ALTERNATIVE DISPUTE RESOLUTION (ADR), CERTIFICATE OF COUNSEL, CLASS ACTION COMPLAINT, NOTICE OF DEPARTMENT ASSIGNMENT, NOTICE OF CONFIRMATION OF ELECTRONIC FILING, RECEIPT, SUMMONS (Received Aug 17, 2021 at 6:21pm CDT)

Additional Comments:

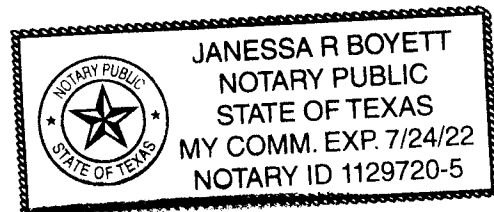
1) Successful Attempt: Aug 20, 2021, 1:15 pm CDT at 4050 Valley View Ln 150, IRVING, TX 75038 received by DAVACO, INC. Other: Kayla Messner c/o Melissa Maner at DAVACO, INC.;

Bill Boyett
BILL BOYETT *8-21-21* Date

DALLAS CIVIL PROCESS AND LEGAL SUPPORT SERVICE
113 LAKEVIEW DR.
SUNNYVALE, TX 75182
214-202-6733

Subscribed and sworn to before me by the affiant who is personally known to me.

Janessa R Boyett
Notary Public
8-21-21 Date *7-24-22* Commission Expires



1 Vassi Iliadis (Bar No. 296382)
2 Brhan Ahmed (Bar No. 328157)
3 **HOGAN LOVELLS US LLP**
4 1999 Avenue of the Stars, Suite 1400
5 Los Angeles, California 90067
6 Telephone: (310) 785-4600
7 Facsimile: (310) 785-4601
8 vassi.iliadis@hoganlovells.com
9 brhan.ahmed@hoganlovells.com

6 Michelle A. Kisloff
7 (*pro hac vice application to be submitted*)
8 **HOGAN LOVELLS US LLP**
9 Columbia Square
10 555 Thirteenth Street, NW
11 Washington, D.C. 20004
12 Telephone: 202.637.5600
13 Facsimile: 202.637.5910
14 michelle.kisloff@hoganlovells.com

11 *Attorneys for Defendant*
12 *Davaco, Inc.*

13 UNITED STATES DISTRICT COURT
14 CENTRAL DISTRICT OF CALIFORNIA

15 CHARLES CHACON, individually
16 and on behalf of all others similarly
17 situated,

18 Plaintiff,

19 v.

20 DAVACO, INC.,

21 Defendant.

Case No. 5:21-cv-1589

PROOF OF SERVICE

(Riverside County Superior Court Case
No. CVRI2103666)

PROOF OF SERVICE

I am a citizen of the United States and employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Hogan Lovells US LLP, 1999 Avenue of the Stars, Suite 1400, Los Angeles, California 90067.

On September 17, 2021, I served a copy of the within document(s):

NOTICE OF REMOVAL OF ACTION TO FEDERAL COURT UNDER 28, U.S.C. SECTIONS 1332, 1441, 1446, AND 1453;

- ☐ by transmitting via facsimile the document(s) listed above to the fax number(s) set forth below on this date before 5:00 p.m.
- ☒ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, the United States mail at Los Angeles, California addressed as set forth below.
- ☐ by placing the document(s) listed above in a sealed Federal Express envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a Federal Express agent for delivery.
- ☐ by personally delivering the document(s) listed above to the person(s) at the address(es) set forth below.
- ☒ by transmitting via e-mail or electronic transmission the document(s) listed above to the person(s) at the e-mail address(es) set forth below.

SWIGART LAW GROUP, APC
Joshua B. Swigart
Rahil Swigart
Evan Thamamahong
2221 Camino Del Rio S., Suite 308
San Diego, California 92108
josh@swigartlawgroup.com
rahil@swigartlawgroup.com
evan@swigartlawgroup.com

Attorneys for Plaintiff

Casey Gerry Schenk Francavilla Blatt & Penfield LLP
Gayle M. Blatt
110 Laurel St.
San Diego, CA 92101
gmb@cglaw.com

Attorneys for Plaintiff

I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

1 I declare that I am employed in the office of a member of the bar of this court at whose
2 direction the service was made.

3 Executed on September 17, 2021, at Los Angeles, California.
4

5 _____
6 Mae F. Chester
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ClassAction.org

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