



AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_.

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_, who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

I returned the summons unexecuted because \_\_\_\_\_; or

Other *(specify)*:

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00.

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA  
SOUTHERN DIVISION

BRETT RIGAS, et al.  
Plaintiff(s),

v.

CALIFORNIA PIZZA KITCHEN, INC.  
Defendant(s).

CASE NO:  
8:21-cv-02004-DOC-KES

**INITIAL STANDING ORDER  
FOLLOWING ASSIGNMENT OF  
CIVIL CASE TO JUDGE CARTER**

This case has been assigned to the calendar of Judge David O. Carter. Whenever a new civil case is assigned to Judge Carter, the Court issues this Initial Standing Order. It lays out some of the Judge's rules and expectations that litigants should be familiar with from the beginning of their case. In addition to this Initial Standing Order, litigants are required to follow the Federal Rules of Civil Procedure and the Local Rules of the Central District of California.<sup>1</sup>

The Court ORDERS as follows:

\_\_\_\_\_

<sup>1</sup>The most recent version of the Local Rules is available on the Central District of California's website ([www.cacd.uscourts.gov](http://www.cacd.uscourts.gov)), under "Court Procedures."

1 **I. Court Appearances**

2 The parties must appear in person for hearings and conferences before the  
3 Court. The Court does not permit telephonic appearances.

4 Unless a party is representing him or herself, parties shall be represented by  
5 **lead counsel** at all court appearances, including scheduling conferences.

6 Under no circumstances should counsel, or a party if the party is appearing  
7 *pro se*, fail to appear at a court appearance unless their appearance has been waived  
8 by prior order of the Court. Even if a settlement has been reached, counsel for all  
9 parties, or the party if appearing *pro se*, must appear at court appearances until  
10 a stipulation of dismissal signed by all parties has been lodged with the Court.

11 **II. Scheduling**

12 Pursuant to Rule 16(b), the Court will set a scheduling conference and issue a  
13 scheduling order in each case. Litigants should familiarize themselves with the  
14 Court's standard Order Setting Scheduling Conference and the Court's standard  
15 Scheduling Order & Order re: Pretrial and Trial Procedures, which describe the  
16 typical schedule and procedures used in this Court.<sup>2</sup>

17 The Court is flexible in setting initial dates. Therefore, Parties should meet  
18 and confer to select mutually agreeable dates. The Court strongly encourages  
19 Parties to stipulate to the initial schedule, and endeavor to accommodate counsel's  
20 previously scheduled dates that produce good faith calendar conflicts. Counsel are  
21 encouraged to reference the Central District's Civility and Professionalism  
22 Guidelines, which can be found on the Court's website.

23 **III. Continuances and Extensions of Deadlines**

24 This Court has a strong interest in adhering to scheduled dates. Changes in  
25 dates are disfavored. Trial dates set by the Court are firm and will rarely be  
26 changed, except that the Court may advance the trial date up to two weeks.

27 \_\_\_\_\_  
28 <sup>2</sup>All of Judge Carter's standing orders are available at Judge Carter's home page  
located under "Judges' Procedures and Schedules."

1 Therefore, any request, whether by application or stipulation, to continue the  
2 date of any matter before this Court must be supported by a detailed explanation  
3 of the grounds for the requested continuance or extension of time. Without  
4 compelling factual support, requests to continue dates set by this Court will  
5 not be approved. Proposed stipulations extending scheduling dates do not become  
6 effective unless and until this Court so orders.

7 **IV. Motions**

8 Counsel should note the timing and service requirements of Local Rules 6  
9 and 7 and its subparts including:

- 10 (1) Rule 6–1: Notice of motion and the moving papers must be filed and  
11 served twenty–eight (28) days before the noticed hearing date, unless  
12 the notice is served by mail, in which case service is required thirty–one  
13 (31) days prior to the noticed hearing date;
- 14 (2) Rule 7–9: Opposing papers shall be filed twenty–one (21) calendar days  
15 before the hearing date; and
- 16 (3) Rule 7–10: Reply papers, if any, shall be filed fourteen (14) calendar  
17 days before the hearing date.
- 18 (4) Rule 7–11: If the hearing date is continued, the deadlines for filing  
19 opposing and reply papers are automatically extended unless the  
20 Court orders otherwise.

21 Counsel must comply with the timing requirements of the Local Rules so  
22 that chambers can properly prepare for motion matters.

23 Parties should note, the Court will only entertain one Motion for Summary  
24 Judgment from each party, typically after discovery is closed.

25 **V. Ex Parte Applications**

26 Ex parte applications are solely for extraordinary relief and should be used  
27 with discretion. *See Mission Power Eng'g Co. v. Continental Cas. Co.*, 883 F.  
28 F. Supp. 488 (C.D. Cal. 1995). In this Court's experience, ex parte applications

1 “are nearly always improper.” *In re Intermagnetics Am., Inc.*, 101 B.R. 191,  
2 192–93 (C.D. Cal. 1989). The Federal Rules of Civil Procedure and Local Rules  
3 “contemplate that regular noticed motions are most likely to produce a just result.”  
4 *Mission Power*, 883 F. Supp. at 491.

5 Ex parte applications that fail to conform to Local Rule 7–19 and 7–19.1,  
6 including a statement of opposing counsel’s position, will not be considered except  
7 on a specific showing of good cause. Concurrently with service of the ex parte  
8 papers by electronic service, facsimile, or personal service, the moving party shall  
9 notify the opposition that opposing papers must be filed no later than twenty–four  
10 (24) hours following service. If opposing counsel does not intend to oppose the  
11 ex parte application, counsel must inform the Courtroom Deputy Clerk by  
12 telephone or email as soon as possible.

### 13 **VI. Jury Demand**

14 Litigants who are entitled to a jury trial and who wish to have a jury trial are  
15 reminded to file and serve a jury demand in accordance with Federal Rule of Civil  
16 Procedure 38.

### 17 **VII. Applications to File Documents Under Seal**

18 There is a strong presumption that the public has a right of access to records  
19 in civil cases. For non–dispositive motions, the party seeking to maintain the  
20 confidentiality of the document(s) or portions thereof must show good cause. For  
21 dispositive motions, the party seeking protection must articulate compelling reasons  
22 for maintaining the confidentiality of the document(s) and must seek relief that is  
23 narrowly tailored to the protected interest. See *Pintos v. Pacific Creditors Ass’n*,  
24 605 F.3d 665, 677–79 (9th Cir. 2010). No document will be filed under seal in its  
25 entirety unless it is shown in the application that it is not feasible to file a redacted  
26 version for public viewing. Any proposed redactions must be highlighted in the  
27 under seal version of the document so that the Court may readily determine what  
28 information the party or parties seek to maintain as confidential.

1 In accordance with Local Rule 79–5.1, absent authorization by rule or statute,  
2 no case or document(s) may be filed under seal without written application to, and  
3 prior approval by, the Court. The existence of a Protective Order, a Stipulated  
4 Confidentiality Order, or the like, issued by the assigned Magistrate Judge relating  
5 to the treatment of documents produced during discovery, does not constitute a  
6 court Order permitting an under seal filing. An application to seal that is based  
7 solely on the existence of such an Order will be summarily denied. In addition,  
8 reliance upon the parties’ designation of documents as “Confidential,” “Highly  
9 Confidential,” “Attorneys’ Eyes Only,” etc. is insufficient. Rather, the party must  
10 provide competent evidence explaining why the document(s) should be filed under  
11 seal.

12 If the party seeking to file documents under seal (the “filing party”) is not  
13 the party with an interest in the sealing/confidentiality of the documents, then the  
14 filing party shall provide the interested party with its proposed application to seal  
15 at least two (2) business days in advance of any filing. If the interested party seeks  
16 to have the documents filed under seal, it shall file a Declaration setting forth  
17 competent evidence explaining why the document(s) should be filed under seal.  
18 If the interested party fails to file a Declaration within this two–day period, the  
19 filing party is relieved of any obligation to file an application to seal and may  
20 publicly file the documents along with a Declaration of Compliance with this  
21 paragraph.

### 22 **VIII. Settlement**

23 If settlement is reached at any time in this litigation, the parties shall  
24 immediately notify the Court by telephone, email, or by filing a notice of  
25 settlement. Local Rule 40–2.

### 26 **IX. Communication with the Court**

27 All appropriate inquiries should be directed to Judge Carter’s Courtroom  
28 Deputy Clerk at (714) 338–4543 or DOC\_Chambers@cacd.uscourts.gov.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Counsel should not attempt to contact chambers directly. Counsel should list their email addresses and phone numbers on their papers in order to facilitate communication by the Courtroom Deputy Clerk.

**X. Notice of this Order**

Plaintiff's counsel or plaintiff (if appearing on his or her own behalf) shall immediately serve this Order on all parties, including any new parties to the action. If this case came to the Court by a Notice of Removal, the removing defendant(s) shall serve this Order on all other parties.

**IT IS SO ORDERED.**

Dated: December 17, 2021



---

David O. Carter  
United States District Judge

Revised: January 20, 2015



UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

Brett Rigas et al

CASE NUMBER

8:21-cv-02004-JLS-DFMx

PLAINTIFF(S)

v.

California Pizza Kitchen, Inc.

ORDER RE TRANSFER PURSUANT  
TO GENERAL ORDER 21-01  
(RELATED CASES)

DEFENDANT(S).

CONSENT

I hereby consent to the transfer of the above-entitled case to my calendar, pursuant to General Order 21-01.

December 10, 2021

Date

*David O. Carter*

United States District Judge

DECLINATION

I hereby decline to transfer the above-entitled case to my calendar for the reasons set forth:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Date

\_\_\_\_\_  
United States District Judge

REASON FOR TRANSFER AS INDICATED BY COUNSEL

Case 8:21-cv-01928-DOC-KESx and the present case:

- A. Arise from the same or closely related transactions, happenings or events; or
- B. Call for determination of the same or substantially related or similar questions of law and fact; or
- C. For other reasons would entail substantial duplication of labor if heard by different judges; or
- D. Involve one or more defendants from the criminal case in common, and would entail substantial duplication of labor if heard by different judges (applicable only on civil forfeiture action).

NOTICE TO COUNSEL FROM CLERK

Pursuant to the above transfer, any discovery matters that are or may be referred to a Magistrate Judge are hereby transferred from Magistrate Judge Douglas F. McCormick to Magistrate Judge Karen E. Scott.

On all documents subsequently filed in this case, please substitute the initials DOC(KESx) after the case number in place of the initials of the prior judge, so that the case number will read 8:21-cv-02004-DOC(KESx). This is very important because the documents are routed to the assigned judges by means of these initials

cc:  Previous Judge  Statistics Clerk

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

BRETT RIGAS , et al.

Case No.: 8:21-cv-02004-JLS-DFM

Plaintiff(s),

**INITIAL STANDING ORDER FOR  
CIVIL CASES ASSIGNED TO  
JUDGE JOSEPHINE L. STATON**

v.

CALIFORNIA PIZZA KITCHEN, INC.

Defendant(s).

**PLEASE READ THIS ORDER CAREFULLY. IT GOVERNS THIS CASE  
AND DIFFERS IN SOME RESPECTS FROM THE LOCAL RULES.**

This case has been assigned to the calendar of Judge Josephine L. Staton. Both the Court and counsel bear responsibility for the progress of this litigation in federal court. To “secure the just, speedy, and inexpensive determination” of this case, as called for in Federal Rule of Civil Procedure 1, all parties or their counsel are ordered to become familiar with the Federal Rules of Civil Procedure, the Local Rules of the Central District of California, and this Court’s Orders.

\\

\\

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**THE COURT ORDERS AS FOLLOWS:**

Judge Staton’s Procedures web page is incorporated in this Order.

The parties and counsel are ORDERED to review and comply with those procedures and notices, which may be accessed at:

<http://www.cacd.uscourts.gov/honorable-josephine-l-staton>

**1. Filing of Civil Cases**

The initiating documents (*e.g.*, complaints and notices of removal) of most civil cases must be e-filed. *See* Local Rule 3-2.

**2. Service of the Complaint**

Service is governed by Federal Rule of Civil Procedure 4. The plaintiff shall promptly serve the complaint in accordance with Fed. R. Civ. P. 4 and file the proofs of service. Although Fed. R. Civ. P. 4(m) allows 90 days for service of the summons and complaint, the Court expects service to be effectuated more promptly. The Court will require plaintiffs to show good cause to extend the service deadline beyond 90 days.

**3. TROs and Injunctions**

Parties seeking emergency or provisional relief shall comply with Fed. R. Civ. P. 65 and Local Rule 65. The Court will not rule on any application for such relief for at least twenty-four (24) hours after the party subject to the requested order has been served, unless service is excused. Such party may file opposing or responding papers in the interim.

**4. Cases Removed from State Court**

All documents filed in state court, including documents appended to the complaint, answers, and motions, must be refiled in this Court as a supplement to the notice of removal. *See* 28 U.S.C. § 1447(b). If the defendant has not yet answered or filed a pre-answer motion, the defendant’s answer or motion must be filed in this Court and must comply with the Federal Rules of Civil Procedure and the Local Rules. If a motion was pending in state court before the case was

1 removed, it must be re-noticed for hearing in accordance with Local Rule 6-1.  
2 Counsel shall file with their first appearance a Notice of Interested Parties in  
3 accordance with Local Rule 7.1-1.

4 If the complaint, answer, or any similar pleading in an action that is removed  
5 to this Court consists of only a form pleading in which boxes are checked, the party  
6 or parties utilizing the form pleading must file an appropriate pleading with this  
7 Court within thirty (30) days of the filing of the Notice of Removal. The new  
8 pleading must comply with the requirements of Federal Rules of Civil Procedure  
9 7 through 11.

10 **5. Status of Fictitiously Named Defendants**

11 This Court intends to adhere to the following procedures where a matter is  
12 removed to this Court on diversity grounds with fictitiously named defendants.

13 *See* 28 U.S.C. §§ 1441(b)(1) and 1447.

14 a. Plaintiff is normally expected to ascertain the identity of and serve any  
15 fictitiously named defendants within 90 days of the removal of the action to this  
16 Court.

17 b. If plaintiff believes (by reason of the necessity for discovery or  
18 otherwise) that fictitiously named defendants cannot be fully identified within  
19 the 90-day period, an *ex parte* application or stipulation requesting permission  
20 to extend that period to effectuate service may be filed with the Court. Such  
21 application or stipulation shall state the reasons therefor, and will be granted only  
22 upon a showing of good cause. An *ex parte* application seeking such relief shall  
23 be served upon all appearing parties, and shall state that appearing parties may  
24 comment within seven (7) days of the filing of the *ex parte* application.

25 c. If plaintiff wants to substitute a defendant for one of the fictitiously  
26 named defendants, plaintiff shall first seek the consent of counsel for all defendants  
27 (and counsel for the fictitiously named party, if that party has separate counsel).  
28 If consent is withheld or denied, plaintiff should file a motion on regular notice.

1 The motion and opposition should address whether the matter should thereafter  
2 be remanded to the superior court if diversity of citizenship is destroyed by the  
3 addition of the newly substituted party. *See* U.S.C. § 1447(c), (d).

4 **6. Discovery**

5 **a. Discovery Matters Referred to Magistrate Judge**

6 All discovery matters have been referred to the assigned United States  
7 Magistrate Judge, who will hear all discovery disputes. Any party may move for  
8 review and reconsideration of a discovery ruling within fourteen days after such  
9 ruling. *See* Local Rule 72-2. However, in accordance with 28 U.S.C. § 636(b)  
10 (1)(A), the Court will not reverse any order of the Magistrate Judge unless the  
11 moving party demonstrates that the ruling is clearly erroneous or contrary to law.  
12 The motion must specify which portions of the ruling are clearly erroneous or  
13 contrary to law and support the contention with points and authorities. As to all  
14 filings related to motions for review and reconsideration of a discovery order,  
15 counsel shall deliver mandatory chambers copies to both the District Judge and  
16 the Magistrate Judge.

17 **b. Compliance with Fed. R. Civ. P. 26(a)**

18 The parties shall comply fully with the letter and spirit of Fed. R. Civ. P. 26(a).  
19 The Court's Scheduling Order will impose firm deadlines to complete discovery.

20 **7. Applications to Seal**

21 Counsel are directed to consider carefully whether to seek leave to file  
22 documents under seal. The procedure for obtaining leave is lengthy. Applications  
23 must in all instances be supported by good cause, and at times are subjected to an  
24 even higher standard. Most of the time, documents may not be filed under seal  
25 in their entirety, and appropriately redacted documents must still be filed on the  
26 public docket.

27 When seeking leave to file any material under seal in a civil case, the parties  
28 and counsel are directed to fully comply with all steps of the multi-step procedure

1 set forth in Local Rule 79-5. The parties are directed to carefully review the  
2 Court's Local Rule 79-5 Overview and to follow the instructions in the Guide to  
3 Electronically Filing Under-Seal Documents in Civil Cases, both of which are  
4 attached in PDF format to Judge Staton's Procedures web page.

5 Counsel are reminded that there is a strong presumption that the public has  
6 a right of access to records in civil cases. For materials related to non-dispositive  
7 motions, the Designating Party must show good cause for the materials to be  
8 filed and maintained under seal. For materials related to dispositive motions, the  
9 standard is higher, and the Designating Party must articulate compelling reasons  
10 for maintaining the confidentiality of the document(s) and must seek relief that is  
11 narrowly tailored to the protected interest. *See Pintos v. Pacific Creditors Ass'n*,  
12 605 F.3d 665, 667-79 (9th Cir. 2010).

## 13 **8. Motions**

### 14 **a. Time for Filing and Hearing Motions**

15 Motions shall be filed in accordance with Local Rule 7. This Court hears  
16 motions on **Fridays**, beginning at 10:30 a.m. It is not necessary to clear a hearing  
17 date with the Court Clerk before filing a motion in a civil motion. Counsel  
18 must check the Court's website for Closed Motion Dates.

### 19 **b. Pre-Filing Requirement To Meet and Confer**

20 Counsel must comply with Local Rule 7-3, which requires counsel to  
21 engage in a pre-filing conference "to discuss thoroughly . . . the substance of the  
22 contemplated motion and any potential resolution." Counsel should discuss the  
23 issues to a sufficient degree that if a motion is still necessary, the briefing may  
24 be directed to those substantive issues requiring resolution by the Court. Counsel  
25 should resolve minor procedural or other non-substantive matters during the  
26 conference. This provision applies even to self-represented parties; there is no  
27 exception to this rule for parties who appear *pro se*.

28 \\\

1           **c. Supporting Evidence**

2           Parties shall not proffer evidence other than the specific items of evidence  
3 testimony in support of or in opposition to a motion. For example, the parties  
4 should provide excerpts rather than entire deposition transcripts or entire sets  
5 of interrogatory responses. Where a motion must be supported by *admissible*  
6 evidence, authenticity must be established by stipulation of the parties, declaration,  
7 or other appropriate means.

8           **d. Citations to Legal Authority**

9           Citations to legal authority should include pinpoint citations to specific  
10 page(s), section(s), and subsection(s) referenced. Citations to secondary sources  
11 such as treatises, manuals, and other materials should include the volume, section,  
12 and page(s) cited.

13           **9. Specific Motions**

14           **a. Motions Pursuant to Rule 12**

15           Many motions to dismiss or to strike can be avoided if the parties confer in  
16 good faith (as required by Local Rule 7-3), especially for pleading deficiencies  
17 that could be corrected by amendment. *See Chang v. Chen*, 80 F.3d 1293, 1296  
18 (9th Cir. 1996) (where a motion to dismiss is granted, a district court should  
19 provide leave to amend unless it is clear that the complaint could not be saved by  
20 any amendment). Moreover, a party has the right to amend the complaint “once  
21 as a matter of course” within 21 days after service of the answer or Rule 12(b)  
22 motion. Fed. R. Civ. P. 15(a)(1)(A)-(B).

23           **b. Motions to Amend**

24           In addition to meeting the requirements of Local Rule 15-1, counsel shall  
25 attach as an appendix to the moving papers a “redlined” version of the proposed  
26 amended pleading indicating all additions and deletions of material. All motions  
27 to amend pleadings shall: (1) state the effect of the amendment and (2) identify  
28 the page and line number(s) and wording of any proposed change or addition

1 of material. The proposed amended pleading shall be serially numbered to  
 2 differentiate it from previously amended pleadings (*e.g.*, “Second Amended  
 3 Complaint” or “Third Amended Answer and Counterclaims”). If leave to amend  
 4 is granted, the filing party must comply with Local Rule 15-1 through 15-3 in filing  
 5 the amended pleading.

6 **c. Summary Judgment Motions**

7 A party may file only one summary judgment motion in a case. Parties need  
 8 not wait until the motion cutoff date to bring motions for summary judgment or  
 9 partial summary judgment. The parties should prepare papers in a fashion that will  
 10 assist the Court in absorbing the facts (*e.g.*, generous use of tabs, tables of contents,  
 11 headings, indices, etc.).

12 **i. Statements of Uncontroverted Facts and Genuine Issues**

13 The Statement of Uncontroverted Facts and Conclusions of Law (“Statement  
 14 of Uncontroverted Facts”), as required by Local Rule 56-1 shall be formatted based  
 15 on the following example:

16 1. (Moving party’s first uncontroverted fact)	(Supporting evidence citation(s))
17 2. (Moving party’s second undisputed fact)	(Supporting evidence citation(s))

19 The opposing party’s Statement of Genuine Disputes of Material Fact  
 20 (required by Local Rule 56-2) must be in two columns and track the movant’s  
 21 Statement of Uncontroverted Facts exactly as prepared, but must combine the  
 22 moving party’s fact statements and the supporting evidence into one column.  
 23 Thus, the first column must restate the allegedly undisputed fact ***and the alleged***  
 24 ***supporting evidence***, and the second column must state either that the fact  
 25 proffered by the moving party is undisputed or disputed. The opposing party may  
 26 dispute all or only a portion of the statement, but if disputing only a portion, it  
 27 must clearly indicate what part is being disputed. Whenever all or part of a  
 28 proffered fact is disputed, the opposing party must ***briefly*** state why it disputes



1 the moving party's proffered fact, cite to the relevant exhibit(s) or other evidence,  
 2 and must describe what it is in that exhibit or evidence that refutes the proffered  
 3 fact. To illustrate:

4 1. (Moving party's first uncontroverted fact). (Supporting evidence citation(s)).	1. Undisputed.
5 2. (Moving party's second undisputed fact). (Supporting evidence citation(s)).	2. Disputed. Plaintiff's Rule 30(b)(6) witness testified to the contrary. (Pltf's Ex. 14, Clark Depo. at 24:5-26:17.)

8 The opposing party may submit additional material facts that bear on or relate  
 9 to the issues raised by the movant. Presentation of those additional material facts  
 10 by the non-moving party shall follow the format described above for the moving  
 11 party's Statement of Uncontroverted Facts. These additional facts shall continue  
 12 in sequentially numbered paragraphs and shall set forth in the right hand column  
 13 the evidence that supports that statement. A Reply fact statement may be filed by  
 14 the moving party.

15 *No legal argument should be set forth in the Statement of Uncontroverted*  
 16 *Facts or the Statement of Genuine Disputes of Material Fact. Legal argument*  
 17 *should be reserved for the parties' briefs. Objections and the relevant Federal*  
 18 *Rule of Evidence or other basis therefor may be noted, but citations to case law*  
 19 *and/or legal argument should be presented in the separate document described*  
 20 *below.*

## 21 ii. Objections to Evidence

22 If a party relies in whole or in part on an evidentiary objection to dispute  
 23 a material fact, the ground(s) of the objection(s) shall be succinctly stated in a  
 24 separate statement of evidentiary objections in a two-column format. The left  
 25 column should identify and describe the item(s) objected to (including page and  
 26 line number if applicable) and the right column should set forth a concise objection  
 27 (e.g., hearsay, lacks foundation, etc.) with a citation to the Federal Rules of  
 28 Evidence or, where applicable, a case citation. Any response to the objections shall

1 incorporate and build upon the two-column format set forth in the objections in the  
2 same manner as the Statement of Genuine Disputes of Material Fact incorporates  
3 and builds upon the Statement of Uncontroverted Facts.

4 The Court will expressly rule on objections only when it deems it necessary  
5 to do. Generally, the Court will expressly rule on objections only as to evidence  
6 that factors into the Court's rationale for its rulings.

7 **d. *Daubert* Motions**

8 Unlike other motions *in limine*, *Daubert* motions are usually due to be filed  
9 within seven days after the expert discovery cut-off date set in the Scheduling  
10 Order.<sup>1</sup> The parties shall notice *Daubert* motions for hearing on the first available  
11 motions date at the time of their filing, unless that date is after the final pretrial  
12 conference date, in which case the *Daubert* motions will be heard at the final  
13 pretrial conference.

14 **10. Notice of This Order**

15 Plaintiff's counsel or plaintiff (if appearing on his or her own behalf) shall  
16 immediately serve this Order on all parties, including any new parties to the action.  
17 If this case was removed from state court, the removing defendant(s) shall serve  
18 this Order on all other parties.

19 IT IS SO ORDERED.

20  
21 Dated: December 9, 2021

**JOSEPHINE L. STATON**  
United States District Judge

22  
23 Revised: October 1, 2018  
24  
25  
26

27 \_\_\_\_\_  
28 <sup>1</sup> In some instances, a later date may be set.

---

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

---

BRETT RIGAS, et al.

PLAINTIFF(S),

v.

CALIFORNIA PIZZA KITCHEN, INC.

DEFENDANT(S).

CASE NUMBER:

8:21-cv-02004-JLS-DFM

---

**Notice to Counsel Re Consent to Proceed  
Before a United States Magistrate Judge**

The parties are advised they may consent to proceed before any available magistrate judge participating in the Voluntary Consent to Magistrate Judges Program to conduct all further proceedings in the case pursuant to 28 U.S.C. § 636(c) and Federal Rules of Civil Procedure 73. The consent list and consent form are available on the court's website at <http://www.cacd.uscourts.gov/judges-requirements/court-programs/voluntary-consent-magistrate-judges-program>. To confirm a particular magistrate judge's availability to schedule the trial in the time frame desired by the parties and/or willingness to accommodate any other special requests of the parties, please contact the magistrate judge's courtroom deputy prior to filing the consent.

Since magistrate judges do not handle felony criminal trials, civil trial dates are not at risk of being preempted by a felony criminal trial, which normally has priority. Further, in some cases, the magistrate judge may be able to assign an earlier trial date than a district judge. The parties can select a participating Magistrate Judge from any of the three divisions in the Central District of California. There may be other advantages or disadvantages which you will want to consider.

The plaintiff or removing party must serve this Notice on each named party in the case.

---

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

---

BRETT RIGAS, et al.

Plaintiff(s)

v.

CALIFORNIA PIZZA KITCHEN, INC.

Defendant(s).

CASE NUMBER:

8:21-cv-02004-JLS-DFM

---

**NOTICE TO PARTIES OF  
COURT-DIRECTED ADR PROGRAM**

---

**NOTICE TO PARTIES:**

It is the policy of this Court to encourage settlement of civil litigation when such is in the best interest of the parties. The Court favors any reasonable means, including alternative dispute resolution (ADR), to accomplish this goal. *See* L.R. 16-15. Unless exempted by the trial judge, parties in all civil cases must participate in an ADR process before trial. *See* L.R. 16-15.1.

The district judge to whom the above-referenced case has been assigned is participating in an ADR Program that presumptively directs this case to either the Court Mediation Panel or to private mediation. *See* General Order No. 11-10, §5. For more information about the Mediation Panel, visit the Court website, [www.cacd.uscourts.gov](http://www.cacd.uscourts.gov), under "ADR."

Pursuant to L.R. 26-1(c), counsel are directed to furnish and discuss with their clients the attached ADR Notice To Parties *before* the conference of the parties mandated by Fed.R.Civ.P. 26(f). Based upon the consultation with their clients and discussion with opposing counsel, counsel must indicate the following in their Joint 26(f) Report: 1) whether the case is best suited for mediation with a neutral from the Court Mediation Panel or private mediation; and 2) when the mediation should occur. *See* L.R. 26-1(c).

At the initial scheduling conference, counsel should be fully prepared to discuss their preference for referral to the Court Mediation Panel or to private mediation and when the mediation should occur. The Court will enter an Order/Referral to ADR at or around the time of the scheduling conference.

Clerk, U.S. District Court

December 8, 2021  
Date

By /s/ Geneva Hunt  
Deputy Clerk

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**NOTICE TO PARTIES: COURT POLICY ON SETTLEMENT  
AND USE OF ALTERNATIVE DISPUTE RESOLUTION (ADR)  
Counsel are required to furnish and discuss this Notice with their clients.**

Despite the efforts of the courts to achieve a fair, timely and just outcome in all cases, litigation has become an often lengthy and expensive process. For this reason, it is this Court's policy to encourage parties to attempt to settle their disputes, whenever possible, through alternative dispute resolution (ADR).

ADR can reduce both the time it takes to resolve a case and the costs of litigation, which can be substantial. ADR options include mediation, arbitration (binding or non-binding), neutral evaluation (NE), conciliation, mini-trial and fact-finding. ADR can be either Court-directed or privately conducted.

The Court's ADR Program offers mediation through a panel of qualified and impartial attorneys who will encourage the fair, speedy and economic resolution of civil actions. Panel Mediators each have at least ten years of legal experience and are appointed by the Court. They volunteer their preparation time and the first three hours of a mediation session. This is a cost-effective way for parties to explore potential avenues of resolution.

This Court requires that counsel discuss with their clients the ADR options available and instructs them to come to the initial scheduling conference prepared to discuss the parties' choice of ADR option. The ADR options available are: a settlement conference before the magistrate judge assigned to the case or the magistrate judge in Santa Barbara, the Court Mediation Panel, and private mediation. Counsel are also required to indicate the client's choice of ADR option in advance of the initial scheduling conference. *See* L.R. 26-1(c) and Fed.R.Civ.P. 26(f).

Clients and their counsel should carefully consider the anticipated expense of litigation, the uncertainties as to outcome, the time it will take to get to trial, the time an appeal will take if a decision is appealed, the burdens on a client's time, and the costs and expenses of litigation in relation to the amounts or stakes involved.

Each year thousands of civil cases are filed in this district, yet typically no more than one percent go to trial. Most cases are settled between the parties, voluntarily dismissed, resolved through Court-directed or other forms of ADR, or dismissed by the Court as lacking in merit or for other reasons provided by law.

For more information about the Court's ADR Program, the Mediation Panel, and the profiles of mediators, visit the Court website, [www.cacd.uscourts.gov](http://www.cacd.uscourts.gov), under "ADR."

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**NOTICE OF ASSIGNMENT TO UNITED STATES JUDGES**

This case has been assigned to:

District Judge **Josephine L. Staton**  
Magistrate Judge **Douglas F. McCormick**

The case number on all documents filed with the Court should read as follows:

**8:21-cv-02004 JLS (DFMx)**

District judges in the Central District of California refer all discovery-related motions to the assigned magistrate judge pursuant to General Order No. 05-07. Discovery-related motions should be noticed for hearing before the assigned magistrate judge. Please refer to the assigned judges' Procedures and Schedules, available on the Court's website at [www.cacd.uscourts.gov/judges-requirements](http://www.cacd.uscourts.gov/judges-requirements), for additional information.

Clerk, U.S. District Court

December 8, 2021  
Date

By /s/ Geneva Hunt  
Deputy Clerk

---

**ATTENTION**

*The party that filed the case-initiating document in this case (for example, the complaint or the notice of removal) must serve a copy of this Notice on all parties served with the case-initiating document. In addition, if the case-initiating document in this case was electronically filed, the party that filed it must, upon receipt of this Notice, promptly deliver mandatory chambers copies of all previously filed documents to the newly assigned-district judge. See L.R. 5-4.5. A copy of this Notice should be attached to the first page of the mandatory chambers copy of the case-initiating document.*

NAME, ADDRESS, AND TELEPHONE NUMBER OF ATTORNEY(S)  
 OR OF PARTY APPEARING IN PRO PER  
 Rachele R. Byrd (SBN 190634)  
 WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP  
 750 B Street, Suite 1820, San Diego, CA 92101  
 Tel: 619/239-4599 Fax: 619/234-4599

ATTORNEY(S) FOR: Plaintiffs

**UNITED STATES DISTRICT COURT  
 CENTRAL DISTRICT OF CALIFORNIA**

BRETT RIGAS and EVENCIO DIAZ, individually  
 and on behalf of all others similarly situated,  
 Plaintiff(s),  
 v.  
 CALIFORNIA PIZZA KITCHEN, INC.,  
 Defendant(s)

CASE NUMBER:

**CERTIFICATION AND NOTICE  
 OF INTERESTED PARTIES  
 (Local Rule 7.1-1)**

TO: THE COURT AND ALL PARTIES OF RECORD:

The undersigned, counsel of record for Plaintiffs  
 or party appearing in pro per, certifies that the following listed party (or parties) may have a pecuniary interest in  
 the outcome of this case. These representations are made to enable the Court to evaluate possible disqualification  
 or recusal.

(List the names of all such parties and identify their connection and interest. Use additional sheet if necessary.)

PARTY	CONNECTION / INTEREST
Brett Rigas	Plaintiff
Evencio Diaz	Plaintiff
California Pizza Kitchen, Inc.	Defendant

December 7, 2021  
 Date

/s/ Rachele R. Byrd  
 Signature

Attorney of record for (or name of party appearing in pro per):

Plaintiffs





AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_.

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_, who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

I returned the summons unexecuted because \_\_\_\_\_; or

Other *(specify)*: \_\_\_\_\_

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00.

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA

CIVIL COVER SHEET

**I. (a) PLAINTIFFS** ( Check box if you are representing yourself  ) **DEFENDANTS** ( Check box if you are representing yourself  )

BRETT RIGAS and EVENCIO DIAZ, individually and on behalf of all others similarly situated  
 CALIFORNIA PIZZA KITCHEN, INC.

**(b) County of Residence of First Listed Plaintiff** Orange County, FL **County of Residence of First Listed Defendant** \_\_\_\_\_

*(EXCEPT IN U.S. PLAINTIFF CASES)* *(IN U.S. PLAINTIFF CASES ONLY)*

**(c) Attorneys (Firm Name, Address and Telephone Number) If you are representing yourself, provide the same information.**

Rachele R. Byrd (SBN 190634)  
 WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP  
 750 B Street, Suite 1820, San Diego, CA 92101  
 Tel: 619/239-4599 Fax: 619/234-4599

**II. BASIS OF JURISDICTION** (Place an X in one box only.)

1. U.S. Government Plaintiff  
 2. U.S. Government Defendant  
 3. Federal Question (U.S. Government Not a Party)  
 4. Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES**-For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

**IV. ORIGIN** (Place an X in one box only.)

1. Original Proceeding  2. Removed from State Court  3. Remanded from Appellate Court  4. Reinstated or Reopened  5. Transferred from Another District (Specify) \_\_\_\_\_  6. Multidistrict Litigation - Transfer  8. Multidistrict Litigation - Direct File

**V. REQUESTED IN COMPLAINT: JURY DEMAND:**  Yes  No (Check "Yes" only if demanded in complaint.)

**CLASS ACTION under F.R.Cv.P. 23:**  Yes  No **MONEY DEMANDED IN COMPLAINT:** \$ \_\_\_\_\_

**VI. CAUSE OF ACTION** (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)

1) 28 U.S.C. § 1332(d); (2) Negligence; (3) Breach of Implied Contract; (4) Invasion of Privacy; (5) Breach of Confidence; (6) Unjust Enrichment

**VII. NATURE OF SUIT** (Place an X in one box only.)

OTHER STATUTES	CONTRACT	REAL PROPERTY CONT.	IMMIGRATION	PRISONER PETITIONS	PROPERTY RIGHTS
<input type="checkbox"/> 375 False Claims Act	<input type="checkbox"/> 110 Insurance	<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 462 Naturalization Application	<b>Habeas Corpus:</b>	<input type="checkbox"/> 820 Copyrights
<input type="checkbox"/> 376 Qui Tam (31 USC 3729(a))	<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 463 Alien Detainee	<input type="checkbox"/> 830 Patent
<input type="checkbox"/> 400 State Reapportionment	<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 290 All Other Real Property	<b>TORTS</b>	<input type="checkbox"/> 510 Motions to Vacate Sentence	<input type="checkbox"/> 835 Patent - Abbreviated New Drug Application
<input type="checkbox"/> 410 Antitrust	<input type="checkbox"/> 140 Negotiable Instrument	<b>TORTS</b>	<b>PERSONAL PROPERTY</b>	<input type="checkbox"/> 530 General	<input type="checkbox"/> 840 Trademark
<input type="checkbox"/> 430 Banks and Banking	<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 370 Other Fraud	<input type="checkbox"/> 535 Death Penalty	<input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 (DTSA)
<input type="checkbox"/> 450 Commerce/ICC Rates/Etc.	<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 315 Airplane Product Liability	<input type="checkbox"/> 371 Truth in Lending	<b>Other:</b>	<b>SOCIAL SECURITY</b>
<input type="checkbox"/> 460 Deportation	<input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Vet.)	<input type="checkbox"/> 320 Assault, Libel & Slander	<input type="checkbox"/> 380 Other Personal Property Damage	<input type="checkbox"/> 540 Mandamus/Other	<input type="checkbox"/> 861 HIA (1395ff)
<input type="checkbox"/> 470 Racketeer Influenced & Corrupt Org.	<input type="checkbox"/> 153 Recovery of Overpayment of Vet. Benefits	<input type="checkbox"/> 330 Fed. Employers' Liability	<input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 550 Civil Rights	<input type="checkbox"/> 862 Black Lung (923)
<input type="checkbox"/> 480 Consumer Credit	<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 340 Marine	<b>BANKRUPTCY</b>	<input type="checkbox"/> 555 Prison Condition	<input type="checkbox"/> 863 DIWC/DIWW (405 (g))
<input type="checkbox"/> 485 Telephone Consumer Protection Act	<input type="checkbox"/> 190 Other Contract	<input type="checkbox"/> 345 Marine Product Liability	<input type="checkbox"/> 422 Appeal 28 USC 158	<input type="checkbox"/> 560 Civil Detainee Conditions of Confinement	<input type="checkbox"/> 864 SSID Title XVI
<input type="checkbox"/> 490 Cable/Sat TV	<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 350 Motor Vehicle	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<b>FORFEITURE/PENALTY</b>	<input type="checkbox"/> 865 RSI (405 (g))
<input type="checkbox"/> 850 Securities/Commodities/Exchange	<input type="checkbox"/> 196 Franchise	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<b>CIVIL RIGHTS</b>	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	<b>FEDERAL TAX SUITS</b>
<input type="checkbox"/> 890 Other Statutory Actions	<b>REAL PROPERTY</b>	<input type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 440 Other Civil Rights	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)
<input type="checkbox"/> 891 Agricultural Acts	<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 362 Personal Injury-Med Malpractice	<input type="checkbox"/> 441 Voting	<b>LABOR</b>	<input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
<input type="checkbox"/> 893 Environmental Matters	<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 365 Personal Injury-Product Liability	<input type="checkbox"/> 442 Employment	<input type="checkbox"/> 710 Fair Labor Standards Act	
<input type="checkbox"/> 895 Freedom of Info. Act	<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability	<input type="checkbox"/> 443 Housing/Accommodations	<input type="checkbox"/> 720 Labor/Mgmt. Relations	
<input type="checkbox"/> 896 Arbitration		<input type="checkbox"/> 368 Asbestos Personal Injury Product Liability	<input type="checkbox"/> 445 American with Disabilities-Employment	<input type="checkbox"/> 740 Railway Labor Act	
<input type="checkbox"/> 899 Admin. Procedures Act/Review of Appeal of Agency Decision			<input type="checkbox"/> 446 American with Disabilities-Other	<input type="checkbox"/> 751 Family and Medical Leave Act	
<input type="checkbox"/> 950 Constitutionality of State Statutes			<input type="checkbox"/> 448 Education	<input type="checkbox"/> 790 Other Labor Litigation	
				<input type="checkbox"/> 791 Employee Ret. Inc. Security Act	

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**

**VIII. VENUE:** Your answers to the questions below will determine the division of the Court to which this case will be initially assigned. This initial assignment is subject to change, in accordance with the Court's General Orders, upon review by the Court of your Complaint or Notice of Removal.

<b>QUESTION A: Was this case removed from state court?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question B. If "yes," check the box to the right that applies, enter the corresponding division in response to Question E, below, and continue from there.	STATE CASE WAS PENDING IN THE COUNTY OF:		INITIAL DIVISION IN CACD IS:
	<input type="checkbox"/> Los Angeles, Ventura, Santa Barbara, or San Luis Obispo		Western
	<input type="checkbox"/> Orange		Southern
	<input type="checkbox"/> Riverside or San Bernardino		Eastern

<b>QUESTION B: Is the United States, or one of its agencies or employees, a PLAINTIFF in this action?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question C. If "yes," answer Question B.1, at right.	<b>B.1.</b> Do 50% or more of the defendants who reside in the district reside in Orange Co?  check one of the boxes to the right →	<input type="checkbox"/> YES. Your case will initially be assigned to the Southern Division. Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question B.2.
	<b>B.2.</b> Do 50% or more of the defendants who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)  check one of the boxes to the right →	<input type="checkbox"/> YES. Your case will initially be assigned to the Eastern Division. Enter "Eastern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Your case will initially be assigned to the Western Division. Enter "Western" in response to Question E, below, and continue from there.

<b>QUESTION C: Is the United States, or one of its agencies or employees, a DEFENDANT in this action?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question D. If "yes," answer Question C.1, at right.	<b>C.1.</b> Do 50% or more of the plaintiffs who reside in the district reside in Orange Co?  check one of the boxes to the right →	<input type="checkbox"/> YES. Your case will initially be assigned to the Southern Division. Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question C.2.
	<b>C.2.</b> Do 50% or more of the plaintiffs who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)  check one of the boxes to the right →	<input type="checkbox"/> YES. Your case will initially be assigned to the Eastern Division. Enter "Eastern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Your case will initially be assigned to the Western Division. Enter "Western" in response to Question E, below, and continue from there.

<b>QUESTION D: Location of plaintiffs and defendants?</b>  Indicate the location(s) in which 50% or more of <i>plaintiffs who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)  Indicate the location(s) in which 50% or more of <i>defendants who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)	<b>A.</b> Orange County	<b>B.</b> Riverside or San Bernardino County	<b>C.</b> Los Angeles, Ventura, Santa Barbara, or San Luis Obispo County
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<b>D.1. Is there at least one answer in Column A?</b> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No  If "yes," your case will initially be assigned to the SOUTHERN DIVISION. Enter "Southern" in response to Question E, below, and continue from there.  If "no," go to question D2 to the right. →	<b>D.2. Is there at least one answer in Column B?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "yes," your case will initially be assigned to the EASTERN DIVISION. Enter "Eastern" in response to Question E, below.  If "no," your case will be assigned to the WESTERN DIVISION. Enter "Western" in response to Question E, below. ↓
---	---

<b>QUESTION E: Initial Division?</b>  Enter the initial division determined by Question A, B, C, or D above: →	INITIAL DIVISION IN CACD  SOUTHERN
--	--

<b>QUESTION F: Northern Counties?</b>  Do 50% or more of plaintiffs or defendants in this district reside in Ventura, Santa Barbara, or San Luis Obispo counties? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
---

**CIVIL COVER SHEET**

**IX(a). IDENTICAL CASES:** Has this action been previously filed in this court?  NO  YES

If yes, list case number(s): \_\_\_\_\_

**IX(b). RELATED CASES:** Is this case related (as defined below) to any civil or criminal case(s) previously filed in this court?  NO  YES

If yes, list case number(s): 8:21-cv-01928; 2:21-cv-09345; 8:21-cv-01970

Civil cases are related when they (check all that apply):

- A. Arise from the same or a closely related transaction, happening, or event;
- B. Call for determination of the same or substantially related or similar questions of law and fact; or
- C. For other reasons would entail substantial duplication of labor if heard by different judges.

Note: That cases may involve the same patent, trademark, or copyright is not, in itself, sufficient to deem cases related.

A civil forfeiture case and a criminal case are related when they (check all that apply):

- A. Arise from the same or a closely related transaction, happening, or event;
- B. Call for determination of the same or substantially related or similar questions of law and fact; or
- C. Involve one or more defendants from the criminal case in common and would entail substantial duplication of labor if heard by different judges.

**X. SIGNATURE OF ATTORNEY (OR SELF-REPRESENTED LITIGANT):** /s/ Rachele R. Byrd DATE: 12/07/2021

**Notice to Counsel/Parties:** The submission of this Civil Cover Sheet is required by Local Rule 3-1. This Form CV-71 and the information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. For more detailed instructions, see separate instruction sheet (CV-071A).

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405 (g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))

1 BETSY C. MANIFOLD (SBN 182450)  
RACHELE R. BYRD (SBN 190634)  
2 ALEX TRAMONTANO (SBN 276666)\_  
3 **WOLF HALDENSTEIN ADLER**  
**FREEMAN & HERZ LLP**  
750 B Street, Suite 1820  
4 San Diego, CA 92101  
Telephone: (619) 239-4599  
5 Facsimile: (619) 234-4599  
manifold@whafh.com  
6 byrd@whafh.com  
tramontano@whafh.com  
7

8 *Attorneys for Plaintiffs and*  
*the Proposed Class*  
9

10 **UNITED STATES DISTRICT COURT**  
**CENTRAL DISTRICT OF CALIFORNIA**  
11

12 BRET RIGAS and EVENCIO DIAZ,  
individually and on behalf of all others  
13 similarly situated,

14 Plaintiffs,

15 v.

16 CALIFORNIA PIZZA KITCHEN,  
17 INC.,

18 Defendant.  
19

Case No.: \_\_\_\_\_

**CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

1 Plaintiffs Brett Rigas and Evencio Diaz (“Plaintiffs”), in their individual  
2 capacity and on behalf of all others similarly situated, bring this Class Action  
3 Complaint against California Pizza Kitchen, Inc. (“Defendant”) and allege, upon  
4 personal knowledge as to their own actions and their counsels’ investigation, and  
5 upon information and belief as to all other matters, as follows:

6 **I. INTRODUCTION**

7 1. Plaintiffs bring this class action against Defendant for its failure to  
8 properly secure and safeguard Personally Identifiable Information (“PII”) of its  
9 employees and former employees, including (without limitation) names and Social  
10 Security Numbers.

11 2. Plaintiffs also allege Defendant failed to provide timely, accurate, and  
12 adequate notice to Plaintiffs and similarly situated current and former employees  
13 (“Class Members”) that their PII had been lost and precisely what type of  
14 information was unencrypted and is now in the possession of unknown third parties.

15 3. Defendant is a restaurant chain company that operates more than 250  
16 restaurants throughout 32 states and 10 foreign countries. Defendant’s employees  
17 entrust them with an extensive amount of their PII. Defendant retains this  
18 information—even after the employment relationship ends.

19 4. On or around September 15, 2021, Defendant “learned of a disruption  
20 to certain systems on our computing environment.”<sup>1</sup> The hacker gained access to  
21 directories where PII was stored. “On October 4, 2021, the investigation confirmed  
22 that certain files on our systems had been subject to unauthorized access.”<sup>2</sup>

23 5. More than a month later, Defendant issued a “Notice of Data Breach,”  
24 dated November 15, 2021, to those whose PII may have been impacted.

25 6. By obtaining, collecting, using, and deriving a benefit from the PII of  
26

27 <sup>1</sup> [https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-](https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-%20Sample%20Notice.pdf)  
28 [%20Sample%20Notice.pdf](https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-%20Sample%20Notice.pdf) (last visited Dec. 7, 2021).

<sup>2</sup> *Id.*

1 Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those  
2 individuals to protect and safeguard that information from unauthorized access and  
3 intrusion. Defendant admits that the unencrypted PII that the attacker viewed and  
4 took included at least individuals' names, and Social Security numbers.

5 7. Hackers can access and then offer for sale the PII to criminals. The  
6 exposed PII of Plaintiffs and Class Members can, and on information and belief, has  
7 been sold on the dark web. Plaintiffs and Class Members now face a present and  
8 lifetime risk of identity theft, which is heightened here by the loss of Social Security  
9 Numbers.

10 8. This PII was compromised due to Defendant's negligent and/or careless  
11 acts and omissions and the failure to protect the PII of Plaintiffs and Class Members.  
12 In addition to Defendant's failure to prevent the Data Breach, after discovering the  
13 breach, Defendant waited more than a month to report it to the states' Attorneys  
14 General and affected individuals. Defendant has not informed Plaintiffs or Class  
15 Members what the specific vulnerabilities and root causes of the breach are.

16 9. As a result of this delayed response, Plaintiffs and Class Members had  
17 no idea their PII had been compromised, and that they were, and continue to be, at  
18 significant risk of identity theft and various other forms of personal, social, and  
19 financial harm. The risk will remain for their respective lifetimes.

20 10. Plaintiffs bring this action on behalf of all persons whose PII was  
21 compromised as a result of Defendant's failure to: (i) adequately protect the PII of  
22 Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's  
23 inadequate information security practices; and (iii) effectively secure hardware  
24 containing protected PII using reasonable and effective security procedures free of  
25 vulnerabilities and incidents. Defendant's conduct amounts to negligence and  
26 violates federal and state statutes.

27 11. Plaintiffs and Class Members have suffered injury as a result of  
28 Defendant's conduct. These injuries include: (i) lost or diminished value of PII;

1 (ii) out-of-pocket expenses associated with the prevention, detection, and recovery  
2 from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost  
3 opportunity costs associated with attempting to mitigate the actual consequences of  
4 the Data Breach, including but not limited to lost time; and (iv) the continued and  
5 certainly increased risk to their PII, which: (a) remains unencrypted and available  
6 for unauthorized third parties to access and abuse; and (b) may remain backed up in  
7 Defendant's possession and is subject to further unauthorized disclosures so long as  
8 Defendant fails to undertake appropriate and adequate measures to protect the PII.

9 12. Defendant disregarded the rights of Plaintiffs and Class Members by  
10 intentionally, willfully, recklessly, or negligently failing to implement and maintain  
11 adequate and reasonable measures to ensure that the PII of Plaintiffs and Class  
12 Members was safeguarded, failing to take available steps to prevent an unauthorized  
13 disclosure of data, and failing to follow applicable, required, and appropriate  
14 protocols, policies, and procedures regarding the encryption of data, even for internal  
15 use. As a result, the PII of Plaintiffs and Class Members was compromised through  
16 disclosure to an unknown and unauthorized third party. Plaintiffs and Class  
17 Members have a continuing interest in ensuring that their information is and remains  
18 safe, and they should be entitled to injunctive and other equitable relief.

## 19 II. PARTIES

20 13. Plaintiff Brett Rigas is a resident and citizen of Florida. Defendant  
21 obtained and continues to maintain Plaintiff Rigas's PII and has a legal duty and  
22 obligation to protect that PII from unauthorized access and disclosure. Plaintiff Rigas  
23 would not have entrusted his PII to Defendant, his former employer, had he known  
24 that it would fail to maintain adequate data security. Plaintiff Rigas's PII was  
25 compromised and disclosed as a result of the Data Breach.

26 14. Plaintiff Evencio Diaz is a resident and citizen of Florida. Defendant  
27 obtained and continues to maintain Plaintiff Diaz's PII and has a legal duty and  
28 obligation to protect that PII from unauthorized access and disclosure. Plaintiff Diaz



1 would not have entrusted his PII to Defendant, his former employer, had he known  
2 that it would fail to maintain adequate data security. Plaintiff Diaz's PII was  
3 compromised and disclosed as a result of the Data Breach.

4 15. Defendant California Pizza Kitchen, Inc., is a Delaware corporation  
5 with its headquarters in Costa Mesa, California.

6 16. All of Plaintiffs' claims stated herein are asserted against Defendant and  
7 any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

### 8 **III. JURISDICTION AND VENUE**

9 17. This Court has subject matter and diversity jurisdiction over this action  
10 under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of  
11 controversy exceeds the sum or value of \$5 million, exclusive of interest and costs,  
12 there are more than 100 members in the proposed Class, and at least one Class  
13 Member is a citizen of a state different from Defendant to establish minimal  
14 diversity.

15 18. This court has personal jurisdiction over Defendant named in this action  
16 because Defendant is headquartered in this District and conducts substantial business  
17 in this District.

18 19. Venue is proper in this District under 28 U.S.C. §1391(b) because  
19 Defendant is headquartered in this District and a substantial part of the events or  
20 omissions giving rise to Plaintiff's claims occurred in this District.

### 21 **IV. FACTUAL ALLEGATIONS**

#### 22 ***Background***

23 20. Defendant is a very large restaurant chain, with more than 250  
24 restaurants throughout the United States. Defendant has employed tens of thousands  
25 of people to operate and supply these restaurants. As of this writing, it has  
26  
27  
28

1 approximately 14,000 employees.<sup>3</sup>

2 21. Plaintiffs and Class Members employed by Defendant were required to  
3 provide Defendant with sensitive and confidential information, including their  
4 names and Social Security Numbers. In particular, Social Security Numbers are  
5 static, do not change, and can be used to commit countless different types of financial  
6 crimes.

7 22. Plaintiffs and Class Members, as current and former employees of  
8 Defendant, relied on the sophistication of Defendant to keep their PII confidential  
9 and securely maintained, to use this information for business purposes only, and to  
10 make only authorized disclosures of this information. Plaintiffs and Class Members  
11 demand security to safeguard their PII.

12 23. Defendant had a duty to adopt reasonable measures to protect the PII of  
13 Plaintiffs and Class Members from involuntary disclosure to third parties.

14 ***The Data Breach***

15 24. Beginning on or about November 15, 2021, Defendant sent Plaintiffs  
16 and other current and former employees a *Notice of Data Breach*. Defendant  
17 informed the recipients of the notice that:

18 **What Happened?**

19 On or about September 15, 2021, CPK learned of a disruption to certain  
20 systems on our computing environment. We immediately secured our  
21 environment and, with the assistance of leading third-party computer  
22 forensic specialists, launched an investigation to determine the nature  
23 and scope of the incident. On October 4, 2021, the investigation  
24 confirmed that certain files on our systems had been subject to  
25 unauthorized access.  
26

27  
28 <sup>3</sup> See <https://www.zippia.com/california-pizza-kitchen-careers-17850/#> (last visited Dec. 7, 2021).

1           **What Information Was Involved?**

2           Our investigation determined that the information related to you that  
3           may have been affected includes your name and Social Security  
4           number.

5  
6           25. On or about November 19, 2021, Defendant sent data breach  
7           notifications to various state Attorneys General, including New Hampshire's  
8           Attorney General, signed by Katie Butler at Mullen Coughlin as counsel for  
9           Defendant.<sup>4</sup>

10           26. Defendant admitted that unauthorized individuals accessed directories  
11           that contained PII and was capable of "accessing and acquiring" the PII, names and  
12           Social Security Numbers, stating that "that certain files on our systems had been  
13           subject to unauthorized access."<sup>5</sup>

14           27. However, in neither the Notice of Data Breach nor in the Notice of Data  
15           Event to the states' Attorneys General did Defendant state that it had notified law  
16           enforcement of the breach at the time it learned of it.

17           28. The PII of Plaintiffs and Class Member is, already, upon information  
18           and belief for sale on the dark web, and may have already fallen into the hands of  
19           companies that will use the detailed PII for targeted marketing without the approval  
20           of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII  
21           of Plaintiffs and Class Members.

22           29. Defendant did not use reasonable security procedures and practices  
23           appropriate to the nature of the sensitive information they were maintaining for  
24           Plaintiffs and Class Members, causing the exposure of PII for many current and

25  
26           <sup>4</sup> See [https://www.doj.nh.gov/consumer/security-](https://www.doj.nh.gov/consumer/security-breaches/documents/california-pizza-kitchen-20211119.pdf)  
27           breaches/documents/california-pizza-kitchen-20211119.pdf (last visited Dec. 7,  
28           2021).

28           <sup>5</sup> [https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-](https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-%20Sample%20Notice.pdf)  
              %20Sample%20Notice.pdf (last visited Dec. 7, 2021).

1 former employees, such as encrypting the information or deleting it when it is no  
2 longer needed.

3 30. As explained by the Federal Bureau of Investigation, “[p]revention is  
4 the most effective defense against ransomware and it is critical to take precautions  
5 for protection.”<sup>6</sup>

6 31. To prevent and detect cyber-attacks and/or ransomware attacks  
7 Defendant could and should have implemented, as recommended by the United  
8 States Government, the following measures:

- 9
- 10 • Implement an awareness and training program. Because end users are  
11 targets, employees and individuals should be aware of the threat of  
12 ransomware and how it is delivered.
  - 13 • Enable strong spam filters to prevent phishing emails from reaching the  
14 end users and authenticate inbound email using technologies like Sender  
15 Policy Framework (SPF), Domain Message Authentication Reporting and  
16 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to  
17 prevent email spoofing.
  - 18 • Scan all incoming and outgoing emails to detect threats and filter  
19 executable files from reaching end users.
  - 20 • Configure firewalls to block access to known malicious IP addresses.
  - 21 • Patch operating systems, software, and firmware on devices. Consider  
22 using a centralized patch management system.
  - 23 • Set anti-virus and anti-malware programs to conduct regular scans  
24 automatically.
  - 25 • Manage the use of privileged accounts based on the principle of least  
26 privilege: no users should be assigned administrative access unless

---

27 <sup>6</sup> See *How to Protect Your Networks from RANSOMWARE*, at 3,  
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 7, 2021).

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

- 3 • Configure access controls—including file, directory, and network share  
4 permissions—with least privilege in mind. If a user only needs to read  
5 specific files, the user should not have write access to those files,  
6 directories, or shares.
- 7 • Disable macro scripts from office files transmitted via email. Consider  
8 using Office Viewer software to open Microsoft Office files transmitted  
9 via email instead of full office suite applications.
- 10 • Implement Software Restriction Policies (SRP) or other controls to  
11 prevent programs from executing from common ransomware locations,  
12 such as temporary folders supporting popular Internet browsers or  
13 compression/decompression programs, including the  
14 AppData/LocalAppData folder.
- 15 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 16 • Use application whitelisting, which only allows systems to execute  
17 programs known and permitted by security policy.
- 18 • Execute operating system environments or specific programs in a  
19 virtualized environment.
- 20 • Categorize data based on organizational value and implement physical  
21 and logical separation of networks and data for different organizational  
22 units.<sup>7</sup>

22 32. To prevent and detect cyber-attacks Defendant could and should have  
23 implemented, as recommended by the United States Cybersecurity & Infrastructure  
24 Security Agency, the following measures:

- 25 • **Update and patch your computer.** Ensure your applications and  
26 operating systems (OSs) have been updated with the latest patches.

---

28 <sup>7</sup> See *id.* at 3-4.

1 Vulnerable applications and OSs are the target of most ransomware  
2 attacks....

- 3 • **Use caution with links and when entering website addresses.** Be  
4 careful when clicking directly on links in emails, even if the sender  
5 appears to be someone you know. Attempt to independently verify  
6 website addresses (e.g., contact your organization's helpdesk, search the  
7 internet for the sender organization's website or the topic mentioned in  
8 the email). Pay attention to the website addresses you click on, as well as  
9 those you enter yourself. Malicious website addresses often appear almost  
10 identical to legitimate sites, often using a slight variation in spelling or a  
11 different domain (e.g., .com instead of .net)....
- 12 • **Open email attachments with caution.** Be wary of opening email  
13 attachments, even from senders you think you know, particularly when  
14 attachments are compressed files or ZIP files.
- 15 • **Keep your personal information safe.** Check a website's security to  
16 ensure the information you submit is encrypted before you provide it....
- 17 • **Verify email senders.** If you are unsure whether or not an email is  
18 legitimate, try to verify the email's legitimacy by contacting the sender  
19 directly. Do not click on any links in the email. If possible, use a previous  
20 (legitimate) email to ensure the contact information you have for the  
21 sender is authentic before you contact them.
- 22 • **Inform yourself.** Keep yourself informed about recent cybersecurity  
23 threats and up to date on ransomware techniques. You can find  
24 information about known phishing attacks on the Anti-Phishing Working  
25 Group website. You may also want to sign up for CISA product  
26 notifications, which will alert you when a new Alert, Analysis Report,  
27 Bulletin, Current Activity, or Tip has been published.
- 28 • **Use and maintain preventative software programs.** Install antivirus

1 software, firewalls, and email filters—and keep them updated—to reduce  
2 malicious network traffic....<sup>8</sup>

3 33. To prevent and detect cyber-attacks or ransomware attacks Defendant  
4 could and should have implemented, as recommended by the Microsoft Threat  
5 Protection Intelligence Team, the following measures:

6 **Secure internet-facing assets**

- 7 - Apply latest security updates  
8 - Use threat and vulnerability management  
9 - Perform regular audit; remove privileged credentials;

10 **Thoroughly investigate and remediate alerts**

- 11 - Prioritize and treat commodity malware infections as potential  
12 full compromise;

13 **Include IT Pros in security discussions**

- 14 - Ensure collaboration among [security operations], [security  
15 admins], and [information technology] admins to configure  
16 servers and other endpoints securely;

17 **Build credential hygiene**

- 18 - Use [multifactor authentication] or [network level  
19 authentication] and use strong, randomized, just-in-time local  
20 admin passwords;

21 **Apply principle of least-privilege**

- 22 - Monitor for adversarial activities  
23 - Hunt for brute force attempts  
24 - Monitor for cleanup of Event Logs  
25 - Analyze logon events;

26  
27 <sup>8</sup> See Dept. of Homeland Security, *Security Tip (ST19-001) Protecting Against*  
28 *Ransomware* (original release date Apr. 11, 2019), <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Dec. 7, 2021).

1           **Harden infrastructure**

- 2           -     Use Windows Defender Firewall  
3           -     Enable tamper protection  
4           -     Enable cloud-delivered protection  
5           -     Turn on attack surface reduction rules and [Antimalware Scan  
6           Interface] for Office [Visual Basic for Applications].<sup>9</sup>

7           34.    Given that Defendant was storing the PII of its current and former  
8 employees, Defendant could and should have implemented all of the above measures  
9 to prevent and detect ransomware attacks.

10          35.    The occurrence of the Data Breach indicates that Defendant failed to  
11 adequately implement one or more of the above measures to prevent ransomware  
12 attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed  
13 amount of current and former employees, including Plaintiffs and Class Members.

14                   ***Defendant Acquires, Collects, and Stores the PII of Plaintiffs and***  
15                   ***Class Members***

16          36.    Defendant has historically acquired, collected, and stored the PII of  
17 Plaintiffs and Class Members.

18          37.    As a condition of maintaining employment with Defendant, Defendant  
19 requires that its employees entrust them with highly confidential PII.

20          38.    By obtaining, collecting, and storing the PII of Plaintiffs and Class  
21 Members, Defendant assumed legal and equitable duties and knew or should have  
22 known that it was responsible for protecting the PII from disclosure.

23          39.    Plaintiffs and Class Members have taken reasonable steps to maintain  
24 the confidentiality of their PII and relied on Defendant to keep their PII confidential  
25 and maintained securely, to use this information for business purposes only, and to  
26

---

27 <sup>9</sup>     See Microsoft, *Human-operated ransomware attacks: A preventable disaster*  
28 (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Dec. 7, 2021).



1 make only authorized disclosures of this information.

2 ***Securing PII and Preventing Breaches***

3 40. Defendant could have prevented this Data Breach by properly securing  
4 and encrypting the files and file servers containing the PII of Plaintiffs and Class  
5 Members. Alternatively, Defendant could have destroyed the data, especially data  
6 from former employees such as Plaintiffs.

7 41. Defendant's policies on its website include promises and legal  
8 obligations to maintain and protect PII, demonstrating an understanding of the  
9 importance of securing PII. For example, Defendant's Privacy Statement provides  
10 in part that "We take the security of your information seriously. We use technical  
11 and administrative security measures designed to reduce the risks of loss, misuse,  
12 unauthorized access, disclosure and alteration."<sup>10</sup>

13 42. Defendant's negligence in safeguarding the PII of Plaintiffs and Class  
14 Members is exacerbated by the repeated warnings and alerts directed to protecting  
15 and securing sensitive data.

16 43. Despite the prevalence of public announcements of data breach and data  
17 security compromises, Defendant failed to take appropriate steps to protect the PII  
18 of Plaintiffs and Class Members from being compromised.

19 ***Value of Personally Identifiable Information***

20 44. The Federal Trade Commission ("FTC") defines identity theft as "a  
21 fraud committed or attempted using the identifying information of another person  
22 without authority."<sup>11</sup> The FTC describes "identifying information" as "any name or  
23 number that may be used, alone or in conjunction with any other information, to  
24 identify a specific person," including, among other things, "[n]ame, Social Security  
25 number, date of birth, official State or government issued driver's license or  
26

27 \_\_\_\_\_  
28 <sup>10</sup> See <https://www.cpk.com/legal/privacy-policy> (last visited Dec. 7, 2021).

<sup>11</sup> 17 C.F.R. § 248.201 (2013).

1 identification number, alien registration number, government passport number,  
2 employer or taxpayer identification number.”<sup>12</sup>

3 45. The PII of individuals remains of high value to criminals, as evidenced  
4 by the prices they will pay through the dark web. Numerous sources cite dark web  
5 pricing for stolen identity credentials. For example, Personal Information can be sold  
6 at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to  
7 \$200.<sup>13</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to  
8 \$110 on the dark web.<sup>14</sup> Criminals can also purchase access to entire company data  
9 breaches from \$900 to \$4,500.<sup>15</sup>

10 46. Social Security numbers, for example, are among the worst kind of PII  
11 to have stolen because they may be put to a variety of fraudulent uses and are  
12 difficult for an individual to change. The Social Security Administration stresses that  
13 the loss of an individual’s Social Security number, as is the case here, can lead to  
14 identity theft and extensive financial fraud:

15  
16 A dishonest person who has your Social Security number can use it to  
17 get other personal information about you. Identity thieves can use your  
18 number and your good credit to apply for more credit in your name.  
19 Then, they use the credit cards and don’t pay the bills, it damages your

20  
21 <sup>12</sup> 17 C.F.R. § 248.201 (2013).

22 <sup>13</sup> Anita George, *Your personal data is for sale on the dark web. Here’s how*  
23 *much it costs*, DIGITALTRENDS, Oct. 16, 2019,  
24 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Dec. 7, 2021).

25 <sup>14</sup> Brian Stack, *Here’s How Much Your Personal Information Is Selling for on*  
26 *the Dark Web*, EXPERIAN, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Dec. 7, 2021).

27 <sup>15</sup> *In the Dark*, VPNOVERVIEW, 2019,  
28 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Dec. 7, 2021).

1 credit. You may not find out that someone is using your number until  
2 you're turned down for credit, or you begin to get calls from unknown  
3 creditors demanding payment for items you never bought. Someone  
4 illegally using your Social Security number and assuming your identity  
5 can cause a lot of problems.<sup>16</sup>

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

12 48. Even then, a new Social Security number may not be effective.  
13 According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit  
14 bureaus and banks are able to link the new number very quickly to the old number,  
15 so all of that old bad information is quickly inherited into the new Social Security  
16 number.”<sup>17</sup>

17 49. Based on the foregoing, the information compromised in the Data  
18 Breach is significantly more valuable than the loss of, for example, credit card  
19 information in a retailer data breach because, there, victims can cancel or close credit  
20 and debit card accounts. The information compromised in this Data Breach is  
21 impossible to “close” and difficult, if not impossible, to change—Social Security  
22 number, driver’s license number, name, and date of birth.

23 50. This data demands a much higher price on the black market. Martin  
24

---

25 <sup>16</sup> Social Security Administration, *Identity Theft and Your Social Security*  
26 *Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Dec. 7, 2021).

27 <sup>17</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to*  
28 *Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Dec. 7, 2021).

1 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to  
2 credit card information, personally identifiable information and Social Security  
3 numbers are worth more than 10x on the black market.”<sup>18</sup>

4 51. Among other forms of fraud, identity thieves may obtain driver’s  
5 licenses, government benefits, medical services, and housing or even give false  
6 information to police.

7 52. The fraudulent activity resulting from the Data Breach may not come  
8 to light for years.

9 53. There may be a time lag between when harm occurs versus when it is  
10 discovered, and also between when PII is stolen and when it is used. According to  
11 the U.S. Government Accountability Office (“GAO”), which conducted a study  
12 regarding data breaches:

13 [L]aw enforcement officials told us that in some cases, stolen data may  
14 be held for up to a year or more before being used to commit identity  
15 theft. Further, once stolen data have been sold or posted on the Web,  
16 fraudulent use of that information may continue for years. As a result,  
17 studies that attempt to measure the harm resulting from data breaches  
18 cannot necessarily rule out all future harm.<sup>19</sup>

19 54. At all relevant times, Defendant knew, or reasonably should have  
20 known, of the importance of safeguarding the PII of Plaintiffs and Class Members,  
21 including Social Security numbers and dates of birth, and of the foreseeable  
22 consequences that would occur if Defendant’s data security system was breached,  
23

---

24 <sup>18</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*  
25 *Credit Card Numbers*, NETWORKWORLD, (Feb. 6, 2015),  
26 [https://www.networkworld.com/article/2880366/anthem-hack-personal-data-](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)  
27 [stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last visited Dec. 7,  
2021).

28 <sup>19</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007),  
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Dec. 7, 2021).

1 including, specifically, the significant costs that would be imposed on Plaintiffs and  
2 Class Members as a result of a breach.

3 55. Plaintiffs and Class Members now face years of constant surveillance  
4 of their financial and personal records, monitoring, and loss of rights. The Class is  
5 incurring and will continue to incur such damages in addition to any fraudulent use  
6 of their PII.

7 56. Defendant was, or should have been, fully aware of the unique type and  
8 the significant volume of data on Defendant's servers, amounting to potentially  
9 thousands of individuals' detailed, PII and, thus, the significant number of  
10 individuals who would be harmed by the exposure of the unencrypted data.

11 57. In the breach notification letter, Defendant made an offer of 12 months  
12 of identity monitoring services. This is wholly inadequate to compensate Plaintiffs  
13 and Class Members as it fails to provide for the fact that victims of data breaches  
14 and other unauthorized disclosures commonly face multiple years of ongoing  
15 identity theft, medical and financial fraud, and it entirely fails to provide sufficient  
16 compensation for the unauthorized release and disclosure of Plaintiffs' and Class  
17 Members' PII.

18 58. The injuries to Plaintiffs and Class Members were directly and  
19 proximately caused by Defendant's failure to implement or maintain adequate data  
20 security measures for the PII of Plaintiffs and Class Members.

21 59. The ramifications of Defendant's failure to keep secure the PII of  
22 Plaintiffs and Class Members are long lasting and severe. Once PII is stolen,  
23 particularly Social Security numbers, fraudulent use of that information and damage  
24 to victims may continue for years.

25 ***Plaintiff Brett Rigas's Experience***

26 60. Plaintiff Rigas was required to provide his PII to Defendant in  
27 connection with his employment, which started in or about 2004 and ended in or  
28 about 2020.

1           61. On or about November 2021, Plaintiff Rigas received notice from  
2 Defendant that his PII had been improperly accessed and/or obtained by  
3 unauthorized third parties. This notice indicated that Plaintiff Rigas's PII, including  
4 name and Social Security Number was compromised as a result of the Data Breach.

5           62. Plaintiff Rigas made reasonable efforts to mitigate the impact of the  
6 Data Breach, including but not limited to: researching the Data Breach; reviewing  
7 credit reports and financial account statements for any indications of actual or  
8 attempted identity theft or fraud; reversing fraudulent charges that he believes are  
9 due to criminal gaining access to his account via his Social Security Number and  
10 contacting services in order to reset passwords. Plaintiff Rigas has spent at least 20  
11 hours dealing with the Data Breach, valuable time Plaintiff Rigas otherwise would  
12 have spent on other activities, including but not limited to work and/or recreation.

13           63. Additionally, Plaintiff Rigas has been notified by his credit monitoring  
14 service since the Data Breach that individuals have attempted to make fraudulent  
15 financial transactions in his name.

16           64. Furthermore, since the Data Breach, Plaintiff Rigas has noticed a sharp  
17 increase in the number of spam texts and calls the he has received on a daily basis.  
18 These calls and texts require are a near-constant annoyance and have required time  
19 and attention to address as much as possible.

20           65. As a result of the Data Breach, Plaintiff Rigas has suffered emotional  
21 distress due to the release of his PII, which he believed would be protected from  
22 unauthorized access and disclosure, including anxiety about unauthorized parties  
23 viewing, selling, and/or using his PII for purposes of identity theft and fraud.  
24 Plaintiff Rigas is very concerned about identity theft and fraud, as well as the  
25 consequences of such identity theft and fraud resulting from the Data Breach.

26           66. Plaintiff Rigas suffered actual injury from having his PII compromised  
27 as a result of the Data Breach including, but not limited to: (a) damage to and  
28 diminution in the value of his PII, a form of property that Defendant obtained from

1 Plaintiff Rigas; (b) violation of his privacy rights; and (c) actual, present, imminent  
2 and impending injury arising from the increased risk of identity theft and fraud.

3 67. As a result of the Data Breach, Plaintiff Rigas anticipates spending  
4 considerable time and money on an ongoing basis to try to mitigate and address  
5 harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rigas is  
6 at a present risk and will continue to be at increased risk of identity theft and fraud  
7 for years to come.

8 ***Plaintiff Evencio Diaz's Experience***

9 68. Plaintiff Diaz was required to provide his PII to Defendant in  
10 connection with his employment, which started in or about February 2019 and ended  
11 in or about March 2020.

12 69. On or about November 2021, Plaintiff Diaz received notice from  
13 Defendant that his PII had been improperly accessed and/or obtained by  
14 unauthorized third parties. This notice indicated that Plaintiff Diaz's PII, including  
15 name and Social Security Number, was compromised as a result of the Data Breach.

16 70. Plaintiff Diaz made reasonable efforts to mitigate the impact of the Data  
17 Breach, including but not limited to: researching the Data Breach; reviewing credit  
18 reports and financial account statements for any indications of actual or attempted  
19 identity theft or fraud; and reversing fraudulent charges that he believes are due to  
20 criminal gaining access to his account via his Social Security Number. Plaintiff Diaz  
21 has spent at least 10 hours dealing with the Data Breach, valuable time Plaintiff Diaz  
22 otherwise would have spent on other activities, including but not limited to work  
23 and/or recreation.

24 71. Furthermore, since the Data Breach, Plaintiff Diaz has noticed a sharp  
25 increase in the number of spam texts and calls the he has received on a daily basis.  
26 These calls and texts require are a near-constant annoyance and have required time  
27 and attention to address as much as possible.





1 their immediate family members.

2 77. Plaintiffs reserve the right to modify or amend the definition of the  
3 proposed Class before the Court determines whether certification is appropriate.

4 78. Numerosity, Fed. R. Civ. P. 23(a)(1): The Class is so numerous that  
5 joinder of all members is impracticable. The Class is apparently identifiable within  
6 Defendant's records. A notification to the Maine Attorney General indicates that the  
7 size of the Class is at least 103,767 individuals.<sup>20</sup>

8 79. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and  
9 fact common to the Class exist and predominate over any questions affecting only  
10 individual Class Members. These include:

- 11 a. Whether and to what extent Defendant had a duty to protect the PII of  
12 Plaintiffs and Class Members;
- 13 b. Whether Defendant had a duty not to disclose the PII of Plaintiffs and  
14 Class Members to unauthorized third parties;
- 15 c. Whether Defendant had a duty not to use the PII of Plaintiffs and Class  
16 Members for non-business purposes;
- 17 d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs  
18 and Class Members;
- 19 e. Whether and when Defendant actually learned of the Data Breach;
- 20 f. Whether Defendant adequately, promptly, and accurately informed  
21 Plaintiffs and Class Members that their PII had been compromised;
- 22 g. Whether Defendant violated the law by failing to promptly notify  
23 Plaintiffs and Class Members that their PII had been compromised;
- 24 h. Whether Defendant failed to implement and maintain reasonable security  
25 procedures and practices appropriate to the nature and scope of the  
26

27  
28 <sup>20</sup> See <https://apps.web.maine.gov/online/aeviewer/ME/40/ea812f00-c605-4b8e-a6e2-9dd53169b256.shtml> (last visited Dec. 7, 2021).

1 information compromised in the Data Breach;

2 i. Whether Defendant adequately addressed and fixed the vulnerabilities  
3 which permitted the Data Breach to occur;

4 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices  
5 by failing to safeguard the PII of Plaintiffs and Class Members;

6 k. Whether Plaintiffs and Class Members are entitled to actual damages,  
7 statutory damages, and/or nominal damages as a result of Defendant's  
8 wrongful conduct;

9 l. Whether Plaintiffs and Class Members are entitled to restitution as a  
10 result of Defendant's wrongful conduct; and

11 m. Whether Plaintiffs and Class Members are entitled to injunctive relief to  
12 redress the imminent and currently ongoing harm faced as a result of the  
13 Data Breach.

14 80. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of  
15 those of other Class Members because they had their PII compromised as a result of  
16 the Data Breach due to Defendant's misfeasance.

17 81. Policies Generally Applicable to the Class: This class action is also  
18 appropriate for certification because Defendant acted or refused to act on grounds  
19 generally applicable to the Class, thereby requiring the Court's imposition of  
20 uniform relief to ensure compatible standards of conduct toward the Class Members  
21 and making final injunctive relief appropriate with respect to the Class as a whole.  
22 Defendant's policies challenged herein apply to and affect Class Members uniformly  
23 and Plaintiff's challenge of these policies hinges on Defendant's conduct with  
24 respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

25 82. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately  
26 represent and protect the interests of the Class Members in that they have no  
27 disabling conflicts of interest that would be antagonistic to those of the other  
28 Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the

1 Members of the Class and the infringement of the rights and the damages they have  
2 suffered are typical of other Class Members. Plaintiffs have retained counsel  
3 experienced in complex class action litigation, and Plaintiffs intend to prosecute this  
4 action vigorously.

5 83. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class  
6 litigation is an appropriate method for fair and efficient adjudication of the claims  
7 involved. Class action treatment is superior to all other available methods for the fair  
8 and efficient adjudication of the controversy alleged herein; it will permit a large  
9 number of Class Members to prosecute their common claims in a single forum  
10 simultaneously, efficiently, and without the unnecessary duplication of evidence,  
11 effort, and expense that hundreds of individual actions would require. Class action  
12 treatment will permit the adjudication of relatively modest claims by certain Class  
13 Members, who could not individually afford to litigate a complex claim against a  
14 large corporation, like Defendant. Further, even for those Class Members who could  
15 afford to litigate such a claim, it would still be economically impractical and impose  
16 a burden on the courts.

17 84. The nature of this action and the nature of laws available to Plaintiffs  
18 and Class Members make the use of the class action device a particularly efficient  
19 and appropriate procedure to afford relief to Plaintiffs and Class Members for the  
20 wrongs alleged because Defendant would necessarily gain an unconscionable  
21 advantage since it would be able to exploit and overwhelm the limited resources of  
22 each individual Class Member with superior financial and legal resources; the costs  
23 of individual suits could unreasonably consume the amounts that would be  
24 recovered; proof of a common course of conduct to which Plaintiffs were exposed  
25 is representative of that experienced by the Class and will establish the right of each  
26 Class Member to recover on the cause of action alleged; and individual actions  
27 would create a risk of inconsistent results and would be unnecessary and duplicative  
28 of this litigation.

1 85. The litigation of the claims brought herein is manageable. Defendant's  
2 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable  
3 identities of Class Members demonstrates that there would be no significant  
4 manageability problems with prosecuting this lawsuit as a class action.

5 86. Adequate notice can be given to Class Members directly using  
6 information maintained in Defendant's records.

7 87. Unless a Class-wide injunction is issued, Defendant may continue in its  
8 failure to properly secure the PII of Class Members, Defendant may continue to  
9 refuse to provide proper notification to Class Members regarding the Data Breach,  
10 and Defendant may continue to act unlawfully as set forth in this Complaint.

11 88. Further, Defendant has acted or refused to act on grounds generally  
12 applicable to the Class and, accordingly, final injunctive or corresponding  
13 declaratory relief with regard to the Class Members as a whole is appropriate under  
14 Rule 23(b)(2) of the Federal Rules of Civil Procedure.

15 89. Likewise, particular issues under Rule 23(c)(4) are appropriate for  
16 certification because such claims present only particular, common issues, the  
17 resolution of which would advance the disposition of this matter and the parties'  
18 interests therein. Such particular issues include, but are not limited to:

- 19 a. Whether Defendant owed a legal duty to Plaintiffs and Class  
20 Members to exercise due care in collecting, storing, using, and  
21 safeguarding their PII;
- 22 b. Whether Defendant breached a legal duty to Plaintiffs and Class  
23 Members to exercise due care in collecting, storing, using, and  
24 safeguarding their PII;
- 25 c. Whether Defendant failed to comply with its own policies and  
26 applicable laws, regulations, and industry standards relating to data  
27 security;
- 28 d. Whether an implied contract existed between Defendant on the one

1 hand, and Plaintiffs and Class Members on the other, and the terms  
2 of that implied contract;

- 3 e. Whether Defendant breached the implied contract;
- 4 f. Whether Defendant adequately and accurately informed Plaintiffs  
5 and Class Members that their PII had been compromised;
- 6 g. Whether Defendant failed to implement and maintain reasonable  
7 security procedures and practices appropriate to the nature and scope  
8 of the information compromised in the Data Breach;
- 9 h. Whether Defendant engaged in unfair, unlawful, or deceptive  
10 practices by failing to safeguard the PII of Plaintiffs and Class  
11 Members; and,
- 12 i. Whether Class Members are entitled to actual damages, statutory  
13 damages, nominal damages, and/or injunctive relief as a result of  
14 Defendant's wrongful conduct.

15 **COUNT I**  
16 **NEGLIGENCE**

17 **(On Behalf of Plaintiffs and the Class)**

18 90. Plaintiffs and the Class re-allege and incorporate by reference herein all  
19 of the allegations contained in paragraphs 1 through 89.

20 91. As a condition of their employment with Defendant or by purchasing  
21 goods from Defendant, Defendant's current and former employees and customers  
22 were obligated to provide Defendant with PII, among other sensitive PII, their names  
23 and Social Security Numbers.

24 92. Plaintiffs and the Class entrusted their PII to Defendant on the premise  
25 and with the understanding that Defendant would safeguard their information, use  
26 their PII for business purposes only, and/or not disclose their PII to unauthorized  
27 third parties.

28 93. Defendant has full knowledge of the sensitivity of the PII and the types

1 of harm that Plaintiffs and the Class could and would suffer if the PII were  
2 wrongfully disclosed.

3 94. Defendant knew or reasonably should have known that the failure to  
4 exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the  
5 Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the  
6 harm occurred through the criminal acts of a third party.

7 95. Defendant had a duty to exercise reasonable care in safeguarding,  
8 securing, and protecting such information from being compromised, lost, stolen,  
9 misused, and/or disclosed to unauthorized parties. This duty includes, among other  
10 things, designing, maintaining, and testing Defendant's security protocols to ensure  
11 that the PII of Plaintiffs and the Class in Defendant's possession was adequately  
12 secured and protected.

13 96. Defendant also had a duty to exercise appropriate clearinghouse  
14 practices to remove former employees' PII that Defendant was no longer required to  
15 retain pursuant to regulations.

16 97. Defendant also had a duty to have procedures in place to detect and  
17 prevent the improper access and misuse of the PII of Plaintiffs and the Class.

18 98. Defendant's duty to use reasonable security measures arose as a result  
19 of the special relationship that existed between Defendant and Plaintiffs and the  
20 Class. That special relationship arose because Plaintiffs and the Class entrusted  
21 Defendant with their confidential PII, a necessary part of employment with the  
22 company or making purchases from Defendant.

23 99. Defendant was subject to an "independent duty," untethered to any  
24 contract between Defendant and Plaintiffs or the Class.

25 100. A breach of security, unauthorized access, and resulting injury to  
26 Plaintiffs and the Class was reasonably foreseeable, particularly in light of  
27 Defendant's inadequate security practices.

28 101. Plaintiffs and the Class were the foreseeable and probable victims of

1 any inadequate security practices and procedures. Defendant knew or should have  
2 known of the inherent risks in collecting and storing the PII of Plaintiffs and the  
3 Class, the critical importance of providing adequate security of that PII, and the  
4 necessity for encrypting or redacting PII stored on Defendant's systems.

5 102. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs  
6 and the Class. Defendant's misconduct included, but was not limited to, its failure  
7 to take the steps and opportunities to prevent the Data Breach as set forth herein.  
8 Defendant's misconduct also included its decisions to not comply with industry  
9 standards for the safekeeping of the PII of Plaintiffs and the Class, including basic  
10 encryption techniques freely available to Defendant.

11 103. Plaintiffs and the Class had no ability to protect their PII that was in,  
12 and possibly remains in, Defendant's possession.

13 104. Defendant was in a position to protect against the harm suffered by  
14 Plaintiffs and the Class as a result of the Data Breach.

15 105. Defendant had and continues to have a duty to adequately disclose that  
16 the PII of Plaintiffs and the Class within Defendant's possession might have been  
17 compromised, how it was compromised, and precisely the types of data that were  
18 compromised and when. Such notice was necessary to allow Plaintiffs and the Class  
19 to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use  
20 of their PII by third parties.

21 106. Defendant had a duty to employ proper procedures to prevent the  
22 unauthorized dissemination of the PII of Plaintiffs and the Class.

23 107. Defendant has admitted that the PII of Plaintiffs and the Class was  
24 wrongfully lost and potentially disclosed to unauthorized third persons as a result of  
25 the Data Breach.

26 108. Defendant, through its actions and/or omissions, unlawfully breached  
27 its duties to Plaintiffs and the Class by failing to implement industry protocols and  
28 exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the

1 Class during the time the PII was within Defendant's possession or control.

2 109. Defendant improperly and inadequately safeguarded the PII of  
3 Plaintiffs and the Class in deviation of standard industry rules, regulations, and  
4 practices at the time of the Data Breach.

5 110. Defendant failed to heed industry warnings and alerts to provide  
6 adequate safeguards to protect the PII of Plaintiffs and the Class in the face of  
7 increased risk of theft.

8 111. Defendant, through its actions and/or omissions, unlawfully breached  
9 its duty to Plaintiffs and the Class by failing to have appropriate procedures in place  
10 to detect and prevent dissemination of its current and former employees' PII.

11 112. Defendant, through its actions and/or omissions, unlawfully breached  
12 its duty to adequately and timely disclose to Plaintiffs and the Class the existence  
13 and scope of the Data Breach.

14 113. But for Defendant's wrongful and negligent breach of duties owed to  
15 Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been  
16 compromised.

17 114. There is a close causal connection between Defendant's failure to  
18 implement security measures to protect the PII of Plaintiffs and the Class and the  
19 present harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII  
20 of Plaintiffs and the Class was lost and accessed as the proximate result of  
21 Defendant's failure to exercise reasonable care in safeguarding such PII by adopting,  
22 implementing, and maintaining appropriate security measures.

23 115. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices  
24 in or affecting commerce," including, as interpreted and enforced by the FTC, the  
25 unfair act or practice by businesses, such as Defendant, of failing to use reasonable  
26 measures to protect PII. The FTC publications and orders described above also form  
27 part of the basis of Defendant's duty in this regard.

28 116. Defendant violated Section 5 of the FTC Act by failing to use



1 reasonable measures to protect PII and not complying with applicable industry  
2 standards, as described in detail herein. Defendant's conduct was particularly  
3 unreasonable given the nature and amount of PII it obtained and stored and the  
4 foreseeable consequences of the immense damages that would result to Plaintiffs  
5 and the Class.

6 117. Defendant's violation of Section 5 of the FTC Act constitutes  
7 negligence *per se*.

8 118. Plaintiffs and the Class are within the class of persons that the FTC Act  
9 was intended to protect.

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

15 120. As a direct and proximate result of Defendant's negligence and  
16 negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury,  
17 including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity  
18 of how their PII is used; (iii) the compromise, publication, and/or theft of their PII;  
19 (iv) out-of-pocket expenses associated with the prevention, detection, and recovery  
20 from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost  
21 opportunity costs associated with effort expended and the loss of productivity  
22 addressing and attempting to mitigate the actual present and future consequences of  
23 the Data Breach, including but not limited to efforts spent researching how to  
24 prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs  
25 associated with placing freezes on credit reports; (vii) the continued risk to their PII,  
26 which remain in Defendant's possession and is subject to further unauthorized  
27 disclosures so long as Defendant fails to undertake appropriate and adequate  
28 measures to protect the PII of Plaintiffs and the Class; and (viii) costs in terms of

1 time, effort, and money that will be expended to prevent, detect, contest, and repair  
2 the impact of the PII compromised as a result of the Data Breach for the remainder  
3 of the lives of Plaintiffs and the Class.

4 121. As a direct and proximate result of Defendant's negligence and  
5 negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer  
6 other forms of injury and/or harm, including, but not limited to, anxiety, emotional  
7 distress, loss of privacy, and other economic and non-economic losses.

8 122. Additionally, as a direct and proximate result of Defendant's negligence  
9 and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the  
10 continued risks of exposure of their PII, which remains in Defendant's possession  
11 and is subject to further unauthorized disclosures so long as Defendant fails to  
12 undertake appropriate and adequate measures to protect the PII in its continued  
13 possession.

14 123. Plaintiffs and Class Members are therefore entitled to damages,  
15 including restitution and unjust enrichment, declaratory and injunctive relief, and  
16 attorney fees, costs, and expenses.

17 **COUNT II**  
18 **BREACH OF IMPLIED CONTRACT**  
19 **(On Behalf of Plaintiffs and the Class)**

20 124. Plaintiffs and the Class re-allege and incorporate by reference herein all  
21 of the allegations contained in paragraphs 1 through 89.

22 125. Defendant required Plaintiffs and the Class to provide their PII,  
23 including names and Social Security numbers, and other PII, as a condition of their  
24 employment.

25 126. As a condition of their employment with or purchases from Defendant,  
26 Plaintiffs and the Class provided their PII. In so doing, Plaintiffs and the Class  
27 entered into implied contracts with Defendant by which Defendant agreed to  
28 safeguard and protect such information, to keep such information secure and

1 confidential, and to timely and accurately notify Plaintiffs and the Class if their data  
2 had been breached and compromised or stolen.

3 127. Plaintiffs and the Class fully performed their obligations under the  
4 implied contracts with Defendant.

5 128. Defendant breached the implied contracts it made with Plaintiffs and  
6 the Class by failing to safeguard and protect their PII, and by failing to provide  
7 timely and accurate notice to them that their PII was compromised as a result of the  
8 Data Breach.

9 129. As a direct and proximate result of Defendant's above-described breach  
10 of implied contract, Plaintiffs and the Class have suffered (and will continue to  
11 suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and  
12 abuse, resulting in monetary loss and economic harm; actual identity theft crimes,  
13 fraud, and abuse, resulting in monetary loss and economic harm; loss of the  
14 confidentiality of the stolen confidential data; the illegal sale of the compromised  
15 data on the dark web; expenses and/or time spent on credit monitoring and identity  
16 theft insurance; time spent scrutinizing bank statements, credit card statements, and  
17 credit reports; expenses and/or time spent initiating fraud alerts, decreased credit  
18 scores and ratings; lost work time; and other economic and non-economic harm.

19  
20 **COUNT III**  
21 **INVASION OF PRIVACY**  
22 **(On Behalf of Plaintiffs and the Class)**

23 130. Plaintiffs and the Class re-allege and incorporate by reference herein  
24 all of the allegations contained in paragraphs 1 through 89.

25 131. Plaintiffs and the Class had a legitimate expectation of privacy to their  
26 PII and were entitled to the protection of this information against disclosure to  
27 unauthorized third parties.

28 132. Defendant owed a duty to its current and former customers and  
employees, including Plaintiffs and the Class, to keep their PII confidential.

1 133. Defendant failed to protect and released to unknown and unauthorized  
2 third parties the PII of Plaintiffs and the Class.

3 134. Defendant allowed unauthorized and unknown third parties access to  
4 and examination of the PII of Plaintiffs and the Class, by way of Defendant's failure  
5 to protect the PII.

6 135. The unauthorized release to, custody of, and examination by  
7 unauthorized third parties of the PII of Plaintiffs and the Class is highly offensive to  
8 a reasonable person.

9 136. The intrusion was into a place or thing which was private and is entitled  
10 to be private. Plaintiffs and the Class disclosed their PII to Defendant as part of the  
11 current and former employees' employment with Defendant and/or during a  
12 consumer transaction with Defendant, but privately with an intention that the PII  
13 would be kept confidential and would be protected from unauthorized disclosure.  
14 Plaintiffs and the Class were reasonable in their belief that such information would  
15 be kept private and would not be disclosed without their authorization.

16 137. The Data Breach at the hands of Defendant constitutes an intentional  
17 interference with Plaintiffs' and the Class's interest in solitude or seclusion, either  
18 as to their persons or as to their private affairs or concerns, of a kind that would be  
19 highly offensive to a reasonable person.

20 138. Defendant acted with a knowing state of mind when it permitted the  
21 Data Breach to occur because it was with actual knowledge that its information  
22 security practices were inadequate and insufficient.

23 139. Because Defendant acted with this knowing state of mind, it had notice  
24 and knew the inadequate and insufficient information security practices would cause  
25 injury and harm to Plaintiffs and the Class.

26 140. As a proximate result of the above acts and omissions of Defendant, the  
27 PII of Plaintiffs and the Class was disclosed to third parties without authorization,  
28 causing Plaintiffs and the Class to suffer damages.

1 141. Unless and until enjoined, and restrained by order of this Court,  
2 Defendant's wrongful conduct will continue to cause great and irreparable injury to  
3 Plaintiffs and the Class in that the PII maintained by Defendant can be viewed,  
4 distributed, and used by unauthorized persons for years to come. Plaintiffs and the  
5 Class have no adequate remedy at law for the injuries in that a judgment for monetary  
6 damages will not end the invasion of privacy for Plaintiffs and the Class.

7  
8 **COUNT IV**  
9 **BREACH OF CONFIDENCE**  
10 **(On Behalf of Plaintiffs and the Class)**

11 142. Plaintiffs and the Class re-allege and incorporate by reference herein all  
12 of the allegations contained in paragraphs 1 through 89.

13 143. At all times during Plaintiffs' and the Class's interactions with  
14 Defendant, Defendant was fully aware of the confidential and sensitive nature of  
15 Plaintiffs' and the Class's PII that Plaintiffs and the Class provided to Defendant.

16 144. As alleged herein and above, Defendant's relationship with Plaintiffs  
17 and the Class was governed by terms and expectations that Plaintiffs' and the Class's  
18 PII would be collected, stored, and protected in confidence, and would not be  
19 disclosed to unauthorized third parties.

20 145. Plaintiffs and the Class provided their PII to Defendant with the explicit  
21 and implicit understandings that Defendant would protect and not permit the PII to  
22 be disseminated to any unauthorized third parties.

23 146. Plaintiffs and the Class also provided Plaintiffs' and the Class's PII to  
24 Defendant with the explicit and implicit understanding that Defendant would take  
25 precautions to protect that PII from unauthorized disclosure.

26 147. Defendant voluntarily received in confidence Plaintiffs' and the Class's  
27 PII with the understanding that PII would not be disclosed or disseminated to the  
28 public or any unauthorized third parties.

1 148. Due to Defendant's failure to prevent and avoid the Data Breach from  
2 occurring, Plaintiffs' and the Class's PII was disclosed and misappropriated to  
3 unauthorized third parties beyond Plaintiffs' and the Class's confidence, and without  
4 their express permission.

5 149. As a direct and proximate cause of Defendant's actions and/or  
6 omissions, Plaintiffs and the Class have suffered damages.

7 150. But for Defendant's disclosure of Plaintiffs' and the Class's PII in  
8 violation of the parties' understanding of confidence, their PII 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 Plaintiffs' and  
11 the Class's PII as well as the resulting damages.

12 151. The injury and harm Plaintiffs and the Class suffered was the  
13 reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs'  
14 and the Class's PII. Defendant knew or should have known its methods of accepting  
15 and securing Plaintiffs' and the Class's PII was inadequate as it relates to, at the very  
16 least, securing servers and other equipment containing Plaintiffs' and the Class's PII.

17 152. As a direct and proximate result of Defendant's breach of its confidence  
18 with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer  
19 injury, including but not limited to: (i) actual identity theft; (ii) the loss of the  
20 opportunity how their PII is used; (iii) the compromise, publication, and/or theft of  
21 their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and  
22 recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost  
23 opportunity costs associated with effort expended and the loss of productivity  
24 addressing and attempting to mitigate the actual present and future consequences of  
25 the Data Breach, including but not limited to efforts spent researching how to  
26 prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs  
27 associated with placing freezes on credit reports; (vii) the continued risk to their PII,  
28 which remain in Defendant's possession and is subject to further unauthorized

1 disclosures so long as Defendant fails to undertake appropriate and adequate  
2 measures to protect the PII of current and former customers and employees; and  
3 (viii) present and future costs in terms of time, effort, and money that will be  
4 expended to prevent, detect, contest, and repair the impact of the PII compromised  
5 as a result of the Data Breach for the remainder of the lives of Plaintiffs and the  
6 Class.

7 153. As a direct and proximate result of Defendant's breaches of confidence,  
8 Plaintiffs and the Class have suffered and will continue to suffer other forms of  
9 injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of  
10 privacy, and other economic and non-economic losses.

11  
12 **COUNT V**  
13 **UNJUST ENRICHMENT**  
14 **(On Behalf of Plaintiffs and the Class)**

15 154. Plaintiffs and the Class re-allege and incorporate by reference herein all  
16 of the allegations contained in paragraphs 1 through 89.

17 155. Defendant benefited from receiving Plaintiffs' and Class Members' PII  
18 by its ability to retain and use that information for its own benefit. Defendant  
19 understood this benefit.

20 156. Defendant also understood and appreciated that Plaintiffs' and Class  
21 Members' PII was private and confidential, and its value depended upon Defendant  
22 maintaining the privacy and confidentiality of that PII.

23 157. Plaintiffs and Class Members conferred a monetary benefit upon  
24 Defendant in the form of their employment and by purchasing goods from  
25 Defendant, and in connection thereto, by providing their PII to Defendant with the  
26 understanding that Defendant would pay for the administrative costs of reasonable  
27 data privacy and security practices and procedures. Specifically, they were required  
28 to provide Defendant with their PII. In exchange, Plaintiffs and Class members

1 should have received adequate protection and data security for such PII held by  
2 Defendant.

3 158. Defendant knew Plaintiffs and Class members conferred a benefit  
4 which Defendant accepted. Defendant profited from these transactions and used the  
5 PII of Plaintiffs and Class Members for business purposes.

6 159. Defendant failed to provide reasonable security, safeguards, and  
7 protections to the PII of Plaintiffs and Class Members.

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

12 161. Defendant wrongfully accepted and retained these benefits to the  
13 detriment of Plaintiffs and Class Members.

14 162. Defendant's enrichment at the expense of Plaintiffs and Class Members  
15 is and was unjust.

16 163. As a result of Defendant's wrongful conduct, as alleged above,  
17 Plaintiffs and the Class Members are entitled to restitution and disgorgement of all  
18 profits, benefits, and other compensation obtained by Defendant, plus attorneys'  
19 fees, costs, and interest thereon.

20 **PRAYER FOR RELIEF**

21 **WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members,  
22 request judgment against Defendant and that the Court grant the following:

- 23 A. For an Order certifying the Class, as defined herein, and appointing  
24 Plaintiffs and their Counsel to represent each such Class;
- 25 B. For equitable relief enjoining Defendant from engaging in the wrongful  
26 conduct complained of herein pertaining to the misuse and/or  
27 disclosure of the PII of Plaintiffs and Class Members, and from refusing  
28 to issue prompt, complete, any accurate disclosures to Plaintiffs and



1 Class Members;

2 C. For injunctive relief requested by Plaintiffs, including but not limited  
3 to, injunctive and other equitable relief as is necessary to protect the  
4 interests of Plaintiffs and Class Members, including but not limited to  
5 an order:

- 6 i. prohibiting Defendant from engaging in the wrongful and unlawful  
7 acts described herein;
- 8 ii. requiring Defendant to protect, including through encryption, all  
9 data collected through the course of its business in accordance with  
10 all applicable regulations, industry standards, and federal, state or  
11 local laws;
- 12 iii. requiring Defendant to delete, destroy, and purge the personal  
13 identifying information of Plaintiffs and Class Members unless  
14 Defendant can provide to the Court reasonable justification for the  
15 retention and use of such information when weighed against the  
16 privacy interests of Plaintiffs and Class Members;
- 17 iv. requiring Defendant to implement and maintain a comprehensive  
18 Information Security Program designed to protect the  
19 confidentiality and integrity of the PII of Plaintiffs and Class  
20 Members;
- 21 v. prohibiting Defendant from maintaining the PII of Plaintiffs and  
22 Class Members on a cloud-based database;
- 23 vi. requiring Defendant to engage independent third-party security  
24 auditors/penetration testers as well as internal security personnel to  
25 conduct testing, including simulated attacks, penetration tests, and  
26 audits on Defendant's systems on a periodic basis, and ordering  
27 Defendant to promptly correct any problems or issues detected by  
28 such third-party security auditors;

- 1           vii. requiring Defendant to engage independent third-party security  
2           auditors and internal personnel to run automated security  
3           monitoring;
- 4           viii. requiring Defendant to audit, test, and train its security personnel  
5           regarding any new or modified procedures;
- 6           ix. requiring Defendant to segment data by, among other things,  
7           creating firewalls and access controls so that if one area of  
8           Defendant's network is compromised, hackers cannot gain access to  
9           other portions of Defendant's systems;
- 10          x. requiring Defendant to conduct regular database scanning and  
11          securing checks;
- 12          xi. requiring Defendant to establish an information security training  
13          program that includes at least annual information security training  
14          for all employees, with additional training to be provided as  
15          appropriate based upon the employees' respective responsibilities  
16          with handling personal identifying information, as well as protecting  
17          the personal identifying information of Plaintiffs and Class  
18          Members;
- 19          xii. requiring Defendant to routinely and continually conduct internal  
20          training and education, and on an annual basis to inform internal  
21          security personnel how to identify and contain a breach when it  
22          occurs and what to do in response to a breach;
- 23          xiii. requiring Defendant to implement a system of tests to assess its  
24          respective employees' knowledge of the education programs  
25          discussed in the preceding subparagraphs, as well as randomly and  
26          periodically testing employees' compliance with Defendant's  
27          policies, programs, and systems for protecting personal identifying  
28          information;

1           xiv. requiring Defendant to implement, maintain, regularly review, and  
2           revise as necessary a threat management program designed to  
3           appropriately monitor Defendant's information networks for threats,  
4           both internal and external, and assess whether monitoring tools are  
5           appropriately configured, tested, and updated;

6           xv. requiring Defendant to meaningfully educate all Class Members  
7           about the threats that they face as a result of the loss of their  
8           confidential PII to third parties, as well as the steps affected  
9           individuals must take to protect themselves;

10          xvi. requiring Defendant to implement logging and monitoring programs  
11          sufficient to track traffic to and from Defendant's servers; and for a  
12          period of 10 years, appointing a qualified and independent third-  
13          party assessor to conduct a SOC 2 Type 2 attestation on an annual  
14          basis to evaluate Defendant's compliance with the terms of the  
15          Court's final judgment, to provide such report to the Court and to  
16          counsel for the class, and to report any deficiencies with compliance  
17          of the Court's final judgment;

18          D. For an award of damages, including actual, statutory, nominal, and  
19          consequential damages, as allowed by law in an amount to be  
20          determined;

21          E. For an award of attorneys' fees, costs, and litigation expenses, as  
22          allowed by law;

23          F. For prejudgment interest on all amounts awarded; and

24          G. Such other and further relief as this Court may deem just and proper.

25       ///

26       ///

27       ///

28       ///

