

1 Teresa C. Chow (SBN 237694)

tchow@bakerlaw.com

2 **BAKER & HOSTETLER LLP**

11601 Wilshire Boulevard, Suite 1400

3 Los Angeles, CA 90025-0509

Telephone: 310.820.8800

4 Facsimile: 310.820.8859

5 Attorneys for Defendant

AMERICAN FINANCIAL RESOURCES, INC.

6
7
8 **UNITED STATES DISTRICT COURT**

9 **NORTHERN DISTRICT OF CALIFORNIA**

10 EDWINA PARRAS and ROBERT PARRAS,
individually and on behalf of all others
11 similarly situated,

12 Plaintiffs,

13 v.

14 AMERICAN FINANCIAL RESOURCES,
INC.,

15 Defendant.
16

Case No.: 4;22-cv-002659

[Alameda County Superior Court Case
No. 22CV009276]

**DEFENDANT'S NOTICE OF REMOVAL
OF CIVIL ACTION**

*[Filed Concurrently with Civil Case Cover
Sheet; Notice of Pendency of Other Action;
Certification of Interested Entities or Persons;
and Request for Judicial Notice]*

Action Filed: April 1, 2022

Action Removed: May 3, 2022

PLEASE TAKE NOTICE that Defendant AMERICAN FINANCIAL RESOURCES, INC. (“Defendant” or “AFR”), by and through its undersigned counsel, hereby removes the above-captioned action from the Superior Court of the State of California in and for the County of Alameda (the “State Court”) to this Court on the grounds of original jurisdiction based on the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), and on all other grounds for jurisdiction to the extent applicable. In support of its Notice of Removal, and in accordance with 28 U.S.C. § 1446, Defendant avers as follows:

1. On April 1, 2022, Plaintiffs EDWINA PARRAS and ROBERT PARRAS (collectively, “Plaintiffs”) filed a putative Class Action Complaint (the “Complaint”) against Defendant in the State Court, styled as *Edwina Parras and Robert Parras, individually and on behalf of all others similarly situated v. American Financial Resources, Inc.*, Case No. 22CV009276 (the “State Court Action”). A true and correct copy of the Complaint is attached hereto as **Exhibit A**.

2. Plaintiffs' Complaint alleges three causes of action for: (1) Violations of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* (the "CCPA"); (2) Violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (the "UCL"), based on Defendant's alleged violations of the CCPA; and (3) breach of contract.

3. By letter dated March 31, 2022, Plaintiffs served upon Defendant via Certified Mail a CCPA demand, which included as an enclosure the Complaint in the State Court Action. Defendant received the letter and Complaint on approximately April 8, 2022. True and correct copies of the CCPA demand letter and enclosed Complaint served upon Defendant, and the State Court Action case file are attached hereto as the Exhibits identified below:

A CCPA demand letter, with unfiled Complaint enclosed

B Summons

- C Complaint
- D Civil Case Cover Sheet
- E Notice of Case Management Conference

4. Defendant is informed and believes that the aforementioned documents and exhibits constitute all of the process, pleadings, and orders on file in the State Court Action.

REMOVAL JURISDICTION – CAFA JURISDICTION

A. Statement of Jurisdiction

5. Defendant avers that this Court has original subject matter jurisdiction over this action pursuant to the Class Action Fairness Act (“CAFA”). *See* 28 U.S.C. § 1332(d)(2). CAFA grants federal district courts original jurisdiction over civil class action lawsuits filed under federal or state law in which any member of a putative class of plaintiffs is a citizen of a state different from any defendant, the matter in controversy exceeds \$5 million exclusive of interest and costs, and the number of members of all proposed plaintiff classes in the aggregate is at least 100 class members. *See* 28 U.S.C. § 1332(d). CAFA authorizes removal of such actions under 28 U.S.C. § 1446.

6. There is no presumption against removal under CAFA. *See, e.g., Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 89 (2014) (“[N]o antiremoval presumption attends cases invoking CAFA, which Congress enacted to facilitate adjudication of certain class actions in federal court.”). To the contrary, “CAFA’s ‘provisions should be read broadly, with a strong preference that interstate class actions should be heard in federal court if properly removed by any defendant.’” *Id.* at 554 (quoting S. Rep. No. 109-14, p. 43 (2005)).

7. This Court has jurisdiction over this case under CAFA, and this case may be removed pursuant to 28 U.S.C. § 1441(a), because: (1) the proposed class contains more than 100 members; (2) Defendant is not a state, state official, or other governmental entity; (3) the total amount in controversy for all class members exceeds \$5,000,000; and (4) there is diversity of citizenship between at least one class member and Defendant.

8. Removal to this Court is proper because the action was filed and is pending in the Superior Court of the State of California in and for Alameda County, which is within this judicial district. 28 U.S.C. §§ 128(b), 1446(a); *see also* Civil L.R. 3-2.

9. As set forth below, this case meets all of CAFA's requirements for removal and is timely and properly removed by the filing of this Notice.

B. THIS ACTION IS A CLASS ACTION UNDER CAFA

10. Pursuant to Section 4 of CAFA, 28 U.S.C. § 1332(d)(2):

The district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, and is a class action in which —

(A) any member of a class of plaintiffs is a citizen of a State different from any defendant;

11. CAFA defines a "class action" to include civil actions filed under state statutes or rules of procedure similar to Rule 23 of the Federal Rules of Civil Procedure ("Rule 23") that authorize an action to be brought by one or more representative persons as a class action. The Complaint alleges that "[t]his is a data breach class action" and that "Plaintiffs seek to represent and intend to seek certification of a class" *See* Complaint (Exh. A), ¶¶ 1, 48; *see also id.* at 12:10 ("Class Action Allegations"); *id.* at 19:15-20 (seeking certification of "this action ... as a class action," appointment of class counsel, and designation of Plaintiffs as representatives of the class). Therefore, this action is a "class action" under CAFA.

C. MINIMUM DIVERSITY OF CITIZENSHIP EXISTS

12. Minimum diversity exists pursuant to 28 U.S.C. § 1332(d)(2)(A).

13. **Plaintiffs' Citizenship.** The Complaint alleges that, at all relevant times, Plaintiffs resided in Alameda County, California. Complaint, ¶ 11. Further, Defendant is informed and believes that Plaintiffs currently reside in and intend to indefinitely remain living continuously in the State of California. As such, Defendant is informed and believes that Plaintiffs are both citizens of the State of California for purposes of CAFA. *See* 28 U.S.C. § 1332(a)(1) (an individual is a citizen of the state in which he or she is domiciled); *Lew v. Moss*, 797 F.2d 747, 751-52 (9th Cir. 1986) (party domiciled in state of party's address); *State Farm Mut. Auto. Ins. Co. v. Dyer*, 19 F.3d 514,

520 (10th Cir. 1994) (residence is *prima facie* evidence of domicile for purposes of determining citizenship).¹

14. **Defendant's Citizenship.** As Plaintiffs allege, Defendant “is a corporation organized under the laws of the state of New Jersey, with its principal place of business and/or headquarters located at 9 Sylvan Way, Parsippany, New Jersey 07054.” Complaint, ¶ 13; *see also* URL at <https://bizfileonline.sos.ca.gov/search/business> (search for “American Financial Resources, Inc.”). At its corporate headquarters in New Jersey, Defendant’s officers direct, control, and coordinate its activities, and its executive and administrative functions are performed there. Thus, Defendant was not and is not a citizen of the State of California, but rather was and is a citizen of the State of New Jersey for the purpose of determining jurisdiction. *See* 28 U.S.C. § 1332(c)(1); *see also Hertz Corp. v. Friend*, 559 U.S. 77, 92-93 (2010).

15. Accordingly, Defendant is a citizen of New Jersey, while Plaintiffs are citizens of California. *See* 28 U.S.C. § 1332(d)(10). Thus, the minimum diversity requirement under CAFA is satisfied. 28 U.S.C. § 1332(d)(2) (providing that CAFA jurisdiction exists over any civil action in which “any member of a class of plaintiffs is a citizen of a State different from any defendant”).

D. THE AMOUNT IN CONTROVERSY EXCEEDS \$5 MILLION

16. Defendant avers, based on the following calculations and authority, that the amount in controversy exceeds \$5,000,000 only for the purpose of establishing subject matter jurisdiction under CAFA. Defendant’s allegations and calculations are not admissions of liability or damages with respect to any aspect of this case, the proper legal test(s) applicable to Plaintiffs’ allegations, or whether a class action is proper. *See LaCrosse v. Knight Truck and Trailer Sales, LLC*, 775 F.3d 1200, 1203 (9th Cir. 2015) (“Even when defendants have persuaded a court upon a CAFA removal that the amount in controversy exceeds \$5 million, they are still free to challenge the actual amount of damages in subsequent proceedings and trial.”) (quoting *Ibarra v. Manheim Invs., Inc.*, 775 F.3d 1193, 1198 n.1 (9th Cir. 2015)).

¹ *See also Mondragon v. Capital One Auto Fin.*, 776 F.3d 880, 885-86 (9th Cir. 2013) (holding that, in connection with removal to federal court, a person’s continuing domicile in a state establishes citizenship “unless rebutted with sufficient evidence of change”).

17. Consistent with Fed. R. Civ. P. 8(a), a removing defendant's notice of removal need only contain plausible allegations to demonstrate the amount in controversy. Evidentiary submissions are **not required** unless and until the removing defendant's allegations are contested by the plaintiff or questioned by the Court:

In sum, as specified in § 1446(a), a defendant's notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold. Evidence establishing the amount is required by § 1446(c)(2)(B) only when the plaintiff contests, or the court questions, the defendant's allegation.

Dart Cherokee, 574 U.S. at 89. This standard applies to complaints, **like the Complaint in this action**, that do not allege or seek a specific amount of damages:

When plaintiffs favor state court and have prepared a complaint that does not assert the amount in controversy ... the Supreme Court has said that a defendant can establish the amount in controversy by an unchallenged, plausible assertion of the amount in controversy in its notice of removal

Ibarra, 775 F.3d at 1197-98 (citing *Dart Cherokee*).

18. A plaintiff's complaint is a court's "first source of reference in determining the amount in controversy." *LaCrosse*, 775 F.3d at 1202 (citing *St. Paul Mercury Indem. Co. v. Red Cab Co.*, 303 U.S. 283, 289 (1938) ("*St. Paul*"). Here, in determining the amount in controversy for purposes of removal, the ultimate inquiry is what amount is put "in controversy" by Plaintiffs' Complaint—not what a court or jury might later determine to be the actual amount of damages, if any. See, e.g., *Ibarra*, 775 F.3d at 1198 n.1 (defendants "are not stipulating to damages suffered" in a removal petition, "but only estimating the damages that are *in controversy*," because "jurisdiction must be analyzed on the basis of pleadings filed at the time of removal" (emph. added)); *St. Paul*, 303 U.S. at 291 ("the status of the case as disclosed by the complaint is controlling in the case of a removal"); *Scherer v. Equitable Life Assurance Soc'y of the United States*, 347 F.3d 394, 399 (2d Cir. 2003) (the "'amount in controversy' ... for jurisdictional purposes, [is] the sum put in controversy by the plaintiff's complaint"); see also, e.g., *Wilder v. Bank of Am.*, 2014 WL 6896116, at *4 (C.D. Cal. Dec. 5, 2014) (determining amount in controversy requires the court to assume that the allegations of the complaint are true and that a jury will return a verdict for the plaintiff on all

claims made in the complaint because the ultimate inquiry is what amount is put “in controversy” by the complaint, not what a defendant will actually owe).

19. Additionally, as recently confirmed by the Ninth Circuit, “the amount in controversy is not limited to damages incurred prior to removal ... [r]ather, the amount in controversy is determined by the complaint operative at the time of removal and encompasses *all relief a court may grant on that complaint if the plaintiff is victorious.*” *Chavez v. JPMorgan Chase & Co.*, 888 F.3d 413, 414-15, 417-18 (9th Cir. 2018) (emph. added). Accordingly, the amount in controversy properly includes all relief available to Plaintiffs through the end of trial.

20. Here, Plaintiffs purport to bring this action on behalf of themselves and the following putative class, collectively referred to as the “Class”:

All California residents whose [personally identifiable information (“PII”)] was subjected to the Data Breach [as that term is defined in the Complaint].

Complaint, ¶ 48. Plaintiffs and the Class seek, among other things, actual and punitive damages, equitable relief, attorneys’ fees and litigation expenses under Cal. Civ. Proc. Code § 1021.5 “and other applicable law,” and statutory damages. *Id.*, ¶ 67 and at 19:21-28.

21. CAFA authorizes the removal of class actions in which, among the other factors mentioned above, the aggregate amount in controversy for all class members exceeds five million dollars (\$5,000,000). *See* 28 U.S.C. § 1332(d). Here, the allegations in Plaintiffs’ Complaint and the claimed statutory damages and fees exceed that jurisdictional minimum.

SIZE OF PROPOSED CLASS

22. According to the Complaint, “[t]he Class members are so numerous ... that joinder of all Class members would be impracticable.” Complaint, ¶ 51. The Complaint further alleges that, “[w]hile the exact number of Class members is unknown, ... based on information and belief, *the Class consists of tens of thousands of Defendant’s customers.*” *Id.* (emph. added). Consistent with Plaintiffs’ allegations, Defendant currently estimates that approximately 15,000 California residents may have been impacted by the breach. Therefore, the aggregate membership of the proposed class is at least 100 as required under CAFA. *See* 28 U.S.C. § 1332(d)(5)(B).

AMOUNT IN CONTROVERSY

23. CAFA authorizes the removal of class actions in which, among the other factors mentioned above, Defendant avers that the aggregate amount in controversy for the types of damages sought for all of the PCMs exceeds \$5,000,000, and, therefore the amount in controversy as sought in the Complaint exceeds that jurisdictional minimum. *See* 28 U.S.C. § 1332(d).

24. The claims of the individual PCMs in a “class action” are aggregated to determine if the amount in controversy exceeds the sum or value of \$5 million. *See* 28 U.S.C. §§ 1332(d)(6), (11). In addition, Congress intended for federal jurisdiction to be appropriate under CAFA “if the value of the matter in litigation exceeds \$5,000,000 either from the viewpoint of the plaintiff *or the viewpoint of the defendant*, and regardless of the type of relief sought (*e.g.*, damages, injunctive relief, or declaratory relief).” Senate Judiciary Committee Report, S. Rep. 109-14, at 42 (emph. added). Moreover, the Senate Judiciary Committee’s Report on the final version of CAFA makes clear that any doubts regarding the maintenance of interstate class actions in state or federal court should be resolved in *favor* of federal jurisdiction.²

25. While the Complaint does not specify the amount of damages sought, as demonstrated below, the allegations in the Complaint make it more likely than not that the amount in controversy under CAFA exceeds \$5,000,000.

First Cause Of Action: Violations of the CCPA

26. In their Complaint, Plaintiffs allege that, “[o]n or about March 9, 2022, Defendant announced that an unauthorized party had gained access to its computer systems and certain [of its] files were accessed without authorization between December 6 to December 20, 2021 (the ‘Data Breach’).” Complaint, ¶ 2.

² *See* S. Rep. 109-14, at 42-43 (“[I]f a federal court is uncertain about whether ‘all matters in controversy’ in a purported class action ‘do not in the aggregate exceed the sum or value of \$5,000,000,’ the court should err in favor of exercising jurisdiction over the case ... Overall, new section 1332(d) is intended to expand substantially federal court jurisdiction over class actions. Its provisions should be read broadly, with a strong preference that interstate class actions should be heard in a federal court if properly removed by any defendant.”).

27. In support of their First Cause of Action, Plaintiffs contend that Defendant violated the CCPA because “Plaintiffs’ PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names, Social Security numbers and/or Driver’s License numbers, was wrongfully accessed and taken by unauthorized persons in the Data Breach.” *Id.*, ¶ 65. They further allege that “[t]he Data Breach occurred as a result of Defendant’s failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs’ and Class members’ PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiffs’ and Class members’ PII as a result of the Data Breach.” *Id.*, ¶ 66.

28. Based on the Complaint’s allegations, Plaintiffs, on behalf of themselves and the Class, “seek actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.” Complaint, ¶ 68. Moreover, “[i]f Defendant does not cure the [alleged CCPA] violation within 30 days, Plaintiffs will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).” *Id.*, ¶ 67.

29. The CCPA permits a plaintiff to “recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.” Cal. Civ. Code § 1798.150(a)(1)(A) (emph. added). The Complaint contains no allegations that would support or suggest the amount in actual damages to which Plaintiffs or any of the PCMs are allegedly entitled for alleged violations of the CCPA. Therefore, Defendant looks to the statutory damages permitted under the CCPA for purposes of calculating the amount in controversy on this claim.

30. “When a statutory maximum is provided, the Court may consider the maximum statutory penalty available to decide by a preponderance of the evidence whether the amount in controversy requirement has been satisfied.” *Phan v. Sears, Roebuck & Co.*, 2016 WL 1408057, at *1 (C.D. Cal. Apr. 11, 2016); *Korn v. Polo Ralph Lauren Corp.*, 536 F.Supp.2d 1199, 1205 (E.D. Cal. 2008) (“Where a statutory maximum is specified, courts may consider the maximum statutory penalty available in determining whether the jurisdictional amount in controversy requirement is met.”) (citing *Chabner v. United of Omaha Life Ins. Co.*, 225 F.3d 1042, 1046 n.3 (9th Cir. 2000));

1 *see also Gonzalez v. Comenity Capital Bank*, 2019 WL 5304924, at *5 (E.D. Cal. Oct. 21, 2019)
 2 (“[T]he maximum penalty specified in a statute is properly included in a jurisdictional amount-in-
 3 controversy calculation where a plaintiff could reasonably recover such penalty.”). Therefore,
 4 Defendant calculates the amount in controversy on Plaintiffs’ First Cause of Action to be at least
 5 **\$11,250,000.00** (15,000 PCMs x \$750.00). *See Korn*, 536 F.Supp.2d at 1205-06; *see also Arias v.*
 6 *Residence Inn by Marriott*, 936 F.3d 920, 927 (9th Cir. 2019) (“[T]he amount in controversy reflects
 7 the *maximum* recovery the plaintiff could reasonably recover.” (emph. in orig.)).

8 31. Because the amount in controversy on Plaintiffs’ First Cause of Action exceeds the
 9 total amount in controversy necessary for CAFA jurisdiction, Defendant does not include in this
 10 Notice of Removal calculations of the amounts in controversy on Plaintiffs’ Second and Third
 11 Causes of Action for violations of the UCL and breach of contract, respectively. However, when
 12 other economic damages and/or restitution sought under Plaintiffs’ Second and Third Causes of
 13 Action are combined with the amount in controversy on Plaintiffs’ CCPA claim, the amount in
 14 controversy would *further* exceed CAFA’s \$5,000,000 threshold.³

15 **Statutory Attorneys’ Fees**

16 32. Plaintiffs also seek statutory attorneys’ fees under Cal. Civ. Proc. Code § 1021.5
 17 (“Section 1021.5”). Complaint at 19:25-26.

18 33. In the Ninth Circuit, when attorneys’ fees are authorized by statute, they are
 19 appropriately part of the calculation of the “amount in controversy” for purposes of removal. *Fritsch*
 20 *v. Swift Transp. Co. of Arizona, LLC*, 899 F.3d 785, 794 (9th Cir. 2018); *Kroske v. U.S. Bank Corp.*,
 21 432 F.3d 976, 980 (9th Cir. 2005); *see Galt G/S v. JSS Scandinavia*, 142 F.3d 1150, 1155-56 (9th

22
 23 ³ In the event that Plaintiffs challenge this Court’s jurisdiction under CAFA, Defendant
 24 expressly reserves and does not waive its right to supplement and/or amend this Notice of Removal
 25 or to proffer new calculations or evidence in support of the submissions in this Notice of Removal
 26 to rely on other, higher, reasonable assumptions and/or estimates in calculating the amount in
 27 controversy. *See, e.g., Jauregui v. Roadrunner Trans. Servs., Inc.*, 28 F.4th 989, 991 n.3 (9th Cir.
 28 2022) (“The difference in Roadrunner’s amount in controversy estimates [between removal and its
 opposition to remand] was thus not improper, but rather simply the result of Roadrunner
 appropriately responding to the new standard and new method for supporting its claim at a later point
 in the litigation.; *see also, e.g., Mendoza v. Nat’l Vision, Inc.*, 2019 WL 2929745, at *2 (ND. Cal.
 July 8, 2019) (Keulen, M.J.) (denying remand where defendant’s opposition to a motion to remand
 set forth additional evidence and revised calculations, and included amount-in-controversy
 calculations on three claims that were not included in notice of removal).

1 Cir. 1998) (“[W]here an underlying statute authorizes an award of attorneys’ fees, either with
 2 mandatory or discretionary language, such fees may be included in the amount in controversy.”).
 3 Moreover, “a court **must** include **future** attorneys’ fees recoverable by statute or contract when
 4 assessing whether the amount-in-controversy requirement is met.” *Fritsch*, 899 F.3d at 794 (emph.
 5 added); *see also Chavez*, 888 F.3d at 414-15 (“[T]he amount in controversy is determined by the
 6 complaint operative at the time of removal and encompasses **all** relief a court may grant on that
 7 complaint if the plaintiff is victorious.” (emph. added)).

8 34. Where, as here, a common fund recovery is sought, the Ninth Circuit uses a
 9 benchmark rate of 25% of the total potential award as an estimate for attorneys’ fees. *See, e.g.,*
 10 *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1029 (9th Cir. 1998) (“This circuit has established 25%
 11 ... as a benchmark award for attorney fees.”); *Glass v. UBS Fin. Servs.*, 331 F. App’x 452, 457 (9th
 12 Cir. 2009) (finding 25% of total award, rather than 25% of amount actually collected by the class,
 13 “was proper, and in line with Ninth circuit precedent”); *see also Staton v. Bowing Co.*, 327 F.3d 938,
 14 967 (9th Cir. 2003) (“[A] litigant or a lawyer who recovers a common fund for the benefit of persons
 15 other than himself or his client is entitled to a reasonable attorney’s fee from the fund as a whole.”).
 16 Thus, utilizing Defendant’s calculation of the amount in controversy on Plaintiffs’ First Cause of
 17 Action **only** and the 25% benchmark for attorneys’ fees used in the Ninth Circuit, Defendant
 18 conservatively calculates the amount in controversy on Plaintiffs’ statutory attorneys’ fees request
 19 to be at least **\$2,812,500.00** (\$11,250,000 x 25%).

20 35. However, this amount in controversy is in fact undercalculated because it does not
 21 account for **any** amount in controversy calculations, or any potential statutory attorneys’ fees for the
 22 amounts in controversy, on Plaintiffs’ Second and Third Causes of Action, which amounts have **not**
 23 been included in Defendant’s amount in controversy calculations for purposes of this Notice of
 24 Removal (but which Defendant reserves the right to include in any calculations proffered in response
 25 to any challenge mounted by Plaintiffs to this Court’s jurisdiction under CAFA).

Summary of Amount in Controversy

36. Based on the foregoing, and considering *only* the amount in controversy on Plaintiffs' First Cause of Action the statutory attorneys' fees requested thereon, the amount put in controversy by Plaintiffs' Complaint is not less than **\$14,062,500.00** (\$11,250,000.00 [statutory damages] + \$2,812,500.00 [attorneys' fees]), which exceeds the CAFA jurisdictional threshold, before ever taking into account other forms of compensatory damages, restitution, or punitive damages, which adds even more to the total amount in controversy.⁴

37. Defendant expressly reserves and does not waive its right to amend this Notice of Removal and/or offer evidence supporting the Court's jurisdiction over this action under CAFA or otherwise, including without limitation as to additional and/or different amounts in controversy (including but not limited to amounts in controversy on Plaintiffs' Second and Third Causes of Action and other categories of claimed damages) and as to traditional diversity. *See supra* n.3. Additionally, Defendant assumes that the proposed class is as defined by Plaintiffs in the Complaint for purposes of this Notice of Removal only, but expressly reserves and does not waive its position that the proposed class definition is improper and/or cannot be certified.

38. In addition, nothing in this Notice of Removal is intended or should be construed as any type of express or implied admission by Defendant of any fact, of the validity or merits of any of Plaintiffs' claims, causes of action, or allegations, or of any liability for the same, all of which are hereby expressly denied, or as any type of express or implied waiver or limitation of Defendant's rights, claims, remedies, and defenses in connection with this action, all of which are hereby fully and expressly reserved.

⁴ Notably, the amount in controversy is *undercalculated*. In addition to the damages discussed above, Plaintiffs also request punitive damages and injunctive relief (among other forms of relief not calculated above) on behalf of themselves and the Class. Complaint at 19:21, 19:24. Such amounts are properly included in the amount in controversy – but are not included in Defendant's calculations in this Notice of Removal – and thus provide further evidence that the amount in controversy exceeds \$5,000,000, as already established above. *See, e.g., Gibson v. Chrysler Corp.*, 261 F.3d 927, 946 (9th Cir. 2001), *holding modified by Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 558, 571-72 (2005) (potential punitive damages may be considered for purposes of amount in controversy).

NO CAFA EXCEPTIONS APPLY

39. CAFA contains a number of exceptions to its grant of original jurisdiction, *see* 28 U.S.C. §§ 1332(d)(3)-(5), but none of these exceptions are applicable here.

40. The first is a discretionary exception based on the number of putative class members found in the state where the action was filed. *See* 28 U.S.C. § 1332(d)(3). However, the exception *only* applies where the “primary defendants are citizens of the State in which the action was originally filed.” *See id.* Here, the action was originally filed in the Superior Court of the State of California and, as noted above, Defendant is not a citizen of California. Thus, this exception does not apply.

41. Similarly, 28 U.S.C. § 1332(d)(4) contains two further exceptions to CAFA’s grant of original jurisdiction based on the number of putative class members in the state in which the action was filed. However, these exceptions also apply *only* where all primary defendants, or at least one defendant, is a “citizen of the State in which the action was originally filed.” *See* 28 U.S.C. §§ 1332(d)(4)(A)(i)(II), 1332(d)(4)(B). Given that this action was originally filed in California, and Defendant is not a citizen of California, these exceptions also do not apply.

42. Finally, 28 U.S.C. § 1332(d)(5) presents two additional exceptions applicable to actions where defendants are government entities, or in which the putative class contains less than 100 members in the aggregate. *See* 28 U.S.C. §§ 1332(d)(5)(A)-(B). Given that Defendant is not a governmental entity, and Defendant’s records establish that the putative class in fact *far exceeds* 100 members, these exceptions also do not apply.

VENUE

Based on the Complaint, Plaintiff alleges that the events allegedly giving rise to this action occurred within this judicial district. Defendant disagrees, as the events allegedly giving rise to this action took place in New Jersey. Nevertheless, should Plaintiff’s allegations be accepted as true, removal to this Court is proper because Plaintiffs’ action was filed in the Superior Court of California, County of Alameda. Accordingly, Defendant is entitled to remove this action to the United States District Court for the Northern District of California. 28 U.S.C. § 1441(a).

TIMELINESS OF REMOVAL

43. This removal is timely under CAFA and this case has not previously been removed to federal court. *See* 28 U.S.C. § 1446(b).

44. This action is being removed well-within 30 days of receipt of a copy of the Complaint as an enclosure to Plaintiffs' CCPA demand letter. Defendant is unaware if proper service of a Summons and Complaint, but Defendant is removing the case out of an abundance of caution. *See* 28 U.S.C. § 1446(b). In addition, and regardless, the Ninth Circuit has held and clarified that removal is timely under CAFA ***at any time*** so long as (1) the face of the complaint does not plainly allege all elements needed for traditional diversity (including the amount in controversy), and (2) the plaintiff has not served some other "paper" on the defendant that concedes ***all*** elements needed for traditional diversity. *See Roth v. CHA Hollywood Med. Ctr., L.P.*, 720 F.3d 1121, 1125-26 (9th Cir. 2013) (a removing defendant may remove "on the basis of its own information, provided that it has not run afoul of either of the thirty-day deadlines" set forth in 28 U.S.C. § 1446(b)(1) and (b)(3); "a defendant's subjective knowledge cannot convert a non-removable action into a removable one such that the thirty-day time limit of § 1446(b)(1) or (b)(3) begins to run against the defendant").⁵

45. Here, the Complaint does not plainly allege all of the elements needed for traditional diversity under CAFA, and Plaintiffs have not served some other "paper" on Defendant that concedes all elements needed for such removal. Therefore, this removal is timely under CAFA.

NOTICE TO PLAINTIFFS AND THE STATE COURT

46. Contemporaneously with the filing of this Notice of Removal, written notice of such filing will be served on Plaintiffs' counsel of record as reflected in the attached Proof of Service. *See* 28 U.S.C. § 1446(d). In addition, a copy of this Notice of Removal will be filed with the Clerk

⁵ *See also Rea v. Michaels Stores Inc.*, 742 F.3d 1234, 1238 (9th Cir. 2014) (reaffirming *Roth* holding) ("We also recently held in *Roth v. CHA Hollywood Medical Center, L.P.*, that the two 30-day periods are not the exclusive periods for removal.... In other words, as long as the complaint or 'an amended pleading, motion, order or other paper' does not reveal that the case is removable, the 30-day time period never starts to run and the defendant may remove at any time."); *Taylor v. Cox Commc'ns. California, LLC*, 673 F. App'x 734, 735 (9th Cir. 2016) ("We also hold that Defendants' second Notice of Removal was timely. 'A CAFA case may be removed [by a defendant] at any time, provided that neither of the two thirty-day periods under § 1446(b)(1) and (b)(3) has been triggered.'").

1 of the State Court. *See id.*

2 **WHEREFORE**, Defendant respectfully requests that the above-captioned action now
3 pending in the State Court be removed to this United States District Court.

4 DATED: May 3, 2022

Respectfully submitted,

5
6 **BAKER & HOSTETLER LLP**

7
8 By: /s/Teresa C. Chow
Teresa C. Chow

9 Attorneys for Defendant
10 AMERICAN FINANCIAL RESOURCES, INC.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES

PROOF OF SERVICE

Edwin Parras, et al. v. American Financial Resources, Inc.
USDC Northern District Case No. 4:22-cv-002659

I, Nancy L. Brazil, declare:

I am a citizen of the United States and employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is 11601 Wilshire Boulevard , Suite 1400, Los Angeles, CA 90025-0509. On May 3, 2022, I served a copy of the within document(s):

DEFENDANT'S NOTICE OF REMOVAL OF CIVIL ACTION

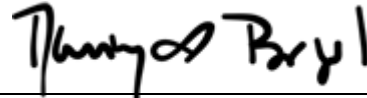
- ☒ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at Los Angeles, California addressed as set forth below.
- ☒ by transmitting via e-mail or electronic transmission the document(s) listed above to the e-mail address(es) set forth below on this date before 5:00 p.m. and the transmission was reported as complete and without error.

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

Attorneys for Plaintiffs
EDWINA PARRAS and ROBERT PARRAS
and the putative class

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

1 I declare that I am employed in the office of a member of the Bar of this Court at whose
2 direction the service was made. Executed on May 3, 2022, at Los Angeles, California.

3
4 

5 _____
Nancy L. Brazil

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES

EXHIBIT A



245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

March 31, 2022

VIA CERTIFIED MAIL

American Financial Resources, Inc.
9 Sylvan Way
Parsippany, NJ 07054

Re: Parras, et al. v. American Financial Resources, Inc.

To Whom It May Concern:

We represent Plaintiffs Edwina and Robert Parras ("Plaintiffs") and all other similarly situated consumers in a putative class action against American Financial Resources, Inc. ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiffs' and the proposed class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on between December 6-20, 2021, as specified in Defendant's "Notice of Data Breach" letter dated March 9, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiffs' Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiffs demand that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiffs with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiffs and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

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

Attorneys for Plaintiffs
Edwina Parras and Robert Parras
and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL

EDWINA PARRAS and ROBERT PARRAS,
individually and on behalf of all others similarly
situated,

Plaintiffs,

vs.

AMERICAN FINANCIAL RESOURCES, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT FOR
VIOLATIONS OF:**

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

DEMAND FOR JURY TRIAL



1 Plaintiffs EDWINA PARRAS AND ROBERT PARRAS (“Plaintiffs”), on behalf of
 2 themselves and the general public and all others similarly situated (“Class members”), by and
 3 through their attorneys, upon personal knowledge as to facts pertaining to themselves and on
 4 information and belief as to all other matters, brings this class action against Defendant
 5 AMERICAN FINANCIAL RESOURCES, INC. (“Defendant” or “AFR”), and alleges as follows:

6 **NATURE OF THE CASE**

7 1. This is a data breach class action against American Financial Resources and its
 8 related entities, subsidiaries, and agents for failing to secure and safeguard the personally
 9 identifiable information (“PII”) that Defendant collected and maintained (collectively “Private
 10 Information”), and for failing to provide timely and adequate notice to Plaintiffs and other Class
 11 members that their information had been stolen. Defendant is a residential mortgage company that
 12 serves thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and
 13 contractors across the country, with their residential financing needs.¹ For its business purposes,
 14 Defendant maintains a substantial amount of PII from its customers in its computer systems.

15 2. On or about March 9, 2022, Defendant announced that an unauthorized party had
 16 gained access to its computer systems and certain AFR files were accessed without authorization
 17 between December 6 to December 20, 2021 (the “Data Breach”). Defendant conducted a review of
 18 the files that were accessed in the Data Breach and on February 4, 2022 it determined files
 19 containing Plaintiffs’ and other similarly situated individuals’ PII, including names, Social Security
 20 numbers, and driver’s license numbers were accessed in the Data Breach.

21 3. Although the Data Breach occurred in December 2021, placing sensitive customer
 22 information in the hands of malicious actors as a result of Defendant’s failure to safeguard
 23 Plaintiffs’ PII, Defendant waited months until on or around March 9, 2022 to provide notice of the
 24 Data Breach to customers. This notice was still lacking in information necessary for Plaintiffs and
 25 Class members to understand the scope and severity of the Data Breach. Due to this lapse in time
 26 between the Data Breach and Defendant’s notice to affected customers, hackers may have already

27
 28
¹ <https://www.afrcorp.com>.

1 been able to acquire and sell Plaintiffs' and the Class members' PII on the black market or dark
2 web, or otherwise fraudulently misuse it for their personal gain.

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

6 5. Defendant breached that duty by, *inter alia*, failing to implement and maintain
7 reasonable security procedures and practices to protect PII from unauthorized access and storing
8 and retaining Plaintiffs' and Class members' personal information on inadequately protected
9 networks.

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

15 7. As set forth in the Prayer for Relief, among other things, Plaintiffs seek, for
16 themselves and the Class, equitable relief, including public injunctive relief, and actual damages.

17 **VENUE AND JURISDICTION**

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

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

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

PARTIES

11. At all relevant times, Plaintiffs resided in Alameda County, California. Plaintiffs are each a consumer who were customers of Defendant and provided their personal information and PII to Defendant.

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

13. Defendant is a corporation organized under the laws of the state of New Jersey, with its principal place of business and/or headquarters located at 9 Sylvan Way, Parsippany, New Jersey 07054.

FACTUAL ALLEGATIONS***PII Is a Valuable Property Right that Must Be Protected***

14. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.² California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

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

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

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

³ FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.

1 16. The value of PII as a commodity is measurable. “PII, which companies obtain at
2 little cost, has quantifiable value that is rapidly reaching a level comparable to the value of
3 traditional financial assets.”⁴ It is so valuable to identity thieves that once PII has been disclosed,
4 criminals often trade it on the “cyber black-market” for several years.

5 17. Companies recognize PII as an extremely valuable commodity akin to a form of
6 personal property. For example, Symantec Corporation’s Norton brand has created a software
7 application that values a person’s identity on the black market.⁵

8 18. As a result of its real value and the recent large-scale data breaches, identity thieves
9 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other
10 sensitive information directly on various illicit Internet websites making the information publicly
11 available for other criminals to take and use. This information from various breaches, including the
12 information exposed in the Data Breach, can be aggregated and become more valuable to thieves
13 and more damaging to victims. In one study, researchers found hundreds of websites displaying
14 stolen PII and other sensitive information. Strikingly, none of these websites were blocked by
15 Google’s safeguard filtering mechanism – the “Safe Browsing list.”

16 19. Recognizing the high value that consumers place on their PII, some companies now
17 offer consumers an opportunity to sell this information to advertisers and other third parties. The
18 idea is to give consumers more power and control over the type of information they share – and
19 who ultimately receives that information. By making the transaction transparent, consumers will
20 make a profit from the surrender of their PII.⁶ This business has created a new market for the sale
21 and purchase of this valuable data.⁷

22 20. Consumers place a high value not only on their PII, but also on the privacy of that
23 data. Researchers shed light on how much consumers value their data privacy – and the amount is
24

25 ⁴ See Soma, *Corporate Privacy Trend*, *supra*.

26 ⁵ Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

27 ⁶ Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010)
available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

28 ⁷ See Julia Angwin and Emil Steel, *Web’s Hot New Commodity: Privacy*, Wall Street Journal
(Feb. 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

1 considerable. Indeed, studies confirm that “when privacy information is made more salient and
2 accessible, some consumers are willing to pay a premium to purchase from privacy protective
3 websites.”⁸

4 21. One study on website privacy determined that U.S. consumers valued the restriction
5 of improper access to their PII between \$11.33 and \$16.58 per website.⁹

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

9 ***Theft of PII Has Grave and Lasting Consequences for Victims***

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

14 24. Theft or breach of PII is serious. The California Attorney General recognizes that
15 “[f]oundational” to every Californian’s constitutional right to privacy is “information security: if
16 companies collect consumers’ personal data, they have a duty to secure it. An organization cannot
17 protect people’s privacy without being able to secure their data from unauthorized access.”¹⁰

18 25. The United States Government Accountability Office noted in a June 2007 report on
19 Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts,
20 open new financial accounts, receive government benefits and incur charges and credit in a person’s
21 name.¹¹ As the GAO Report states, this type of identity theft is so harmful because it may take time
22 for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

23
24
25 ⁸ Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An*
26 *Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), available at
<https://www.jstor.org/stable/23015560?seq=1#>

27 ⁹ II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation*
28 (Mar. 2003) at table 3, available at <https://ideas.repec.org/p/wpa/wuwpio/0304001.html> (emphasis
added).

¹⁰ California Data Breach Report, Kamala D. Harris, Attorney General, California Department
of Justice, February 2016.

¹¹ See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.



26. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records ... [and their] good name.” According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.¹²

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.¹³ According to Experian, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID; use the victim’s information in the event of arrest or court action.¹⁴

28. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report, the average cost of a data breach per consumer was \$150 per record.¹⁵ Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was \$298 dollars.¹⁶ And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was \$375.¹⁷

¹² See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

¹³ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

¹⁴ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

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

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

¹⁷ Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, available at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin report).

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

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

30. For example, in 2012, hackers gained access to LinkedIn’s users’ passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.¹⁸

31. It is within this context that Plaintiffs and thousands of Defendant’s customers must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Defendant’s Collection of Customers’ PII

32. Defendant’s Privacy Statement states “American Financial Resources, Inc. (herein referred to as AFR) has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997.”¹⁹

33. Defendant acknowledges that it collects, stores, and transmits a substantial amount of confidential, personal, and other sensitive information from its customers for its mortgage loan origination and related services.²⁰ In the course of its regular business Defendant collects, at minimum, the following information:

- Social Security number and employment information including tax returns, w-2s, paystubs and related documents
- Account balances and transaction history
- Credit history and investment experience
- Social Security Number
- Current and previous home ownership experience, including physical and mailing addresses

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

¹⁹ See Defendant’s Privacy Statement: <https://www.afrcorp.com/privacy-statement/>

²⁰ Defendant’s “Related Services” may include, but are not limited to real estate services, insurance, escrow and other closing services, notary, appraisal, other consumer credit services, home warranty, and other services related to home purchase, home ownership, or related consumer transactions. <https://www.afrcorp.com/privacy-statement/>

- Letters of explanation regarding credit or employment events
- Date of birth / age
- Other information required by Defendant's investors or insurers (such as HUD)

34. With regard to its collection of Social Security numbers in particular, Defendant's Privacy Statement states:

Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.

35. The types of information Defendant collects are further detailed in its Privacy Statement (last updated February 1, 2021),²¹ which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

- Identifiers – such as: a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – such as: name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, any other financial information, or medical information. Some personal information included in this category may overlap with other categories.
- Protected classification characteristics under California or federal law – such as: age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, veteran or military status, genetic information.
- Commercial information – such as: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

²¹ See Defendant's Privacy Statement: <https://www.afrcorp.com/privacy-statement/>

- Internet or other similar network activity – such as: Browsing history, search history, information on a consumer’s interaction with a website, application, or advertisement.
- Professional or employment-related information – such as: Current or past job history or performance evaluations.
- Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) – such as: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
- Inferences drawn from other personal information – such as: Profile reflecting

The Data Breach

36. On or around March 9, 2022 Defendant sent official notice of the Data Breach to Plaintiffs and other customers stating, “[AFR] recently concluded an investigation into a security incident involving some of [AFR’s] computer systems.”

37. According to Defendant, “[AFR] conducted a comprehensive review of the files that were accessed [in the Data Breach] and, on February 4, 2022, determined that a file contained [Plaintiffs’ and the Class members’] name, Social Security number, and for some individuals, driver’s license number.” Through its investigation “[AFR] determined that certain AFR files were accessed without authorization between December 6-20, 2021.”

38. Defendant also claimed to have launched its own investigation and notified law enforcement.

39. Defendant’s Notice of Data Breach letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding when it learned of the Data Breach or how many people were affected by the Data Breach.

40. Following the Data Breach, Plaintiffs have experienced an amplified number of SPAM emails, have had their bank cards compromised, and have experienced fraud and financial harm in the form of unauthorized charges on Plaintiffs’ account.

41. After receiving notice of the Data Breach notification letter, Plaintiffs have spent numerous hours filtering through unwanted SPAM emails which sharply increased following the Data Breach. As a result of the Data Breach, Plaintiffs have suffered an invasion and loss of their

1 privacy, and Plaintiffs have spent time monitoring their financial accounts, which was time that
2 Plaintiffs otherwise would have spent performing other activities or leisurely events for the
3 enjoyment of life rather than mitigating the impact of the Data Breach.

4 42. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for
5 financial fraud, medical fraud, and/or identity theft, and the associated damages resulting from it,
6 for years to come.

7 ***Defendant Knew or Should Have Known PII Are High Risk Targets***

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

10 44. The Identity Theft Resource Center reported that the banking/credit/financial sector
11 had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135
12 data breaches exposing at least 1,709,013 million records in 2018.²²

13 45. Prior to the breach there were many reports of high-profile data breaches that should
14 have put a company like Defendant on high alert and forced it to closely examine its own security
15 procedures, as well as those of third parties with which it did business and gave access to its
16 subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a
17 hacker had gained access to 100 million U.S. customer accounts and credit card applications.
18 Similarly, in May 2019, First American Financial reported a security incident on its website that
19 potentially exposed 885 million real estate and mortgage related documents, among others. Across
20 industries, financial services have the second-highest cost per breached record, behind healthcare. In
21 financial services, an average breach costs \$210 per record, while a “mega breach,” like Capital
22 One’s, can cost up to \$388 per record.²³

23 46. Anurag Kahol, CTO of Bitglass recently commented that “[g]iven that organizations
24 in the financial services industry are entrusted with highly valuable, personally identifiable
25

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

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

1 information (PII), they represent an attractive target for cybercriminals[.]” HelpNetSecurity reports
 2 that “[h]acking and malware are leading the charge against financial services and the costs
 3 associated with breaches are growing. Financial services organizations must get a handle on data
 4 breaches and adopt a proactive security strategy if they are to properly protect data from an
 5 evolving variety of threats.”²⁴

6 47. As such, Defendant was aware that PII is at high risk of theft, and consequently
 7 should have but did not take appropriate and standard measures to protect Plaintiffs’ and Class
 8 members’ PII against cyber-security attacks that Defendant should have anticipated and guarded
 9 against.

10 **CLASS ACTION ALLEGATIONS**

11 48. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiffs seek to
 12 represent and intend to seek certification of a class (the “Class”) defined as:

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

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

19 50. Certification of Plaintiffs’ claims for class wide treatment is appropriate because
 20 Plaintiffs can prove the elements of their claims on a class wide basis using the same evidence as
 21 would be used to prove those elements in individual actions alleging the same claims.

22 51. The Class members are so numerous and geographically dispersed throughout
 23 California that joinder of all Class members would be impracticable. While the exact number of
 24 Class members is unknown, Defendant acknowledges the Data Breach, and based on information
 25 and belief, the Class consists of tens of thousands of Defendant’s customers, including Plaintiffs
 26

27
 28 ²⁴ HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), available at <https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/>.

1 and the Class members. Plaintiffs therefore believes that the Class is so numerous that joinder of all
2 members is impractical.

3 52. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed
4 members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members
5 were injured by the same wrongful acts, practices, and omissions committed by Defendant, as
6 described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that
7 give rise to the claims of all Class members.

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

- 12 (a) Whether Defendant had a duty to implement and maintain reasonable security
- 13 procedures and practices appropriate to the nature of the PII it collected, stored,
- 14 and maintained from Plaintiffs and Class members;
- 15 (b) Whether Defendant breached its duty to protect the PII of Plaintiffs and each
- 16 Class member; and
- 17 (c) Whether Plaintiffs and each Class member are entitled to damages and other
- 18 equitable relief.

19 54. Plaintiffs will fairly and adequately protect the interests of the Class members.
20 Plaintiffs are each an adequate representative of the Class in that Plaintiffs have no interests adverse
21 to or that conflicts with the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with
22 substantial experience and success in the prosecution of complex consumer protection class actions
23 of this nature.

24 55. A class action is superior to any other available method for the fair and efficient
25 adjudication of this controversy since individual joinder of all Class members is impractical.
26 Furthermore, the expenses and burden of individual litigation would make it difficult or impossible
27 for the individual members of the Class to redress the wrongs done to them, especially given that
28 the damages or injuries suffered by each individual member of the Class are outweighed by the

costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

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

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 (“CCPA”)

Cal. Civ. Code §§ 1798.100, *et seq.*

57. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

58. As more personal information about consumers is collected by businesses, consumers’ ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: “The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.”²⁵

59. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are

²⁵ CALIFORNIA CONSUMER PRIVACY ACT (CCPA) COMPLIANCE, <https://buergenomics.com/ccpa-compliance/>.

1 appropriate to the nature of the information collected. Defendant failed to implement such
2 procedures which resulted in the Data Breach.

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

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

14 62. Plaintiffs and Class members are “consumer[s]” as defined by Civ. Code
15 § 1798.140(g) because they are “natural person[s] who [are] California resident[s], as defined in
16 Section 17014 of Title 18 of the California Code of Regulations, as that section read on September
17 1, 2017.”

18 63. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because Defendant:

- 19 a) is a “sole proprietorship, partnership, limited liability company,
20 corporation, association, or other legal entity that is organized or operated
21 for the profit or financial benefit of its shareholders or other owners”;
- 22 b) “collects consumers’ personal information, or on the behalf of which is
23 collected and that alone, or jointly with others, determines the purposes and
24 means of the processing of consumers’ personal information”;
- 25 c) does business in and is headquartered in California; and
- 26 d) has annual gross revenues in excess of \$25 million; annually buys, receives
27 for the business’ commercial purposes, sells or shares for commercial
28 purposes, alone or in combination, the personal information of 50,000 or

more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

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

65. Plaintiffs' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names, Social Security numbers and/or Driver's License numbers, was wrongfully accessed and taken by unauthorized persons in the Data Breach.

66. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiffs' and Class members' PII as a result of the Data Breach.

67. On March 31, 2022, Plaintiffs provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not cure the violation within 30 days, Plaintiffs will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

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

SECOND CAUSE OF ACTION

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

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

69. Plaintiffs re-allege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

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

71. In the course of conducting its business, Defendant committed “unlawful” business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Class members’ PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I, Section 1 of the California Constitution (California’s constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiffs and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant’s above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

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

73. Defendant’s above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts and practices in violation of the UCL in that Defendant’s wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant’s practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant’s wrongful

1 conduct outweighs any alleged benefits attributable to such conduct. There were reasonably
2 available alternatives to further Defendant's legitimate business interests other than engaging in the
3 above-described wrongful conduct.

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

7 75. As a direct and proximate result of Defendant's above-described wrongful actions,
8 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
9 and its violations of the UCL, Plaintiffs and Class members have suffered (and will continue to
10 suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an
11 imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks
12 justifying expenditures for protective and remedial services for which they are entitled to
13 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory
14 damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-
15 established national and international market, and/or (vi) the financial and temporal cost of
16 monitoring their credit, monitoring financial accounts, and mitigating damages.

17 76. Unless restrained and enjoined, Defendant will continue to engage in the above-
18 described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of
19 themselves, Class members, and the general public, also seeks restitution and an injunction,
20 including public injunctive relief prohibiting Defendant from continuing such wrongful conduct,
21 and requiring Defendant to modify its corporate culture and design, adopt, implement, control,
22 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,
23 procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted
24 to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code
25 § 17203.

26 //

27 //

28 //

THIRD CAUSE OF ACTION

Breach of Contract

77. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

78. Plaintiffs and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

79. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Defendant's products and services.

80. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

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

PRAYER FOR RELIEF

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

- (i) actual and punitive damages to be determined by the trier of fact;
- (ii) equitable relief, including restitution;
- (iii) pre- and post-judgment interest at the highest legal rates applicable;
- (iv) appropriate injunctive relief;
- (v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;
- (vi) costs of suit; and
- (vii) such other and further relief the Court deems just and proper.

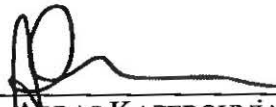
DEMAND FOR JURY TRIAL

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

Dated: March 31, 2022

KAZEROUNI LAW GROUP, APC

By: _____


ABBAS KAZEROOUNIAN, ESQ.
MONA AMINI, ESQ.

Attorneys for Plaintiffs

KAZEROUNI
LAW GROUP, APC

EXHIBIT B

SUMMONS
(CITACION JUDICIAL)

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):
AMERICAN FINANCIAL RESOURCES, INC.

ELECTRONICALLY FILED
Superior Court of California
County of Alameda
04/01/2022

Chad Finke, Executive Officer / Clerk of the Court

By: C. Clark Deputy

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):
EDWINA PARRAS and ROBERT PARRAS, individually and on behalf
of all others similarly situated

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

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

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (www.lawhelpcalifornia.org), the California Courts Online Self-Help Center (www.courtinfo.ca.gov/selfhelp), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.

¡AVISO! Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.

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

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

The name and address of the court is:
(El nombre y dirección de la corte es):
Superior Court of California for the County of Alameda
1225 Falcon Street, Oakland, CA 94612

CASE NUMBER:
(Número del Caso):

22CV009276

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Abbas Kazrounian & Mona Amini - Kazrouni Law Group, APC, 245 Fischer Ave., Unit D1, Costa Mesa, California 92626 Tel: 800-400-6808

Chad Finke, Executive Officer / Clerk of the Court

DATE: **04/01/2022**
(Fecha)

Clerk, by _____, Deputy
(Secretario) **C. Clark** (Adjunto)

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)
(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons, (POS-010)).

NOTICE TO THE PERSON SERVED: You are served

1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of (specify):

3. ☐ on behalf of (specify):

- under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
☐ other (specify):

4. ☐ by personal delivery on (date):

[SEAL]



EXHIBIT C

ELECTRONICALLY FILED

Superior Court of California,
County of Alameda

04/01/2022 at 12:00:00 AM

By: Cheryl Clark, Deputy Clerk

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

*Attorneys for Plaintiffs
Edwina Parras and Robert Parras
and the putative class*

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

EDWINA PARRAS and ROBERT PARRAS,
individually and on behalf of all others similarly
situated,

Plaintiffs,

vs.

AMERICAN FINANCIAL RESOURCES, INC.,

Defendant.

Case No. **22CV009276**

**CLASS ACTION COMPLAINT FOR
VIOLATIONS OF:**

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

DEMAND FOR JURY TRIAL



1 Plaintiffs EDWINA PARRAS AND ROBERT PARRAS (“Plaintiffs”), on behalf of
 2 themselves and the general public and all others similarly situated (“Class members”), by and
 3 through their attorneys, upon personal knowledge as to facts pertaining to themselves and on
 4 information and belief as to all other matters, brings this class action against Defendant
 5 AMERICAN FINANCIAL RESOURCES, INC. (“Defendant” or “AFR”), and alleges as follows:

6 **NATURE OF THE CASE**

7 1. This is a data breach class action against American Financial Resources and its
 8 related entities, subsidiaries, and agents for failing to secure and safeguard the personally
 9 identifiable information (“PII”) that Defendant collected and maintained (collectively “Private
 10 Information”), and for failing to provide timely and adequate notice to Plaintiffs and other Class
 11 members that their information had been stolen. Defendant is a residential mortgage company that
 12 serves thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and
 13 contractors across the country, with their residential financing needs.¹ For its business purposes,
 14 Defendant maintains a substantial amount of PII from its customers in its computer systems.

15 2. On or about March 9, 2022, Defendant announced that an unauthorized party had
 16 gained access to its computer systems and certain AFR files were accessed without authorization
 17 between December 6 to December 20, 2021 (the “Data Breach”). Defendant conducted a review of
 18 the files that were accessed in the Data Breach and on February 4, 2022 it determined files
 19 containing Plaintiffs’ and other similarly situated individuals’ PII, including names, Social Security
 20 numbers, and driver’s license numbers were accessed in the Data Breach.

21 3. Although the Data Breach occurred in December 2021, placing sensitive customer
 22 information in the hands of malicious actors as a result of Defendant’s failure to safeguard
 23 Plaintiffs’ PII, Defendant waited months until on or around March 9, 2022 to provide notice of the
 24 Data Breach to customers. This notice was still lacking in information necessary for Plaintiffs and
 25 Class members to understand the scope and severity of the Data Breach. Due to this lapse in time
 26 between the Data Breach and Defendant’s notice to affected customers, hackers may have already
 27

28
 1 <https://www.afrcorp.com>.

1 been able to acquire and sell Plaintiffs' and the Class members' PII on the black market or dark
2 web, or otherwise fraudulently misuse it for their personal gain.

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

6 5. Defendant breached that duty by, *inter alia*, failing to implement and maintain
7 reasonable security procedures and practices to protect PII from unauthorized access and storing
8 and retaining Plaintiffs' and Class members' personal information on inadequately protected
9 networks.

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

15 7. As set forth in the Prayer for Relief, among other things, Plaintiffs seek, for
16 themselves and the Class, equitable relief, including public injunctive relief, and actual damages.

17 **VENUE AND JURISDICTION**

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

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

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

PARTIES

11. At all relevant times, Plaintiffs resided in Alameda County, California. Plaintiffs are each a consumer who were customers of Defendant and provided their personal information and PII to Defendant.

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

13. Defendant is a corporation organized under the laws of the state of New Jersey, with its principal place of business and/or headquarters located at 9 Sylvan Way, Parsippany, New Jersey 07054.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

14. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.² California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

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

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

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

³ FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.



1 16. The value of PII as a commodity is measurable. “PII, which companies obtain at
2 little cost, has quantifiable value that is rapidly reaching a level comparable to the value of
3 traditional financial assets.”⁴ It is so valuable to identity thieves that once PII has been disclosed,
4 criminals often trade it on the “cyber black-market” for several years.

5 17. Companies recognize PII as an extremely valuable commodity akin to a form of
6 personal property. For example, Symantec Corporation’s Norton brand has created a software
7 application that values a person’s identity on the black market.⁵

8 18. As a result of its real value and the recent large-scale data breaches, identity thieves
9 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other
10 sensitive information directly on various illicit Internet websites making the information publicly
11 available for other criminals to take and use. This information from various breaches, including the
12 information exposed in the Data Breach, can be aggregated and become more valuable to thieves
13 and more damaging to victims. In one study, researchers found hundreds of websites displaying
14 stolen PII and other sensitive information. Strikingly, none of these websites were blocked by
15 Google’s safeguard filtering mechanism – the “Safe Browsing list.”

16 19. Recognizing the high value that consumers place on their PII, some companies now
17 offer consumers an opportunity to sell this information to advertisers and other third parties. The
18 idea is to give consumers more power and control over the type of information they share – and
19 who ultimately receives that information. By making the transaction transparent, consumers will
20 make a profit from the surrender of their PII.⁶ This business has created a new market for the sale
21 and purchase of this valuable data.⁷

22 20. Consumers place a high value not only on their PII, but also on the privacy of that
23 data. Researchers shed light on how much consumers value their data privacy – and the amount is
24

25 ⁴ See Soma, *Corporate Privacy Trend*, *supra*.

26 ⁵ Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

27 ⁶ Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010)
available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

28 ⁷ See Julia Angwin and Emil Steel, *Web’s Hot New Commodity: Privacy*, Wall Street Journal
(Feb. 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”⁸

21. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between \$11.33 and \$16.58 per website.⁹

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

Theft of PII Has Grave and Lasting Consequences for Victims

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

24. Theft or breach of PII is serious. The California Attorney General recognizes that “[f]oundational” to every Californian’s constitutional right to privacy is “information security: if companies collect consumers’ personal data, they have a duty to secure it. An organization cannot protect people’s privacy without being able to secure their data from unauthorized access.”¹⁰

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person’s name.¹¹ As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

⁸ Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study* *Information Systems Research* 22(2) 254, 254 (June 2011), available at <https://www.jstor.org/stable/23015560?seq=1#>

⁹ II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, available at <https://ideas.repec.org/p/wpa/wuwpio/0304001.html> (emphasis added).

¹⁰ California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

¹¹ See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.



26. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records ... [and their] good name.” According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.¹²

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.¹³ According to Experian, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID; use the victim’s information in the event of arrest or court action.¹⁴

28. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report, the average cost of a data breach per consumer was \$150 per record.¹⁵ Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was \$298 dollars.¹⁶ And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was \$375.¹⁷

¹² See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

¹³ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

¹⁴ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

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

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

¹⁷ Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, available at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin report).

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

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

30. For example, in 2012, hackers gained access to LinkedIn’s users’ passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.¹⁸

31. It is within this context that Plaintiffs and thousands of Defendant’s customers must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Defendant’s Collection of Customers’ PII

32. Defendant’s Privacy Statement states “American Financial Resources, Inc. (herein referred to as AFR) has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997.”¹⁹

33. Defendant acknowledges that it collects, stores, and transmits a substantial amount of confidential, personal, and other sensitive information from its customers for its mortgage loan origination and related services.²⁰ In the course of its regular business Defendant collects, at minimum, the following information:

- Social Security number and employment information including tax returns, w-2s, paystubs and related documents
- Account balances and transaction history
- Credit history and investment experience
- Social Security Number
- Current and previous home ownership experience, including physical and mailing addresses

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

¹⁹ See Defendant’s Privacy Statement: <https://www.afrcorp.com/privacy-statement/>

²⁰ Defendant’s “Related Services” may include, but are not limited to real estate services, insurance, escrow and other closing services, notary, appraisal, other consumer credit services, home warranty, and other services related to home purchase, home ownership, or related consumer transactions. <https://www.afrcorp.com/privacy-statement/>

- Letters of explanation regarding credit or employment events
- Date of birth / age
- Other information required by Defendant's investors or insurers (such as HUD)

34. With regard to its collection of Social Security numbers in particular, Defendant's Privacy Statement states:

Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.

35. The types of information Defendant collects are further detailed in its Privacy Statement (last updated February 1, 2021),²¹ which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

- Identifiers – such as: a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – such as: name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, any other financial information, or medical information. Some personal information included in this category may overlap with other categories.
- Protected classification characteristics under California or federal law – such as: age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, veteran or military status, genetic information.
- Commercial information – such as: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

²¹ See Defendant's Privacy Statement: <https://www.afrcorp.com/privacy-statement/>

- Internet or other similar network activity – such as: Browsing history, search history, information on a consumer’s interaction with a website, application, or advertisement.
- Professional or employment-related information – such as: Current or past job history or performance evaluations.
- Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) – such as: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
- Inferences drawn from other personal information – such as: Profile reflecting

The Data Breach

36. On or around March 9, 2022 Defendant sent official notice of the Data Breach to Plaintiffs and other customers stating, “[AFR] recently concluded an investigation into a security incident involving some of [AFR’s] computer systems.”

37. According to Defendant, “[AFR] conducted a comprehensive review of the files that were accessed [in the Data Breach] and, on February 4, 2022, determined that a file contained [Plaintiffs’ and the Class members’] name, Social Security number, and for some individuals, driver’s license number.” Through its investigation “[AFR] determined that certain AFR files were accessed without authorization between December 6-20, 2021.”

38. Defendant also claimed to have launched its own investigation and notified law enforcement.

39. Defendant’s Notice of Data Breach letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding when it learned of the Data Breach or how many people were affected by the Data Breach.

40. Following the Data Breach, Plaintiffs have experienced an amplified number of SPAM emails, have had their bank cards compromised, and have experienced fraud and financial harm in the form of unauthorized charges on Plaintiffs’ account.

41. After receiving notice of the Data Breach notification letter, Plaintiffs have spent numerous hours filtering through unwanted SPAM emails which sharply increased following the Data Breach. As a result of the Data Breach, Plaintiffs have suffered an invasion and loss of their

1 privacy, and Plaintiffs have spent time monitoring their financial accounts, which was time that
 2 Plaintiffs otherwise would have spent performing other activities or leisurely events for the
 3 enjoyment of life rather than mitigating the impact of the Data Breach.

4 42. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for
 5 financial fraud, medical fraud, and/or identity theft, and the associated damages resulting from it,
 6 for years to come.

7 ***Defendant Knew or Should Have Known PII Are High Risk Targets***

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

10 44. The Identity Theft Resource Center reported that the banking/credit/financial sector
 11 had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135
 12 data breaches exposing at least 1,709,013 million records in 2018.²²

13 45. Prior to the breach there were many reports of high-profile data breaches that should
 14 have put a company like Defendant on high alert and forced it to closely examine its own security
 15 procedures, as well as those of third parties with which it did business and gave access to its
 16 subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a
 17 hacker had gained access to 100 million U.S. customer accounts and credit card applications.
 18 Similarly, in May 2019, First American Financial reported a security incident on its website that
 19 potentially exposed 885 million real estate and mortgage related documents, among others. Across
 20 industries, financial services have the second-highest cost per breached record, behind healthcare. In
 21 financial services, an average breach costs \$210 per record, while a “mega breach,” like Capital
 22 One’s, can cost up to \$388 per record.²³

23 46. Anurag Kahol, CTO of Bitglass recently commented that “[g]iven that organizations
 24 in the financial services industry are entrusted with highly valuable, personally identifiable
 25 _____

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

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

information (PII), they represent an attractive target for cybercriminals[.]” HelpNetSecurity reports that “[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats.”²⁴

47. As such, Defendant was aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiffs’ and Class members’ PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS ACTION ALLEGATIONS

48. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiffs seek to represent and intend to seek certification of a class (the “Class”) defined as:

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

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

50. Certification of Plaintiffs’ claims for class wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

51. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and based on information and belief, the Class consists of tens of thousands of Defendant’s customers, including Plaintiffs

²⁴ HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), available at <https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/>.

1 and the Class members. Plaintiffs therefore believes that the Class is so numerous that joinder of all
2 members is impractical.

3 52. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed
4 members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members
5 were injured by the same wrongful acts, practices, and omissions committed by Defendant, as
6 described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that
7 give rise to the claims of all Class members.

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

- 12 (a) Whether Defendant had a duty to implement and maintain reasonable security
13 procedures and practices appropriate to the nature of the PII it collected, stored,
14 and maintained from Plaintiffs and Class members;
- 15 (b) Whether Defendant breached its duty to protect the PII of Plaintiffs and each
16 Class member; and
- 17 (c) Whether Plaintiffs and each Class member are entitled to damages and other
18 equitable relief.

19 54. Plaintiffs will fairly and adequately protect the interests of the Class members.
20 Plaintiffs are each an adequate representative of the Class in that Plaintiffs have no interests adverse
21 to or that conflicts with the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with
22 substantial experience and success in the prosecution of complex consumer protection class actions
23 of this nature.

24 55. A class action is superior to any other available method for the fair and efficient
25 adjudication of this controversy since individual joinder of all Class members is impractical.
26 Furthermore, the expenses and burden of individual litigation would make it difficult or impossible
27 for the individual members of the Class to redress the wrongs done to them, especially given that
28 the damages or injuries suffered by each individual member of the Class are outweighed by the

costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

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

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 (“CCPA”)

Cal. Civ. Code §§ 1798.100, *et seq.*

57. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

58. As more personal information about consumers is collected by businesses, consumers’ ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: “The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.”²⁵

59. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are

²⁵ CALIFORNIA CONSUMER PRIVACY ACT (CCPA) COMPLIANCE, <https://buyergenomics.com/ccpa-compliance/>.

appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

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

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

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

63. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because Defendant:

- a) is a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners”;
- b) “collects consumers’ personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information”;
- c) does business in and is headquartered in California; and
- d) has annual gross revenues in excess of \$25 million; annually buys, receives for the business’ commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or

1 more consumers, households, or devices; or derives 50 percent or more of
2 its annual revenues from selling consumers' personal information.

3 64. The PII accessed and taken by unauthorized persons in the Data Breach is "personal
4 information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and
5 Class members' unencrypted names, Social Security numbers and/or Driver's License numbers,
6 among other personal information.

7 65. Plaintiffs' PII was subject to unauthorized access and exfiltration, theft, or disclosure
8 because their PII, including names, Social Security numbers and/or Driver's License numbers, was
9 wrongfully accessed and taken by unauthorized persons in the Data Breach.

10 66. The Data Breach occurred as a result of Defendant's failure to implement and
11 maintain reasonable security procedures and practices appropriate to the nature of the information to
12 protect Plaintiffs' and Class members' PII. Defendant failed to implement reasonable security
13 procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of
14 Plaintiffs' and Class members' PII as a result of the Data Breach.

15 67. On March 31, 2022, Plaintiffs provided Defendant with written notice of its
16 violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not
17 cure the violation within 30 days, Plaintiffs will amend their complaint to pursue statutory damages
18 as permitted by Civil Code § 1798.150(a)(1)(A).

19 68. As a result of Defendant's failure to implement and maintain reasonable security
20 procedures and practices that resulted in the Data Breach, Plaintiffs, on behalf of themselves
21 individually and the Class, seek actual damages, equitable relief, including public injunctive relief,
22 and declaratory relief, and any other relief as deemed appropriate by the Court.

23 **SECOND CAUSE OF ACTION**

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

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

26 69. Plaintiffs re-allege and incorporates by reference all proceeding paragraphs as if fully
27 set forth herein.



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

6 71. In the course of conducting its business, Defendant committed “unlawful” business
7 practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee,
8 manage, monitor and audit appropriate data security processes, controls, policies, procedures,
9 protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Class
10 members’ PII, and by violating the statutory and common law alleged herein, including, *inter alia*,
11 California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I,
12 Section 1 of the California Constitution (California’s constitutional right to privacy) and Civil Code
13 § 1798.81.5. Plaintiffs and Class members reserve the right to allege other violations of law by
14 Defendant constituting other unlawful business acts or practices. Defendant’s above-described
15 wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this
16 date.

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

21 73. Defendant’s above-described wrongful actions, inaction, omissions, want of ordinary
22 care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts and
23 practices in violation of the UCL in that Defendant’s wrongful conduct is substantially injurious to
24 consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and
25 unscrupulous. Defendant’s practices are also contrary to legislatively declared and public policies
26 that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize
27 appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the
28 California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant’s wrongful

1 conduct outweighs any alleged benefits attributable to such conduct. There were reasonably
2 available alternatives to further Defendant's legitimate business interests other than engaging in the
3 above-described wrongful conduct.

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

7 75. As a direct and proximate result of Defendant's above-described wrongful actions,
8 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
9 and its violations of the UCL, Plaintiffs and Class members have suffered (and will continue to
10 suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an
11 imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks
12 justifying expenditures for protective and remedial services for which they are entitled to
13 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory
14 damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-
15 established national and international market, and/or (vi) the financial and temporal cost of
16 monitoring their credit, monitoring financial accounts, and mitigating damages.

17 76. Unless restrained and enjoined, Defendant will continue to engage in the above-
18 described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of
19 themselves, Class members, and the general public, also seeks restitution and an injunction,
20 including public injunctive relief prohibiting Defendant from continuing such wrongful conduct,
21 and requiring Defendant to modify its corporate culture and design, adopt, implement, control,
22 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,
23 procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted
24 to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code
25 § 17203.

26 //

27 //

28 //

THIRD CAUSE OF ACTION

Breach of Contract

77. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

78. Plaintiffs and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

79. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Defendant's products and services.

80. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

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

PRAYER FOR RELIEF

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

- (i) actual and punitive damages to be determined by the trier of fact;
- (ii) equitable relief, including restitution;
- (iii) pre- and post-judgment interest at the highest legal rates applicable;
- (iv) appropriate injunctive relief;
- (v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;
- (vi) costs of suit; and
- (vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Dated: March 31, 2022

KAZEROUNI LAW GROUP, APC

By: 

ABBAS KAZEROUNIAN, ESQ.
MONA AMINI, ESQ.

Attorneys for Plaintiffs



EXHIBIT A



245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

March 31, 2022

VIA CERTIFIED MAIL

American Financial Resources, Inc.
9 Sylvan Way
Parsippany, NJ 07054

Re: *Parras, et al. v. American Financial Resources, Inc.*

To Whom It May Concern:

We represent Plaintiffs Edwina and Robert Parras (“Plaintiffs”) and all other similarly situated consumers in a putative class action against American Financial Resources, Inc. (“Defendant”) arising out of, *inter alia*, Defendant’s failure to provide reasonable security for Plaintiffs’ and the proposed class members’ personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the “Data Breach”). To our knowledge the Data Breach occurred on between December 6-20, 2021, as specified in Defendant’s “Notice of Data Breach” letter dated March 9, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiffs’ Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant’s conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiffs demand that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiffs with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiffs and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

EXHIBIT D

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address):
 Abbas Kazerounian (249203); Mona Amini (296829)
 KAZEROUNI LAW GROUP, APC
 245 Fischer Ave., Unit D1, Costa Mesa, CA 92626

TELEPHONE NO.: (800) 400-6808

FAX NO. (Optional): (800) 520-5523

ATTORNEY FOR (Name): Edwina Parras and Robert Parras

FOR COURT USE ONLY

ELECTRONICALLY FILED
 Superior Court of California,
 County of Alameda
04/01/2022 at 12:00:00 AM
 By: Cheryl Clark, Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA

STREET ADDRESS: 1225 Fallon Street

MAILING ADDRESS:

CITY AND ZIP CODE: Oakland, CA 94612

BRANCH NAME: Oakland - Rene C. Davidson Courthouse

CASE NAME:

Parras, et al. v. American Financial Resources, Inc.

CIVIL CASE COVER SHEET

☒ **Unlimited** ☐ **Limited**
 (Amount demanded exceeds \$25,000) (Amount demanded is \$25,000)

Complex Case Designation

☐ Counter ☐ Joinder
 Filed with first appearance by defendant
 (Cal. Rules of Court, rule 3.402)

CASE NUMBER:

22CV009276

JUDGE:

DEPT.:

*Items 1–6 below must be completed (see instructions on page 2).***1. Check one box below for the case type that best describes this case:****Auto Tort**

☐ Auto (22)
☐ Uninsured motorist (46)

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

☐ Asbestos (04)
☐ Product liability (24)
☐ Medical malpractice (45)

Non-PI/PD/WD (Other) Tort

☐ Business tort/unfair business practice (07)
☐ Civil rights (08)
☐ Defamation (13)
☐ Fraud (16)
☐ Intellectual property (19)
☐ Professional negligence (25)
☒ Other non-PI/PD/WD tort (35)

Employment

☐ Wrongful termination (36)
☐ Other employment (15)

Contract

☐ Breach of contract/warranty (06)
☐ Rule 3.740 collections (09)
☐ Other collections (09)
☐ Insurance coverage (18)

Real Property

☐ Other contract (37)
☐ Eminent domain/Inverse condemnation (14)
☐ Wrongful eviction (33)
☐ Other real property (26)

Unlawful Detainer

☐ Commercial (31)
☐ Residential (32)
☐ Drugs (38)

Judicial Review

☐ Asset forfeiture (05)
☐ Petition re: arbitration award (11)
☐ Writ of mandate (02)
☐ Other judicial review (39)

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

☐ Antitrust/Trade regulation (03)
☐ Construction defect (10)
☐ Mass tort (40)
☐ Securities litigation (28)
☐ Environmental/Toxic tort (30)
☐ Insurance coverage claims arising from the above listed provisionally complex case types (41)

Enforcement of Judgment☐ Enforcement of judgment (20)**Miscellaneous Civil Complaint**

☐ RICO (27)
☐ Other complaint (not specified above) (42)

Miscellaneous Civil Petition

☐ Partnership and corporate governance (21)
☐ Other petition (not specified above) (43)

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

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

3. Remedies sought (check all that apply): a. ☒ monetary b. ☒ nonmonetary; declaratory or injunctive relief c. ☒ punitive**4. Number of causes of action (specify):****5. This case ☒ is ☐ is not a class action suit.****6. If there are any known related cases, file and serve a notice of related case. (You may use form CM-015.)**

Date: March 31, 2022

Abbas Kazerounian

(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE

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

Page 1 of 2

INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET

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

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

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

CASE TYPES AND EXAMPLES

Auto Tort

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

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

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

Non-PI/PD/WD (Other) Tort

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

Employment

Wrongful Termination (36)
Other Employment (15)

Contract

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

Real Property

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

Unlawful Detainer

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

Judicial Review

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

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

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

Enforcement of Judgment

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

Miscellaneous Civil Complaint

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

Miscellaneous Civil Petition

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

F. ADDENDUM TO CIVIL CASE COVER SHEET

Short Title:

Case Number:

CIVIL CASE COVER SHEET ADDENDUM

THIS FORM IS REQUIRED IN ALL NEW UNLIMITED CIVIL CASE FILINGS IN THE
SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA

[] Hayward Hall of Justice (447)

[] Oakland, Rene C. Davidson Alameda County Courthouse (446)

[] Pleasanton, Gale-Schenone Hall of Justice (448)

Civil Case Cover Sheet Category	Civil Case Cover Sheet Case Type	Alameda County Case Type (check only one)
Auto Tort	Auto tort (22)	[] 34 Auto tort (G) Is this an uninsured motorist case? [] yes [] no
Other PI /PD / WD Tort	Asbestos (04) Product liability (24) Medical malpractice (45) Other PI/PD/WD tort (23)	[] 75 Asbestos (D) [] 89 Product liability (not asbestos or toxic tort/environmental) (G) [] 97 Medical malpractice (G) [] 33 Other PI/PD/WD tort (G)
Non - PI /PD / WD Tort	Bus tort / unfair bus. practice (07) Civil rights (08) Defamation (13) Fraud (16) Intellectual property (19) Professional negligence (25) Other non-PI/PD/WD tort (35)	[] 79 Bus tort / unfair bus. practice (G) [] 80 Civil rights (G) [] 84 Defamation (G) [] 24 Fraud (G) [] 87 Intellectual property (G) [] 59 Professional negligence - non-medical (G) [] 03 Other non-PI/PD/WD tort (G)
Employment	Wrongful termination (36) Other employment (15)	[] 38 Wrongful termination (G) [] 85 Other employment (G) [] 53 Labor comm award confirmation [] 54 Notice of appeal - L.C.A.
Contract	Breach contract / Wrnty (06) Collections (09) Insurance coverage (18) Other contract (37)	[] 04 Breach contract / Wrnty (G) [] 81 Collections (G) [] 86 Ins. coverage - non-complex (G) [] 98 Other contract (G)
Real Property	Eminent domain / Inv Cdm (14) Wrongful eviction (33) Other real property (26)	[] 18 Eminent domain / Inv Cdm (G) [] 17 Wrongful eviction (G) [] 36 Other real property (G)
Unlawful Detainer	Commercial (31) Residential (32) Drugs (38)	[] 94 Unlawful Detainer - commercial [] 47 Unlawful Detainer - residential [] 21 Unlawful detainer - drugs Is the deft. in possession of the property? [] Yes [] No
Judicial Review	Asset forfeiture (05) Petition re: arbitration award (11) Writ of Mandate (02) Other judicial review (39)	[] 41 Asset forfeiture [] 62 Pet. re: arbitration award [] 49 Writ of mandate Is this a CEQA action (Publ.Res.Code section 21000 et seq) [] Yes [] No [] 64 Other judicial review
Provisionally Complex	Antitrust / Trade regulation (03) Construction defect (10) Claims involving mass tort (40) Securities litigation (28) Toxic tort / Environmental (30) Ins covrg from cmplx case type (41)	[] 77 Antitrust / Trade regulation [] 82 Construction defect [] 78 Claims involving mass tort [] 91 Securities litigation [] 93 Toxic tort / Environmental [] 95 Ins covrg from complex case type
Enforcement of Judgment	Enforcement of judgment (20)	[] 19 Enforcement of judgment [] 08 Confession of judgment
Misc Complaint	RICO (27) Partnership / Corp. governance (21) Other complaint (42)	[] 90 RICO (G) [] 88 Partnership / Corp. governance (G) [] 68 All other complaints (G)
Misc. Civil Petition	Other petition (43)	[] 06 Change of name [] 69 Other petition

EXHIBIT E

SUPERIOR COURT OF CALIFORNIA COUNTY OF ALAMEDA		Reserved for Clerk's File Stamp FILED Superior Court of California County of Alameda 04/01/2022 Clad File, Executive Officer/Clerk of the Court By: <u><i>Cheryl Clark</i></u> Deputy C. C. Clark
COURTHOUSE ADDRESS: Rene C. Davidson Courthouse 1225 Fallon Street, Oakland, CA 94612		
PLAINTIFF: Edwina Parras et al		
DEFENDANT: American Financial Resources, Inc.		
NOTICE OF CASE MANAGEMENT CONFERENCE		CASE NUMBER: 22CV009276

TO THE PLAINTIFF(S)/ATTORNEY(S) FOR PLAINTIFF(S) OF RECORD:

You are ordered to serve all named defendants and file proofs of service on those defendants with the court within 60 days of the filing of the complaint (Cal. Rules of Court, 3.110(b)).

Give notice of this conference to all other parties and file proof of service.

Your Case Management Conference has been scheduled on:

Date: 08/01/2022	Time: 8:30 AM	Dept.: 21
Location: Rene C. Davidson Courthouse Administration Building, 1221 Oak Street, Oakland, CA 94612		

TO DEFENDANT(S)/ATTORNEY(S) FOR DEFENDANT(S) OF RECORD:

The setting of the Case Management Conference does not exempt the defendant from filing a responsive pleading as required by law, you must respond as stated on the summons.

TO ALL PARTIES who have appeared before the date of the conference must:

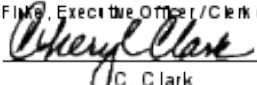
Pursuant to California Rules of Court, 3.725, a completed Case Management Statement (Judicial Council form CM-110) must be filed and served at least 15 calendar days before the Case Management Conference. The Case Management Statement may be filed jointly by all parties/attorneys of record or individually by each party/attorney of record.

Meet and confer, in person or by telephone as required by Cal. Rules of Court, rule 3.724.

Post jury fees as required by Code of Civil Procedure section 631.

If you do not follow the orders above, the court may issue an order to show cause why you should not be sanctioned under Cal. Rules of Court, rule 2.30. Sanctions may include monetary sanctions, striking pleadings or dismissal of the action.

The judge may place a Tentative Case Management Order in your case's on-line register of actions before the conference. This order may establish a discovery schedule, set a trial date or refer the case to Alternate Dispute Resolution, such as mediation or arbitration. Check the court's eCourt Public Portal for each assigned department's procedures regarding tentative case management orders at <https://eportal.alameda.courts.ca.gov>.

<p align="center">SUPERIOR COURT OF CALIFORNIA COUNTY OF ALAMEDA</p>	<p align="center">Reserved for Clerk's File Stamp</p>
<p>COURTHOUSE ADDRESS: Rene C. Davidson Courthouse 1225 Fallon Street, Oakland, CA 94612</p>	<p align="center">FILED Superior Court of California County of Alameda 04/01/2022</p>
<p>PLAINTIFF/PETITIONER: Edwina Parras et al</p>	<p>Chad Finke, Executive Officer / Clerk of the Court By:  Deputy</p>
<p>DEFENDANT/RESPONDENT: American Financial Resources, Inc.</p>	<p align="center">C. Clark</p>
<p align="center">CERTIFICATE OF MAILING</p>	<p>CASE NUMBER: 22CV009276</p>

I, the below-named Executive Officer/Clerk of the above-entitled court, do hereby certify that I am not a party to the cause herein, and that on this date I served the Notice of Case Management Conference upon each party or counsel named below by placing the document for collection and mailing so as to cause it to be deposited in the United States mail at the courthouse in Oakland, California, one copy of the original filed/entered herein in a separate sealed envelope to each address as shown below with the postage thereon fully prepaid, in accordance with standard court practices.

Dated: 04/04/2022

Chad Finke, Executive Officer / Clerk of the Court

By:



C. Clark, Deputy Clerk

CERTIFICATE OF MAILING

ClassAction.org

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