

United States District Court
Northern District of California

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JAMI ZUCCHERO,
Plaintiff,
v.
HEIRLOOM ROSES, INC.,
Defendant.

Case No. 22-cv-00068-KAW

**ORDER GRANTING MOTION FOR
PRELIMINARY APPROVAL**

Re: Dkt. No. 56

Plaintiff Jami Zucchero filed the instant putative class action against Defendant Heirloom Roses, Inc., alleging that Defendant failed to properly secure and safeguard personally identifiable information stored within Defendant’s information network, resulting in a data breach. (*See* First Am. Compl. (“FAC”) ¶ 1, Dkt. No. 25.) Pending before the Court is Plaintiff’s motion for preliminary approval of a settlement agreement between the parties. (Pl.’s Mot. for Prelim. Approval, Dkt. No. 56.) Having considered the parties’ filings and the arguments presented at the November 16, 2023 hearing, and for the reasons set forth below, the Court GRANTS Plaintiff’s motion for preliminary approval.

I. BACKGROUND

A. Factual and Procedural Background

Defendant is a rose nursery, which sells flowers, plants, and gardening accessories through its website. (FAC ¶ 26.) Plaintiff purchased goods/services from Defendant’s website, providing financial information to Defendant. (FAC ¶¶ 14, 17.) Around December 16, 2021, Defendant sent a notice to Plaintiff, stating that malicious code had been added to Defendant’s website for the purpose of capturing credit card data (the “Data Security Incident”). (FAC ¶¶ 19, 38.)

On January 6, 2022, Plaintiff filed the instant case. (Compl., Dkt. No. 1.) Following a motion to dismiss, Plaintiff filed the operative complaint, alleging claims for: (1) negligence, (2)

1 breach of contract, (3) breach of the implied covenant of good faith and fair dealing, (4) unfair
2 business practices under the Unfair Competition Law (“UCL”), and (5) unjust enrichment.

3 Plaintiff sought to represent all individuals within the United States whose financial information
4 was exposed to unauthorized third parties as a result of the Data Security Incident. (FAC ¶ 28.)

5 Defendant filed a second motion to dismiss. (Dkt. No. 26.) On August 2, 2022, the Court
6 granted in part and denied in part the motion to dismiss. (Dismissal Order, Dkt. No. 35.) First, the
7 Court found that while Plaintiff could not establish standing based on the increased risk of future
8 fraud or the diminution of value of Plaintiff’s personal information, she could establish injury in
9 the form of her lost time from dealing with the data breach. (*Id.* at 4.) Second, the Court found
10 that Plaintiff had adequately alleged a negligence claim based on the failure to provide fair,
11 reasonable, or adequate computer systems. (*Id.* at 6-7.) Third, the Court found Plaintiff had
12 adequately alleged a breach of contract claim and implied covenant of good faith and fair dealing
13 claim based on Defendant’s assertions that its “secure server is designed to protect [financial]
14 information and is fully PCI compliant.” (*Id.* at 9.) Finally, the Court dismissed the UCL and
15 unjust enrichment claims with prejudice because there were no factual allegations that Plaintiff
16 paid for data security or otherwise lost money. (*Id.* at 11-12.)

17 After engaging in informal discovery efforts, including the voluntary exchange of
18 information to analyze and value the claims, the parties engaged in mediation before John Bates of
19 JAMS. (8/25/23 Cole Decl. ¶¶ 8, 10, 12, 14, Dkt. No. 56-1.) During the mediation, the parties
20 exchanged information and documents, as well as their analyses of the risks and delays of further
21 litigation. (8/25/23 Cole Decl. ¶ 14.) After the mediation, the parties reached a settlement in
22 principle and negotiated further terms, as articulated by the Settlement Agreement. (8/25/23 Cole
23 Decl. ¶ 15; *see also* 8/25/23 Cole Decl., Exh. A (“Settlement Agreement”).)

24 On May 15, 2023, the parties informed the Court that they had achieved a settlement in
25 principle. (Dkt. No. 51.) On August 25, 2023, Plaintiff filed the instant motion for preliminary
26 approval of the class settlement. On September 14, 2023, the Court requested supplemental
27 briefing. (Dkt. No. 62.) On October 6, 2023, Plaintiff filed a supplemental brief, supported by the
28 declaration of Defendant’s counsel. (10/6/23 Supp. Brief, Dkt. No. 63; 9/30/23 Persson Decl.,

1 Dkt. No. 63-1.) On October 24, 2023, the Court requested further supplemental briefing. (Dkt.
2 No. 67.) On November 3, 2023, Plaintiff filed a second supplemental brief. (11/3/23 Supp. Brief,
3 Dkt. No. 68.) On November 20, 2023, Plaintiff filed the current class notice. (Dkt. No. 74.)

4 **B. Settlement Agreement**

5 Under the terms of the settlement agreement, Defendant agrees to pay up to \$200 per class
6 member for unreimbursed, unauthorized charges or out-of-pocket expenses caused by the Data
7 Security Incident. (Pl.’s Mot. for Prelim. Approval at 3; Settlement Agreement ¶ 2.5.1.) The \$200
8 includes up to two hours of lost time at \$20 per hour. (Settlement Agreement ¶ 2.5.) In order to
9 obtain compensation, a class member must submit a claim form, as well as documentation
10 sufficient to show unauthorized charges or other losses fairly traceable to the Data Security
11 Incident. (Settlement Agreement ¶¶ 2.6, 2.7.) Additionally, Defendant has agreed to make
12 security enhancements, including: (1) requiring third-party vendors and users to utilize strong
13 passwords and two-factor authentication, (2) requiring third-party vendors and users to undergo
14 regular safety training, (3) protecting sensitive data using encryption, access control, and data
15 masking, and (4) migrating to the Shopify platform, which provides built-in security features such
16 as SSL encryption, PCI compliance, secure payment processing, and monitoring features to detect
17 and prevent unauthorized access and suspicious activities. (Settlement Agreement ¶ 2.8.) In
18 exchange, the class agrees to release all claims that relate to the Data Security Incident, whether
19 known or unknown. (Settlement Agreement ¶ 1.29.) The class is not required to release unknown
20 claims unrelated to the Data Security Incident. (11/3/23 Supp. Brief at 3.) The Settlement
21 Agreement permits Plaintiff to seek attorney’s fees and costs up to \$198,500, and a service award
22 for plaintiff in the amount of \$1,500. (Settlement Agreement ¶¶ 9.1, 9.2.) Unlike the class,
23 Plaintiff agrees to release all claims, whether or not related to the Data Security Incident.
24 (Settlement Agreement ¶ 8.3.)

25 After requesting bids from three different companies, the parties have selected CPT Group
26 (“CPT”) to act as the Claims Administrator. (Pl.’s Mot. for Prelim. Approval at 5; 8/25/23 Cole
27 Decl. ¶ 32.) CPT has agreed to a flat fee of \$40,000, which shall be paid by Defendant. (8/25/23
28 Cole Decl. ¶ 32.) Once the Court grants preliminary approval, Defendant will provide contact

1 information for the class to the Settlement Administrator. (Settlement Agreement ¶ 4.2.) The
 2 Settlement Administrator will then be responsible for mailing the Class Notice and claim forms to
 3 the class, including undertaking reasonable efforts to resend notice. (Settlement Agreement ¶
 4 4.3.1.) The Settlement Administrator is also responsible for establishing a dedicated settlement
 5 website. (Settlement Agreement ¶ 4.3.2.)

6 The class is bound by the settlement unless they timely submit a request for exclusion.
 7 (Settlement Agreement ¶ 5.1.) Individuals who submit claims will have their claims reviewed by
 8 the Settlement Administrator, including reaching out to class members who provide insufficient
 9 documentation. (Settlement Agreement ¶¶ 7.1, 7.3.)

10 II. LEGAL STANDARD

11 Per Federal Rule of Civil Procedure 23(e), “[t]he claims, issues, or defenses of a certified
 12 class may be settled, voluntarily dismissed, or compromised only with the court’s approval.” The
 13 purpose of requiring court approval “is to protect the unnamed members of the class from unjust
 14 or unfair settlements affecting their rights.” *In re Syncor ERISA Litig.*, 516 F.3d 1095, 1100 (9th
 15 Cir. 2008). Thus, before approving a settlement, the Court must conclude that the settlement is
 16 “fundamentally fair, adequate, and reasonable.” *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1026
 17 (9th Cir. 1998). This inquiry:

18 requires the district court to balance a number of factors: the
 19 strength of the plaintiff’s case; the risk, expense, complexity, and
 20 likely duration of further litigation; the risk of maintaining class
 21 action status throughout the trial; the amount offered in settlement;
 22 the extent of discovery completed and the stage of the proceedings;
 23 the experience and views of counsel; the presence of a government
 24 participant; and the reaction of the class members to the proposed
 25 settlement.

26 *Id.*; see also *Churchill Vill. L.L.C. v. Gen. Elec.*, 361 F.3d 566, 575 (9th Cir. 2004) (same).

27 Furthermore, the Ninth Circuit has recognized that where no class has been formally
 28 certified, “there is an even greater potential for a breach of fiduciary duty owed the class during
 settlement. Accordingly, such agreements must withstand an even higher level of scrutiny for
 evidence of collusion or other conflicts of interest than is ordinarily required under Rule 23(e)
 before securing the court’s approval as fair.” *In re Bluetooth Headset Prods. Liab. Litig.*, 654 F.3d

1 935, 947 (9th Cir. 2011); *see also Lane v. Facebook, Inc.*, 696 F.3d 811, 819 (9th Cir. 2012)
2 (“when . . . the settlement takes place before formal class certification, settlement approval
3 requires a ‘higher standard of fairness’”). This more “exacting review” is required “to ensure that
4 class representatives and their counsel do not secure a disproportionate benefit at the expense of
5 the unnamed plaintiffs who class counsel had a duty to represent.” *Lane*, 696 F.3d at 819 (internal
6 quotation omitted); *see also Hanlon*, 150 F.3d at 1026 (“The dangers of collusion between class
7 counsel and the defendant, as well as the need for additional protections when the settlement is not
8 negotiated by a court[-]designated class representative, weigh in favor of a more probing inquiry
9 than may normally be required under Rule 23(e)”).

10 When applying Rule 23(e), the courts use a two-step process for the approval of class
11 action settlements. First, the Court decides whether the class action settlement deserves
12 preliminary approval. Second, after notice is given to class members, the Court determines
13 whether final approval is warranted. *See O’Connor v. Uber Techs., Inc.*, 201 F. Supp. 3d 1110,
14 1121-22 (N.D. Cal. 2016). At the preliminary approval stage, courts in this district “have stated
15 that the relevant inquiry is whether the settlement falls within the range of possible approval or
16 within the range of reasonableness.” *Cotter v. Lyft*, 176 F. Supp. 3d 930, 935 (N.D. Cal. 2016)
17 (internal quotation omitted). “In determining whether the proposed settlement falls within the
18 range of reasonableness, perhaps the most important factor to consider is plaintiff’s expected
19 recovery balanced against the value of the settlement offer.” *Id.*; *see also O’Connor*, 201 F. Supp.
20 3d at 1122. This determination “requires evaluating the relative strengths and weaknesses of the
21 plaintiffs’ case; it may be reasonable to settle a weak claim for relatively little, while it is not
22 reasonable to settle a strong claim for the same amount.” *Cotter*, 176 F. Supp. at 936 (citing *In re*
23 *High-Tech Emp. Antitrust Litig.*, Case No: 11-cv-2509-LHK, 2014 WL 3917126, at *4 (N.D. Cal.
24 Aug. 8, 2014).

25 In addition to considering whether the settlement falls within the range of reasonableness,
26 courts in this district also consider whether the settlement: “(1) appears to be the product of
27 serious, informed, non-collusive negotiations; (2) has no obvious deficiencies; [and] (3) does not
28 improperly grant preferential treatment to class representatives or segments of the class.” *In re*

1 *Tableware Antitrust Litig.*, 484 F. Supp. 2d 1078, 1079 (N.D. Cal. 2007) (internal quotation
 2 omitted). With respect to the level of scrutiny applied to this determination, “district courts often
 3 state or imply that scrutiny should be more lax.” *Cotter*, 193 F. Supp. 3d at 1035-36. Several
 4 courts in this district have begun to question that “lax review” as “mak[ing] little practical sense.”
 5 *Id.* at 1036. Instead, these courts suggest that “scrutinizing the agreement carefully at the initial
 6 stage and identifying any flaws that can be identified . . . allows the parties to decide how to
 7 respond to those flaws (whether by fixing them or opting not to settle) before they waste a great
 8 deal of time and money in the notice and opt-out process.” *Id.*

9 III. DISCUSSION

10 A. Class Certification

11 Before determining the fairness of a class action settlement, the Court must as a threshold
 12 matter “ascertain whether the proposed settlement class satisfies the requirements of Rule 23(a) of
 13 the Federal Rules of Civil Procedure applicable to all class actions, namely: (1) numerosity, (2)
 14 commonality, (3) typicality, and (4) adequacy of representation.” *Hanlon*, 150 F.3d at 1019. The
 15 Court must also find that at least one requirement of Rule 23(b) is satisfied. *Id.* at 1022.

16 The Court finds that for the purposes of approval of the class action settlement, the Rule
 17 23(a) requirements are satisfied. First, numerosity exists because the settlement class includes
 18 over 52,000 customers. (9/30/23 Persson Decl. ¶ 11.) Second, commonality exists because there
 19 are “questions of fact and law which are common to the class,” namely whether Defendant’s
 20 alleged failure to prevent the Data Security Incident constituted negligence or breach of contract.
 21 Fed. R. Civ. P. 23(a)(2); *see also Hanlon*, 150 F.3d at 1019-20 (noting that the commonality
 22 requirement is “permissive” and “has been construed permissively”). Third, typicality exists
 23 because the named Plaintiff’s claims are “reasonably co-extensive with those of absent class
 24 members,” as Plaintiff’s information was allegedly exposed during the Data Security Incident.
 25 *See Hanlon*, 150 F.3d at 1020. Finally, adequacy exists because there is no evidence that Plaintiff
 26 and Plaintiff’s counsel have any conflicts of interest with the proposed class, or that Plaintiff and
 27 Plaintiff’s counsel will not vigorously prosecute the case on behalf of the class. *See id.*
 28 (“Resolution of two questions determines legal adequacy: (1) do the named plaintiffs and their

1 counsel have any conflicts of interest with other class members and (2) will the named plaintiffs
2 and their counsel prosecute the action vigorously on behalf of the class?”).

3 The Court also concludes that at the preliminary approval stage, the Rule 23(b)(3)
4 requirement is satisfied. Under Rule 23(b)(3), the Court must find that “the questions of law or
5 fact common to class members predominate over any questions affecting only individual
6 members, and that a class action is superior to other available methods for fairly and efficiently
7 adjudicating the controversy.” Here, the Court finds that predominance is satisfied because
8 Plaintiff’s claims arise from the same Data Security Incident. Further, the Court finds that
9 superiority is satisfied because the alternative method to a class action likely involves “individual
10 claims for a small amount of . . . damages,” resulting in most cases involving “litigation costs
11 [that] dwarf potential recovery.” *Hanlon*, 150 F.3d at 1023.

12 The Court therefore provisionally certifies the class for settlement purposes.

13 **B. Preliminary Approval Factors**

14 **i. Range of Reasonableness**

15 In considering whether the Settlement Agreement falls within the range of possible
16 approval, the Court “primarily consider[s] plaintiffs’ expected recovery balanced against the value
17 of the settlement offer.” *Viceral v. Mistras Grp., Inc.*, Case No. 15-cv-2198-EMC, 2016 WL
18 5907869, at *7 (N.D. Cal. Oct. 11, 2016).

19 The expected value of the Settlement Agreement is variable, as there is no common fund;
20 rather, it is dependent on the number of claims that are submitted. Defendant believes the claim
21 rate will fall between 1-3% based on prior experience in data breach matters and because only
22 2.3% (approximately 1,200 individuals) of those affected by the Data Security Incident activated
23 the complimentary identity protection and credit monitoring services offered by Defendant.
24 (9/30/23 Persson Decl. ¶ 13.) This would likely result in a total payment of less than \$75,000.
25 (9/30/23 Persson Decl. ¶ 13.) Additionally, Defendant has agreed to implement security
26 enhancements, which it estimates will cost approximately \$500,000. (11/2/23 Persson Decl. ¶ 5,
27 Dkt. No. 68.) This is in addition to other costs Defendant has agreed to pay, including class
28 counsel’s attorney’s fees and the Settlement Administrator’s costs.

1 While the Court has never encountered a case with no common fund, the Court observes
2 that this does not appear to be a high-value case. The Court previously found that Plaintiff could
3 not establish standing based on the increased risk of future fraud or the diminution of value of
4 Plaintiff's personal information, but that she could establish injury in the form of her lost time
5 from dealing with the data breach or actual fraudulent charges. (Dismissal Order at 4-6.) This
6 significantly limited damages, as Plaintiff acknowledges that "[g]iven that only credit card
7 information was impacted by the Breach, and fraudulent charges must be reimbursed by law and
8 are indemnified by the credit card companies, the potential for extraordinary loss is essentially
9 zero." (11/3/23 Supp. Brief at 2.) Thus, the primary recovery would be lost time damages.
10 Plaintiff estimates that such recovery may average to \$45/class member, or approximately \$2.3
11 million. (*Id.*) At the same time, again, the parties acknowledge that only 2.3% of those affected
12 by the Data Security Incident activated the complimentary identity protection and credit
13 monitoring services offered by Defendant, which would suggest that the actual lost time damages
14 is significantly lower than \$45 for every class member. (*See* 9/30/23 Persson Decl. ¶ 9.) In any
15 case, the proposed settlement would allow class members who submit claims to recover \$40 for
16 lost time, which represents almost 90% of the likely lost time spent on this data breach (if any).
17 This is in addition to the security enhancements, which Defendant has estimated will cost
18 approximately \$500,000 to implement. (11/2/23 Persson Decl. ¶ 5, Dkt. No. 68.)

19 The parties also identify significant risks that make the proposed settlement fall within a
20 range of reasonableness. A primary risk is whether Plaintiff would have been able to obtain
21 certification given that most of the class likely spent no time responding to the Data Security
22 Incident, and thus would have no damages. (*See* 9/30/23 Persson Decl. ¶ 9.) Additionally, to the
23 extent Plaintiff was basing her breach of contract claim on Defendant's privacy policy and its
24 assurances that its "secure server is designed to protect this information and is fully PCI
25 compliant," there is a question as to whether Plaintiff had ever read or relied on the privacy policy.
26 (9/30/23 Persson Decl. ¶ 9.) Thus, there is an additional question of whether Plaintiff would have
27 been an adequate class representative as to the breach of contract claim, in addition to whether
28 there would need to be individualized proof demonstrating that class members had actually read

1 and relied upon the privacy policy. In short, given the substantial risks and the limited value of
2 this case, the Court finds that the proposed settlement falls within the range of reasonableness.
3 This factor thus weighs in favor of preliminary approval.

4 **ii. Serious, Informed Negotiations**

5 Next, the Court considers how the parties arrived at the settlement, specifically whether the
6 settlement was “the product of an arms-length, non-collusive, negotiated resolution.” *Rodriguez v.*
7 *W. Publ'g Co.*, 563 F.3d 948, 965 (9th Cir. 2009). Here, the parties engaged in extensive informal
8 discovery and production of data to analyze and evaluate the case. (8/25/23 Cole Decl. ¶ 12.)
9 This included requesting information to develop a damages and penalties analysis for each
10 primary claim. (8/25/23 Cole Decl. ¶ 13.) The parties then attended mediation with John Bates of
11 JAMS, after which they reached a settlement in principle before spending the next two months
12 negotiating various settlement terms. (8/25/23 Cole Decl. ¶¶ 14-15.) The Court finds that the
13 parties reached the settlement via an arms-length, non-collusive, negotiated resolution, and that
14 this factor weighs in favor of preliminary approval.

15 **iii. No Obvious Deficiencies**

16 The Court finds no obvious deficiencies at this time. Defendant’s counsel has confirmed
17 that CAFA notice was completed on September 1, 2023, and that no other lawsuits have been filed
18 against Defendant relating to the Data Security Incident. (9/30/23 Persson Decl. ¶¶ 18-19.)
19 Additionally, the Court requested certain changes to the Class Notice, which the Court has
20 confirmed have been made. (10/29/23 Supp. Brief at 5; Dkt. No. 74.)

21 With respect to the attorney’s fees request, however, the Court expects counsel to provide
22 further information at the final approval stage, as presently Plaintiff’s counsel has failed to provide
23 a breakdown of hours spent or substantive information as to the experience of Attorneys Jaramillo
24 or Bolce beyond their California State Bar admission dates. (*See* 11/3/23 Van Note Decl. ¶¶ 4-5.)
25 Such information is necessary to fulfill the Court’s “independent obligation to ensure that the
26 [attorney’s fees] award, like the settlement itself, is reasonable, even if the parties have already
27 agreed to an amount.” *In re Bluetooth*, 654 F.3d at 941.

28 **iv. Preferential Treatment**

United States District Court
Northern District of California

1 Finally, the Court considers whether the Settlement provides preferential treatment to any
2 class members. The Court concludes that the Settlement does not. The Settlement compensates
3 all class members in the same way, based on any time spent responding to the Data Security
4 Incident or out of pocket losses. Thus, this factor weighs in favor of preliminary approval.

5 **v. Notice Procedure**

6 The Court has reviewed the content of the proposed notice submitted on November 20,
7 2023, and finds it sufficient.

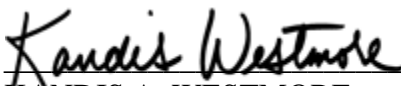
8 **IV. CONCLUSION**

9 The Court finds that based on the above factors, preliminary approval is warranted. The
10 Court therefore GRANTS preliminary approval of the parties' proposed Settlement Agreement,
11 including the provisional certification of the class action. The Court APPOINTS, for settlement
12 purposes only, Jamie Zucchero as class representative; Cole & Van Note as class counsel; and
13 CPT Group, Inc. as Settlement Administrator. The Court sets the following schedule:

Action:	Date:
Defendants to provide class member contact information to Settlement Administrator	15 days from the date of this order
Settlement Administrator to mail Notice Packets	29 days from the date of this order
Last Day for class members to object or opt out to the Settlement Agreement	75 days from the date of this order
Last day for class members to submit claim forms	90 days after Notice Deadline
Class Counsel to file Motion for Attorney's fees, costs, and class representative service awards	45 days before the Final Approval Hearing
Plaintiff to file Motion for Final Settlement Approval	45 days before the Final Approval Hearing
Final Approval Hearing	May 2, 2024 at 1:30 p.m.

14
15
16
17
18
19
20
21
22
23
24 IT IS SO ORDERED.

25 Dated: November 30, 2023

26 
27 KANDIS A. WESTMORE
28 United States Magistrate Judge