

1 **WO**

2

3

4

5

NOT FOR PUBLICATION

6

IN THE UNITED STATES DISTRICT COURT

7

FOR THE DISTRICT OF ARIZONA

8

9

Patricia Murray, et al.,

No. CV-07-2578-PHX-FJM

10

Plaintiffs,

ORDER

11

vs.

12

Financial Visions, Inc., et al.,

13

Defendants.

14

15

16

17

The court has before it plaintiffs Patricia Murray, Robert Ortiz, and Murray Financial, LLC's ("plaintiffs") motion for class certification (doc. 55), defendants Principal Financial Group, Inc., Principal Life Insurance Company, and Princor Financial Services' ("Principal defendants") response (doc. 77), defendant Fiserv, Inc.'s ("Fiserv") response (doc. 75), and plaintiffs' reply (doc. 84). We also have before us defendant LiveOffice LLC's¹ motion to dismiss (doc. 43), Fiserv's joinder in the motion to dismiss (doc. 59), plaintiffs' response (doc. 70), and Fiserv's reply (doc. 90). Finally, we have Principal defendants' motion for judgment on the pleadings (doc. 78), plaintiffs' response (doc. 87), and Principal defendants' reply (doc. 91).

26

27

¹After LiveOffice filed its motion to dismiss, plaintiffs' moved to voluntarily dismiss all claims against LiveOffice. On August 13, 2008, LiveOffice was dismissed from this case. We thus decide it only on behalf of Fiserv.

28

1 **I. Background**

2 Defendant Principal Financial Group, Inc., (“Principal”) is a registered securities
3 broker-dealer and investment advisor. Plaintiff Patricia Murray has worked for Principal as
4 a registered representative (“Principal representative”) since 1992, selling securities and
5 other investment products offered through Principal. Murray and her husband, plaintiff
6 Robert Ortiz, manage plaintiff Murray Financial, LLC. Principal provided plaintiffs with a
7 list of approved vendors of website hosting services, including defendants Financial Visions,
8 Inc., Fiserv, and LiveOffice (collectively, “Web Host defendants”). In September 2002 and
9 April 2003, plaintiffs contracted with Financial Visions for website and email services,
10 respectively.

11 Plaintiffs allege that in August 2007, Principal requested that the Web Host
12 Defendants intercept and automatically transmit all email sent from or received by any
13 Principal representatives. Plaintiffs acknowledge that, in order to comply with SEC
14 regulations, Principal representatives were required to provide Principal with copies of all
15 correspondence related to securities and give Principal permission to monitor and print
16 information on their websites. Amended Complaint ¶ 22. Beginning in August 2007, the
17 Web Host defendants began intercepting and transmitting email sent from or received by
18 Principal’s representatives. Principal stopped the interception program in September 2007.
19 Plaintiffs filed this action against the Principal defendants and the Web Host defendants
20 alleging that every email intercepted by the defendants constitutes a violation of the
21 Electronic Communications Privacy Act of 1985 (“ECPA”), 18 U.S.C. §§ 2510 et seq., and
22 violated their privacy rights under state law.

23 Congress passed the ECPA to address advances in electronic technology by
24 “afford[ing] privacy protection to electronic communications.” Konop v. Hawaiian Airlines,
25 Inc., 302 F.3d 868, 874 (9th Cir. 2002). A private right of action is available to “any . . .
26 person aggrieved by any violation of this chapter.” 18 U.S.C. § 2707(a). There are two
27 distinct claims under the ECPA. Title I amended the Wiretap Act, id. §§ 2510-2522, and
28 governs unauthorized interception of electronic communications, making it an offense to

1 “intentionally intercept[] . . . any wire, oral, or electronic communication,” id. § 2511(1)(a).
2 Title II created the Stored Communications Act, id. § 2701-2712, which governs
3 unauthorized access to stored communications and makes it unlawful to “intentionally
4 access[] without authorization a facility through which an electronic communication service
5 is provided . . . and thereby obtain[], alter[], or prevent[] authorized access to a wire or
6 electronic communication while it is in electronic storage.” Id. § 2701(a)(1).²

7 Plaintiffs allege that the three Web Host defendants forwarded to the Principal
8 defendants email correspondence sent to and received by plaintiffs and other putative class
9 members without their permission. Although they acknowledge that they contracted with
10 Financial Visions only, they now seek certification of a class consisting of every Principal
11 employee, contractor, and broker who used any of the Web Host defendants’ email services
12 and had email automatically forwarded to Principal, as well as those individuals who sent
13 email to or received email from Principal employees, contractors, and brokers that were
14 automatically forwarded to Principal.

15 **II. Motion for Class Certification**

16 We may certify a class if the prerequisites under Rule 23(a), Fed. R. Civ. P., are
17 satisfied: (1) numerosity of the parties; (2) commonality of legal and factual issues; (3)
18 typicality of claims and defenses of the class representatives; and (4) adequacy of
19 representation. In addition to satisfying Rule 23(a) prerequisites, parties seeking class
20 certification must show that the proposed class action fits within one or more of three
21 categories of class actions described in Rule 23(b), Fed. R. Civ. P.

22 **A. Rule 23(a), Fed. R. Civ. P.**

23
24
25 ²Plaintiffs refer generally to the ECPA in their amended complaint; they do not
26 specify under which section of the Act their claim is brought. However, in their response to
27 the motion for judgment on the pleadings, plaintiffs clarify that their claim is asserted only
28 under the Wiretap Act. Response at 3 (“Nowhere in the First Amended Complaint have
Plaintiffs made any allegation that any of the e-mails in question were ever in any type of
electronic storage.”).

1 Rule 23(a)(1) requires that the class be “so numerous that joinder of all members is
2 impracticable.” Plaintiffs have identified 48 putative class members who sent email to or
3 received email from the plaintiffs’ email address during the relevant time. In addition, they
4 claim that there were at least 37 other Principal representatives using Financial Visions, and
5 29 Principal representatives using Fiserv, for a purported minimum class size of 114
6 members. This is sufficient to meet the numerosity requirement.

7 Under Rule 23(a)(2), plaintiffs must show that there are questions of law or fact
8 common to the class. Here, plaintiffs challenge the common scheme of interception and
9 transmission of email by the Web Host defendants and Principal defendants in violation of
10 the Wiretap Act and state privacy laws. Their claims arise from a common set of facts and
11 are based on identical legal theories. Therefore, the commonality prerequisite is satisfied.

12 Rule 23(a)(3) requires that “the claims or defenses of the representative parties are
13 typical of the claims or defenses of the class.” “Typicality refers to the nature of the claim
14 or defense of the class representative, and not to the specific facts from which it arose or the
15 relief sought.” Hanon v. Dataproducts Corp., 976 F.2d 497, 508 (9th Cir. 1992). Defendants
16 argue that plaintiffs’ proposed class lacks typicality because plaintiffs have no cause of
17 action against Fiserv. Although typicality is generally lacking when the representative
18 plaintiff’s claim is against a defendant unrelated to the defendants against whom the class
19 members’ claim lies, La Mar v. H&B Novelty & Loan Co., 489 F.2d 461, 465 (9th Cir.
20 1973), this limitation does not apply where “all injuries are the result of a conspiracy or
21 concerted schemes between the defendants at whose hands the class suffered injury.” Id. at
22 466.

23 Plaintiffs allege that Principal instructed the Web Host defendants to intercept and
24 forward email. While Principal interacted with each of the Web Hosts defendants, the Web
25 Host defendants are not alleged to have had any contact with each other and in fact are
26 competitors. Therefore, it is doubtful whether a concerted scheme existed sufficient to
27 satisfy the typicality requirement, or even whether plaintiffs have standing to assert claims
28 against Fiserv. Nevertheless, because we conclude that plaintiffs cannot establish that their

1 proposed class action fits within one of the three categories described in Rule 23(b), we need
2 not decide this issue.

3 Finally, under Rule 23(a)(4), plaintiffs must establish that “the representative parties
4 will fairly and adequately protect the interests of the class.” The “class representative must
5 be part of the class and possess the same interest and suffer the same injury as the class
6 members.” Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 625-26, 117 S. Ct. 2231, 2250-
7 51 (1997) (quotation and citation omitted). To establish adequacy of representation,
8 plaintiffs must show: (1) that their interests are common with, and not antagonistic to, the
9 class’ interests; and (2) that they are “able to prosecute the action vigorously through
10 qualified counsel.” Lerwill v. Inflight Motion Pictures, Inc., 582 F.2d 507, 512 (9th Cir.
11 1978).

12 Defendants assert that plaintiff Murray has filed a separate gender discrimination
13 action against Principal and therefore her motives in this case may not be consistent with
14 those of the other class members. We agree that Murray’s pursuit of a separate, unrelated
15 discrimination claim against Principal creates at least an issue as to whether she has an
16 undivided loyalty to the class. Pursuing two separate actions against Principal creates a
17 possibility of leveraging a global settlement to serve her own individual interests as opposed
18 to those of the class, and calls into question her ability to vigorously represent the class.
19 Again, while we have significant reservations about whether Murray can satisfy Rule
20 23(a)(4), we need not decide the issue because we conclude that plaintiffs do not satisfy
21 Rule 23(b).

22 **B. Rule 23(b), Fed. R. Civ. P.**

23 In addition to satisfying the prerequisites of Rule 23(a), plaintiffs must also establish
24 that the proposed class action fits within one or more of three categories of class actions
25 described in Rule 23(b). Rule 23(b)(1) permits a class action if prosecuting separate actions
26 would create a risk of (A) inconsistent or varying adjudications that would establish
27 incompatible standards of conduct for the party opposing the class; or (B) adjudications that
28

1 would, as a practical matter, be dispositive of the interests of those class members not joining
2 in the litigation.

3 Plaintiffs argue only generally that the requirements of Rule 23(b)(1) are met, simply
4 repeating the rule. Motion at 10. This is insufficient to establish their burden of proof and
5 accordingly we reject Rule 23(b)(1) as a basis for class certification.

6 Rule 23(b)(2) permits class certification where the party opposing the class has acted
7 on grounds generally applicable to the class, thereby making injunctive relief or declaratory
8 relief appropriate with respect to the class as a whole. Rule 23(b)(2) class actions can
9 include claims for monetary damages as long as such damages are not the “predominant”
10 relief sought, but instead are “secondary to the primary claim for injunctive or declaratory
11 relief.” Molski v. Gleich, 318 F.3d 937, 947 (9th Cir. 2003). We must look to the “specific
12 facts and circumstances of each case, focusing predominantly on the plaintiffs’ intent in
13 bringing the suit.” Dukes v. Wal-Mart, Inc., 509 F.3d 1168, 1186 (9th Cir. 2007).

14 Here, the predominant remedy sought is monetary damages. Plaintiffs seek not only
15 statutory damages, but damages for emotional distress and mental anguish, as well as
16 punitive and exemplary damages. Plaintiffs’ original complaint requested only monetary
17 damages. It was not until they sought class certification that they added claims for injunctive
18 and declaratory relief. Moreover, given that Principal terminated the email forwarding
19 program as soon as plaintiffs complained, and has thereafter committed not to resume the
20 program, the need for declaratory or injunctive relief is negligible at best. Under these facts
21 we cannot conclude that the monetary damages claim is secondary to the request for
22 injunctive relief. Therefore, Rule 23(b)(2) is inapplicable.

23 Finally, under Rule 23(b)(3), a class action is available where common questions of
24 law or fact “predominate over any questions affecting only individual members,” and the
25 class action device is “superior to other available methods for fairly and efficiently
26 adjudicating the controversy.” Both predominance and superiority must be established for
27 certification under Rule 23(b)(3).
28

1 The predominance requirement of Rule 23(b)(3) “tests whether proposed classes are
2 sufficiently cohesive to warrant adjudication by representation.” Amchem Prods, 521 U.S.
3 at 623, 117 S. Ct. at 2249. The proponent of a Rule 23(b)(3) class must show not only the
4 existence of common questions of law or fact, but must also show that the common questions
5 of law or fact *predominate* over any questions affecting only individual members. Rule
6 23(b)(3) involves a stricter standard than the typicality requirement of Rule 23(a)(3), which
7 addresses, as a threshold matter, whether Rule 23 certification has any applicability at all.
8 Id. at 623 n.18, 117 S. Ct. 2249 n.18. In contrast, Rule 23(b)(3) addresses whether
9 certification will have any practical utility. Only where questions common to the class
10 predominate over questions affecting individual members will the court achieve economies
11 of time, effort, and expenses contemplated by Rule 23. Rule 23(b)(3) (adv. comm. notes).

12 The Wiretap Act prohibits only the unauthorized interception of electronic
13 communications. Therefore, consent is a complete defense to such a claim. 18 U.S.C. §
14 2511(2)(d). The question of consent, either express or implied, is often a fact-intensive
15 inquiry and may vary with the circumstances of the parties. For example, plaintiffs
16 acknowledge that SEC regulations mandate that they provide Principal with copies of all
17 correspondence related to securities. Amended Complaint ¶ 22. Therefore, an issue arises
18 as to whether plaintiffs, as well as the putative class members, either expressly or impliedly
19 because of their knowledge of Principal’s policy, consented to the interception of the email,
20 or whether the representatives themselves may have forwarded copies of any particular email
21 to Principal. Accordingly, defendants’ liability under the Wiretap Act will require an
22 individualized showing of each class member’s knowledge and consent with respect to each
23 intercepted email.

24 Similarly, invasion of privacy claims require highly individualized determinations of
25 fact and law that make class certification under Rule 23(b)(3) inappropriate. Defendants’
26 liability as to each class member will vary based upon whether the substance of each email
27 was such that the representative was obligated under Principal’s policy to copy Principal on
28 the email correspondence, whether each class member had a reasonable expectation of

1 privacy in each intercepted email, and whether disclosure of the subject matter of each email
2 was confidential or highly personal such that its forwarding could be deemed highly
3 offensive to a reasonable person. Because such fact-intensive inquiries would require a
4 series of separate “mini-trials,” these claims are not appropriate for class certification under
5 Rule 23(b)(3).

6 The issue of damages is also highly individualized. Plaintiffs seek emotional distress
7 damages as to both the Wiretap Act and invasion of privacy claims. Individual hearings for
8 each class member would be required to quantify each class member’s emotional injuries.

9 Where the disparity among class members will likely present “significant questions,
10 not only of damages but of liability and defenses of liability . . . affecting the individuals in
11 different ways,” class certification is “ordinarily not appropriate.” Rule 23(b)(3) (adv.
12 comm. notes). Because of the highly individualized inquiry inherent in these claims,
13 defenses, and damages we conclude that little, if any, value as to efficiency would be gained
14 by certifying the putative class under Rule 23(b)(3). Because plaintiffs have failed to
15 establish that their putative class fits within Rule 23(b), we deny plaintiffs’ motion for class
16 certification (doc. 55).³

17 **III. Motion for Judgment on the Pleadings**

18 The Wiretap Act prohibits the intentional “interception” of “any wire, oral, or
19 electronic communication.” 18 U.S.C. § 2511(1)(a). It does not address access to electronic
20 communications that are in “electronic storage.” The Principal defendants argue in their
21 motion for judgment on the pleadings that plaintiffs have failed to state a valid claim under
22 the Wiretap Act because the intercepted email messages were in “electronic storage,” as
23 defined in 18 U.S.C. § 2510(17), and therefore were not subject to the Wiretap Act.
24

25
26 ³Because we deny plaintiffs’ motion for class certification, we also grant Fiserv’s
27 motion to dismiss. Plaintiffs admittedly have no claim against Fiserv and only sought to join
28 it by way of class certification. Plaintiffs have no standing to assert a claim against Fiserv
and its motion to dismiss is granted (doc. 43).

1 In Konop, the Ninth Circuit noted that the intersection of the Wiretap Act and the
2 Stored Communications Act “is a complex, often convoluted, area of the law, [and] the
3 existing statutory framework is ill-suited to address modern forms of communication.”
4 Konop, 302 F.3d at 874. The court held that an interception of electronic communications
5 is unlawful under the Wiretap Act only if it is “acquired during transmission, not while it is
6 in electronic storage.” Id. at 878. In other words, the interception must occur
7 “contemporaneous with transmission.” Id. No interception can occur, for purposes of
8 liability under the Wiretap Act, once the communication is in “electronic storage.” Id.

9 The Ninth Circuit noted that “[e]mail and other electronic communications are stored
10 at various junctures in various computers between the time the sender types the message and
11 the recipient reads it.” Id. at 879 n.6. The court recognized that because storage is a
12 necessary incident to the transmission of electronic communications, the Wiretap Act would
13 have “virtually no effect” on email interceptions. Id. The court concluded that Congress
14 intended this limitation given that it “defined ‘electronic storage’ as ‘any temporary,
15 intermediate storage of a wire or electronic communication incidental to the electronic
16 transmission thereof.’ ” Id. (quoting 18 U.S.C. § 2510(17)(a) (“Congress chose to afford
17 stored electronic communications less protection than other forms of communication.”)).

18 Relying on Konop, the Principal defendants argue that email interception can never
19 form the basis of a claim under the Wiretap Act, and that accordingly plaintiffs’ claims must
20 be dismissed. We decline to interpret Konop so broadly. At least one court has noted that,
21 even under the narrow reading adopted by the Ninth Circuit, certain email interceptions may
22 still fall within the Wiretap Act. While noting that “very few seizures of electronic
23 communications from computers will constitute ‘interceptions,’ ” United States v. Steiger,
24 318 F.3d 1039, 1050 (11th Cir. 2003), the court nevertheless concluded that “[t]here
25 [remains] a narrow window during which an E-mail interception may occur—the seconds
26 or mili-seconds before which a newly composed message is saved to any temporary location
27 following a send command.” Id. (citation and quotation omitted). For example, when an
28

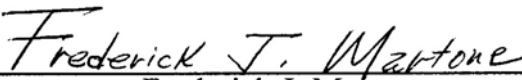
1 “automatic routing software is used [and] a duplicate of all of an employee’s messages are
2 automatically sent to the employee’s boss.” Id.

3 We are presented with no facts describing the process of email transmissions or
4 interceptions in this case. Plaintiffs have alleged that defendants “automatically forwarded
5 copies of all e-mails . . . at the time the messages were sent.” Amended Complaint ¶ 18.
6 There is no allegation that any email was ever in electronic storage. While we are skeptical
7 of the validity of plaintiffs’ claims given the Ninth Circuit’s narrow reading of the Wiretap
8 Act, we are not prepared at this early stage of the proceedings to conclude as a matter of law
9 that these email transmissions necessarily involved “electronic storage” so as to defeat
10 plaintiffs’ claims. Accordingly, the Principal defendants’ motion for judgment on the
11 pleadings is denied (doc. 78).

12 **IV. Conclusion**

13 **IT IS ORDERED DENYING** plaintiffs’ motion for class certification (doc. 55),
14 **GRANTING** Fiserv’s motion to dismiss (doc. 43), and **DENYING** the Principal defendants’
15 motion for judgment on the pleadings (doc. 78).

16 DATED this 6th day of November, 2008.

17
18
19 
20

 Frederick J. Martone
United States District Judge