

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

TIANA FRECHETTE, et al.,	:	
	:	
Plaintiffs,	:	Case No. 2:19-cv-4453
	:	
v.	:	Chief Judge Algenon L. Marbley
	:	
HEALTH RECOVERY SERVICES, INC.,	:	Magistrate Judge Jolson
	:	
Defendant.	:	

OPINION & ORDER

This matter is before the Court on Plaintiffs’ Motion for Class Certification. (ECF No. 60). This case involves a dispute between the parties arising from unauthorized third-party access (the “breach”) to Defendant’s computer storage systems, which contained Plaintiffs’ personal and medical information. (ECF No. 38 ¶ 1). For the following reasons, Plaintiffs’ Motion is **DENIED**.

I. BACKGROUND

A. Factual Background

Defendant Health Recovery Services (“HRS”) is a non-profit that provides services to those suffering from mental illness or substance abuse issues, including Plaintiffs and their putative class. (ECF No. 38 ¶¶ 2–5). Plaintiff Tiana Frechette was a patient of HRS at the time of the breach. (*Id.* ¶ 2). Minors J.F. and C.F., represented in this lawsuit by their mother and guardian, Jane Doe, were also patients of HRS at the time of breach. (*Id.* ¶¶ 3–4).

On February 5, 2019, HRS discovered that an unauthorized IP address remotely had accessed its computer network since November 14, 2018. (*Id.* ¶¶ 1, 30). On the network, HRS stored the personal and medical information of its clients, including Plaintiffs and the class they

seek to represent. (*Id.* ¶¶ 1, 6). HRS sent notice of this data breach on April 4, 2019, two months after it was discovered. (*Id.* ¶ 30). Specifically, HRS sent out 20,845 data breach notification letters containing the following language:

On March 15, 2019, our third-party forensic expert determined that this unauthorized access to our network occurred from November 14, 2018 until its discovery on February 5, 2019. While the forensic expert has indicated to us that they do not believe that any of HRS' patient information was ever in fact accessed, they were unable to definitively rule out that possibility.

While our investigation is ongoing, we have no evidence that the unknown third party accessed or acquired protected health information stored on the HRS server. Nevertheless, we confirmed this server stored files and a software application which may have contained your (your minor's) name, address, phone number, (and) date of birth, (and Social Security number). If you (your minor) were a patient of HRS after 2014, the information stored in the files and software application also included your (your minor's) medical information, health insurance information, diagnosis, and treatment information. Out of an abundance of caution, we are providing notice of this incident to you given we cannot rule out unauthorized access to this information occurred.

(ECF No. 60-1 at 4–5; ECF No. 62-3 at 1).

According to HRS, not all of the 20,845 people to whom it sent the data breach notification letter (the “notification letters”) were patients. (ECF No. 66 at 14). As HRS's Chief Financial Officer Regina Smith stated in her deposition, that number “could have included people that [HRS had] never seen, never talked to, had no record, never patients.” (Regina Smith Deposition, ECF No. 62-2 at 25:23–26:1).

Plaintiffs allege that HRS failed “to maintain reasonable and adequate procedures to protect and secure the Personal Information,” “to timely discover the unauthorized access,” and “to provide Plaintiffs and the Data Breach Class members with timely information regarding the unauthorized access.” (ECF No. 28 ¶ 33). Plaintiffs state that their personal and medical information was “compromised,” “misappropriated,” “access[ed],” and “stolen” through the breach. (*Id.* ¶¶ 30, 31, 39, 40). HRS's alleged failures “resulted in financial injuries to Plaintiffs

and [the class] and has placed [them] at grave risk of identity theft and other possible fraud and abuse.” (*Id.* ¶ 33). Those alleged injuries stem from invasion of privacy; out-of-pocket costs for protective and reactive measures such as credit monitoring; and mental and emotional distress from having highly sensitive health information disclosed. (*Id.* ¶¶ 40–46, 49–52). According to HRS, there is no evidence that anyone’s information was accessed by the interloper. (ECF No. 66 at 4). Instead, it argues, the unauthorized access was only to a dummy server containing “pseudo-client” information on it to test its new system. (Regina Smith Declaration, ECF No. 66-1 ¶¶ 16–17; ECF No. 66 at 1). HRS represents that it sent letters to every individual with information in HRS’s entire computer system notifying them of the data security incident merely out of an abundance of caution. (Smith Declaration ¶ 18; ECF No. 66 at 4).

B. Procedural Background

On October 6, 2019, Plaintiffs filed their original Complaint. (ECF No. 1). It was superseded on January 6, 2020, by Plaintiffs’ First Amended Complaint (ECF No. 6), which HRS moved to dismiss (ECF No. 9). This Court issued an Opinion, granting dismissal on six of ten counts in the First Amended Complaint for failure to state a claim—but preserving four counts for breach of implied contract, unjust enrichment, and willful and negligent violations of the Fair Credit Reporting Act (“FCRA”). (ECF No. 23). Those are the only counts alleged in the Second Amended Complaint, which Plaintiffs filed on February 17, 2021. (ECF No. 38). This is the operative Complaint in this case.

The factual allegations largely track those in the First Amended Complaint. This Court issued another Opinion, granting dismissal on two of the four counts in the Second Amended Complaint for failure to state a claim—this time preserving only two counts for breach of implied contract and unjust enrichment. (ECF No. 44).

On January 9, 2023, Plaintiffs filed their Motion for Class Certification. (ECF No. 60). In their Motion, Plaintiffs seek an order from this Court to allow the case to proceed as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure. Specifically, Plaintiffs argue that this case satisfies the requirements of Rule 23(a) and should be certified under Rule 23(b)(3). Plaintiffs request the following class definition:

All HRS patients whose personal information or medical information was compromised as a result of the data breach first disclosed by Defendant Health Recovery Services, Inc. on April 5, 2019.

(ECF No. 60-1 at 6).

Plaintiffs' Motion is ripe for this Court's consideration.

II. STANDARD OF REVIEW

A plaintiff seeking class certification bears the burden of establishing compliance with all four requirements of Rule 23(a), referred to by the shorthand of “(1) numerosity, (2) commonality, (3) typicality, and (4) adequacy.” Fed. R. Civ. P. 23(a); *Alkire v. Irving*, 330 F.3d 802, 820 (6th Cir. 2003). Additionally, even though Rule 23 has no express ascertainability requirement, the Sixth Circuit has held that it is implicitly required for class certification. *Cole v. City of Memphis*, 839 F.3d 530, 541 (6th Cir. 2016); *see also Carrera v. Bayer Corp.*, 727 F.3d 300 (3d Cir. 2013). Ascertainability is met where the “class description [is] sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual is a member.” *Cole*, 839 F.3d at 541 (quoting *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 538 (6th Cir. 2012)).

In ruling on a motion for class certification, a district court should not consider the merits of the plaintiffs' claims but may consider evidence outside of the pleadings to determine whether the prerequisites of Rule 23 are met. *Eisen v. Carlisle & Jacquelin*, 417 U.S. 156, 177 (1974). That said, on occasion, “it may be necessary for the court to probe behind the pleadings before

coming to rest on the certification question,” *see Gen. Tele. Co. of Southwest v. Falcon*, 457 U.S. 147, 160 (1982), and “rigorous analysis” may involve some overlap between the proof necessary for class certification and the proof required to establish the merits of the plaintiffs’ underlying claims.” *Wal-Mart Store, Inc. v. Dukes*, 564 U.S. 338, 350–51 (2011). A court, however, should not conduct free-ranging merits inquiries at this stage, but may consider the merits only to the extent “they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied.” *Amgen Inc. v. Conn. Retirement Plans & Trust Funds*, 568 U.S. 455, 466 (2013).

In addition, under Rule 23(b)(3), class certification is appropriate if “the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3) (referred to by the shorthand of “predominance and superiority”).

III. LAW AND ANALYSIS

A. CLASS CERTIFICATION

1. Class Certification – Rule 23(a)

A plaintiff seeking class certification bears the burden of establishing compliance with all four requirements of Rule 23(a): “(1) numerosity, (2) commonality, (3) typicality, and (4) adequacy.” Fed. R. Civ. P. 23(a). Further, while Rule 23(a) does not contain an express requirement of ascertainability, the Sixth Circuit has held it to be an “implicit requirement” of class certification. *Cole*, 839 F.3d at 541.

Because Plaintiffs fail to satisfy either the numerosity or ascertainability requirements under Rule 23(a), this Court finds it unnecessary to consider whether the proposed class satisfies the other requirements of Rule 23(a) or of Rule 23(b)(3).

a. Numerosity

Plaintiffs argue that it is evident in this case that the requirement of numerosity has been satisfied because HRS itself acknowledged that it sent the notification letters to 20,845 people. Although Plaintiffs acknowledge that Regina Smith explained that not all of the 20,845 recipients were HRS patients, they argue that her testimony confirms that HRS has the *ability* to confirm which recipients were patients. Plaintiffs contend that the proposed class is therefore both sufficiently numerous and sufficiently defined. According to Plaintiffs, HRS cannot credibly suggest that less than 40 of the recipients who received data breach notices were patients.

HRS responds that Plaintiffs lack any evidence that the number of putative class members satisfies numerosity. HRS emphasizes that neither the total number of letter recipients nor the number of recipients who were patients are probative of the number of individuals who fit the class definition. Instead, HRS contends, the proposed class definition only includes HRS patients whose personal or medical information was *compromised*. HRS argues that Plaintiffs have offered no evidence or method to ascertain the number of HRS patients whose information was compromised and would thereby fit the proposed class definition.

Federal Rule of Civil Procedure 23(a)(1) requires that “the class [be] so numerous that joinder of all members is impracticable.” Fed. R. Civ. P. 23(a)(1). To satisfy numerosity, “impracticability of joinder must be positively shown, and cannot be speculative.” *Golden v. City of Columbus*, 404 F.3d 950, 966 (6th Cir. 2005). The Sixth Circuit has found even classes of 35 to be sufficient to meet this requirement. *Young*, 693 F.3d at 542 (citing *In re Am. Med. Sys., Inc.*, 75 F.3d 1069, 1076 (6th Cir. 1996)).

Plaintiffs have introduced no evidence that would permit this Court to find that numerosity is met in this case. In essence, Plaintiffs ask this Court to conclude that, because the total number of letter recipients is 20,845, the number of recipients who (1) are patients and (2) had their data compromised in the data breach *must* be great enough that joinder is impracticable. Even this is a generous read of Plaintiffs' argument—Plaintiffs only argue that numerosity is satisfied because a significant number of the letter recipients are likely to be patients. Plaintiffs fail to offer argument or evidence relating to the number of HRS patients whose data was compromised. It appears to this Court that Plaintiffs either: (1) assume that an individual only received a notification letter if his or her data was breached; or (2) forget that their own proposed class definition requires that eligible members must not only be HRS patients but must also have had their information compromised. Either way, Plaintiffs have erred.

Plaintiffs also confusingly argue that HRS fails to show that Plaintiffs' proposed class is insufficiently numerous because *HRS* cannot prove that less than 40 of the letter recipients were patients. But it is *Plaintiffs'* burden to show that numerosity is met. *In re Am. Med. Sys., Inc.*, 75 F.3d at 1079 (explaining that “[t]he party seeking the class certification bears the burden of proof.”). Even if this Court can assume that a sufficient number of the letter recipients are HRS patients, it cannot determine, based on mere speculation, that a sufficient number of the patients had their data compromised. Given this state of affairs, Plaintiffs' Motion is **DENIED** at the outset for failing to satisfy numerosity. *See id.* (instructing that all four prerequisites under Rule 23(a) must be met to warrant class certification). For the sake of thoroughness, however, this Court will explain why dismissal is also warranted on the additional and independent basis that Plaintiffs fail to show that the proposed class is ascertainable.

b. Ascertainability

Plaintiffs argue that class membership is readily ascertainable because all that must be shown is that a letter recipient was an HRS patient whose personal and medical information was compromised in the data breach. Plaintiffs analogize this case to *Geary v. Green Tree Servicing, LLC*, No. 2:14-CV-00522, 2017 WL 2608691 (S.D. Ohio June 16, 2017) (Marbley, J.). According to Plaintiffs, this Court in *Geary* found a proposed class definition appropriate although only six of the eleven versions of the letters that the defendants sent to 31,000 individuals gave rise to viable claims under the Fair Debt Collection Practices Act (“FDCPA”). There, Plaintiffs contend, this Court was not moved by the defendant’s argument that the class was not ascertainable because it would be forced to conduct an intensive manual review to determine which of the letter recipients qualified for class membership. Plaintiffs here argue that this case is similar in that the ascertainability of Plaintiffs’ proposed class is not undermined by the mere fact that HRS may be forced to conduct a manual search of 20,845 files to determine which of the letter recipients were HRS patients.

HRS responds that Plaintiffs’ ascertainability argument rests upon the flawed premise that every HRS patient who received the notification letter qualifies for class membership. According to HRS, Plaintiffs’ proposed class is not ascertainable for the following reasons: (1) Plaintiffs do not suggest any method to identify the people who received the 20,845 letters in the first place; (2) it is not administratively feasible to determine which recipients of the notification letters were patients of HRS; and (3) Plaintiffs do not even attempt to determine or suggest a method to determine which patients had their information compromised, an important omission given that HRS has no evidence that anyone’s personal information was ever breached.

The determination that a class is ascertainable “requires only the existence of objective criteria upon which class membership is based.” *McNamee v. Nationstar Mortg., LLC*, No. 2:14-CV-1948, 2018 WL 1557244, at *4 (S.D. Ohio Mar. 30, 2018) (Marbley, J.) (citing *Young*, 693 F.3d at 538–39). A previous ruling by this Court provides an instructive example:

To illustrate the difference between ascertainability and susceptibility to individualized inquiry, consider, for example, a class defined as “all people in the State of Ohio who currently have a pint of mint chocolate chip ice cream in the freezer.” Such a class is certainly ascertainable: every Ohioan either is a class member, or she is not. The inquiry is an objective one.

Id. In essence, the ascertainability requirement necessitates “a class description [that is] sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual is a member.” *Cole*, 839 F.3d at 541.

In *Geary*, the plaintiffs were Ohio residents who sued a loan servicer for sending to each of 31,000 debtors-in-default any one of eleven types of letters, six of which allegedly violated the FDCPA. 2017 WL 2608691, at *1. There, this Court found that class membership was ascertainable because it was determinable by two objective factors: (1) whether the loan servicer sent one of six letters to the plaintiffs; and (2) whether the loan servicer did so within a certain time frame. *Id.* at *12. As this Court there reasoned, ascertainability is not defeated merely because a class would require “substantial review” to determine its members. *See id.* (citing *Rikos v. Procter & Gamble Co.*, 799 F.3d 497, 526 (6th Cir. 2015)). Therefore, this Court found, class membership remained ascertainable because the loan servicer possessed the ability to find that information. *Id.* This Court deemed irrelevant the loan servicer’s protests that the process of ascertaining class membership would require it to conduct a manual review of 31,000 files. *Id.* This Court’s ruling also dismissed the loan servicer’s concerns about the additional difficulty of confirming whether each letter recipient took out a consumer loan such that he or she was

entitled to relief under the relevant statute. *Id.* This Court there reasoned that, if the loan servicer’s search of its own records failed to answer whether a given letter recipient received a consumer loan, his or her eligibility could be confirmed by asking the “single question” of whether he or she received a consumer loan. *Id.*

This case is quite different. As an initial point, this Court does not consider ascertainability to be defeated in this case merely because HRS must engage in substantial review to determine which of the 20,845 letter recipients were patients. *See Young*, 693 F.3d at 539–40 (finding that administrative feasibility is not undermined merely because the defendants would be required to review manually a voluminous number of individual files to ascertain class membership). After all, Plaintiffs present deposition testimony from Regina Smith indicating that it is possible for HRS to determine the number of patients who received the letters. (Smith Deposition at 38:16–39:16). But it is not enough for ascertaining class membership merely to identify the HRS patients.

The problem here—which differentiates this case from *Geary*—is that it is virtually impossible to determine whether a letter recipient’s data was: (1) compromised at all; and (2) comprised specifically in the data breach at issue. This is true for two reasons. First, HRS has offered evidence that it has been unable to identify anyone whose information was compromised, to which Plaintiffs have offered no counterevidence. (ECF No. 66-2; ECF No. 73-1 at 7; Smith Declaration ¶ 24). So, HRS is likely unable to help ascertain the class members. Second, it is incredibly difficult, if not virtually impossible, for a letter recipient to confirm that his or her data was compromised in *this* breach that occurred more than four years ago.

In *Geary*, the determination that a putative class member received one of the six letters at issue would, in most cases, render him or her eligible to join the class. 2017 WL 2608691, at

*12. Only a “small number” of the recipients in that case received “non-consumer loans” such that they would not be eligible for the class even if they received one of the six letters. *Id.* If the loan servicer could not conclusively determine whether a letter recipient received the type of loan that would entitle him or her to join the class, the recipient could be simply asked what type of loan he or she received. *Id.*

In this case, HRS presents evidence that it has been yet unable to find that any individual’s data was compromised in the breach. (ECF No. 66-2; ECF No. 73-1 at 7; Smith Declaration ¶ 24). Not even the named Plaintiffs have indicated that they *know* their data was compromised or have identified any post-breach incident or evidence justifying their apparent beliefs that their data was compromised. (Tiana Frechette Deposition, ECF No. 66-4 at 43:5-43:15; C.F. Deposition, ECF No. 66-5 at 19:19–20:1, 22:4–22:8; J.F. Deposition, ECF No. 66-6 at 19:10–20:6, 23:2–23:6). Unlike in *Geary*, this Court has no way to determine whether most, some, or none of the patients who received a notification letter suffered an injury qualifying them for class membership. This Court cannot even confirm that the *named Plaintiffs* qualify for the class. And here, unlike in *Geary*, HRS has presented evidence that it could not (or has at least been unable to) identify the putative class members through a search of its records. Further, unlike *Geary*, the difficulty of tracing compromised information to a particular breach undermines any party’s ability in this case simply to ask a letter recipient to confirm whether he or she suffered an injury (having his or her data comprised in the HRS breach) qualifying him or her for class membership. At best, determining whether a letter recipient is qualified for class membership in this case would require an incredibly fact-intensive process. At worst, determining whether a letter recipient is qualified is impossible. In either event, determining whether a letter recipient is qualified is not feasible administratively.

The Sixth Circuit affirmed the denial of class certification in a Telephone Consumer Protection Act (“TCPA”) case on ascertainability grounds for a similar reason: there existed no administratively feasible method to identify putative class members in the absence of records from the defendant company showing which consumers were sent the problematic junk faxes, and there was no realistic expectation that the putative class members could reliably recall having received the junk faxes that were allegedly sent seven years prior. *Sandusky Wellness Ctr., LLC v. ASD Specialty Healthcare, Inc.*, 863 F.3d 460, 471–72 (6th Cir. 2017), *as corrected on denial of reh'g en banc* (Sept. 1, 2017).

In short, although Plaintiffs’ proposed class definition is certainly objective, it is not administratively feasible to determine class membership. On this record, there is no evidence that either HRS or Plaintiffs would be able to identify the putative class members. For those reasons, Plaintiffs’ proposed class definition fails the ascertainability prong. Plaintiffs’ Motion is thus due dismissal on this second, independent basis.


Because “[t]o be certified, a class must satisfy all four of the Rule 23(a) prerequisites,” *Young*, 693 F.3d at 537, this Court does not consider whether Plaintiffs satisfy the other Rule 23(a) requirements or those of Rule 23(b)(3). It is sufficient for denial of class certification that Plaintiffs have failed to satisfy these Rule 23(a) prerequisites.

IV. CONCLUSION

For the foregoing reasons, this Court **DENIES** Plaintiffs’ Motion for Class Certification. (ECF No. 60).

IT IS SO ORDERED.

DATED: August 29, 2023


ALGENON L. MARBLEY
CHIEF UNITED STATES DISTRICT JUDGE