

Greco v Syracuse ASC, LLC
2022 NY Slip Op 32104(U)
June 28, 2022
Supreme Court, Onondaga County
Docket Number: Index No. 000105/2022
Judge: Donald A. Greenwood
Cases posted with a "30000" identifier, i.e., 2013 NY Slip Op <u>30001</u> (U), are republished from various New York State and local government sources, including the New York State Unified Court System's eCourts Service.
This opinion is uncorrected and not selected for official publication.

**At a Motion Term of the Supreme
Court of the State of New York,
held in and for the County of
Onondaga on June 21, 2022.**

**PRESENT: HON. DONALD A. GREENWOOD
Supreme Court Justice**

**STATE OF NEW YORK
SUPREME COURT COUNTY OF ONONDAGA**

**GRETCHEN GRECO, individually and on behalf of
All others similarly situated,**

Plaintiff,

v.

**SYRACUSE ASC, LLC d/b/a SPECIALTY SURGERY
CENTER OF CENTRAL NEW YORK,**

Defendant.

**DECISION AND ORDER
ON MOTION**

Index No.: 000105/2022

**APPEARANCES: TODD SETH GARBER, ESQ., of FINKELSTEIN, BLANKINSHIP, FREI-
PEARSON & GARBER, LLP
For Plaintiff**

**DANIEL M BRAUDE, ESQ., OF WILSON ELSER MOSKOWITZ
EDELMAN & DICKER LLP
For Defendant**

The defendant Syracuse ASC d/b/a Special Surgery Center of CNY (SSC) has made a pre-answer motion to dismiss the class action complaint in this matter. Plaintiff, a former patient of defendant, alleges that SSC failed to safeguard and protect her confidential information as well as other that of class members, including private health information (PHI) protected under HIPAA and sensitive personal information such as names, dates of birth, and Social Security numbers. It is alleged that a data breach occurred on March 31, 2021, where cybercriminals were able to gain access to approximately 24,891 class members' sensitive information. The complaint contains the

following causes of action: negligence in the handling of plaintiff's and the class's sensitive information, breach of express contract, breach of implied contract, violation of General Business Law sections 899-AA and 349, invasion of privacy, and an injunction pursuant to CPLR Article 63. At the same time, defendant filed a second motion seeking to strike plaintiff's class allegations.

Defendant's Pre-Answer Motion to Dismiss

The motion to dismiss is premised on two grounds. Defendant first argues that plaintiff lacks standing because she did not sustain actual concrete injury fairly traceable to SSC, cannot link her alleged injuries to SSC and any alleged increased risk of future harm to her is purely hypothetical. The second basis is that plaintiff's clauses of action are inadequately pled.

A. Standing

Defendant first contends that the complaint is subject to dismissal at this early stage as plaintiff lacks standing. Standing is a threshold issue and plaintiff may not proceed without it. Whether a person seeking relief is a proper party to request an adjudication is an aspect of justiciability which, when challenged, must be considered at the beginning of litigation. *See, Society of Plastics Indus. v. County of Suffolk*, 77 NY2d 761 (1991). In order to have standing to sue, a plaintiff must allege the existence of an injury in fact that ensures that she has some concrete interest and prosecuting the action. *See, Society of Plastics, supra*. A class representative must have individual standing, which means that the representative must have an individual injury which is cognizable at law. *See, Raske v. Next Mgmt, LLC*, 40 Misc.3d 1240(A) (NY Co. 2013). The test for determining a litigant's standing it is as follows: plaintiff must allege injury in fact that falls within his or her zone of interest and have a concrete interest in prosecuting the action, which casts the dispute in a form traditionally capable of judicial resolution. *See, Silver v. Pataki*, 96NY2d 532 (2001).

Defendant contends that no facts are offered to support the potential misuse of information and that general allegations that individuals whose confidential information has been exposed during a data breach are more likely to experience future identity theft are insufficient and conclusory, not raising plaintiff's claims that there are at imminent risks of future harm above a speculative level. *See, In re Practicefirst Data Breach Litig.*, 2022 US Dist. LEXIS 19272. Defendant further contends that plaintiff does not allege any unreimbursed charges or out of pocket expenses, as plaintiff must allege that she was monetarily harmed by the defendant's actions. *See, Manning v. Pioneer Sav. Bank*, 56 Misc3d 796 (Rensselaer Co. 2016). Likewise, defendant argues that plaintiff lacks standing because her alleged increased risk of future harm is insufficient to confer standing. *See, Hammond v. Bank of NY Mellon Corp.*, 2010 WL 2643307 (SDNY 2010). Defendant further asserts that plaintiff cannot use monitoring to manufacture an injury, particularly when monitoring one's accounts for fraudulent activity is something that many individuals do regardless of whether they have been informed if their information is at risk. *See, In Re Brinker Data Incident Litigation*, 2019 WL 3502993 (MD Fla. 2019). It is further argued that alleged diminished value of PHI is insufficient to confer standing.

The defendant is not entitled to dismissal on this ground. First, it is important to note that issue has not been joined at this early stage and there has been no discovery. Defendant has not served a demand for a bill of particulars to allow plaintiff to amplify her pleadings, nor has it yet sought any other type of discovery. Moreover, plaintiff has established at this early stage that she has standing to bring her claims as the law allows recovery by certain tort victims even if their harms may be difficult to prove or measure. *See, Spokeo, Inc. v. Robins*, 578 US 330 (2016). Certain intangible harms can be concrete and have been recognized as providing a basis for lawsuit, including reputational harms, disclosure of private information and intrusion upon seclusion. *See,*

TransUnion LLC v. Ramirez, 141 SCT 2190(2021). In addition, while standing requires a concrete injury, this does not mean that the risk of harm cannot satisfy that requirement. *See, id.* Plaintiff has alleged that her sensitive and private information was taken by cybercriminals and she may demonstrate a substantial risk of future harm sufficiently imminent to confer standing by virtue of a data breach. *See, Remijas v. Neiman Marcus Group*, 794 F3d 688 (7th Cir. 2015); *see also, Krottner v. Starbucks Corporation*, 628 F3d 1139 (9th Cir. 2010). While defendant argues that this attack is analogous to a ransomware attack, (*citing, Practicefirst, supra*), where the court found that the accessed private information was permanently deleted after the ransom was paid, there has been no assertion here that the compromised sensitive information was deleted. In addition, in data breach cases where hackers, who intentionally target and steal sensitive information, provide a near certainty of impending injury to the victims because the primary incentive for hackers is to steal information to use it to commit identity theft and fraud. *See, Lewert v. PF Chang's China Bistro*, 819 F3d 963 (7th Cir. 2016). Courts have found that victims of targeted data breaches have standing based on an imminent risk of threat to seek redress from a defendant negligence, notably including where the stolen data has not yet been used. *See, Galaria v. Nationwide Mutual Insurance Co.*, 663 F App 384 (6th Cir. 2016); *see also, Lewert, supra*. Nor has defendant established that the diminution in value of plaintiff's sensitive information is insufficient to establish standing. The loss of value in one's sensitive information has been found to be a cognizable injury and allegations of diminution in value of a plaintiff's personal information have been found to be sufficient to show contract damages for pleading purposes. *See, In re Facebook Privacy Litig*, 572 F App 494 (9th Cir. 2014); *see also, Swenson v. Google, Inc.*, 2015 WL 1503429 at 2 (ND Cal. 2015). Based upon the foregoing, this motion is denied.

B. Dismissal for Failure to State A Cause of Action

Defendant is equally unsuccessful in its alternative motion for dismissal for failure to state a cause of action. *See, CPLR § 3211(a)(7)*. Such a motion must be denied if from the pleadings' four corners the factual allegations are discerned which taken together manifest any cause of action that is cognizable at law. *See, Shanley v. Welch*, 6AD3d 1065 (4th Dept. 2004). The criterion is whether the proponent of the pleading has a cause of action, not whether she has stated one. *See, Gerrish v. State University of New York at Buffalo*, 129 AD3d 1611 (4th Dept. 2015). A plaintiff's complaint is to be afforded a liberal construction, the facts alleged therein are accepted as true and plaintiff is to be afforded every possible inference in order to determine whether the facts alleged in the complaint fit within any cognizable legal theory. *See, White v. Diocese of Buffalo*, 138 AD3d 1470 (4th Dept. 2016). Given those requirements, the defendant is not entitled to the relief sought.

With respect to the first cause of action for negligence, defendant argues that plaintiff did not allege an injury that was proximately caused by its actions and that the negligence claim is barred by the economic loss doctrine, as plaintiff is barred from recovering purely economic loss in a negligence action. *See, Shiavone Constr. Co v. Elgood Mayo Corp.*, 56 NY2d 667 (1982). This is incorrect. The economic loss rule should not be used outside of the product liability context and that is a duty-based analysis that should be instead applied. *See, Travelers Casualty & Surety Co. v. Dormitory Authority of State of NY*, 734 F Supp 2d 368 (SDNY 2010). Courts have explicitly rejected attempts to expand this ruling beyond the product liability context. *See, 532 Madison Avenue Gourmet Foods, Inc. v. Finlandia Center, Inc.*, 96 NY2d 280 (2001). In addition, courts have rejected the application of the economic loss doctrine in in the data breach context. *See, Sackin v. TransPerfect Glob., Inc.*, 278 FSupp 3d 739 (SDNY 2017); *see also, Wallace v. Health Quest Sys. Inc.*, 2021 WL 1109727 (SDNY 2021). Therefore, the economic loss rule does not bar a

negligence claim where a duty arises independent of contract. *See, Potter v. Grage*, 19 NYS2d 384 (4th Dept. 2015).

With respect to the second cause of action, defendant contends that plaintiff fails to allege a cognizable claim for breach of an express contract. To successfully plead a breach of contract claim, plaintiff must establish the existence of a contract, the performance pursuant to the contract, defendant's breach and resulting damages. *See, Abdale v. Northshore Long Island Jewish Health Sys.*, 49 Misc3d 1039. Defendant, though counsel who has no personal knowledge, relies on the factual argument that SSC did not violate the terms of its privacy policy as alleged. It further claims that the policy did not guarantee that PHI stored in its system would never be compromised or exposed in a data breach as any such guarantee would be unrealistic and unattainable. It further contends that no consideration was paid to it for data security and plaintiff does not allege that she paid SSC a specific sum. Absent allegations of additional consideration for this purported promise, there is no valid contract formed as respect to the provision of data security. *See, Practicefirst, supra*. It asserts the factual claim, again without support, that there were no cognizable damages and only a perceived risk of future harm is insufficient. *See, Kenford Co. v. County of Erie*, 67 NY2d 257 (1986). Plaintiff, however, has alleged the sufficient elements: the existence of an agreement, adequate performance by plaintiff, breach of the contract by defendant and damages. *See, Eternity Global Master Fund v. Morgan Guar. Trust Co. of NY*, 375 F3d 168 (2d Cir. 2004). Plaintiff points to the defendant's policy language that defendant will "maintain the privacy and security of your protected health information" and "will let you know promptly if a breach occurs that may have compromised the privacy or security of your information." The privacy notice continues, listing specific limited circumstances for which defendant will disclose sensitive information, including providing class members with treatment, billing, medical research and

responding to government request, none of which apply to the data breach. Defendant further contracted that “we will not use or share your information other than as described here unless you tell us we can in writing.” Although defendant claims that these statements do not commit it to any particular level of data security and protection, the language plainly states that it has suitable safeguards in place and complied with data protection law and the data would not be disclosed without the plaintiff’s knowledge. These are specific representations. In addition, the courts should hold parties to their bargain and the definiteness doctrine is a doctrine of last resort. *See, Cappelli Enters., Inc. v. F&J Cont’l Food Corp.*, 792 NYS2d 553 (2d Dept. 2005). Courts are reluctant to find contract terms insufficiently definite because of the definiteness doctrine is applied with a heavy hand, it may defeat the reasonable expectations of the parties entering into the contract. *See, Cobble Hill Nursing Home, Inc. v. Henry & Warren Corp.*, 548 NE2d 308 (1989). In addition, even if the level of data security promise was construed as ambiguous, plaintiff’s breach of contract claim still survives because a claim which is predicated on a materially ambiguous contract term is not dismissible on the pleadings. *See, Eternity Global Master Fund Ltd.*, 375 F3d 168 (2d Cir. 2004).

Defendant makes an analogous argument concerning the third cause of action for breach of implied contract. This requires the same element as an express contract: consideration, mutual assent, legal capacity and legal subject matter. *See, Maas v. Cornell University*, 94Y2d 87 (1999). Like an express contract, an implied in fact contract requires a meeting of the minds between the parties as to the terms and conditions of the agreement; a contract implied in fact may result as an inference from the facts and circumstances of the case and is derived from the presumed intention of the parties as indicated by their conduct. *See, id.* Therefore, the terms of an implied contract turns on the conduct of the parties. *See, Beth Israel Medical Center v. Horizon Blue Cross and*

Blue Shield of NJ, Inc., 448 F3d 573 (2d Cir. 2006). Plaintiff is not required to plead the exact terms of an implied contract to survive a motion to dismiss. *See, Wallace, supra*. An implied contract is naturally formed where a person discloses sensitive information to receive a benefit, with the expectation that such information will be protected. *See, Sackin, supra*. The presumed intention of the parties is demonstrated by the existence and content of defendant's privacy notice, which can only be read as a promise by defendant that it intended to securely store and safeguard the sensitive information; this is sufficient at the pleading stage. *See, International Technicians Marketing v. Verint Sys.*, 157 FSupp 3d 352 (SDNY 2016). Moreover, the existence of an implied contract will ordinarily be a question of fact as it involves the assessment of the parties conduct and the extent to which such contract demonstrates a meeting of the minds. *See, Monahan v. Lewis*, 858 NYS2d 812 (2d Dept. 2008).

Defendant seeks dismissal of the fourth cause of action for violation of General Business Law section 899-AA, arguing that the New York Legislature has not provided a private right of action. *See, Abdale, supra*. It argues that plaintiff alleges that she was not notified of the incident in the most expedient time possible, but the statute does not set forth a strict deadline for notification, because the legislature recognized the timing may vary based on the facts and circumstances of each situation. The statute requires that "any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security system ... in the most expedient time possible and without unreasonable delay." *GBL, 899-AA*. Based upon the documents relied upon by defendant, it is clear that it failed to provide notice for more than six months. While a private action is not expressly authorized in the statute, courts decide whether a statute fairly implies a private cause of action by analyzing three factors: whether the plaintiff is one of the class for whose particular benefit the statute was enacted,

whether recognition of a private right of action would promote the legislative purpose and whether creation of such a right would be consistent with the legislative scheme. *See, Sackin, supra*. Even where the legislature has delegated administrative enforcement of a statute, courts have found that a private right of action, and addition to administrative enforcement, is fully consistent with a legislative scheme and may therefore be implied. *See, Maimonides Med. Ctr v. First United Amer. Life Ins. Co.*, 981 NYS2d 739 (2d Dept. 2014); *see also, Gerel Corp. v. Prime Eastside Holdings, LLC*, 783 NYS2d 355 (1st Dept. 2004). Again, defendant is not entitled to dismissal at this early stage.

With respect to the fifth cause of action for violation of General Business Law section 349, defendant claims that plaintiff cannot show the defendant engaged in a consumer-oriented act or practice that was “deceptive or misleading in a material way and that the plaintiff had been injured by reason therefor.” *Abdale, supra*. It concedes that plaintiff alleges the violation by arguing that defendant failed to enact adequate privacy and security measures, failed to take proper action following known security risks knowingly, by deceptively misrepresenting that it would maintain adequate data privacy and by failing to disclose the breach in a timely manner. Defendant argues that the only basis for the purported misrepresentations are contained in the privacy policy, but a written privacy policy that does not expressly guarantee the protection of personal confidential information does not constitute a misrepresentation under section 349. *See, Abdale, supra*. Plaintiff has sufficiently alleged that the defendant engaged in consumer-oriented conduct that is materially misleading and that plaintiff suffered injury as a result of that deceptive act or practice. *See, Orlander v. Staples, Inc.*, 803 F3d 289 (2d Cir. 2015). A plaintiff bringing a claim under this section must simply raise a reasonable inference of causation rather than demonstrating reliance. *See, Stutman v. Chemical Bank*, 731 NE2d 608 (2000). At this stage, plaintiff has sufficiently

alleged that she was harmed by defendant's misrepresentations and omissions and a section 349 claim has been properly stated. *See, In re Anthem, supra; see also, In re Experian*, 2016 WL 7973595 at 4; *see also, In re Zapp's.com, Inc.*, 2013 WL 4830497. Moreover, whether a representation is misleading is a question of fact and inappropriate for a motion to dismiss. *See, Goldemberg v. Johnson & Johnson Consumer Cos.*, 8 FSupp 3d 467 (SDNY 2014).

With respect to the sixth cause of action it is alleged that plaintiff has failed to allege a cognizable claim for invasion of privacy by intrusion. Plaintiff relies on the Restatement (Second) of Torts, which provides that one who intentionally intrudes upon the solitude or seclusion of another, his private affairs or concerns is subject to liability to the other for the invasion of his privacy if the intrusion would be highly offensive to a reasonable person. *See, § 652B*. Courts do not recognize a claim under this section and the right to privacy is governed exclusively by sections 50 and 51 of the Civil Rights Law and there is no common law of privacy. *See, Howell v. New York Post*, 81 NY2d 115 (1993). However, invasion and loss of privacy arising out of tracking and disclosure of a user's online behavior has been found to be sufficient. *See, Gourley v. Google, Inc.*, 137 SCt 36 (2016).

Finally, with respect to defendant's motion to dismiss the injunctive relief sought, plaintiff has alleged that her sensitive information remains in defendant's possession and may be subject to further breaches so long as defendant fails to undertake appropriate and adequate measures to protect the information. The risk of future damage from her personal information being in defendant's inadequately secured system, and the injunctive relief that seeks to cure this risk, fits squarely within the requirements and remedies provided by law. *See, In re Home Depot, Inc. Customer Data Security Breach Litigation*, 2016 WL 2897520 at 4; *see also, Gordon v. Chipotle*

Mexican Grill, Inc., 344 FSupp 3d 1231 (D. Colo. 2018). This is sufficiently pled at this early stage. Based upon the foregoing, defendant's motion pursuant to CPLR § 3211(a)(7) is denied.

Defendant's Motion to Strike Plaintiff's Class Allegations

Defendant argues that the complaint on its face fails to satisfy the class action requirements of CPLR section 901(a) and must be dismissed pursuant to CPLR section 3211(a)(7). The statute provides that a matter may proceed as a putative class action where the complaint satisfies all of the following prerequisites: the class is so numerous that joinder of all members, whether otherwise required or permitted, is impracticable; there are questions of law or fact common to the class which predominate over any questions affecting only individual members; the claims or defenses of their representative parties are typical of the claims or defenses of the class; the representative parties will fairly and adequately protect the interests of the class; and the class action is superior to other available methods for the fair and efficient adjudication of the controversy. *See, CPLR § 901(a)*. Section 901 provides that one or more members of a class may sue or be sued as representative parties on behalf of all where five factors - referred to as numerosity, commonality, typicality, adequacy of representation and superiority- are met. *See, Maddicks v. Big City Props, LLC*, 34NY3d 116 (2019). Motions to strike are generally looked upon with disfavor and a motion to strike class allegations is even more disfavored because it requires a reviewing court to preemptively terminate the class aspects of litigation solely on the basis of what is alleged in the complaint and before plaintiffs are permitted to complete discovery to which they would otherwise be entitled, such as questions relevant to class certification. *See, Ironforge.com v. Paychex, Inc.*, 747 FSupp2d 384 (WDNY 2010); *see also, In re Tronox Secs. Litig.*, 2010 WL 2835545 at 4 (SDNY 2010). In addition, in considering the standards of the statute, a court must be mindful that class certification should be liberally construed. *See, Kudinov v. Kel-Tech Constr. Inc.*, 65 AD3d

481 (1st Dept. 2009); *see also*, *Englade v. Harper Collins Pub. Inc.*, 289 AD2d 159 (1st Dept. 2001). This Court finds that at this stage of the proceeding and in applying said standard, defendant is not entitled to dismissal. Plaintiff's proposed class is: all persons whose sensitive information, provided to defendant in connection with receiving medical services at SC, was exposed to unauthorized access by way of the data breach of defendants computer system on or about March 31, 2021. *See, Complaint para 44*. Plaintiff has adequately alleged that questions of fact and law applicable to all members predominate over individual issues, which include: whether defendant's data security systems prior to the breach met the requirements of relevant laws, whether defendant's data security systems prior to the breach met industry standards, whether plaintiff's and other class members' sensitive information was compromised in the data breach and whether plaintiff and other class members are entitled to damages as a result of defendant's conduct. Courts have routinely held that such allegations satisfy the commonality requirement and data breach cases under the statute and the equivalent federal standard, FRCP rule 23. *See, In re Brinker Data Incident Litig.*, 2021WL 1405508 at 8 (MD Fla. 2021). Nor is defendant's argument that each member of a class is required to submit evidence of personal standing. *See, Denney v. Deutsch Bank AG*, 443F3d 1205 (10th Cir. 2014). In a class action, unnamed plaintiffs need not make any individual showing of standing to obtain relief because the standing issue focuses on whether plaintiff is properly before the court, not whether representative parties or absent class members are properly before the court. *See, Lewis v. Casey*, 518 US 343 (1996). Likewise, the contention that plaintiff failed to adequately investigate the claims is unpersuasive at this time. Defendant's statute of limitations argument is premature. There are no facts before the court to support the claim that any class members may be subject to a statute of limitations defense in such a ruling would be inappropriate on a motion to strike during the pre-discovery motion to dismiss stage of

litigation. *See, Bryant v. Food Lion, Inc*, 774 FSupp 1484 (1991). Even if it is ultimately determined that the statute of limitations applies, CPLR section 906 permits a court to certify and maintain a class as to particular issues, such as questions of liability unrelated to any statute of limitations defenses. *See, In re Target Corp. Customer Data Sec. Breach Litig.*, 309FRD 482 (D. Minn. 2015).

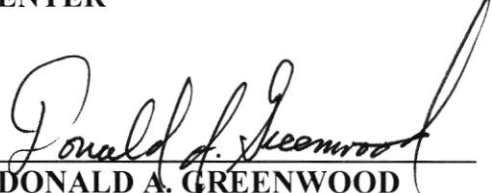
NOW, therefore, for the foregoing reasons, it is

ORDERED, that all of defendant's motions are denied in their entirety, and it is further

ORDERED, that any relief requested not addressed herein is denied.

ENTER

Dated: June 28, 2022
Syracuse, New York


DONALD A. GREENWOOD
Supreme Court Justice

Papers Considered:

1. Defendant's Notice of Motion to Dismiss Plaintiff's Complaint, dated March 7, 2022 (NYSCEF Doc. No. 3).
2. Affirmation of Daniel M. Braude, Esq., dated March 7, 2022, and attached exhibits (NYSCEF Doc. No. 4).
3. Defendant's Memorandum of Law, dated March 7, 2022 (NYSCEF Doc. No. 6).
4. Defendant's Application Pursuant to Uniform Rule 202.8-b, dated March 7, 2022 (NYSCEF Doc. No. 7).
5. Defendant's Notice of Motion to Strike Plaintiff's Class Allegations, dated March 7, 2022 (NYSCEF Doc. No. 10).
6. Affirmation of Daniel M. Braude, Esq., dated March 7, 2022, and attached exhibits (NYSCEF Doc. No. 11).
7. Defendant's Memorandum of Law, dated March 7, 2022 (NYSCEF Doc. No. 12).
8. So Ordered Stipulation, dated April 28, 2022(NYSCEF Doc. No. 22).
9. So Ordered Stipulation, dated April 28, 2022(NYSCEF Doc. No. 23).
10. Affirmation of Todd S. Garber, Esq., dated May 17, 2022, and attached exhibits (NYSCEF Doc. No. 26).
11. Plaintiff's Memorandum of Law, dated May 17, 2022 (NYSCEF Doc. No. 27).

12. Plaintiff's Application Pursuant to Uniform Rule 202.8-b, dated May 17, 2022 (NYSCEF Doc. No. 28).
13. Plaintiff's Memorandum of Law, dated May 17, 2022 (NYSCEF Doc. No. 29).
14. Application Pursuant to Uniform Rule 202.8-b, dated June 14, 2022 (NYSCEF Doc. No. 31).
15. Defendant's Reply Memorandum of Law, dated June 14, 2022 (NYSCEF Doc. No. 32)
16. So Ordered Application, dated, June 15, 2022 (NYSCEF Doc. No. 33).
17. Defendant's Reply Memorandum of Law, dated June 16, 2022 (NYSCEF Doc. No. 34)