69 Misc.3d 597
Supreme Court, Westchester County, New York.

Michelle SMAHAJ, Individually and On behalf of All Others Similarly Situated, Plaintiff,
v.
RETRIEVAL-MASTERS CREDITORS BUREAU, INC. d/b/a American Medical Collections Agency, and CBLPATH, Inc., Defendants.

62076/2019
|
Decided on September 4, 2020

Synopsis

Background: Consumer brought putative class action against debt collection agency and creditor, a medical laboratory, asserting causes of action including negligence and breach of contract, arising from alleged data breach when nonparty hackers accessed agency's database. Creditor brought motion to dismiss for lack of standing and failure to state a claim.

Holdings: The Supreme Court, Westchester County, Ecker, J., held that:

[1] consumer failed to establish that she and putative class members suffered actual injury, or that alleged injury was imminent, as required for standing;

[2] consumer failed to demonstrate that creditor had control over agency's systems that were compromised in data breach, as would support standing;

[3] creditor had no duty to protect consumer from harm by third parties who unforeseeably hacked into agency's database;

[4] consumer did not sufficiently plead breach of contract cause of action;

[5] consumer failed to state a cause of action under a theory of implied contract;

[6] consumer could not maintain cause of action against creditor for negligence per se based on alleged violation of unfair competition provision of the Federal Trade Commission (FTC) Act; and

[7] creditor's alleged failure to safeguard consumer's personal information on agency's networks was not a deceptive practice that would give rise to a statutory cause of action.

Motion granted.

Procedural Posture(s): Motion to Dismiss.

West Headnotes (23)

[1] **Pretrial Procedure** Parties, Defects as to
Pretrial Procedure Presumptions and burden of proof

On a defendant's motion to dismiss a complaint based upon the plaintiff's alleged lack of standing, the burden is on the moving defendant to establish, prima facie, the plaintiff's lack of standing. N.Y. CPLR § 3211(a) (3).

[2] **Pretrial Procedure** Parties, Defects as to
Pretrial Procedure Fact questions

A motion to dismiss for lack of standing will be defeated if the plaintiff's submissions raise a question of fact as to its standing. N.Y. CPLR § 3211(a) (3).

[3] **Finance, Banking, and Credit** Parties; standing
Finance, Banking, and Credit Right of action; standing

Consumer failed to establish that she and putative class members suffered actual injury from data breach at debt collection agency, or that alleged injury was imminent, as required for standing in putative class action alleging negligence and breach of contract against creditor that used agency's services; although access to the agency's database by outside hackers created an inference of malicious intent

to steal private information, almost two years had elapsed since data breach began, consumer did not specifically allege any fraudulent charges or actual suspicious activity that directly harmed her or class members, and alleged increased risk of identity theft was speculative and based on conjecture.

1 Case that cites this headnote

[4] **Action** Persons entitled to sue

Fraudulently imposed charges are indicia of fraudulent activity weighing in favor of finding an injury in fact, such as would support standing to bring a lawsuit.

[5] **Finance, Banking, and Credit** Parties; standing

Finance, Banking, and Credit Right of action; standing

Consumer failed to demonstrate that creditor had control over systems of debt collection agency that were compromised in data breach, as would support standing against creditor in putative class action alleging negligence and breach of contract; although consumer alleged that creditor directed and authorized all agency actions that resulted in compromise of personal information, such conclusory allegations were unsupported by any specific details related to control over agency's systems or data security, consumer did not allege any breach of creditor's own systems, and creditor was not alleged to have an agency relationship with debt collection agency or any stake in the collection industry.

[6] **Pretrial Procedure** Evidence

Consumer's allegation, that her private information was for sale on the dark web due to data breach at debt collection agency used by creditor, was not admissible as evidence in opposition to creditor's motion to dismiss consumer's putative class action claim against it for negligence and breach of contract, since assertion was not in a sworn affidavit or verified pleading.

[7] **Affidavits** Knowledge or information of affiant

An attorney's affirmation that is not based upon personal knowledge is generally of no probative value.

[8] **Pretrial Procedure** Insufficiency in general

Pretrial Procedure Construction of pleadings

A motion to dismiss for failure to state a claim should be granted only where, even viewing the allegations as true, the plaintiff still cannot establish a cause of action. N.Y. CPLR § 3211(a)(7).

[9] **Negligence** Elements in general

To establish a prima facie case of negligence, a plaintiff must demonstrate the existence of a duty owed by defendant to plaintiff, a breach of that duty, and resulting injury which was proximately caused by the breach.

[10] **Finance, Banking, and Credit** Obligations Imposed; Practices Prohibited or Required

Creditor had no duty to protect consumer from harm by third parties who unforeseeably hacked into database of debt collection agency used by creditor and obtained consumer's personal information; creditor was in the business of providing medical services, appropriately transferred consumer's data to agency, and had no control over agency, and consumer did not allege that either creditor or agency was aware of any specific risks to agency's data security system.

[11] **Torts** Miscellaneous torts in general

It is a basic principle that an entity storing a plaintiff's confidential information has a duty to exercise reasonable care to safeguard it.

[12] **Contracts** Grounds of action

The elements of a cause of action to recover damages for breach of contract are the existence of a contract, the plaintiff's performance under the contract, the defendant's breach, and resulting damages.

[13] **Contracts** Grounds of action

Generally, a party alleging a breach of contract must demonstrate the existence of a contract reflecting the terms and conditions of the purported agreement.

[14] **Contracts** Pleading contract or specifications

A plaintiff's allegations of breach of contract must identify the provisions of the contract that were breached.

[15] **Finance, Banking, and Credit** Pleading

Finance, Banking, and Credit Actions

Consumer did not sufficiently plead breach of contract cause of action against creditor that used services of debt collection agency at which consumer's information was compromised in data breach; consumer failed to identify which provision of purported contract required creditor to safeguard consumer's information on agency's network, instead simply reciting various passages from creditor's privacy notice.

[16] **Contracts** Implied agreements

An implied-in-fact contract requires the same elements as an express contract including, consideration, mutual assent, legal capacity, and legal subject matter.

[17] **Contracts** Necessity of assent

Contracts Implied agreements

Like an express contract, an implied-in-fact contract requires a showing that there was a meeting of the minds.

[18] **Contracts** Implied agreements

A contract implied in fact may result as an inference from the facts and circumstances of a case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct.

[19] **Finance, Banking, and Credit** Actions

Consumer failed to state a cause of action under a theory of implied contract against creditor that used services of debt collection agency at which consumer's personal information was compromised in data breach; although consumer contended that she was required to provide sensitive personal information in order to receive medical laboratory services from creditor, complaint was devoid of facts supporting an inference that creditor implicitly promised to keep consumer's information safe while it was stored on agency's network.

2 Cases that cite this headnote

[20] **Action** Statutory rights of action

Finance, Banking, and Credit Right of action; standing

Statutes governing data security and requiring disclosure when private information is accessed or acquired without valid authorization do not create a private right of action. N.Y. General Business Law §§ 899-aa, 899-bb.

2 Cases that cite this headnote

[21] **Action** Statutory rights of action

Antitrust and Trade Regulation Private entities or individuals

Consumer could not maintain cause of action against creditor for negligence per se based on creditor's alleged violation of unfair competition provision of the Federal Trade Commission

Act, arising from data breach at debt collection agency, since establishment of negligence per se based on such violation would provide consumer with a private right of action unrecognized by the Act. Federal Trade Commission Act § 5, 15 U.S.C.A. § 45.

6 Cases that cite this headnote

[22] **Antitrust and Trade Regulation** In general; unfairness

A prima facie case under statute prohibiting deceptive acts and practices in business requires a showing that the defendant engaged in a consumer-oriented act or practice that was deceptive or misleading in a material way and that the plaintiff has been injured by reason thereof. N.Y. General Business Law §§ 349(a), 349(h).

3 Cases that cite this headnote

[23] **Antitrust and Trade Regulation** Privacy

Creditor's alleged failure to safeguard consumer's personal information on debt collection agency's networks, which were compromised in data breach, did not mislead consumer and was not a deceptive practice that would give rise to a cause of action against creditor under statute prohibiting deceptive acts and practices in business; nothing set forth in consumer's complaint or creditor's privacy notice was a statement relative to an obligation of creditor to secure data on agency's network, privacy notice disclosed that personal information might be shared with other entities that were required to maintain its privacy and security, and notice did not constitute an unlimited guaranty that consumer's information could not be stolen from such an entity or its network. N.Y. General Business Law §§ 349(a), 349(h).

3 Cases that cite this headnote

Attorneys and Law Firms

****820** Lewis Brisbois Bisgaard & Smith LLP (Jeffrey Spiegel of counsel) for CBLPath, Inc., defendant.

Blau Leonard Law Group LLC (Steven Bennett Blau and Shelly A. Leonard of counsel) and Kleinman LLC (Abraham Kleinman of counsel) for plaintiff.

Opinion

Lawrence H. Ecker, J.

***598** In accordance with CPLR 2219 (a), the decision herein is made upon considering all papers filed in NYSCEF relative to the motion of codefendant CBLPATH, INC. (CBLPATH) (Mot. Seq. 2), made pursuant to CPLR 3211 (a) (3) and (7), for an order dismissing the complaint of plaintiff MICHELLE SMAHAJ, Individually and On Behalf of All Others Similarly Situated, as asserted against CBLPATH.

***599** This is a class action suit stemming from a data breach of a debt collection agency. Plaintiff is an individual residing in Garnerville, NY Defendant Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collections Agency (AMCA) is a debt collection corporation who contracts with laboratories, hospitals, and medical providers to collect unpaid debts from consumers. Codefendant CBLPATH is a provider of sub-specialized anatomic pathology and molecular diagnostic laboratory services with a laboratory facility in the Village of Rye Brook. AMCA retained CBLPATH to provide collection services.

During some unspecified period of time, plaintiff and class members received medical services from CBLPATH and failed to pay an invoice for the services. CBLPATH provided AMCA with personal information of plaintiff and certain class members, including their names, dates of birth, social security numbers, and other information so that AMCA could collect on plaintiff's debt.

From August 2018 to March 2019, a data breach allegedly occurred at AMCA. The nonparty unidentified hackers accessed AMCA's database. Plaintiff alleges that the hackers attempted to "place a batch of 200,000 payment card numbers for sale on a popular Darknet Market." Plaintiff claims that due to the data breach, it is likely that she and other class members' private information "will or has been disclosed already on the Darknet," though there is "uncertainty as to the nature and extent" of the information that was compromised.

Plaintiff claims that the hack was "directly caused by the omissions and commissions of AMCA" and that CBLPATH became aware of the breach on or about May 10, 2019, [1] but allegedly did ****821** not inform plaintiff of the data breach until July 15, 2019.

Plaintiff commenced this action in August 2019, asserting causes of action for negligence, negligence per se, breaches of implied and express contract, and several violations of the General Business Law. In the complaint, plaintiff defines the class as: "[a]ll individuals in the State of New York whose personal information was provided to AMCA by CBLPATH and was compromised as a result of the AMCA data breach." In support of her claims, plaintiff alleges that she and the class suffered three principal categories of damages: (1) an increased risk of suffering from identity theft and fraud; (2) time, money, ***600** and other resources spent to mitigate against risks, both now and in the future, by cancelling credit cards, ability to open new bank accounts, reversing fraudulently imposed charges, and incurring high interest rates due to the inevitable decline in credit score when plaintiff and class members reasonably do not pay for items and services they did not purchase; and (3) the diminution of the value and/or loss of the benefits or products and services purchased directly or indirectly from defendants. [2]

AMCA is bankrupt and has not appeared in this action. In October 2019, CBLPATH filed a pre-answer motion for, among other things, an extension of time to answer or otherwise move with respect to the complaint. This court granted the motion by decision and order in December 2019. Shortly thereafter, CBLPATH made this motion to dismiss the complaint against it pursuant to CPLR 3211 (a) (3) and (7), contending that plaintiff lacks standing and that she failed to state a viable claim for all causes of action asserted in the complaint.

I. Lack of Standing

[1] **[2]** CBLPATH primarily relies on dismissal under CPLR 3211 (a) (3) inasmuch as it claims that plaintiff did not sufficiently allege an injury in fact. " 'On a defendant's motion to dismiss the complaint based upon the plaintiff's alleged lack of standing, the burden is on the moving defendant to establish, prima facie, the plaintiff's lack of standing' " (*Gobindram v. Ruskin Moscou Faltischek, P.C.*, 175 A.D.3d 586, 591, 106 N.Y.S.3d 339 [2d Dept. 2019], quoting *BAC Home Loans Servicing, LP v. Rychik*, 161 A.D.3d 924, 925, 77 N.Y.S.3d 522 [2d Dept. 2018]; *see* CPLR 3211 [a] [3]). "The motion will be defeated if the plaintiff's submissions raise a question of fact as to its standing" (*Gobindram v. Ruskin Moscou Faltischek, P.C.*, 175 A.D.3d at 591, 106 N.Y.S.3d 339).

As the parties point out, *Manning v. Pioneer Sav. Bank,* 56 Misc. 3d 790, 55 N.Y.S.3d 587 (Sup. Ct., Rensselaer County 2016) appears to be the only reported case in New York State addressing standing in the context of a data breach. There, the named plaintiff commenced a class action suit alleging, inter alia, negligence and breach of implied and express contract after a bank-owned laptop containing customer information (including names, social security numbers, addresses, and account numbers) was stolen from a bank employee's vehicle (*see id.* at 791, 55 N.Y.S.3d 587). Ultimately, ***601** the Court in *Manning* dismissed the complaint for lack of standing, finding that plaintiff's claimed injuries were speculative since they were based on future risks of identity theft and, thus, did not constitute an injury in fact (*see id.* at 797, 55 N.Y.S.3d 587).

Plaintiff in this case, however, directs this court's attention to federal and out-of-state ****822** cases involving data breach victims who were found to have standing despite not having suffered actual monetary damages or were the victims of identity theft. For example, in *Sackin v. TransPerfect Global, Inc.,* 278 F. Supp. 3d 739 (S.D. N.Y. 2017), an employee of defendant Transperfect disclosed plaintiffs' personal information to unidentified cyber-criminals in response to a "phishing" email received on or about January 17, 2017 (*id.* at 744). About one month later, the plaintiffs in *Sackin* filed a complaint alleging four categories of injury as a consequence of the data breach: "(1) an imminent risk of future identity theft; (2) lost time and money expended to mitigate the threat of identity theft; (3) diminished value of personal information; and (4) [ ] loss of privacy" (*id.* at 745). In finding that plaintiffs' first two alleged categories constitute injuries in fact, the court in *Sackin* considered the circumstances of the disclosure, which created "a risk of identity theft sufficiently acute as to fall comfortably into the category of 'certainly impending' " (*id.* at 746). In so doing, it distinguished cases where "courts found standing to be lacking when a plaintiff's [information] was on a stolen computer, and the plaintiffs did not allege or could not show that obtaining their [information] was the motivation for the theft" (*id.* at 747).

Notwithstanding the *Sackin* decision, the court notes that a temporal component may factor into determining whether a threatened harm is sufficient for standing within the Second

Circuit. For example, in *Fero v. Excellus Health Plan, Inc.,* 236 F. Supp. 3d 735 (W.D. N.Y. 2017), hackers breached the computer network in December 2013 for a health care provider and accessed certain personal and financial information (*see id.* at 744). About two years later, the initial complaint was filed, and the action was consolidated with some plaintiffs alleging that their information had been misused, while other plaintiffs did not allege any misuse (the non-misuse plaintiffs) (*see id.* at 744-745). The *Fero* Court held that the non-misuse plaintiffs lacked standing because the alleged harm of increased identity fraud, without more, was too speculative given that three years had passed without any suspicious activity, which undercut assertions ***602** of "certainly impending" harm (*id.* at 753).[3] Moreover, the Court in *Fero* found that with respect to those non-misuse plaintiffs, there was a lack of standing based on: (1) the alleged mitigation efforts against future identify fraud because such harm was not imminent; and (2) the alleged diminution in value of their personal information because the complaint lacked "factual allegations to support the proposition that their personal information was made less valuable to them as a result of the breach, or that the data breach negatively impacted the value of their data such that [p]laintiffs could not use or sell it" (*id.* at 755).

[3] **[4]** Here, plaintiff has failed to establish that she and the class members have suffered injuries or that the alleged injuries are imminent (*see Silver v. Pataki*, 96 N.Y.2d 532, 538, 730 N.Y.S.2d 482, 755 N.E.2d 842 [2001]; *Society of Plastics Indus. v. County of Suffolk*, 77 N.Y.2d 761, 772-773, 570 N.Y.S.2d 778, 573 N.E.2d 1034 [1991]; *Warth v. Seldin*, 422 U.S. 490, 503-504, 95 S.Ct. 2197, 45 L.Ed.2d 343 [1975]). In contrast to *Manning*, the data breach at issue creates an inference of malicious intent to steal private information, supporting an increased risk of identity theft (*compare Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d at 746). However, a lengthy passage of time without any suspicious activity weighs against finding ****823** an injury in fact. Nearly one year elapsed from when the subject data breach occurred and more than one year has now passed since when this action was commenced. The complaint asserts that "[p]laintiff and class members have sustained further pecuniary injury and have been compelled to expend time, money[,] and other resources to cancelling credit cards, opening new bank accounts, *reversing fraudulently imposed charges*, and higher interest rates due to the inevitable decline in credit score when [they] reasonably do not pay for items and services they did not purchase" (complaint ¶ 27 [emphasis added]). Fraudulently imposed charges are indicia of fraudulent activity weighing in favor of finding an injury in fact (*cf. Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d at 753). But plaintiff does not specifically allege any fraudulent charges and this allegation appears to hinge on "time, money and other resources" expended to avoid or address future harm. For example, the alleged "higher interest rates" appear to be presented as a future ***603** harm resulting "*when* [p]laintiff and class members reasonably *do not pay* for items and services they did not purchase" (complaint ¶ 27 [emphasis added]). As such, the complaint fails to allege any actual suspicious activity that directly harmed plaintiff. Now, almost two years have elapsed since the data breach began and there is still no evidentiary proof of actual harm that plaintiffs have suffered. *Fero* is thus persuasive as to the temporal factor of the injury-in-fact requirement. The alleged increased risk of identity theft is speculative and based on conjecture so as to not constitute an injury in fact. Therefore, the court likewise finds plaintiff's alleged injuries are insufficient to confer standing (*see Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d at 754-755; *Manning v. Pioneer Sav. Bank*, 56 Misc. 3d at 797, 55 N.Y.S.3d 587).

[5] This case is one step removed from *Sackin* and *Fero* in that the data breach is not alleged to have occurred on (or emanated from) CBLPATH's network, data systems, or any other system within its control. Plaintiff's conclusory allegation that CBLPATH "retained, supervised, controlled, directed[,] and authorized all actions of AMCA, which resulted in [p]laintiff['s] and class members' personal information being compromised" (complaint ¶ 24), is unsupported by any specific details related to control over AMCA's systems or data security. Such a sweeping generalization is undercut by the complaint's averment that "AMCA is one of the nations' largest debt collectors" (*id.* at 9). It does not follow that CBLPATH — which is not alleged to have an agency relationship with AMCA nor any stake in the debt collection industry — would control "all actions" related to the data security of one of America's biggest debt collectors. Without more, plaintiff fails to demonstrate that CBLPATH had control over AMCA's hacked systems (*see generally Rejer v. Professional Referee Org.*, 2020 N.Y. Slip Op. 30507[U], 2020 WL 886159, *4 [Sup. Ct., New York County 2020]).

Plaintiff's reliance on *Remijas v. Neiman Marcus Group, LLC,* 794 F.3d 688 [7th Cir. 2015] to suggest that the data breach is "fairly traceable" to CBLPATH's conduct is misplaced because that case is distinguishable. In *Remijas*, defendant argued that plaintiffs "cannot show that their injuries are

traceable to the data incursion at the company rather than to one of several other large-scale breaches that took place around the same time" (*id.* at 696). The Court nonetheless held that plaintiffs' injuries were "fairly traceable" to the data breach at Neiman Marcus and analogized the facts to a 1948 quail hunt case: *Summers v. Tice*, 33 Cal.2d 80, 199 P.2d 1, 5 [1948]), ***604** wherein the *Summers*' plaintiff ****824** was shot, but did not know which defendant shot him. Ultimately, the *Summers* Court held that plaintiff properly pleaded joint liability and the burden shifted to defendants to show who was responsible (*see Remijas v. Neiman Marcus Group, LLC,* 794 F.3d at 696 [discussing *Summers v. Tice*, 199 P.2d at 5]).

Here, in contrast, plaintiffs did not allege a breach of CBLPATH's network or data systems. When applied to the present matter, these cases suggest an increased probability of identity theft resulting from the nature of the data breach, but a decreased probability of identity theft after a one-to-two year period without suspicious activity, and more importantly, a diminished relationship between the alleged injuries and the challenged conduct of CBLPATH. Therefore, this court finds that the complaint alleges speculative harm that does not constitute an injury in fact that is fairly traceable to CBLPATH's conduct.

[6] **[7]** Plaintiff, however, attempts to raise a question of fact alleging, for the first time in her memorandum of law in opposition, that "following the [d]ata [b]reach, [her] Private Information, including her Social Security number, has been found available for sale on the 'dark web,' and that she knows of no other source of such information besides the [d]ata [b]reach at issue here" (memorandum of law in opposition at 9 [NYSCEF Doc No. 33]). Generally, even an "attorney's affirmation that is not based upon personal knowledge is of no probative [value]" (*Warrington v. Ryder Truck Rental, Inc.*, 35 A.D.3d 455, 456, 826 N.Y.S.2d 152 [2d Dept. 2006]). Here, plaintiff's allegation is asserted in a memorandum of law, is unsworn to in an affidavit or verified pleading, and, therefore, not in admissible form. Plaintiff's allegation in this regard was improper and is thus rejected (*see Countrywide Home Loans, Inc. v. Vittorio*, 178 A.D.3d 1017, 1018-1019, 116 N.Y.S.3d 83 [2d Dept. 2019]). Therefore, based on the allegations set forth in the complaint, plaintiff fails to allege an injury in fact, and lacks standing.

II. Failure to State a Cause of Action

[8] Even assuming that plaintiff established standing, the court must dismiss the complaint based upon a failure to state a cause of action. "On a motion to dismiss pursuant to CPLR 3211 (a) (7), the complaint is to be afforded a liberal construction, the facts alleged are presumed to be true, the plaintiff is afforded the benefit of every favorable ***605** inference, and the court is to determine only whether the facts as alleged fit within any cognizable legal theory" (*Rodriguez v. Daily News, L.P.*, 142 A.D.3d 1062, 1063, 37 N.Y.S.3d 613 [2d Dept. 2016], *lv denied* 28 N.Y.3d 913, 2017 WL 113412 [2017]). "Such a motion should be granted only where, even viewing the allegations as true, the plaintiff still cannot establish a cause of action" (*Hartman v. Morganstern*, 28 A.D.3d 423, 424, 814 N.Y.S.2d 169 [2d Dept. 2006]).

a. Negligence

[9] Turning first to plaintiff's first cause of action, to establish a prima facie case of negligence, a plaintiff must demonstrate the existence of a duty owed by defendant to plaintiff, a breach of that duty, and resulting injury which was proximately caused by the breach (*see Solomon v. City of New York*, 66 N.Y.2d 1026, 1027, 499 N.Y.S.2d 392, 489 N.E.2d 1294 [1985]; *Conneally v. Diocese of Rockville Ctr.*, 116 A.D.3d 905, 906, 984 N.Y.S.2d 127 [2d Dept. 2014]; *Rubin v. Staten Is. Univ. Hosp.*, 39 A.D.3d 618, 618, 833 N.Y.S.2d 241 [2d Dept. 2007]).

[10] In this matter, plaintiff ostensibly failed to pay for medical services provided by CBLPATH, requiring CBLPATH to ****825** enter into an agreement with AMCA for collection of the unpaid monies. Being in the business of providing medical services, CBLPATH had no duty to protect plaintiff from third parties harming her by unforeseeable hacks into AMCA's system, which CBLPATH had no control over (*see Malik v. Ultraline Med. Testing, P.C.*, 177 A.D.3d 515, 515-516, 115 N.Y.S.3d 226 [1st Dept. 2019]). Hence, plaintiff's claim for negligence is untenable.

[11] Nonetheless, plaintiff argues that a common law duty exists and that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes a duty of care on the part of CBLPATH. However, none of the cases cited by plaintiff suggest that one has a common law duty to protect another from the potential breach of a third party's data network — here, being AMCA's network. [4] Moreover, the cases cited by plaintiff purportedly creating a common law duty underscore the foreseeability of harm, such as prior notice to data breaches, lax security measures, disabled security features, etc. (*see Matter of Arby's Rest. Group, Inc., Litigation*, 2018 WL 2128441, *5 [N.D. Ga., 2018] ["Under Georgia ***606** law ... [,] allegations that a company knew of

a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss"]). In contrast, here, plaintiff did not assert that AMCA was aware of any specific risks to its data security system, let alone that CBLPATH was aware of such risks to AMCA's network.

Plaintiff concedes that HIPAA does not provide a private right of action but instead relies on out-of-state cases to argue that "HIPAA may be used to establish an appropriate standard for the protection of health care information" and that "HIPAA [does] not preempt negligence claims based on alleged HIPAA violations" (memorandum of law in opposition at 23-24 [NYSCEF Doc No. 33]).[5] Plaintiff, however, does not dispute CBLPATH's averment that it properly disclosed protected health information to AMCA, its "business association," as that term is defined by HIPAA (45 CFR 164.502 [a] [1] [i], [e]), after obtaining satisfactory security assurances from AMCA. Indeed, the complaint avers the following: "AMCA states that it is 'compliant with all Federal and State Laws and are members of ACA International. We provide our services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm' " (complaint ¶ 10). Critically, HIPAA does *not* require covered entities, such as CBLPATH "to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract"; "[n]or is the covered entity responsible or liable for the actions of its business associates" (Health Information Privacy, U.S. Dept. of Health & Human Servs., *Is a covered entity liable for, or required to monitor, the actions of its business associates?*, available at https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html [Dec. 19, 2002]). In view of the foregoing, plaintiff failed to establish that CBLPATH owed a duty to protect her data that had been appropriately transferred to, and was stored by, a third party. Accordingly, the complaint fails to state a cause of action for negligence as against CBLPATH (*see* ***607** *Fox v. Marshall*, 88 A.D.3d 131, 135-140, 928 N.Y.S.2d 317 [2d Dept. 2011]; ****826** *Engelhart v. County of Orange*, 16 A.D.3d 369, 371, 790 N.Y.S.2d 704 [2d Dept. 2005], *lv denied* 5 N.Y.3d 704, 801 N.Y.S.2d 1, 834 N.E.2d 780 [2005]; *compare Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 49 Misc. 3d 1027, 1041, 19 N.Y.S.3d 850 [Sup. Ct., Queens County 2015]).

b. Breach of Contract

[12] **[13]** **[14]** "The elements of a cause of action to recover damages for breach of contract are the existence of a contract, the plaintiff's performance under the contract, the defendant's breach, and resulting damages" (*Detringo v. South Is. Family Med., LLC*, 158 A.D.3d 609, 609-610, 71 N.Y.S.3d 525 [2d Dept. 2018]). "Generally, a party alleging a breach of contract must demonstrate the existence of a contract reflecting the terms and conditions of their purported agreement. Moreover, the plaintiff's allegations must identify the provisions of the contract that were breached" (*Canzona v. Atanasio*, 118 A.D.3d 837, 839, 989 N.Y.S.2d 44 [2d Dept. 2014] [internal citations, quotation marks, and ellipses omitted]).

[15] Here, it is undisputed that plaintiff's alleged harm stems from a data breach on AMCA's network. Plaintiff, however, fails to identify which provision of the purported contract required CBLPATH to safeguard plaintiff's information on AMCA's network. Plaintiff simply recites various passages from CBLPATH's privacy notice, which she claims constitutes a part of the contract, but nothing in the privacy notice suggests that CBLPATH would safeguard plaintiff's information on AMCA's network. As such, plaintiff failed to plead the material terms of the alleged contract by which CBLPATH supposedly agreed to safeguard plaintiff's information on a third party's network (*see Canzona v. Atanasio*, 118 A.D.3d at 839, 989 N.Y.S.2d 44). Plaintiff's allegations of an alleged contract are, therefore, insufficient to plead a breach of contract cause of action against CBLPATH (*see id.*).

c. Breach of Implied Contract

[16] **[17]** **[18]** "An implied-in-fact contract requires the same elements as an express contract including, consideration, mutual assent, legal capacity, and legal subject matter" (*Canon U.S.A., Inc. v. Stereo Advantage, Inc.*, 2019 N.Y. Slip Op. 32394[U], 2019 WL 3765351, *2 [Sup. Ct., New York County 2019], citing *Maas v. Cornell Univ.*, 94 N.Y.2d 87, 93-94, 699 N.Y.S.2d 716, 721 N.E.2d 966 [1999]). "Like an express contract, an implied-in-fact contract requires a showing that there was a meeting of the minds" (*Canon U.S.A., Inc. v. Stereo Advantage, Inc.*, 2019 N.Y. Slip Op. 32394[U] at *3). "A contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct" ***608** (*Jemzura v. Jemzura*, 36 N.Y.2d 496, 503-504, 369 N.Y.S.2d 400, 330 N.E.2d 414 [1975] [internal citations and quotation marks omitted]).

[19] Here, plaintiff contends that CBLPATH required her to provide sensitive personal information in exchange for specialized pathological and diagnostic services, and her reliance on those services evinced an implicit promise by CBLPATH to act reasonably to keep plaintiff's information safe. However, the complaint is devoid of any facts supporting an inference that CBLPATH implicitly promised to keep plaintiff's information safe when it was stored on a third-party business associate's network (*cf. Hammond v. Bank of NY Mellon Corp.*, 2010 WL 2643307, *9, 2010 U.S. Dist. LEXIS 71996, *37-38 [S.D. N.Y., 2010] [finding lack of any evidence of defendant's assent]). Hence, the complaint fails to state a cause of action to recover ****827** damages under a theory of implied contract as asserted against CBLPATH (*see id.*).

d. Violations of New York State General Business Law and Negligence Per Se

[20] As to plaintiff's fourth and fifth causes of action, plaintiff alleges that CBLPATH violated New York General Business Law §§ 349, 899-aa, 899-bb, and section 45 of the Federal Trade Commission Act (FTC Act) (15 USC § 45), with the latter forming the basis for plaintiff's negligence per se claim. First, apart from General Business Law § 349, none of the cited laws provide a private right of action (*see Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 49 Misc. 3d at 1036-1038, 19 N.Y.S.3d 850 [finding that General Business Law § 899-aa does not create a private right of action]). Thus, plaintiff's claims under General Business Law §§ 899-aa and 899-bb must be dismissed.

[21] Plaintiff's negligence per se claim based on an alleged violation of the FTC Act must also be dismissed because "[i]f mere proof of a violation of ... were to establish negligence per se, plaintiff would effectively be afforded a private right of action that [the statute] does not recognize" (*Lugo v. St. Nicholas Assoc.*, 2 Misc. 3d 212, 218, 772 N.Y.S.2d 449 [Sup. Ct., New York County 2003], *affd* 18 A.D.3d 341, 795 N.Y.S.2d 227 [2005] [analyzing the Americans with Disabilities Act]; *see generally Moore v. New York Cotton Exchange*, 270 U.S. 593, 602-603, 46 S.Ct. 367, 70 L.Ed. 750 [1926]).

[22] Next, General Business Law § 349 (a) provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful" (*see Keshin v. Montauk Homes, LLC*, 162 A.D.3d 758, 760, 79 N.Y.S.3d 240 [2d Dept. 2018]*lv denied* ***609** 32 N.Y.3d 910, 2018 WL 6176093 [2018]); and subsection 349 (h) provides a private right of action to "any person who has been injured by reason of any violation of this section." A prima facie case under General Business Law § 349 (h) requires "a showing that the defendant engaged in a consumer-oriented act or practice that was 'deceptive or misleading in a material way and that the plaintiff has been injured by reason thereof' " (*Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 49 Misc. 3d at 1039, 19 N.Y.S.3d 850, quoting *Goshen v. Mutual Life Ins. Co. of N.Y.*, 98 N.Y.2d 314, 324, 746 N.Y.S.2d 858, 774 N.E.2d 1190 [2002]).

[23] In this regard, plaintiff argues that the complaint sufficiently alleges the elements of a cause of action predicated on General Business Law § 349 (a) and (h), referring to a litany of alleged failures, misrepresentations, and omissions by CBLPATH. Plaintiff further contends that CBLPATH violated section 349 by neglecting to disclose its inadequate cyber security practices and misrepresented its efforts to safeguard plaintiff's personal information.

The data breach was of AMCA's network, not CBLPATH, and plaintiff does not allege that CBLPATH exercised control over AMCA's network or data security. Nothing set forth in the complaint or in CBLPATH's privacy notice can be considered a statement relative to an obligation of CBLPATH to secure data on AMCA's network. In fact, CBLPATH's privacy notice discloses that it may share a patient's personal information with "other entities ... known as 'business associates' " — which "are required to maintain the privacy and security" of that information. Indeed, the privacy notice reflects that CBLPATH itself will maintain the privacy and security of that information after it has been shared and is in the custody of its business associate. "[T]he statements allegedly ****828** made by [CBLPATH] in the privacy notice ... do not constitute an unlimited guaranty that patient information could not be stolen [from a business associate] or that computer data could not be hacked" on the network of a business associate (*Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 49 Misc. 3d at 1039, 19 N.Y.S.3d 850). CBLPATH's alleged failure to safeguard information on AMCA's networks did not mislead plaintiff in any material way and does not constitute a deceptive practice within the meaning of General Business Law § 349 (*see id.*). Therefore, plaintiff fails to state a cause of action under that statute as asserted against CBLPATH. Based on the foregoing, CBLPATH's motion to dismiss is granted.

The court has considered the additional contentions of the parties not specifically addressed herein. To the extent any ***610** relief requested by the parties was not addressed, it is hereby denied. Accordingly, it is hereby:

ORDERED that the motion of codefendant CBLPATH, INC. (Mot. Seq. 2), made pursuant CPLR 3211 (a) (3) and (7), for an order dismissing the complaint of plaintiff MICHELLE SMAHAJ, Individually and On Behalf of All Others Similarly Situated, as asserted against CBLPATH, INC., is granted in its entirety; and it is further

ORDERED that the complaint of plaintiff MICHELLE SMAHAJ, Individually and On Behalf of All Others Similarly Situated, is dismissed as against codefendant CBLPATH, INC.

The foregoing constitutes the Decision/Order of the court.

All Citations

69 Misc.3d 597, 131 N.Y.S.3d 817, 2020 N.Y. Slip Op. 20222

Footnotes

1 Specifically, the complaint, filed on August 10, 2019, alleges that CBLPATH "became aware of [the data breach] approximately three months ago" (complaint ¶ 18 [NYSCEF Doc No. 1]).

2 Plaintiff asserts that other class members have not been notified of the loss of their data.

3 Oral argument was heard in that case on September 8, 2016 (*see Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 745 [W.D. N.Y. 2017]).

4 CBLPATH agrees with the basic principle that an entity storing a plaintiff's confidential information has a duty to exercise reasonable care to safeguard it.

5 In so doing, plaintiff relies on *Acosta v. Byrum*, 180 N.C.App. 562, 638 S.E.2d 246 (2006) and *Sheldon v. Kettering Health Network,* 40 N.E.3d 661 (Ohio Ct. App. 2015).