#19

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

SUPERIOR COURT
CIVIL ACTION
NO. 2173CV00498C

CATHY SHEDD[1]
vs.
STURDY MEMORIAL HOSPITAL, INC.
(and a companion case[2])

MEMORANDUM OF DECISION AND ORDER ON DEFENDANT'S MOTIONS TO DISMISS

A ransomware attack hit Sturdy Memorial Hospital (Defendant or Sturdy Memorial) on or about February 9, 2021. One or more unauthorized persons gained access to Sturdy Memorial's computer systems and to the personal and confidential information of Sturdy Memorial's patients and others (Personally Identifiable Information or PII). Sturdy Memorial paid a ransom, secured its systems, and obtained assurances that the PII had been destroyed and would not be further distributed. Sturdy Memorial notified those individuals whose PII had been stolen four months later on May 28, 2021.

Two separate class action cases were filed to obtain damages, restitution, and injunctive relief. The class plaintiff in the Lead Case, Cathy Shedd (Shedd), asserts claims of Negligence (Count I), Breach of Implied Contract (Count II), Breach of Fiduciary Duty (Count III), Unjust Enrichment (Count IV), and Violation of G. L. c. 93A

[1] Individually and on behalf of all others similarly situated

[2] Barbara Ragan Bennett, et al., individually and on behalf of all others similarly situated vs. Sturdy Memorial Hospital, Inc., Plymouth Superior Court, Civil No. 2183CV00688, after Order of Transfer and Consolidation, Bristol Superior Court, Civil No. 2273CV00162C.

(Count V). The class plaintiffs in the Consolidated Case, Barbara Ragan Bennett (Bennett), et al, also brought claims of negligence, unjust enrichment, and violation of G. L. c. 93A and asserted a claim for invasion of privacy under G. L. c. 214, § 1B. Where appropriate, I refer to both sets of named plaintiffs as "Plaintiffs."

Sturdy Memorial filed Motions to Dismiss Pursuant to Mass. R. Civ. P. 12(b)(6) (Motions) in both the Lead and Consolidated Cases. The parties argued both Motions on March 16, 2022. After hearing and review, and for the reasons stated below, the Motions are **Allowed-in-part** and **Denied-in-part.**

BACKGROUND

In deciding a Motion to Dismiss, I accept as true the factual allegations in the Complaint. See Iannacchino v. Ford Motor Co., 451 Mass. 623, 625 n.7, 636 (2008). I need not and do not accept as true legal conclusions. See id. at 632-633. Further, I may consider documents upon which the Complaint relies and matters susceptible to judicial notice. See Polay v. McMahon, 468 Mass. 379, 381 n.3 (2014), and cases cited. Certain facts are reserved for discussion below.[3]

I. Allegations of the Shedd Complaint

A. Confidential Patient Information

Shedd filed an Amended Class Action Complaint (Shedd Complaint) on September 3, 2021. Sturdy Memorial is a 126-bed community hospital that provides a full range of inpatient and outpatient services to approximately 7,000 patients yearly. Sturdy Memorial's emergency department treats approximately 50,000 patients per year. Sturdy Memorial also operates an affiliate medical group, Sturdy Medical

[3] Issues concerning class certification are not before me. Accordingly, I do not address the class action allegations. Further, both Complaints cite to various allegedly applicable statutes and regulations and contain a significant amount of legal argument and legal conclusions, as well as explanatory information about cyber criminals and ransomware attacks, which I also do not address, unless specifically discussed below.

Associates, Inc., with more than twenty locations in Massachusetts. Sturdy Memorial employs 2,000 people and provides primary care, pediatric, oncology, emergency medicine, surgery, orthopedic, pregnancy and other medical services.

In the ordinary course of rendering healthcare, Sturdy Memorial requires patients to provide sensitive personal information including contact and demographic information, dates of birth, social security numbers, financial information, medical histories, information about other medical providers, and employment information. Sturdy Memorial also may receive information from others including the patient's other doctors, family, and friends. The provision of healthcare is conditioned on the receipt of such highly sensitive personal information.

Sturdy Memorial provides it patients with a HIPAA[4] compliant privacy notice that explains how it handles patients' sensitive and confidential information. The notice informs patients that Sturdy Memorial is required to maintain the privacy of Protected Health Information (PHI) and may not use or disclose such information without patient authorization except in limited circumstances. The notice informs patients of their right to receive notification if there is a breach of their health information. Further, Sturdy Memorial informs patients that they have a right to privacy in their PHI and the right to notification of how and when PHI is disclosed.

Patients have taken reasonable steps to maintain the confidentiality of their private information and rely on Sturdy Memorial to keep their private information confidential and secure and to use the information for authorized purposes only.

B. The Ransomware Attack

A ransomware attack uses malicious software to block access to a computer system or data, usually by encryption, coupled with a demand for the payment of a fee,

---

[4] Health Insurance Portability & Accountability Act of 1996. Pub. L. No. 104-191, 104th Cong., 2nd Sess.

or ransom, to the attacker. On February 9, 2021, Sturdy Memorial identified an incident that disrupted its IT systems and determined it was the victim of a targeted ransomware attack. Sturdy Memorial paid the ransom and re-secured its IT systems that same date.

Sturdy Memorial launched a review to determine the nature and scope of the attack. On April 21, 2021, the investigation revealed that the attackers gained access to encrypted and locked away Sturdy Memorial's patients' PII, including:

> Patients' names, addresses, phone numbers, dates of birth, Social Security numbers, Drivers' license number or other government issued identification numbers, financial account numbers, routing numbers and/or bank names, credit card numbers, and security codes, Medicare Health Insurance Claim numbers, medical history information, treatment or diagnosis information, procedure or diagnosis codes, prescription information, provider names, medical record numbers, Medicare/Medicaid numbers, health insurance information, and/or treatment cost information.

Sturdy Memorial had not encrypted the PII and Plaintiff alleges that Sturdy Memorial was targeted because it collects, creates, and maintains such PII. Due to recent high profile cybersecurity incidents at healthcare providers and companies, Sturdy Memorial should have known that its electronic records were at risk and taken steps, such as encryption, to prevent the successful ransomware attack. According to the Shedd Complaint, the Federal Trade Commission provides guidelines for businesses to protect personal information including the use of an intrusion detection system and monitors for all incoming traffic and large data transmissions, creation of a response plan, and time limitations on the maintenance of PII, among other measures. Sturdy Memorial did not implement these "basic data security practices" or comply with industry best practices.

Sturdy Memorial began notifying impacted patients on May 28, 2021, nearly four months after discovering the attack. The notice indicated that the attackers "acquired" the PII, meaning it was removed from the network. The notice informed patients and

others that, after it paid the ransom, Sturdy Memorial obtained "assurances that the information acquired would not be further distributed and that it had been destroyed." Sturdy Memorial could not definitively establish that the attackers had not copied the data before providing proof of deletion. Sturdy Memorial offered two years of credit monitoring services to affected persons.

C. Harm to Plaintiffs and Class Members

Shedd believes that her PII remains in the hands of the ransomware attackers and has been sold on the dark web[5], alleging that is the "modus operandi of all cybercriminals." Shedd alleges that she and the class members "face an increased risk of fraud and identify theft" and cites information and studies from researchers, government agencies, officials, and others regarding those alleged risks. (Compl. ¶¶ 88-108). Plaintiff alleges that "[t]here is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future." As a result, they must vigilantly monitor their financial and medical accounts for years. According to the Shedd Complaint, social security numbers and confidential medical information are among the most valuable PII on the black market.

After she received the notice from Sturdy Memorial about the ransomware attack, Shedd conducted research, reviewed credit reports and financial account

---

[5] "The dark web is a collection of thousands of websites that use anonymity tools . . . to hide their IP address. While it's most famously been used for black market drug sales and even child pornography, the Dark Web also enables anonymous whistleblowing and protects users from surveillance and censorship." Andy Greenberg, Hacker Lexicon: What Is the Dark Web? (Nov. 19, 2014), https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/; Andrew Bloomenthal, Dark Web (Updated Feb. 26, 2022), https://www.investopedia.com/terms/d/dark-web.asp ("The term dark web refers to encrypted online content that is not indexed by conventional search engines.").

statements and researched credit monitoring and identity theft protection services. She spends approximately fifteen minutes per day reviewing her bank accounts and other sensitive accounts. As of the filing of the Complaint, Shedd had spent at least seven and one-half hours on these tasks. Shedd has also suffered emotional distress from the increased anxiety of the misuse of her PII. She anticipates spending considerable time and money in an ongoing basis to mitigate and address harms. Shedd alleges that the value of her private information has been damaged and that her privacy rights have been violated. Shedd alleges that, after the ransomware attack, she experienced a significant increase in suspicious unsolicited phishing telephone calls she believes were intended to obtain personal information for "identity theft by way of social engineering" and that she and the class members face substantial risk of being targeted for future phishing and data intrusion. Finally, Shedd and the class members may also incur out of pocket costs for protective measures such as "credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack."

II. Allegations of the Bennett Complaint

Bennet filed a First Amended Class Action Complaint on December 9, 2021 (Bennett Complaint). The allegations generally track those made in the Shedd Complaint. In addition, Bennett alleges that, had Sturdy Memorial properly monitored its IT systems, it could have prevented the ransomware attack as shown by the fact that, after the attack, Sturdy Memorial implemented additional safeguards and security measures.

Sturdy Memorial did not offer two years of credit monitoring services to the class members, including named plaintiff Sandra L. Jackson-Thibodeau, whose social security numbers were not accessed. Jackson-Thibodeau alleges that she has, as a result, arranged for and paid for her own credit monitoring services.

DISCUSSION

Sturdy Memorial makes seven distinct arguments in support of its Motions. First, that allegations of an alleged risk of future harm are insufficient to state a cognizable claim for damages, a necessary element of each of the claims for relief. Second, that the G. L. c. 93A claim must be dismissed because Sturdy Memorial is a non-profit community hospital, and its data security procedures are incidental to its core function of providing medical services. Third, the negligence claims are barred by the economic loss doctrine and objective symptomatology rules. Fourth, the Plaintiffs have failed to allege facts sufficient to establish the existence of a fiduciary duty. Fifth, Plaintiff have not alleged facts sufficient to show the existence of an implied contract. Sixth, the unjust enrichment claims fail because there are alternate remedies at law. And, finally, seventh, the G. L. c. 214, § 1B claim should be dismissed because it is founded on negligence, not invasion of privacy, and Plaintiffs have failed to allege damages.

I discuss each argument in turn, applying the well-known standard, which is that in deciding a motion to dismiss pursuant to Rule 12(b)(6), I must "look beyond the conclusory allegations in the complaint," Curtis v. Herb Chambers I-95 Inc., 458 Mass. 674, 676 (2011), and determine if the nonmoving party has pleaded "factual allegations plausibly suggesting (not merely consistent with) an entitlement to relief" (citation omitted). Iannacchino, 451 Mass. at 636. In doing so, I must accept as true "all facts pleaded by the nonmoving party" (citation omitted). Jarosz v. Palmer, 436 Mass. 526, 529-530 (2002). I also must accept as true "such inferences as may be drawn [from those facts] in the [nonmoving party's] favor[.]" Blank v. Chelmsford Ob/Gyn, P.C., 420 Mass. 404, 407 (1995).

I. Motion to Dismiss for Failure to Allege Injury or Damages

The parties do not dispute that injury or damages is an element of Plaintiffs' claims of negligence, breach of fiduciary duty, breach of contract, and violation of G. L.

c. 93A. E.g., Bulwer v. Mount Auburn Hosp., 473 Mass. 672, 690 (2016); Estate of Moulton v. Puopolo, 467 Mass. 478, 492 (2014); Tyler v. Michaels Stores, Inc., 464 Mass. 492, 501–502 (2013); Cannon v. Sears, Roebuck & Co., 374 Mass. 739, 742 (1978). Nor do they dispute that unjust enrichment is the "retention of money or property of another against the fundamental principles of justice or equity and good conscience." Santagate v. Tower, 64 Mass. App. Ct. 324, 329 (2005). The parties hotly dispute whether injury or damages are sufficiently alleged in the Complaints to state these claims for relief.

Sturdy Memorial argues first that the allegations peppered throughout the Complaint that the named and class plaintiffs face the risk of identity fraud in the future because their information remains on the dark web is insufficient as a matter of law. Sturdy Memorial relies heavily on a recent Superior Court decision, John Reidy, et al. v. UMass Memorial Medical Center, Inc., WOCV2020- 01101, slip op. at 5 (Mass. Super. Ct. June 17, 2021) (Reardon, J.), in which the court dismissed class claims stemming from a ransomware attack against UMass Memorial Medical Center (UMMC). There, a third-party vendor notified UMMMC that an unauthorized party had gained access to the vendor's databases and "may have acquired a backup of a database UMMMC uses for fundraising purposes." Id. at 2. UMMMC notified its patients that identifying information may have been disclosed, but stated that "the patients' social security numbers and financial and credit card account information were not stored [at the vendor] and were not seized" and that the incident "did not involve any access to medical systems or electronic health records." Id.

The court allowed UMMMC's motion to dismiss for failure to allege any cognizable damages. Noting that the only specific allegations of harm were that the named plaintiff received several phone calls and one mail request soliciting donations and that he and other class members purchased identity theft protection, the court held that the allegations were "speculative and conclusory and do not sufficiently allege an identifiable, actual harm[.]" Id. at 4. See id. ("Reidy's assertions are, at best, abstract

concerns about possible future impairments of his rights as a patient, without actual damages, and, as such, are insufficient to state his claims[.]"). In particular, the court relied on the fact that the plaintiff had not alleged that the patients' social security numbers or any financial account information might have been accessed. Id. Indeed, the court noted that the data in the vendor's possession was the type of information used for fundraising, which UMMMC was authorized to disclose. Id. at 4-5. It was on this basis, the fact that the potentially stolen information was fundraising data, that the court held that credit monitoring costs did not constitute harm, and distinguished Donovan v. Philip Morris USA, Inc., 455 Mass. 215, 226 (2009). See id. at 5 n.6.

Plaintiffs, for their part, rely on another Superior Court decision, Walker v. Boston Med. Ctr. Corp., 33 Mass. L. Rptr. 179 (Mass. Super. Ct. 2015). In that case, Boston Medical Center informed its patients that their medical records had been made available to the public for some unknown period of time. Id. at 179. The court denied BMC's motion to dismiss for lack of standing and for failure to allege damages under Rule 12(b)(6). Id. at 180. In connection with the Mass. R. Civ. P. 12(b)(6) motion, the court held:

> Plaintiff's general allegation of injury from the data breach, inferring, as I do, that there likely was or will be access to plaintiffs' confidential medical information by unauthorized persons, is sufficient. For example, a claim for an invasion of privacy involving disclosure of confidential medical records may give rise to damages for mental distress, harm to interest in privacy and special or economic harm. Restatement (Second) of Torts § 652H (1977). Depending on the identity of a person who accessed the records, there could be financial damages. At the pleading stage, before discovery has determined whether plaintiffs' records were accessed, more specificity regarding the kind of injury suffered by plaintiffs is not required.

Id.

After careful review, I conclude that this case is more like Walker than Reidy. First, the ransomware attack in Reidy was not directed at the hospital but at a vendor which held patient information only for fundraising purposes. The Reidy court

focused carefully on the plaintiff's failure to allege that social security numbers or other financial information had been disclosed. Walker on the other hand involved the most confidential information, medical records. Here, as noted, Sturdy Memorial conceded that social security numbers and other financial data had been taken directly from Sturdy Memorial's IT systems – not a third-party – and Plaintiffs allege that confidential health information, such as medical records and prescription history information, had been taken from Sturdy. Plaintiffs further allege that these types of information are the most valuable to identity thieves. I agree with the Walker court that, drawing "every reasonable inference in favor of the plaintiff," Curtis, 458 Mass. at 676, Plaintiffs have alleged enough injury or harm to avoid dismissal.[6] See In re

---

[6] This is especially true where Plaintiffs allege, in reliance on data from the U.S. Government Accountability Office, that "stolen data may be held for up to a year or more before being used to commit identity theft."

To the extent that the parties rely on federal cases addressing Article III standing in connection with motions brought under Fed. R. Civ. P. 12(b)(1), I conclude that the Plaintiffs have, under Massachusetts law, alleged non-speculative injury such that they have standing to proceed and survive dismissal. See Pishev v. City of Somerville, 95 Mass. App. Ct. 678, 683 (2019) ("Standing is an 'elastic concept[ ]' whose meaning depends on the particular circumstances" [quoting Enos v. Secretary of Envtl. Affairs, 432 Mass. 132, 135 (2000)].). Plaintiffs' and the class members' highly confidential personal medical and financial information, including social security numbers and health information, was stolen from Sturdy Memorial. Plaintiffs have alleged the means and manner by which persons use such information on the web to conduct identity fraud and that Sturdy Memorial cannot guarantee the information was not put on the web for public use prior to having received "assurances" from the attackers. Those allegations allege sufficient *imminent* or real and immediate risk of harm to have standing to proceed. See Pugsley v. Police Dep't of Boston, 472 Mass. 367, 371 (2015) (noting that "real and immediate" risk of injury may be enough for standing); Portier v. NEO Tech. Sols., 2019 WL 7946103, at *6 (D. Mass. Dec. 31, 2019), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020) ("[A]n allegation of future injury may suffice [for standing] if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur" [citation omitted].).

Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1315 (N.D. Ga. 2019) (Applying Georgia law, denying motion to dismiss for failure to state a claim, and holding "[p]laintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief.").[7]

Having concluded that Plaintiffs have alleged sufficient injury or harm to survive dismissal, I need not address the competing arguments and cases concerning whether loss of time does or does not constitute actual damages. Compare Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 829 (7th Cir. 2018) ("[T]he principle that the time value of money is 'money or property' controls."); In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010) ("An individual's time, alone, is not legally protected from the negligence of others"). I also need not address the arguments that Plaintiffs may not recover for the alleged overpayment of health care services, or for the alleged diminution in value of the PII. Those damages claims can be fleshed out and addressed at a later stage of this proceeding or at trial.

With respect to the Plaintiffs' claim to recover the future costs of credit monitoring, Massachusetts has, unlike other jurisdictions, held that costs incurred to mitigate or prevent a substantial risk of harm are recoverable as damages in certain circumstances. In Donovan, the Supreme Judicial Court held that tobacco smokers' allegations of present injury in the form of identifiable lung damage resulting in substantially increased risk of cancer, together with allegations of causation, stated a

[7] Although not before me, I note that, at the hearing on these Motions, counsel in the Bennett case stated that he has identified a class member who has suffered identity fraud from the ransomware attack and will be moving to amend the complaint.

claim to recover the costs of medical monitoring in tort. 455 Mass. at 225-226. The Court recognized that tort law "developed in the late Nineteenth and early Twentieth centuries," and that the Court must "adapt" to permit compensation for "injury which should be compensable even if the full effects are not immediately apparent." Id. at 225.

Here, the law of damages could not contemplate the reality of 2022, that the theft of highly personal health and financial information and its disbursement on the dark web would create the real risk that a person's identity could be stolen to his or her significant detriment. Vigilant credit monitoring, like the ongoing medical monitoring in Donovan, may be the only option available for the Plaintiffs and class members to prevent, mitigate, or ameliorate that future grave harm. I conclude, analogizing to Donovan, that plaintiffs who allege that their most valuable and personal information has wrongfully been disclosed to unauthorized persons, or stolen in a ransomware attack, and which is likely to remain on the dark web (like minute changes to lung tissue), can state a claim to recover the future costs of credit monitoring (like medical monitoring) to prevent identity theft.

II. Motion to Dismiss 93A Claim[8]

Sturdy argues next that it does not operate in trade or commerce and therefore the G. L. c. 93A claim must be dismissed. I agree. General Laws c. 93A makes unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." G. L. c. 93A, § 2(a). In Lantner v. Carson, 374 Mass. 606, 611 (1978), the Supreme Judicial Court (SJC) held that the terms "person who engaged in the conduct of any trade or commerce" referred "specifically to individuals acting in a business context." In All Seasons Servs., Inc. v. Commissioner of Health & Hosps. Of Boston, 416 Mass. 269, 271 (1993), the SJC held that a charitable hospital was

[8] Both the Shedd and Bennett Complaint allege a violation of G. L. c. 93A.

not engaged in trade or commerce for purposes of G. L. c. 93A even when soliciting bids and awarding contracts "for food and vending services at its facility." The SJC considered the factors laid out in Begelfer v. Najarian, 381 Mass. 177, 190–191 (1980), and concluded that the hospital's conduct "did not take place in a business context" because it did not seek to "profit from its 'transaction'" because "[c]ontracting for food services is merely incidental to the hospital's primary function of providing medical services." All Seasons Servs., Inc., 416 Mass. at 271. Here, Sturdy Memorial is a non-profit corporation formed to operate a hospital and provide surgical and medical treatment and care of the sick and injured. Sturdy Memorial does not receive and retain confidential PII to make a profit but does so as part of its provision of medical care.

Plaintiffs rely on Linkage Corp. v. Trustees of Bos. Univ., 425 Mass. 1 (1997) and its progeny. In Linkage Corp., the SJC reiterated that "[a]n entity's 'status as a 'charitable' corporation is not, in and of itself, dispositive of the issue whether c. 93A applies.'" Id. at 23, quoting Planned Parenthood Fed'n of Am., Inc. v. Problem Pregnancy of Worcester, Inc., 398 Mass. 480, 492–493 (1986). The SJC confirmed that "each case requires examination of its own circumstances to determine whether it arose in a 'business context'" (citations omitted). Id. at 24. Applying the Begelfer factors, which include the "nature of the transaction, the character of the parties . . . , and the[ir] activities[,] . . . and whether the transaction [was] motivated by business or personal reasons[,]" 381 Mass. at 191, the SJC in Linkage Corp. concluded that Boston University had engaged in trade or business in the circumstances of that case. 425 Mass. at 24. The Court reiterated, however, that "[i]n most circumstances, a charitable institution will not be engaged in trade or commerce when it undertakes activities *in furtherance of its core mission*" [emphasis added]. Id. at 26.

Here, there are no factual allegations that would take the receipt and maintenance of confidential patient information, necessary to render and bill for

medical services, outside of Sturdy Memorial's core mission. Sturdy Memorial must obtain information from its clients to provide medical care. It must keep that information confidential under state and federal law. The alleged failure to do so does not make that *conduct*, namely the receipt and maintenance of confidential information, conduct in trade or commerce. It is conduct in furtherance of Sturdy Memorial's core mission of providing health care. The Motion to Dismiss the G. L. c. 93A claim must be ALLOWED.

III. Motion to Dismiss Negligence Claim[9]

Sturdy Memorial argues next that all the Plaintiffs' and class members' damages consist of economic or emotional damages which are not recoverable on a theory of negligence. The economic loss doctrine bars recovery of economic damages on a claim of negligence, "unless the plaintiffs can establish that the injuries they suffered due to the defendant['s] negligence involved physical harm or property damage, and not solely economic loss." Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 455 Mass. 458, 469 (2009), citing Aldrich v. ADD Inc., 437 Mass. 213, 222 (2002), quoting FMR Corp. v. Boston Edison Co., 415 Mass. 393, 395 (1993) ("purely economic losses are unrecoverable in tort . . . actions").

In Cumis, credit unions sued after a data breach at BJ's Wholesale Club, Inc. stores. Id. at 459. Thieves stole magnetic stripe data from credit card holders who had purchased merchandise and used the data to engage in "fraudulent credit card transactions worth millions of dollars." Id. The credit unions sued to recover costs they incurred to cancel and reissue new credit cards. Id. at 459-460. The SJC affirmed the dismissal of the credit unions' negligence claims based on the economic loss doctrine. Id. at 470. Similarly, the First Circuit relied on Cumis in upholding the dismissal of negligence claims brought by banks against TJX Companies, Inc. for a data

[9] Both the Shedd and Bennett Complaint assert a claim for negligence.

breach under the economic loss doctrine. In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009), as amended on rehearing in part, (May 5, 2009) (TJX Companies).

Those cases lead to the conclusion that the Plaintiffs' negligence claims here must similarly be dismissed based on the economic loss doctrine. However, Plaintiffs rely on the thorough and well-reasoned decision in Portier v. NEO Tech. Solutions, 2019 WL 7946103 (D. Mass. Dec. 31, 2019), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020). There, the court refused to dismiss negligence claims that plaintiff/employees brought against their employers stemming from the disclosure of "the employees' 2016 Internal Revenue Service ('IRS') Form W-2 information, including their Social Security numbers, to an unauthorized third party" based on the economic loss doctrine. Id. at *1, *18. The court recognized that Cumis and TJX Companies dismissed similar claims based on the economic loss doctrine, but noted that the plaintiffs in both of those cases were banks or credit unions. Id. The court further noted that the "[d]efendants have not identified any case that applied Massachusetts' view of the economic loss doctrine to a claim for negligence based on the theft and misuse of employees' PII that they entrusted to their employer as a condition of employment, and the court has not found any." Id.

Because the facts in Cumis and TJX Companies were distinguishable, and "because the legal landscape concerning liability for data breaches and identity theft is substantially different than it was when [those cases] were decided ten years ago, and because the application of the economic loss doctrine in Massachusetts and Pennsylvania has been similar," the Portier court determined that the "Massachusetts appellate courts would likely follow a recent decision of the Pennsylvania Supreme Court, which permitted recovery for pecuniary losses caused by negligence in a case with comparable facts." Id., citing Dittman v. UPMC, 196 A.3d 1036, 1056 (Pa. 2018).

The Portier court noted that (i) "Massachusetts permits recovery of purely economic losses for a range [of] torts," (ii) "courts applying Massachusetts law have examined the source of the duty that was allegedly breached and have permitted recovery in tort if the duty arises independently of a party's contractual obligations[,]" and (iii) there is authority stating that "Massachusetts courts have declined to apply the economic loss doctrine to tort claims against a fiduciary" (citations and quotations omitted). Id. at *21. Given that legal landscape, and based on the allegations of the Complaint, namely that the employers had "exclusive control over their employees' PII that it collected and stored," the employees were "powerless to protect their PII [and] relied on [the employer] to safeguard their PII from cyber thieves, and [the employer] should have reasonably foreseen the harm that befell Plaintiffs when it failed to adequately secure their PII," the Portier court concluded that the SJC would not apply the economic loss doctrine to the employees' claims.[10] Id. at *21-*22.

I find the analysis in Portier persuasive. Cumis and TJX Companies are distinguishable. Here, the harm at issue is not limited to the unlawful and fraudulent use of credit card information. Given the disclosure of social security numbers, financial information, and confidential medical information, the harm to the Plaintiffs is much greater. There is no appellate authority directly on point regarding the application of the economic loss doctrine in the circumstances presented here, namely, where patients are required to provide highly sensitive PII to a hospital to obtain medical care, are powerless to protect that information but rely on the hospital to do so consistent with state and federal law, and the hospital should reasonably have foreseen

[10] The court recognized "the difficulty of predicting the course the SJC would follow with respect to the application of the economic loss doctrine to Plaintiffs' negligence claims" and made clear that the presiding district court judge could certify the question to the SJC if the judge determined that the course the SJC would take was not reasonably clear. Portier, 2019 WL 7946103, at *22.

and guarded against the risk of disclosure. In those circumstances, there may well be a "special relationship" eliminating the application of the economic loss doctrine.

Finally, both the internet and the ability to use and abuse information contained on the dark web has changed drastically in the twelve years since Cumis was decided. Accordingly, on this record, and at this stage of the proceeding, dismissal of the negligence claims based on the economic loss doctrine is not appropriate.[11]

IV. Motion to Dismiss Breach of Fiduciary Duty Claim

Sturdy Memorial argues next that the claim for breach of fiduciary duty in the Shedd Complaint must be dismissed because Sturdy Memorial did not owe its patients such a duty as a matter of law. "A fiduciary relationship is one founded on the trust and confidence reposed by one party in the integrity and fidelity of another." Estate of Moulton, 467 Mass. at 492, citing Locator Servs. Group, Ltd. v. Treasurer & Receiver Gen., 443 Mass. 837, 853–855 (2005), and cases cited. "Although some fiduciary relationships, such as that between guardian and ward, are created by law, others arise from the nature of the parties' interactions. The 'circumstances which may create a fiduciary relationship are so varied that it would be unwise to attempt the formulation of any comprehensive definition that could be uniformly applied in every case.'" Germain v. Girard, 72 Mass. App. Ct. 409, 413 (2008), quoting Doe v. Harbor Schs., Inc., 446 Mass. 245, 252 (2006), quoting in turn, Warsofsky v. Sherman, 326 Mass. 290, 292 (1950). "It is for this reason that the determination of whether a fiduciary duty exists is largely fact specific" (internal quotations and citation omitted). Baker v. Wilmer Cutler

---

[11] Having concluded that the negligence claim survives, I need not address the argument regarding the "objective symptomology" doctrine to the recovery of emotional distress damages in the absence of physical harm manifested by objective symptomatology. See Nancy P. v. D'Amato, 401 Mass. 516, 519 (1988) ("[A] plaintiff may not recover for negligent infliction of emotional distress unless she has suffered physical harm."). Any claim to recover for emotional distress damages can await summary judgment.

Pickering Hale & Dorr LLP, 91 Mass. App. Ct. 835, 846 (2017). "[F]iduciary duties may arise wherever 'faith, confidence, and trust' is reposed by one party 'in another's judgment and advice.'" UBS Fin. Servs., Inc. v. Aliberti, 483 Mass. 396, 408, (2019), citing Doe, 446 Mass. at 252.

The Shedd Complaint alleges that "Plaintiff and the Class Members relied on [Sturdy Memorial] to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information." After careful review of the Complaints, which I accept as true for purposes of this motion, and taking all reasonable inferences in the Plaintiffs' favor, I cannot conclude that Plaintiff has failed to state a claim of breach of fiduciary duty in connection with Sturdy Memorial's failure to protect highly confidential information in its database from a ransomware attack. See Adams v. Congress Auto Ins. Agency, Inc., 90 Mass. App. Ct. 761, 766 (2016) (defendant insurance agency had a duty to the plaintiff, "a member of a large but clearly defined class of third parties, to prevent its employee's foreseeable misuse of the information that [plaintiff] provided to process his automobile insurance claim"). Whether or not the relationship here was sufficient to give rise to a fiduciary duty cannot be decided on a Motion to Dismiss but, as it is so deeply fact specific, must await further development.

V. Motion to Dismiss Implied Contract Claim

Sturdy Memorial argues next that the claim for breach of an implied contract in the Shedd Complaint must be dismissed for failure to allege mutual assent. Shedd alleges that "[w]hen Plaintiff and Class Members provided their Private Information to Sturdy [Memorial] in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information" and they "reasonably believed and expected that Defendant's data security practices complied with relevant federal and state laws and regulations and

were consistent with industry standards" and that "Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure." Sturdy Memorial argues that, because the Shedd Complaint does not contain allegations that she read or relied on Sturdy Memorial's documents or statements regarding data security, the Complaint fails to state a claim for relief. I disagree.

"In the absence of an express agreement, a contract implied in fact may be found to exist from the conduct and relations of the parties." Sullivan v. O'Connor, 81 Mass. App. Ct. 200, 212 (2012), quoting LiDonni, Inc. v. Hart, 355 Mass. 580, 583 (1969). See id. at 212-213 (finding an implied contract to pay assessments to neighborhood association because plaintiffs purchased property with actual knowledge of the association and its services). "[A] contract implied in law is an obligation created by law 'for reasons of justice, without any expression of assent and sometimes even against a clear expression of dissent . . . . [C]onsiderations of equity and morality play a large part ... in constructing a quasi-contract.'" Id. at 212, quoting Salamon v. Terra, 394 Mass. 857, 859, quoting in turn, 1 Corbin, Contracts § 19 (1963).

Here, Shedd provided the PII to Sturdy Memorial to obtain medical and healthcare information, and Sturdy Memorial took receipt of the information to provide (and bill for) such health care. Shedd alleges that she understood that Sturdy Memorial would keep her confidential information safe and acted in reliance on that understanding. Although the court was applying California law, I agree with the reasoning in Castillo v. Seagate Tech., LLC, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016), a case involving an employer's disclosure of confidential employee data, including W-2 data, in response to a phishing scam. In declining to dismiss the breach of implied contract claim, the court stated:

> The upshot of the averments in the plaintiffs' complaint however, is quite clear: The employees provided their personal information for tax purposes

> and to receive employment and benefits, with the understanding that Seagate, while it held the information, would take adequate measures to protect it. Seagate received the personal information so that it could employ the plaintiffs, and provide them with employment and benefits. While Seagate made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently.

Id. at *9. See id. ("Plaintiffs' claim is a far more realistic reflection of the mutual agreement that occurs in most data-sharing transactions: When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected.")

Here, the claim is similarly simple. When a patient hands over sensitive information to receive medical care, they expect an implicit assurance that the information will be protected. In the absence of cases in the Commonwealth (state or federal) addressing this issue, namely whether there can be an implied contract by a hospital to safeguard PII disclosed by patients, on this record and stage of the proceeding, dismissal is not appropriate.

VI. Motion to Dismiss Claim of Unjust Enrichment[12]

To support their unjust enrichment claim, Shedd alleges that she and the class members "conferred a benefit on Defendant, by paying Defendant money for healthcare services, a portion of which was to have been used for data security measures to secure" the PII but Sturdy Memorial enriched itself by not using the funds to provide a reasonable level of security. The Bennett Complaint similarly alleges that "Plaintiffs and class members conferred a monetary benefit on Defendant, either by paying Defendant money, or by the advantages that accrued to Defendant through having

[12] Both the Shedd and Bennett Complaint assert a claim for unjust enrichment.

Plaintiffs and the Class's PII or Defendant's participation in a group of healthcare providers for purposes of coordinating patient care . . . ."

"Unjust enrichment is defined as retention of money or property of another against the fundamental principles of justice or equity and good conscience.'" Santagate, 64 Mass. App. Ct. at 329, quoting Taylor Woodrow Blitman Constr. Corp. v. Southfield Gardens Co., 534 F.Supp. 340, 347 (D.Mass. 1982), quoting in turn, 66 Am.Jur.2d Restitution and Implied Contracts § 3 (1962). "An equitable remedy for unjust enrichment is not available to a party with an adequate remedy at law" (citations omitted). Id. Sturdy Memorial moves to dismiss the unjust enrichment claim arguing that Plaintiffs have an adequate remedy at law. That argument fails for three reasons.

> First a claim of unjust enrichment can accompany a claim for breach of contract.
>
> (1) If a deliberate breach of contract results in profit to the defaulting promisor and the available damage remedy affords inadequate protection to the promisee's contractual entitlement, the promisee has a claim to restitution of the profit realized by the promisor as a result of the breach. Restitution by the rule of this section is an alternative to a remedy in damages.
> (2) A case in which damages afford inadequate protection to the promisee's contractual entitlement is ordinarily one in which damages will not permit the promisee to acquire a full equivalent to the promised performance in a substitute transaction.
> (3) Breach of contract is profitable when it results in gains to the defendant (net of potential liability in damages) greater than the defendant would have realized from performance of the contract. Profits from breach include saved expenditure and consequential gains that the defendant would not have realized but for the breach, as measured by the rules that apply in other cases of disgorgement (§ 51(5)).

Restatement (Third) of Restitution and Unjust Enrichment § 39 (2011). See id. at cmt. a ("Compared to other forms of legal entitlement, contract rights may often be easier to value in money; but they would be vulnerable to the same risks of underenforcement if the exclusive remedy for breach were an action for money damages[.] . . . Restitution

affords comparable protection after the fact, awarding the gains from a profitable breach of a contract that the defendant can no longer be required to perform.").

Second, "[a] determination of unjust enrichment is one in which '[c]onsiderations of equity and morality play a large part'" (citation omitted). Metropolitan Life Ins. Co. v. Cotter, 464 Mass. 623, 644 (2013). "A plaintiff asserting a claim for unjust enrichment must establish not only that the defendant received a benefit, but also that such a benefit was unjust, 'a quality that turns on the reasonable expectations of the parties.'" Id., quoting Global Investors Agent Corp. v. National Fire Ins. Co., 76 Mass. App. Ct. 812, 826 (2010), quoting in turn, Community Builders, Inc. v. Indian Motorcycle Assocs., Inc., 44 Mass. App. Ct. 537, 560 (1998). Determination of the justness or unjustness of Sturdy Memorial's retention of funds paid, as Plaintiffs allege, in part for data security, cannot be decided on a motion to dismiss.

Third, Plaintiffs can plead in the alternative. Here, where there are competing tort and contract-based claims, at this stage of the proceeding, and where I must make all reasonable inferences from the facts alleged in the Plaintiffs favor, it would be inappropriate to dismiss the unjust enrichment claim simply because Plaintiffs have asserted as well claims of breach of implied contract, and or statutory and tort-based claims for relief.

VII. Motion to Dismiss Invasion of Privacy Claim

General Laws c. 214, § 1B provides: "A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages." To succeed on a claim under the statute, a "plaintiff must show that there was a "gathering and dissemination of information which [she contends] was private" (quotations and citation omitted). Nelson v. Salem State Coll., 446 Mass. 525, 536 (2006). Plaintiffs allege that unauthorized persons gained access to their personal and highly confidential information due to Sturdy Memorial's inadequate, negligent

and/or intentionally insufficient security measures. Although negligence is a tort separate from invasion of privacy, as Sturdy Memorial argues, at the pleading stage, Plaintiffs may plead in the alternative. They have stated a claim for invasion of privacy.

ORDER

For the foregoing reasons, Defendant's Motions to Dismiss are **ALLOWED** as to the claims asserted pursuant to G. L. c. 93A and otherwise **DENIED**.

/S/ Debra Squires-Lee
Debra A. Squires-Lee
Justice of the Superior Court

April 5, 2022