IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

IN RE: BLACKBAUD, INC., CUSTOMER DATA BREACH LITIGATION	Case No.: 3:20-mn-02972-JMC MDL No. 2972 **ORDER AND OPINION**

THIS DOCUMENT RELATES TO: ALL ACTIONS:

This matter is before the court on Defendant Blackbaud, Inc.'s ("Blackbaud") Motion to Dismiss four (4) of Plaintiffs' common law claims pursuant to Federal Rule of Civil Procedure 12(b)(6). (ECF No. 124.) For the reasons set forth below, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion. (*Id.*)

I. RELEVANT BACKGROUND

Blackbaud is a publicly traded cloud software company incorporated in Delaware and headquartered in Charleston, South Carolina. (ECF No. 77 at 110–11 ¶ 419, 112 ¶ 424.) The company provides data collection and maintenance software solutions for administration, fundraising, marketing, and analytics to social good entities such as non-profit organizations, foundations, educational institutions, faith communities, and healthcare organizations ("Social Good Entities"). (*Id.* at 4 ¶ 4, 114 ¶ 430.) Blackbaud's services include collecting and storing Personally Identifiable Information ("PII") and Protected Health Information ("PHI") from its customers' donors, patients, students, and congregants. (*Id.* at 3 ¶ 2, 114 ¶ 429.)

In this action, Plaintiffs represent a putative class of individuals whose data was provided to Blackbaud's customers and managed by Blackbaud. (*Id.* at 6 ¶ 12.) Thus, Plaintiffs are patrons

of Blackbaud's customers rather than direct customers of Blackbaud. (ECF Nos. 92-1 at 9; 109 at 7–8.) Plaintiffs assert that, from February 7, 2020 to May 20, 2020, cybercriminals orchestrated a two-part ransomware attack on Blackbaud's systems ("Ransomware Attack"). (ECF No. 77 at 11–12 ¶ 25.) Cybercriminals first infiltrated Blackbaud's computer networks, copied Plaintiffs' data, and held it for ransom. (*Id.* at 11 ¶ 25, 137 ¶ 496; ECF No. 92-1 at 7.) When the Ransomware Attack was discovered in May 2020, the cybercriminals then attempted but failed to block Blackbaud from accessing its own systems. (*Id.*) Blackbaud ultimately paid the ransom in an undisclosed amount of Bitcoin in exchange for a commitment that any data previously accessed by the cybercriminals was permanently destroyed. (ECF Nos. 77 at 9 ¶ 20, 138 ¶ 499; 92-1 at 7.)

Plaintiffs maintain that the Ransomware Attack resulted from Blackbaud's "deficient security program[.]" (ECF No. 77 at 117–18 ¶ 439.) They assert that Blackbaud failed to comply with industry and regulatory standards by neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields. (*Id.* at 117–18 ¶ 439, 134 ¶ 486, 136 ¶ 491, 142 ¶ 510.)

Plaintiffs further allege that after the Ransomware Attack, Blackbaud launched a narrow internal investigation into the attack that analyzed a limited number of Blackbaud systems and did not address the full scope of the attack. (*Id.* at 143 ¶ 514.) Plaintiffs contend that Blackbaud failed to provide them with timely and adequate notice of the Ransomware Attack and the extent of the resulting data breach. (*Id.* at 130–31 ¶ 473.) They claim that they did not receive notice of the Ransomware Attack "until July of 2020 at the earliest[.]" (*Id.* at 156 ¶ 555.) Plaintiffs allege that they subsequently received notices of the Ransomware Attack from various Blackbaud customers at different points in time from July 2020 to January 2021. (*See, e.g.*, *id.* at 25 ¶ 63, 29 ¶ 82, 32 ¶ 93, 109 ¶ 414.) Plaintiffs maintain that although Blackbaud initially represented that sensitive

information such as SSNs and bank account numbers were not compromised in the Ransomware Attack, Blackbaud informed certain customers in September and October 2020 that SSNs and other sensitive data were in fact stolen in the breach. (*Id.* at 141–42 ¶ 509.) Additionally, on September 29, 2020, Blackbaud filed a Form 8-K with the Securities and Exchange Commission stating that SSNs, bank account information, usernames, and passwords may have been exfiltrated during the Ransomware Attack. (*Id.* at 12 ¶ 26, 143 ¶ 512.)

After the Ransomware Attack was made public, putative class actions arising out of the intrusion into Blackbaud's systems and subsequent data breach were filed in state and federal courts across the country. (ECF No. 1 at 1.) On December 15, 2020, the Judicial Panel on Multidistrict Litigation consolidated all federal litigation related to the Ransomware Attack into this multidistrict litigation ("MDL") for coordinated pretrial proceedings.[1] (*Id.* at 3.)

On April 2, 2021, thirty-four (34) named Plaintiffs[2] from twenty (20) states filed a Consolidated Class Action Complaint ("CCAC") alleging that their PII and/or PHI was compromised during the Ransomware Attack. (ECF No. 77.)[3] They assert six (6) claims on behalf of a putative nationwide class as well as ninety-one (91) statutory claims on behalf of putative state subclasses. (*Id.* at 173 ¶ 627 – 424 ¶ 1815.)

To facilitate the efficient resolution of the litigation, the court ordered various phases of motions practice to address jurisdictional issues, certain statutory claims, and specific common law claims. (ECF Nos. 23 at 2; 78 at 1.) This phase addresses the common law claims. Blackbaud

[1] As of October 19, 2021, this MDL is comprised of twenty-nine (29) member cases.

[2] The named Plaintiffs are identified in paragraphs 45 through 418 of the CCAC. (*See* ECF No. 77 at 20 ¶ 45 – 110 ¶ 418.) Since the CCAC was filed, Plaintiff Rosalie Simkins voluntarily dismissed her individual claims on September 17, 2021. *See Simkins v. Blackbaud, Inc.*, No. 3:21-cv-00431-JMC (ECF No. 72).

[3] The CCAC supersedes all other complaints in this MDL filed on behalf of Blackbaud's customer's patrons against Blackbaud. (ECF Nos. 23 at 4; 77.)

filed the instant Motion to Dismiss pursuant to Rule 12(b)(6) on July 9, 2021, contending that Plaintiffs' negligence, negligence *per se*, gross negligence, and unjust enrichment claims should be dismissed for failure to state a claim. (ECF No. 124.) Plaintiffs filed a Response on August 9, 2021. (ECF No. 142.) The court held a hearing on the Motion to Dismiss on September 2, 2021. (ECF No. 147.)

II. LEGAL STANDARD

A. Applicable Law

1. Choice of Law: Negligence, Negligence Per Se, and Gross Negligence

The parties have stipulated to the application of South Carolina choice of law principles. (ECF No. 93.) For tort claims, South Carolina uses the *lex loci delicti* analysis of the First Restatement of Conflict of Laws. The goals of the First Restatement were to "reduce forum shopping and increase predictability and uniformity" of result. *See* Yasamine J. Christopherson, *Conflicted About Conflicts? A Simple Introduction to Conflicts of Laws*, 21 S.C. LAW. 30, Sept. 2009, at 31. Under the traditional or "vested-rights" rule, "the cause of action was considered to be created in the state of the tort, and the capacity to sue or immunity or defense was considered part and parcel of those rights." 29 A.L.R.3d 603 (1970); *see also Trahan v. E.R. Squibb & Sons, Inc.*, 567 F. Supp. 505, 508 (M.D. Tenn. 1983) ("The *lex loci* doctrine is derived from the vested right approach which holds that a plaintiff's cause of action 'owes its creation to the law of the jurisdiction where the injury occurred and depends for its existence and extent solely on such law.'") (quoting *Winters v. Maxey*, 481 S.W.2d 755, 756 (Tenn. 1972)). Accordingly, under the traditional *lex loci delicti* test, the court applies "the law of the place in which the event occurred that created the right on which the party brings suit." *Choice of Law in Tort and Contract Actions Chart, Practical Law Checklist*, 2-558-2049, THOMAS REUTERS (Oct. 18, 2021).

Here, Plaintiffs assert the place of wrong is South Carolina because the last act making Blackbaud liable in tort was its negligent conduct in South Carolina where it "manages, maintains, and provides cloud computing software, services, and cybersecurity." (ECF No. 142 at 20 (citing ECF No. 77).) Conversely, Blackbaud contends the last event necessary was Plaintiffs' injuries and that the injuries must have occurred in Plaintiffs' respective home states. (ECF No. 124-1 at 23 (citing *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *41 (D. Or. July 29, 2019); *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1153 (W.D. Wash. 2017)).)

The acts and events necessary to constitute a tort is a question of law that varies depending on the state. RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 377 cmt. a (AM. L. INST. 1934). Under South Carolina's choice of law rules, the place of wrong is the location where the injury occurred, which is not necessarily the domicile of the plaintiffs. *Rogers v. Lee*, 777 S.E.2d 402, 407 (S.C. Ct. App. 2015) ("[W]e are not persuaded our courts should blindly apply the residence of a plaintiff in a legal malpractice claim as the location of the injury"). Further, under South Carolina law, "*lex loci delicti* is determined by the state in which *the injury occurred*, not where the results of the injury were felt or where the damages manifested themselves." *Id.* at 405 (emphasis original).

Determination of the last act necessary to identify the place of wrong "necessarily turns on the elements of the specific tort at issue." *Cockrum v. Donald J. Trump for President, Inc.*, 365 F. Supp. 3d 652, 667 (E.D. Va. 2019). The elements of negligence are duty, breach, causation, and damages. *Savannah Bank, N.A. v. Stalliard*, 734 S.E.2d 161, 163–64 (S.C. 2012) (citing *Thomasko v. Poole*, 561 S.E.2d 597, 599 (S.C. 2002); *Kleckley v. Nw. Nat'l Cas. Co.*, 526 S.E.2d 218, 221 (S.C. 2000). Thus, the last event necessary for a defendant to be liable for negligence is damage

to the plaintiff. *See Bank of Louisiana v. Marriott Int'l, Inc.*, 438 F. Supp. 3d 433, 443 (D. Md. 2020) (claim for negligence would not exist without injury); *Cockrum v. Donald J. Trump for President, Inc.*, 365 F. Supp. 3d at 667–68 (looking to the "point of completion" of the specific tort at issue to determine the place of wrong); *Tolman v. Stryker Corp.*, 926 F. Supp. 2d 1255, 1258–59 (D. Wyo. 2013) (the last event necessary for negligence claims is the injury). Plaintiffs allege that they "have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach." (ECF No. 77 at 156 ¶ 555.) Plaintiffs assert they have suffered injuries arising from Blackbaud's negligence in the form of risk of extortion (*id.* ¶ 560), unauthorized disclosure of their Private Information to third-party cybercriminals (*id.* ¶ 563), loss of value in their Private Information (*id.* ¶ 564), risk of future identity theft or fraud (*id.* ¶ 566), and out-of-pocket mitigation expenses (*id.* ¶¶ 568–70).

The alleged risk of identity theft and diminished value of data occurred when Plaintiffs' Private Information was exposed. The actual identity theft, emotional distress, and time and/or money spent to mitigate the harm all manifest from the initial injury—the exposure of Plaintiffs' Private Information. Thus, Plaintiffs' alleged injury—and the last event necessary for Blackbaud to be potentially liable in tort—was the data being accessed by a third party. *See Rogers v. Lee*, 777 S.E.2d at 405 (citing *Boone v. Boone*, 546 S.E.2d 191, 193 (S.C. 2001)); *Gray v. S. Facilities, Inc.*, 183 S.E.2d 438, 442 (S.C. 1971) ("[A] cause of action for negligence occurs only when injury or damage have been caused thereby to the complaining party.") Therefore, to determine the place of wrong for the choice of law analysis, the court must determine where the breach occurred.

Nothing in the CCAC (ECF No. 77), Blackbaud's Motion to Dismiss (ECF No 124), or Plaintiffs' Response in Opposition (ECF No. 142) indicates how or where the data breach took

place. (*See* ECF No. 77 at 155 ¶ 551 (noting that both Blackbaud and the forensic report[4] stop short of identifying "the original point of intrusion—that is how the Data Breach began in the first instance").) The fact that Blackbaud's headquarters is in South Carolina might suggest that its servers are in this state or that the hackers entered its system here, but the court cannot make that determination based upon the present record. (*See* ECF No. 77 at 172 ¶ 625 ("Blackbaud maintained and maintains servers in several states . . .").) Additionally, neither of the parties allege any facts to support an inference that the breach occurred in Plaintiffs' respective home states. Because it is presently unclear where the breach occurred, the court will apply South Carolina law with respect to Plaintiffs' common law claims for negligence, gross negligence, and negligence *per se*.[5]

Application of South Carolina law, as the law of the forum, is proper because the place of the breach cannot be determined without further discovery and South Carolina is the only Blackbaud location specifically enumerated in the record. *See Cockrum*, 365 F. Supp. 3d at 670; *cf. In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 393 (E.D. Va. 2020)

[4] As part of its internal investigation into the Ransomware Attack, Blackbaud obtained a forensic report and provided a redacted version to Plaintiffs pursuant to a court order. (ECF No. 61.)

[5] The court observes that some courts have postponed determination of choice of law issues at the motion to dismiss stage, noting the difficulty of locating the place of wrong without a complete record. *See Santee-Lynches Affordable Hous. & Cmty. Dev. Corp. v. Ellinger*, No. 3:09-cv-01015-CMC, 2010 WL 670096, at *2 (D.S.C. Feb. 22, 2010) (declining to resolve the choice of law issue until motion was renewed with further argument from the parties); *Malinoswki v. Lichter Grp., LLC*, No. WDQ-14-917, 2015 WL 1129522, at *4 (D. Md. March 11, 2015) (applying forum law to the motion to dismiss and explaining that "[g]iven the fact-intensive, context specific and complexity of the choice-of-law analysis, consideration of what law governs . . . may be properly deferred until after the parties have engaged in discovery") (internal quotations omitted). Other courts, however, have made choice of law findings for the purpose of ruling on motions to dismiss, and noted facts developed during discovery may change the choice of law finding. *See Advanced Comm. Credit Int'l (ACI) Ltd. v. Citisculpt, LLC*, No. 6:17-cv-69-AMQ, 2018 WL 2149296, at *4 n.1 (D.S.C. May 10, 2018) (explaining that its choice of law finding was "not intended to serve as a final determination of choice of law issues for all purposes" in the case if different facts developed during discovery).

(applying the law of each jurisdiction where a representative plaintiff resided for the purpose of the motion to dismiss).

In *Cockrum*, the plaintiffs brought claims for private disclosure of public facts resulting from the unauthorized publication of their personal information on the internet. 365 F. Supp. 3d at 654–55. The plaintiffs allege that their information was illegally obtained by a third party who conspired with the defendant to release the information via WikiLeaks. *Id.* at 655. The plaintiffs argued their home states constituted the place of wrong because the tort of private disclosure of public facts was completed when they were injured in their respective home states. *Id.* at 667. The court determined that injury to the plaintiff was not an element of public disclosure of private facts. *Id.* at 668. Because no actual injury is required, the tort was complete upon the publishing of the information. *Id.* As such, the defendant contended that the place of wrong must be the state where it was headquartered. *Id.* at 670. The court noted, however, that the plaintiffs did not allege that the defendant physically published their information. *Id.* Instead, the plaintiffs alleged the publication was done by a third party (Wikileaks) at an undisclosed location. *Id.*

Ultimately, the court found that it could not determine where the publication occurred based on the amended complaint and, as a result, the court applied the law of the forum. *Id.* In so doing, the court explained that "[a]lthough neither the Supreme Court of Virginia nor the Fourth Circuit have resolved this point, numerous district courts in Virginia have applied the law of the forum state in a situation in which they were unable to determine the place of the wrong from the pleadings." *Id.* at 670 n.17 (citing *Jeffrey J. Nelson & Assocs. v. LePore*, No. 4:11cv75, 2012 WL 2673242, at *7 (E.D. Va. July 5, 2012) ("Because it is presently unclear where the allegedly wrongful acts took place, the Court will also apply [forum law]."); O*verstock.com, Inc. v. Visocky*, No. 1:17-cv-1331, 2018 WL 5075511, at *9 n.5 (E.D. Va. Aug. 23, 2018) ("[B]ecause Plaintiff

has provided no information upon which to conduct a formal choice-of-law analysis, the undersigned will utilize Virginia law, as the law of the forum state . . .")).

At this stage in the litigation, applying South Carolina law is also supported by the policy behind the *lex loci delicti* law analysis.

> The long-time traditional reasons and arguments advanced for following, adopting, or adhering to the *lex loci* rule have been that it is relatively easy to apply, furnishes certainty and predictability of outcome (thus aiding litigants, lawyers, and insurers in assessing rights, liabilities, defenses, and damages), and, in addition is symmetrical—all persons injured, etc., in a single incident will have their rights adjusted by the same law.

1 AMERICAN LAW OF TORTS § 2:9 (1970); *see also* 29 A.L.R.3d 603 ("The cardinal virtue of the traditional rule was its certainty, ease of application, and predictability."). Employing South Carolina law, as the law of the forum and the law of the state where Blackbaud is headquartered, meets the goals of the *lex loci delicti* approach by providing uniformity of results for Plaintiffs and predictability for all parties. Accordingly, the court will apply South Carolina law, for the purpose of the present motion, to determine whether Plaintiffs have stated claims for negligence, gross negligence, and negligence *per se*.

2. *Choice of Law: Unjust Enrichment*

Unlike the choice of law analysis applicable to tort claims, it is unclear whether South Carolina would apply the First or Second Restatement's choice of law analysis to unjust enrichment claims. *See Ashmore v. Dodds*, 262 F. Supp. 3d 341, 365 (D.S.C. 2017); *Thomerson v. DeVito*, 844 S.E.2d 378, 384 n.11 (S.C. 2020) (noting that claims for unjust enrichment do not belong to either the category of contract or tort) (citing *Quasi-Contract*, *Black's Law Dictionary* (11th ed. 2019)). The court finds the result would be the same under either Restatement test and, therefore, it is unnecessary to determine which test South Carolina would apply to unjust enrichment claims.

Under the First Restatement of Conflict of Laws, "[w]hen a person is alleged to have been unjustly enriched, the law of the place of enrichment determines whether he is under a duty to repay the amount by which he has been enriched." RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 453. Alternatively, the Second Restatement provides that "[i]n actions for restitution, the rights and liabilities of the parties with respect to the particular issue are determined by the local law of the state which, with respect to that issue, has the most significant relationship to the occurrence and the parties under the principles stated in § 6."[6] RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 221(1) (AM. L. INST. 1971). Factors to consider under this approach include: (1) "the place where a relationship between the parties was centered"; (2) the place where the benefit was received; (3) the place where the acts conferring the benefit were done; and (4) the domicile, place of incorporation and place of business of the parties. *Id.* at § 221(2). These contacts are to be evaluated according to their relative importance with respect to the particular issue. *Id.* at § 221. The Second Restatement also notes that "[t]he place where a relationship between the parties was centered . . . is the contact that, as to most issues, is given the greatest weight in determining the state of the applicable law." *Id.* at cmt. d. Where the claim to restitution does not stem from any relationship between the parties, [however,] the place where the benefit or enrichment was received "will usually be that of greatest importance with respect to most issues." *Id.*; *see also Calloway Golf Co. v. Dunlop Slazenger Grp. Americas, Inc.*, 295 F. Supp. 2d 430, 434–35 (D. Del. 2003) ("Because [Counter-Plaintiff's] claim to restitution does not stem from any relationship between the parties and the alleged benefit of enrichment was received in California, [Counter-

[6] Under South Carolina law, the terms contract implied-in-law, quantum meruit, quasi-contract, restitution, and unjust enrichment have often been used interchangeably to refer to the same type of claim for equitable relief. *See Gignilliat v. Gignilliat, Savitz & Bettis, L.L.P.*, 684 S.E.2d 756, 764 (S.C. 2009).

Defendant's] principal place of business, the court will apply California law to [the] unjust enrichment claim."); *Int'l Brotherhood of Teamsters Loc. 456 Health & Welfare Tr. Fund v. Quest Diagnostics*, No. 10-cv-1692, 2012 WL 13202126, at *26 (E.D.N.Y. April 19, 2012) ("[W]here there is no relationship between the parties, the Restatement gives great weight to 'the place where the benefit or enrichment was received.'").

Here, Plaintiffs do not allege they have a direct or contractual relationship with Blackbaud.[7] Accordingly, the court's focus under either Restatement test for unjust enrichment claims is on the place where the benefit was received. Blackbaud's headquarters and principal place of business is in South Carolina, therefore Blackbaud received any alleged benefit in South Carolina. Accordingly, South Carolina law applies to determine whether Plaintiffs have stated claims for unjust enrichment.

B. Motion to Dismiss

A motion to dismiss pursuant to Rule 12(b)(6) "challenges the legal sufficiency of a complaint." *Francis v. Giacomelli*, 588 F.3d 186, 192 (4th Cir. 2009). It is not intended to "resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses." *Presley v. City of Charlottesville*, 464 F.3d 480, 483 (4th Cir. 2006) (quoting *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999)).

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). Thus, "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible

[7] Plaintiffs allege they have a special relationship with Blackbaud independent of any contract arising from Blackbaud "being entrusted with [Plaintiffs'] Private Information, which provided an independent duty of care." (ECF No. 77 at 130 ¶ 471, 172 ¶ 636.) The court makes no determination on the existence of a special relationship in noting that no direct relationship exists for the purpose of the choice of law analysis.

on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Twombly*, 550 U.S. at 556). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (citing *Twombly*, 550 U.S. at 556). When considering a Rule 12(b)(6) motion to dismiss, the court must accept all well-pled factual allegations as true and view the complaint in the light most favorable to the plaintiff. *See e.g.*, *Aziz v. Alcolac*, 658 F.3d 388, 391 (4th Cir. 2011); *Ostrzenski v. Seigel*, 177 F.3d 245, 251 (4th Cir. 1999). However, the court is not required to accept legal conclusions as true. *Aziz*, 658 F.3d at 391 (citing *Iqbal*, 556 U.S. at 680).

As the court will decide the instant Motion to Dismiss before class certification, the court's rulings will only bind the named Plaintiffs. Manual for Complex Litigation, Fourth § 21.11 ("Motions such as challenges to jurisdiction and venue, motions to dismiss for failure to state a claim, and motions for summary judgment may be decided before a motion to certify the class, although such precertification rulings bind only the named parties.").

III. ANALYSIS

Blackbaud contends that the court should dismiss Plaintiffs' common law negligence, negligence *per se*, gross negligence, and unjust enrichment claims for failure to state a claim. (ECF No. 124 at 17.) The court evaluates Plaintiffs' allegations in the light most favorable to Plaintiffs as the nonmovants and remains mindful that a motion to dismiss "tests only the sufficiency of those allegations and not the ultimate success of Plaintiffs' legal theories." *See In re Target Corp. Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014). The court will address each of Blackbaud's arguments in turn.

A. Negligence - Duty[8]

Plaintiffs assert negligence claims against Blackbaud on behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the subclasses. (ECF No. 77 at 173.) Blackbaud contends Plaintiffs' claims fail because they cannot establish Blackbaud owed Plaintiffs a duty of care. (ECF No. 124-1 at 17.) Initially, Blackbaud contends that "[n]o state court in the relevant states has ever held that a software provider like Blackbaud owes a common law duty of care to third parties like Plaintiffs, with whom Blackbaud had no relationship." (*Id.* at 17.) Blackbaud asserts that Plaintiffs' negligence claims fail as a matter of law because Plaintiffs have not shown Blackbaud owes a duty of care to "strangers" in the absence of "extraordinary and specific facts." (*Id.* at 24 (citing *QDOS, Inc., v. Signature Finance, LLC*, 17 Cal. App. 5th 990, 1000 n.3 (Cal Ct. App. 2017).) As such, Blackbaud explains, Plaintiffs must show a special relationship between the parties "such that social policy justifies the imposition of a duty to act." (*Id.* at 25–26 (citing *Smith v. Anderson*, 72 P.3d 369, 372 (Colo. App. 2002)).) Blackbaud also argues that "there exists no general duty to prevent the criminal acts of third parties." (*Id.*)

To state a cause of action for negligence under South Carolina law, a plaintiff must show: "(1) a duty of care owed by the defendant; (2) a breach of that duty by a negligent act or omission; (3) a negligent act or omission resulted in damages to the plaintiff; and (4) that damages proximately resulted from the breach of duty." *Savannah Bank, N.A. v. Stalliard*, 734 S.E.2d at 163–64 (citing *Thomasko v. Poole*, 561 S.E.2d at 599; *Kleckley*, 526 S.E.2d at 221). The existence of a legal duty of care owed by the defendant to the plaintiff is an essential element in a cause of action for negligence. *Huggins v. Citibank, N.A.*, 585 S.E.2d 275, 276 (S.C. 2003). The existence

[8] As Blackbaud noted at the September 2, 2021 Hearing, the instant Motion (ECF No. 124) focuses primarily on the first element of negligence. (ECF No. 147 at 19:8.)

of a duty owed is a question of law for the courts. *Doe v. Greenville Cnty. Sch. Dist.*, 651 S.E.2d 305, 309 (S.C. 2007) (citing *Doe v. Batson*, 548 S.E.2d 854, 857 (2001)).

"An affirmative legal duty exists only if created by statute, contract, relationship, status, property interest, or some other special circumstance." *Hendricks v. Clemson Univ.*, 578 S.E.2d 711, 714 (S.C. 2003). "It is the relationship between the parties, not the potential 'foreseeability of injury,' that determines whether the law will recognize a duty in a given context." *Williams v. Preiss-Wal Pat III, LLC*, 17 F. Supp. 3d 528, 535 (D.S.C. 2014) (citing *Charleston Dry Cleaners & Laundry, Inc. v. Zurich American Ins. Co.*, 586 S.E.2d 586, 588 (S.C. 2003)). Where an act is voluntarily undertaken, however, the actor assumes the duty to use due care. *Vaughan v. Town of Lyman*, 635 S.E.2d 631 (S.C. 2006); *Hendricks v. Clemson Univ.*, 578 S.E.2d at 714 (citing *Miller v. City of Camden*, 494 S.E.2d 813 (S.C. 1997)); *see also Madison ex rel. Bryant v. Babcock Center, Inc.*, 638 S.E.2d 650, 657 (S.C. 2006) (one who assumes to act, even though under no obligation to do so, thereby becomes obligated to act with due care).

In *Shaw v. Psychemedics Corp.*, the South Carolina Supreme Court held that the contractual relationship between an employer and a drug testing laboratory created a special circumstance to support the imposition of a duty of care owed by the laboratory to employees who are subject to testing. 826 S.E.2d 281, 283–84 (S.C. 2019). In making this finding, the court explained that "[t]he principal purpose of the contract between the laboratory and the employer is to test a given employee's biological specimen for the presence of drugs." *Id.* at 283. At some point during the testing process, if not for the entire duration, the laboratory "possesses and exercises control over the specimen." *Id.* Further, the court explained that "if the laboratory is negligent in testing the employee's specimen, it is foreseeable that the employee will likely suffer a direct economic injury." *Id.* at 283–84. Without the recognition of a duty, the injured employee

would be left without redress. *Id.* Finally, the court noted that the recognition of a duty in this context "advances a major policy goal of tort law: deterrence." *Id.* at 284.

Blackbaud contends that its contracts are much broader than cyber security, (ECF No. 147 at 35:17–18), and as such, *Shaw* is inapplicable. The court disagrees. Plaintiffs allege the primary purpose of Blackbaud's contracts with the Social Good Entities is to provide "computing software, services, and cybersecurity[.]" (ECF No. 77 at 110 ¶ 419.) Blackbaud's customers use its services to collect and protect information of third parties, including Plaintiffs. Therefore, like the contract between the laboratory and the employer in *Shaw*, Blackbaud's contracts with the Social Good Entities support recognition of a duty to Plaintiffs because the purpose of the contracts was to maintain and secure Plaintiffs' Private Information.

Blackbaud also contends that, unlike the laboratory in *Shaw*, the Social Good Entities control the data. (ECF No. 147 at 35: 17–18.) Blackbaud styles itself a "software-as-a-service provider," meaning that it provides a "software shell that its customers can take and use" in other applications with tools for various purposes such as tracking donations or college admissions. (ECF No. 147 at 22:18–25.) Even if the customizable nature of Blackbaud's services gives its customers primary control of the data, however, Blackbaud still has the greatest amount of control over the security of the data that is stored. *See Shaw*, 826 S.E.2d at 283 (explaining that "[d]rug testing laboratories have the greatest amount of control over the accuracy of the testing process") (citing *Landon v. Kroll Lab. Specialists, Inc.*, 999 N.E.2d 1121, 1124 (N.Y. 2013) (finding drug testing laboratory is in the best position to prevent harm)). Thus, Blackbaud remains in the best position to prevent harm associated with a data breach to its systems. Accordingly, the court finds Plaintiffs have alleged facts showing a special circumstance sufficient to impose a common law duty arising from Blackbaud's contracts with the Social Good Entities.

Next, Blackbaud contends that Plaintiffs' negligence claims fail because it had "no duty to protect Plaintiffs against the unlawful conduct of a third-party criminal." (ECF No. 124-1 at 26 (citing *Brown v. Brown*, 739 N.W.2d 313, 316–19 (Mich. 2007)).) Under South Carolina law, "there is no general duty to control the conduct of another or to warn a third person or potential victim of danger." *Faile v. S.C. Dep't of Juv. Just.*, 566 S.E.2d 536, 546 (S.C. 2002) (citing *Rogers v. South Carolina Dep't of Parole & Cmty Corr.*, 464 S.E.2d 330 (1995); *Rayfield v. South Carolina Dep't of Corr.*, 374 S.E.2d 910 (S.C. Ct. App. 1988), *cert. denied*, 379 S.E.2d 133 (1989); RESTATEMENT (SECOND) OF TORTS § 314 (1965)). South Carolina recognizes five (5) exceptions to this rule:

> 1) where the defendant has a special relationship to the victim; 2) where the defendant has a special relationship to the injurer; 3) where the defendant voluntarily undertakes a duty; 4) where the defendant negligently or intentionally creates the risk; and 5) where a statute imposes a duty on the defendant.

Faile, 566 S.E.2d at 546 (citations omitted). Blackbaud contends none of these exceptions apply and therefore it had no duty to protect Plaintiffs from third party criminal conduct.[9] (ECF No. 124-1 at 26–27 n.3.)

In addressing the first exception, Blackbaud maintains that in the absence of "any actual relationship with Blackbaud, Plaintiffs certainly have not pleaded a 'special relationship' sufficient to create a duty where it would not otherwise exist." (ECF No. 124-1 at 29 (citing *Reno v. Chung*, 559 N.W.2d 308, 309 (Mich. Ct. App. 1996)).) South Carolina courts have recognized certain categories of special relationships when the defendant "has the ability to monitor, supervise and control an individual's conduct and when the individual has made a specific threat of harm directed at a specific individual." *Roe v. Bibby*, 763 S.E.2d 645, 649 (S.C. Ct. App. 2014) (quoting *Doe*

[9] The court notes that Blackbaud only substantively addresses the first and third exceptions after pointing out that Plaintiffs do not allege Blackbaud had any relationship to the hackers.

v. Marion, 645 S.E.2d 245, 250 (S.C. 2007) (internal quotations omitted)).[10] However, Plaintiffs allege that Blackbaud had control over the data and the security measures in place to protect the data; they do not allege that Blackbaud had any ability to monitor, supervise, or control the hackers or their conduct. Accordingly, this exception does not apply to create a duty for Blackbaud to protect Plaintiffs from the criminal conduct of third parties.

In addressing the third exception, Blackbaud explains that "the assumption of duty doctrine simply does not apply absent physical harm to the plaintiff." (*Id.* at 27–28 (citing RESTATEMENT (SECOND) OF TORTS § 324A).) The court agrees. In South Carolina, the recognition of a voluntarily assumed duty "is rooted in the Restatement of Torts," *Johnson v. Robert E. Lee Acad.*, 737 S.E.2d 512, 514 (S.C. Ct. App. 2012), which provides that "[o]ne who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for *physical harm* resulting from his failure to exercise reasonable care." RESTATEMENT (SECOND) OF TORTS § 323 (emphasis added); *see also McPherson v. CSX Transp., Inc.*, No. 4:16-CV-2725-BHH, 2017 WL 1135291, at *6 (D.S.C. Mar. 27, 2017) ("South Carolina courts have generally applied the voluntary assumption of duty doctrine 'only to situations in which a person suffers physical harm from the failure to exercise reasonable care and not cases in which financial harm is the only

[10]*See also Faile*, 566 S.E.2d at 546 (finding special relationship between Department of Juvenile Justice and dangerous juvenile/injurer over whom it had custody per court order); *Bishop v. S.C. Dep't of Mental Health*, 502 S.E.2d 78, 81 (S.C. 1998) (finding special relationship between Department of Mental Health and involuntarily-committed patient/injurer in its custody); *Rogers v. S.C. Dep't of Parole & Cmty. Corr.*, 464 S.E.2d at 332 (assuming a special relationship exists between state agencies charged with prisoner parole and prisoner/injurer who was being released from custody, but ultimately finding no specific threat); *Ballou v. Sigma Nu Gen. Fraternity*, 352 S.E.2d 488 (S.C. 1986) (finding a fraternal organization had a duty to an initiate who had become helplessly drunken from alcohol furnished to him by the fraternity).

damage.'"). Thus, this exception also does not apply to create a duty for Blackbaud to protect Plaintiffs from the criminal conduct of third parties.

Plaintiffs also allege, however, that the fourth exception applies: that Blackbaud had a duty to protect Plaintiffs from the criminal conduct of third parties based on Blackbaud's own negligent conduct in creating the risk by failing to use reasonable security measures. (*See* ECF Nos. 77 at 175 ¶ 638, 77 ¶ 646; 142 at 23–24.) A common law duty may arise where a defendant creates "a situation that [it] knew or should have known posed a substantial risk of injury" to a plaintiff. *See Edwards v. Lexington Cnty. Sheriff's Dep't*, 688 S.E.2d 125, 130 (S.C. 2010). Plaintiffs assert that despite Blackbaud's acknowledgement of the risk of cyberattacks and repeated notifications of the inadequacy of its systems, Blackbaud "failed to correct, update, or upgrade its security protections." (ECF No. 142 at 23–24 (citing ECF No. 70 at 13 ¶¶ 28–29, 131–37 ¶¶ 476–96).) The court finds Plaintiffs have alleged facts supporting the application of this exception to the general rule that there is no duty to protect another from the conduct of third parties.

Based upon the foregoing, the court finds Plaintiffs have alleged sufficient facts to support their assertion that Blackbaud owed them a duty based on the special circumstances of Blackbaud's contracts with the Social Good Entities and Blackbaud's alleged creation of the risk. *See In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d at 966 (finding the recognition of a legal duty "to safeguard a consumer's confidential information entrusted to a commercial entity" supported by both "common sense" and the law). Accordingly, the court declines to dismiss Plaintiffs' general negligence claims based on their failure to allege a duty.

B. Gross Negligence

Blackbaud also argues that each of Plaintiffs' claims for gross negligence fail because Plaintiffs cannot show Blackbaud owed them a duty. (ECF No. 124-1 at 31.) Generally, to state

a claim for gross negligence a plaintiff must plead the same elements as a claim for negligence. *See Cockrell v. Lexington Cnty. Sch. Dist. One*, No. 3:11-CV-2042-CMC, 2011 WL 5554811, at *5 (D.S.C. Nov. 15, 2011). However, negligence is the failure to exercise due care, while gross negligence is the failure to exercise slight care. *Clyburn v. Sumter Cnty. Sch. Dist. # 17*, 451 S.E.2d 885, 887 (S.C. 1994) ("Gross negligence has also been defined as a relative term and means the absence of care that is necessary under the circumstances.") (citing *Hollins v. Richland Cnty. Sch. Dist. One*, 427 S.E.2d 654 (S.C. 1993)). Because the court finds Plaintiffs have sufficiently alleged the duty owed by Blackabud and Blackbaud has not challenged Plaintiffs' gross negligence claims on any other basis,[11] the court declines to dismiss Plaintiffs' gross negligence claims at this time.

C. Negligence *Per Se*

Plaintiffs assert claims for negligence *per se* based upon Blackbaud's alleged violations of the Federal Trade Commission Act ("FTC Act"), the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Children's Online Privacy Protection Act ("COPPA"). (ECF No. 77 at 127 ¶ 464.) Blackbaud argues Plaintiffs' negligence *per se* claims fail because South Carolina law requires that "[t]he underlying statute purporting to form the basis for a negligence *per se* claim must itself provide a private claim for relief," but the statutes Plaintiffs cite provide no such relief. (ECF No. 124-1 at 35.)

A claim for negligence *per se* "is established by showing a statute created a duty to the plaintiff and the defendant breached that duty by violating the statute." *Seals by Causey v. Winburn*, 445 S.E.2d 94, 96 (S.C. Ct. App. 1994) (citing *Whitlaw v. Kroger Co.*, 410 S.E.2d 251

[11] Blackbaud also argues that many of Plaintiffs' gross negligence claims are deficient based on the law of Plaintiffs' respective states of residence; however, Blackbaud does not make this argument as to South Carolina law. (*See* ECF No. 124-1 at 31–32 (raising issues under the laws of California, Illinois, Maine, Michigan, Texas, and Wyoming).)

(S.C. 1991)). Generally, "[a] statute must permit a private cause of action in order for plaintiffs to maintain a civil suit" for negligence *per se*. *Salley v. Heartland-Charleston of Hanahan, SC, LLC*, 2011 WL 2728051, at *3 (D.S.C. July 12, 2011). "However, that private cause of action need not be explicit." *J.R. v. Walgreens Boots Alliance Inc.*, 470 F. Supp. 3d 534, 553 (D.S.C. 2020).

> In order to show that the defendant owes him a duty of care arising from a statute, the plaintiff must show two things: (1) that the essential purpose of the statute is to protect from the kind of harm the plaintiff has suffered; and (2) that he is a member of the class of persons the statute is intended to protect.

Whitlaw, 410 S.E.2d at 252 (citing *Rayfield*, 374 S.E.2d at 914). "In South Carolina, however, for a statute to support a claim for negligence *per se*[,] a plaintiff must show that the statute was 'enacted for the special benefit of a private party.'" *Winley v. Int'l Paper Co.*, No. 2:09-cv-02030-CWH, 2012 WL 13047989, at * 10 (D.S.C. Oct. 23, 2012) (citing *Doe v. Marion*, 645 S.E.2d at 248). Thus, to survive a motion to dismiss on their claims for negligence *per se*, Plaintiffs must adequately plead that the "essential purpose" for each of the asserted statutes "is to protect from the kind of harm [P]laintiffs have allegedly suffered and whether [P]laintiffs are members of the class meant to be protected by the statutes." *Walgreens*, 470 F. Supp. 3d at 553.

Initially, Plaintiffs cannot base negligence *per se* claims on the HIPAA because it was "enacted for the protection of the public and not with the protection of an individual private right" in mind. *Winley*, 2012 WL 13047989, at * 10 (citing *Doe v. Marion*, 645 S.E.2d at 248). The purpose of the HIPAA is "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes." *Citizens Bank of Pennsylvania v. Reimbursement Technologies, Inc.*, 609 F. App'x 88, 93 (3rd Cir. 2015) (citing Pub. L. No. 104–191, 110 Stat. 1936); *see also Ruder v. Pequea Valley Sch. Dist.*,

790 F. Supp. 2d 377, 403 (E.D. Penn. 2011) ("The Act makes clear that its purpose is to improve the operation of the health care system and reduce administrative costs."). Thus, the HIPAA was not enacted for the protection of an individual or group and cannot serve as a basis for negligence *per se* under South Carolina law. *See Doe v. Marion*, 645 S.E.2d at 248 ("When a statute does not specifically create a private cause of action, one can be implied only if the legislation was enacted for the special benefit of a private party.") (citing *Citizens of Lee Cnty v. Lee Cnty*, 416 S.E.2d 641 (S.C. 1992)). Accordingly, Plaintiffs' negligence *per se* claims fail to the extent they are premised on violation of the HIPAA.

Turning to the FTC Act as a potential basis for negligence *per se*, the court notes that courts outside of South Carolina appear to be split on whether the FTC Act can serve as the basis for a negligence *per se* claim in the data breach context.[12] Some courts have allowed these claims to go forward at the motion to dismiss stage. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 481–82 (D. Md. 2020) (holding that plaintiffs adequately pled negligence *per se* under Georgia law); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d at 406–08 (holding that a negligence *per se* claim could be premised on the FTC Act under New York law). Other courts have specifically held that the FTC Act cannot serve as a basis for such claims. *See, e.g.*, *In re Brinker Data Incident Litig.*, No. 3:18-cv-686-J-32MCR, 2020 WL 691848, at *9 (M.D. Fl. Jan. 27, 2020) (holding that the FTC Act cannot be the basis of negligence *per se* under Florida law, which disallows negligence *per se* claims that rely on a federal

[12] Although the court has not found any South Carolina cases that definitively decide whether the FTC Act can serve as the basis for a negligence *per se* claim, one South Carolina court has found that "a violation of the [FTC Act] *could* serve as the basis for a negligence *per se* claim." *See Walgreens*, 470 F. Supp. 3d at 555 (emphasis added) (assuming arguendo that the FTC Act could serve as the basis of a negligence *per se* claim, the plaintiffs had failed to sufficiently allege a violation of the act because they did not allege their data was breached by third party hackers).

statute without a private right of action); *In re Sonic Corp. Customer Data Sec. Breach Litig. (Fin. Institutions)*, No. 17-MD-2807, 2020 WL 3577341, at *6 (N.D. Ohio July 1, 2020) ("While the FTC and other courts have interpreted [the FTC Act's] terms to apply to data security requirements, the statute's actual terms do not lay out positive, objective standards that, if violated, could give the standard for a negligence *per se* claim under Oklahoma law.").

The variations in these holdings appear to stem from differences in the standards for negligence *per se* claims under the laws of different states. Under South Carolina's standard, the answer turns on the purpose of the statute. *See Doe v. Marion*, 645 S.E.2d at 248. To base their negligence *per se* claims on the FTC Act, Plaintiffs must show that the statute was designed to protect a particular individual or group of people and that they are members of that group. Plaintiffs have not done so.[13] Although Plaintiffs broadly allege in the CCAC[14] that they are members of the class the FTC Act was designed to protect, they do not actually define or otherwise explain the parameters of such a group. Accordingly, Plaintiffs have not sufficiently alleged a cause of action for negligence *per se* under South Carolina law based on the FTC Act.

[13] *See Orkin Exterminating Co., Inc. v. F.T.C.*, 898 F.2d 1354, 1368 (11th Cir. 1988) ("The purpose of the Federal Trade Commission Act is to protect the public, not punish the wrongdoer . . .") (quoting *Regina Corp. v. F.T.C.*, 322 F.2d 765, 768 (3d Cir. 1963)); *F.T.C. v. Cinderella Career & Finishing Sch., Inc.*, 404 F.2d 1308, 1313 (D.C. Cir. 1968) ("That the basic purpose of the Act is the protection of the public is evident from the clause, 'would be to the interest of the public[.]'").

[14] (*See* ECF No. 77 at 127 ¶ 464 (asserting Blackbaud has a duty under "a number of statutes, including the HIPAA, the [FTC Act], [and the COPPA], to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and the class members from the type of conduct by Blackbaud alleged herein."); *id.* at 179 ¶ 656–57 (same); *id.* at 182 ¶ 676 (citing to the FTC Act, 15 U.S.C. § 45); 182 ¶ 677 (citing to the HIPAA, 42 U.S.C. § 1320d); *id.* 183–83 at ¶ 678 (citing to the COPPA, 15 U.S.C. §§ 6501–6505).) Plaintiffs allege that "[t]he essential purposes of these statutes are to protect from the same or similar kind of harm caused to Plaintiffs, Class and Subclass members, as a direct and proximate result of Blackbaud's breach of those statutory and regulatory duties." (ECF No. 77 at 179 ¶ 657.)

Next, Plaintiffs assert the COPPA as a basis for their negligence *per se* claims. The COPPA requires operators of commercial websites or online services directed to children under the age of thirteen (13) or any operator that has actual knowledge that it is collecting personal information from a child, "to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children." *See* 15 U.S.C. §§ 6501 & 6502. The term "collection" means "the gathering of any personal information from a child" by any means, including:

> (1) Requesting, prompting, or encouraging a child to submit personal information online;
> (2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or
> (3) Passive tracking of a child online.

16 C.F.R. § 312.2. Even if the court were to find the COPPA was an appropriate basis for a negligence *per se* claim, Plaintiffs have not adequately alleged they are within the class the statute seeks to protect. The only Named Plaintiff with claims regarding minor children is Plaintiff Coty Martin. (*See* ECF No. 77 at 78–79 ¶¶ 283–84.) Plaintiff Martin, however, does not allege that Blackbaud operated a commercial website or online service directed to children under the age of thirteen (13) or that Blackbaud collected information from his minor child as defined by 16 C.F.R. § 312.2. Accordingly, Plaintiffs have not sufficiently alleged a cause of action for negligence *per se* under South Carolina law based on a violation of the COPPA.

As a result of the foregoing, Plaintiffs' negligence *per se* claims premised on the HIPAA, the FTC Act, and the COPPA are dismissed.[15]

D. Negligence - Damages

Blackbaud asserts Plaintiffs' claims for negligence, gross negligence, and negligence *per se* all fail because Plaintiffs fail to allege damages cognizable in tort because they merely offer "conclusory allegations that they 'face an imminent risk of future harm,'" and, "to the extent Plaintiffs allege they have already been the victims of fraud, their allegations simply reflect temporal proximity between the alleged fraud and the Ransomware Attack, but with no actual causal link." (ECF No. 124-1 at 36–37.)[16]

Under South Carolina law, "actual damages are when the wrongful act has caused loss or injury which can be assessed in money, the universal and cardinal principle being that person injured shall receive compensation commensurate with his loss or injury, and no more." *Kapuschinsky v. United States*, 259 F. Supp. 1, 6 (D.S.C. 1966) (quoting *Hutchinson v. Town of Summerville*, 45 S.E. 8, 9 (S.C. 1903)). "While neither the existence, causation nor amount of damages can be left to conjecture, guess or speculation, proof with mathematical certainty of the

[15] While these statutes cannot serve as the basis of a negligence *per se* claim, Plaintiffs can use the alleged violation of these statutes to support their general negligence claims. *See In re Brinker Data Incident Litig.*, 2020 WL 691848, at *9.

[16] Blackbaud also argues that Plaintiffs' claims are barred by the economic loss rule. (ECF No. 124-1 at 37–39.) In its Motion to Dismiss (ECF No. 124), Blackbaud briefs the application of the economic loss rule under the laws of Illinois, Maine, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Texas, Virginia, and Wyoming, but not under South Carolina law. (See ECF Nos. 124-1 at 37–39, 124-2 at 12–14.) At the September 2, 2021 Hearing, Blackbaud conceded that they are not arguing that the economic loss rule bars Plaintiffs' claims under South Carolina law for the purposes of the Motion to Dismiss (ECF No. 124), but it may argue that at a later time. (ECF No. 147 at 37:21–24.) As such, the court does not need to address the economic loss doctrine under South Carolina law in ruling on the instant motion.

amount of loss or damage is not required." *Whisenant v. James Island Corp.*, 281 S.E.2d 794, 796 (S.C. 1981) (citing *Piggy Park*, 162 S.E.2d 705).

Injuries similar to those alleged by Plaintiffs have been recognized as cognizable damages in tort actions stemming from data breaches by other courts. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1315 (N.D. Ga. 2019) (holding that allegations that the plaintiffs' private information was compromised in the data breach was legally cognizable under Georgia law); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at * 8 (holding that damages for fraudulent charges stemming from data breach were sufficient to withstand a motion to dismiss); *In re Marriott Int'l, Inc. Consumer Data Sec. Breach Litig.*, 440 F. Supp. at 494–495 (holding that the plaintiffs had adequately alleged actual injury and actual loss including loss of the benefit of the bargain, loss of time and money spent mitigating harms, loss of value of personal information, and losses from identity theft). As stated above, Plaintiffs assert they have suffered injuries arising from Blackbaud's negligence in the form of risk of extortion (*id.* ¶ 560), unauthorized disclosure of their Private Information to third-party cybercriminals (*id.* ¶ 563), loss of value in their Private Information (*id.* ¶ 564), risk of future identity theft or fraud (*id.* ¶ 566), and out-of-pocket mitigation expenses (*id.* ¶¶ 568–70). All thirty-four (34) Named Plaintiffs maintain that they have spent time and money to mitigate their exposure to identity theft or fraud as a result of the Ransomware Attack.[17]

[17] Clayton (ECF No 77 at 22–23 ¶ 54, 23 ¶ 55, 24 ¶¶ 59, 60); Eisen (*id.* at 25 ¶¶ 65, 66, 26 ¶ 70); Estes (*id.* at 27 ¶ 73, 75, 29 ¶¶ 79, 80); Regan (*id.* at 30 ¶¶ 83, 85, 31 ¶¶ 89, 90); Mitchell (*id.* at 33 ¶ 95, 34 ¶ 98); Carpenella (*id.* at 35 ¶ 104, 37 ¶¶ 109, 110); Kamm (*id.* at 38 ¶ 114, 39 ¶¶ 118, 119); Arman (*id.* at 41 ¶ 127, 42 ¶¶ 131, 132); Garcia-Martinez (*id.* at 43–44 ¶ 137, 44 ¶ 138, 45–46 ¶¶ 142, 143); Lofton (*id.* at 47 ¶ 148, 48 ¶¶ 152, 153); Gignac (*id.* at 50 ¶¶ 163, 164, 51 ¶¶ 166, 168, 169); Frontera (*id.* at 52–53 ¶ 174, 54 ¶¶ 179, 180); Bishop (*id.* at 55-56 ¶ 185, 56 ¶ 186, 57 ¶¶ 190, 191); Maher (*id.* at 58 ¶ 196, 59 ¶¶ 200, 201); Glasper (*id.* at 60–61 ¶ 206, 61 ¶¶ 210, 211); Mandel (*id.* at 62-63 ¶ 216, 63–64 ¶ 221); Roth, M. (*id.* at 66 ¶ 232, 67 ¶ 237)); Roth, R. (*id.* at 68 ¶ 241, 69 ¶ 246); Peragine (*id.* at 70–71 ¶ 252, 72 ¶ 257); Zielinski (*id.* at 73 ¶ 262, 74 ¶ 267);

Further, Plaintiffs have sufficiently alleged a causal link between the Ransomware Attack and their damages to survive a motion to dismiss. Plaintiffs plausibly allege that Blackbaud had custody of their Private Information, that Blackbaud's systems were hacked, that these hackers obtained Plaintiffs' Private Information, and that as a result of the Ransomware Attach, they have suffered identity theft and other fraudulent activity. These allegations are sufficient at the pleading stage to establish that the Ransomware Attack was the cause of these injuries. *See In re Equifax, Inc., Consumer Data Sec. Breach Litig.*, 362 F. Supp. 3d at 1318–19. Therefore, the court finds Plaintiffs have alleged injuries cognizable in tort under South Carolina law.

E. Unjust Enrichment

Blackbaud contends Plaintiffs' claims for unjust enrichment should be dismissed because several states do not recognize a freestanding claim for unjust enrichment, Plaintiffs have failed to allege Blackbaud received a benefit from them, and retention of any benefit conferred would not be unjust. (ECF No. 124-1 at 40–41.) Plaintiffs appear to allege that they conferred a benefit on Blackbaud because Blackbaud was paid to store their information safely and that retaining such a benefit would be unjust because Blackbaud did not safely store the information as promised. (*See* ECF No. 77 at 185 ¶¶ 688, 690.)

"A party may be unjustly enriched when it has and retains benefits or money which in justice and equity belong to another." *Dema v. Tenet Physician Servs.-Hilton Head, Inc.*, 678 S.E.2d 430, 434 (S.C. 2009). To recover for unjust enrichment, a plaintiff must show three

Allen (*id.* at 75 ¶ 271, 76 ¶¶ 272, 277); Martin (*id.* at 78 ¶¶ 281, 282, 79 ¶ 286); Pettiford (*id.* at 80 ¶ 291, 80–81 ¶ 292, 81–82 ¶ 296, 82 ¶ 297); Welsh (*id.* at 83 ¶¶ 302, 303, 84 ¶¶ 307, 308); Duranko (*id.* at 85 ¶ 313, 87 ¶ 317); Ford (*id.* at 88 ¶ 324, 89 ¶¶ 329, 330); Scott (*id.* at 90 ¶ 334, 91 ¶ 339); Watts (*id.* at 93 ¶ 346, 94 ¶ 351); Money, J. (*id.* at 96 ¶ 359, 97 ¶ 364); Money, N. (*id.* at 98–99 ¶ 369, 100 ¶ 374); Case (*id.* at 101–02 ¶ 380, 102 ¶ 381, 103 ¶¶ 385, 386); Sheth (*id.* at 105 ¶ 393, 106 ¶¶ 398, 399); Molnar (*id.* at 110 ¶ 415).

elements: "(1) that he conferred a non-gratuitous benefit on the defendant; (2) that the defendant realized some value from the benefit; and (3) that it would be inequitable for the defendant to retain the benefit without paying the plaintiff for its value." *Sauner v. Pub. Serv. Auth. of S.C.*, 581 S.E.2d 161, 167–68 (S.C. 2003) (citing *Niggel Assoc., Inc. v. Polo's of North Myrtle Beach, Inc.*, 374 S.E.2d 507 (S.C. Ct. App. 1988)).

The court in the *Capital One Consumer Data Security Breach Litigation* addressed claims for unjust enrichment in the data breach context. *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d at 411–13. In *Capital One*, the plaintiffs, consumer credit card holders, brought an action against Capital One and Amazon when their private information was compromised in a data breach. *Id.* at 388–90. The court declined to dismiss the plaintiffs' unjust enrichment claims upon finding that the plaintiffs had plausibly alleged that, "in consideration for receiving credit services," the plaintiffs had delivered their PII to the defendants; had the plaintiffs known that the defendants would not adequately protect that data, they would not have sought and purchased those services; and that the plaintiffs' "purchase of Capital One's credit card services conferred a benefit on both Capital One and Amazon, by way of the fees and interest Plaintiffs paid to Capital One and fees Capital One paid to Amazon for its use of [its] servers." *Id.* at 412.

The present facts are distinguishable from *Capital One*. First, Plaintiffs have not alleged that they provided their Private Information "in consideration for" Blackbaud's services. Instead, Plaintiffs allege they provided their Private Information to the Social Good Entities for the use of their services or for the purpose of donating to these organizations. (ECF No. 77 at 183–84 ¶¶ 688, 691.) Second, Plaintiffs do not allege that they chose to utilize Blackbaud's services in the first place, nor have they alleged that they would not have sought or purchased Blackbaud's services had they known its data security was inadequate. Third, the CCAC does not put forth any

allegations that Plaintiffs paid for Blackbaud's services or directly provided their information to Blackbaud. Actually, Plaintiffs gave their Private Information to the Social Good Entities who in turn sought out, paid for, and utilized Blackbaud's services. Consequently, Plaintiffs have not alleged facts to show that they conferred a benefit on Blackbaud to support claims for unjust enrichment. As such, the court finds dismissal of Plaintiffs' unjust enrichment claims appropriate.

IV. CONCLUSION

For the foregoing reasons, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion to Dismiss. (ECF No. 124.) Specifically, the court:

- Denies Blackbaud's Motion to Dismiss Plaintiffs' negligence and gross negligence claims;
- Grants Blackbaud's Motion to Dismiss Plaintiffs' negligence *per se* and unjust enrichment claims.

IT IS SO ORDERED.

J. Michelle Childs
United States District Judge

October 19, 2021
Columbia, South Carolina