UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re GE/CBPS DATA BREACH LITIGATION	20 Civ. 2903 (KPF) **OPINION AND ORDER**

KATHERINE POLK FAILLA, District Judge:

A breach in early 2020 (the "Data Breach") of an email account maintained by Defendant Canon Business Process Services, Inc. ("Canon") resulted in an unauthorized third party gaining access to personally identifiable information ("PII") of current and former employees of Defendant General Electric Company ("GE," and collectively with Canon, "Defendants") and their beneficiaries. Canon maintained this information as a provider of business process and document management services to GE. Plaintiff Steven Fowler ("Plaintiff" or "Fowler"), a former GE employee, then brought suit against Defendants on behalf of himself and all others similarly situated, seeking redress for harms they allegedly have suffered and are at risk of suffering in the future as a result of the Data Breach. Defendants have moved to dismiss the Consolidated Class Action Complaint for lack of subject matter jurisdiction and failure to state a claim upon which relief may be granted. For the reasons set forth herein, the Court grants Defendants' motion in part and denies it in part.

BACKGROUND[1]

A. Factual Background

1. The Parties

Plaintiff Steven Fowler is a citizen of the State of Kentucky. (Compl. ¶ 21). He is a former employee of Defendant GE. (*Id.*). While employed at GE, Fowler was required to provide sensitive personal information to GE. (*Id.*). On or about March 20, 2020, GE notified Fowler that his PII had been compromised in the Data Breach. (*Id.*).

Defendant GE is a New York corporation with its headquarters in Boston, Massachusetts. (Compl. ¶ 22). Defendant Canon is a Delaware corporation with its principal place of business in the State and City of New York. (*Id.* at ¶ 23).

---

[1] This Opinion draws its facts primarily from the well-pleaded allegations of the Consolidated Class Action Complaint ("Complaint" or "Compl." (Dkt. #40)). The Court also considers the Declaration of James Allen in Support of Defendants' Motion to Dismiss ("Allen Decl." (Dkt. #59)), the Declaration of Steven Fowler in Opposition to Defendants' Motion to Dismiss ("Fowler Decl." (Dkt. #64-3)), and several documents incorporated by reference in the Complaint and publicly available on GE's website, including a policy document called "The Spirit and the Letter," available at https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf (last accessed August 2, 2021). Because Defendants move for dismissal under Federal Rule of Civil Procedure 12(b)(1) for lack of standing on the part of Plaintiff Fowler, the Court may also refer to evidence outside the pleadings to determine its subject matter jurisdiction. *See Libertarian Party of Erie Cty.* v. *Cuomo*, 970 F.3d 106, 120-21 (2d Cir. 2020), *cert. denied sub nom. Libertarian Party* v. *Cuomo*, — S. Ct. — , 2021 WL 2519117 (June 21, 2021); *Makarova* v. *United States*, 201 F.3d 110, 113 (2d Cir. 2000).

For ease of reference, the Court refers to Defendants' Memorandum of Law in Support of Defendants' Motion to Dismiss the Consolidated Class Action Complaint as "Def. Br." (Dkt. #58); to Plaintiff's Memorandum of Law in Opposition to Defendants' Motion as "Pl. Opp." (Dkt. #64); and to Defendants' Reply Memorandum of Law as "Def. Reply" (Dkt. #65).

2. GE's Data Collection and Protection Policies

As a condition of employment, GE collects and maintains personal and financial information about its employees and their dependents or other beneficiaries. (Compl. ¶ 27). Among the types of information collected are "employment data obtained in the context of an employment relationship" and "any information relating to a directly or indirectly identifiable person," including "name, address, email, phone, national identifier, and credit card number." (*Id.*).

GE has written and publicly distributed several policy documents that touch on privacy and information security. On its website, GE advertises that it "respects the privacy rights of individuals and is committed to handling Personal Information responsibly, in accordance with applicable law … and GE's Commitment to the Protection of Personal Information[.]" (Compl. ¶ 30). In its Commitment to the Protection of Personal Information, GE states:

> GE strives to protect Personal Information with appropriate technical and organizational measures to ensure its integrity, confidentiality, security and availability. GE will inform individuals of a security breach affecting their GE Personal Information that could pose a high risk to their individual rights and freedoms. In accordance with applicable law, GE will provide reasonable assistance to Customers, where GE is a processor, to ensure the security of their processing and will inform GE Customers of a security breach of GE Customer Personal Information as required under such laws.

(*Id.* at ¶ 31). GE also addresses its handling of PII in its Employment Data Protection Standards and in a policy document called "The Spirit & The Letter." (*Id.* at ¶¶ 33-37). The Employment Data Protection Standards address in

greater detail measures GE takes to protect PII, including measures related to equipment and information security, access security, and training. (*Id.* at ¶ 37). "The Spirit & The Letter" instructs employees in best practices for limiting access to GE information to authorized individuals and preventing unauthorized access, disclosure, or destruction. (*Id.* at ¶ 39). It also provides that "non-controlled affiliates should be encouraged to adopt and follow GE compliance policies." (The Spirit & The Letter at 2).

3. The Data Breach and Its Consequences

GE contracts with Canon to process documents relating to current and former GE employees and their beneficiaries. (Compl. ¶ 41). On March 20, 2020, GE issued a data breach notice stating that in February 2020, one of Canon's employee email accounts had been breached by an unauthorized party. (*Id.* at ¶ 43). The notice states:

> We were notified on February 28, 2020 that Canon had determined that, between approximately February 3-14, 2020, an unauthorized party gained access to an email account that contained documents of certain GE employees, former employees and beneficiaries entitled to benefits that were maintained on Canon's systems.... Canon has indicated that the affected documents, which contained certain personal information, were uploaded by or for GE employees, former employees and beneficiaries entitled to benefits in connection with Canon's workflow routing service. The relevant personal information, which was contained in documents such as direct deposit forms, driver's licenses, passports, birth certificates, marriage certificates, death certificates, medical child support orders, tax withholding forms, beneficiary designation forms and applications for benefits such as retirement, severance and death benefits with related forms and documents, may have included names, addresses, Social Security numbers, driver's license numbers,

> bank account numbers, passport numbers, dates of birth, and other information contained in the relevant forms.

(*Id.* at ¶ 44). Analysis by members of the public suggested that the Data Breach was the result of a "standard credential phishing attack or due to credential reuse on another site." (*Id.* at ¶ 46).

Canon determined that, as a result of the Data Breach, unauthorized persons may have obtained Fowler's name, employee identification number, home address, phone number, and email address. (Allen Decl. ¶ 6). After the Data Breach, Fowler received phishing and scam emails to his personal email address, and phishing and scam phone calls to his personal phone number. (Fowler Decl. ¶¶ 2-3). Other proposed class members allegedly suffered increased risk of identity theft and fraud; the time and expense necessary to remediate and mitigate the increased risk of identity theft and fraud; the inability to use debit cards because those cards had been canceled, suspended, or otherwise rendered unusable; fraudulent debit charges; and loss of confidentiality and value of their personal and financial information. (Compl. ¶¶ 79, 88(l), 104, 112, 119, 125, 182).

Defendants have offered individuals whose data was compromised identity theft and credit monitoring services at no charge for two years. (Compl. ¶ 66). However, no compensation or other form of relief has been provided. (*Id.*).

B. Procedural Background

Plaintiff Fowler filed the original complaint in this case, then captioned *Fowler* v. *Canon Business Process Services, Inc., et al.*, on April 8, 2020. (Dkt. #1). On April 22, 2020, the Court accepted as a related case *Baz* v. *General Electric Co., et al.*, No. 20 Civ. 3149, brought by another former GE employee, Maher Baz ("Baz"). (*See* Dkt. #10). On May 15, 2020, the Court entered a stipulation (i) consolidating the *Fowler* and *Baz* matters as well as any other related cases then pending or subsequently filed in, removed to, or transferred to this District, under case number 20 Civ. 2903 and the case caption *In re GE/CBPS Data Breach Litigation*; (ii) providing rules for applications for appointment as interim class counsel or other designated counsel; and (iii) setting a scheduling for Fowler and Baz to file a consolidated complaint and for Defendants to file a responsive pleading or motion to dismiss. (Dkt. #14). Counsel for Fowler and Baz each sought appointment as interim class counsel. (Dkt. #16-20, 26-28). On June 10, 2020, Fowler and Baz notified the Court that they had agreed to proceed cooperatively and were seeking appointment of their respective counsel as co-lead interim class counsel. (Dkt. #34). The Court held a hearing on the matter the next day, June 11, 2020, and, per Fowler's and Baz's agreement, appointed Joseph I. Marchese of Bursor & Fisher, P.A., Gary M. Klinger of Mason Lietz & Klinger LLP, and Rosemary M. Rivas of Levi & Korsinsky LLP as co-lead interim class counsel. (Minute Entry for June 11, 2020; Dkt. #35).

Fowler and Baz filed the Consolidated Class Action Complaint (the "Complaint"), which is the operative pleading in this matter, on August 11, 2020. (Dkt. #40). On October 5, 2020, Defendants filed a pre-motion letter notifying the Court of their intent to file a motion to compel Baz to arbitrate his claims and a motion to dismiss the Complaint. (Dkt. #41). Fowler and Baz filed a responsive letter on October 8, 2020. (Dkt. #44). The Court held a pretrial conference on October 21, 2020, and set a briefing schedule on Defendants' motion to compel arbitration and to stay Fowler's claims pending resolution of the motion. (Dkt. #47). Defendants filed their motion to compel arbitration on November 5, 2020. (Dkt. #48-50). On December 14, 2020, Baz filed a notice of voluntary dismissal pursuant to Federal Rule of Civil Procedure 41(a)(1)(A)(i). (Dkt. #53-54). Fowler remained in the case as named plaintiff and proposed class representative on behalf of the proposed classes. (*Id.*).

On December 17, 2020, the Court set a briefing schedule on Defendants' anticipated motion to dismiss. (Dkt. #56). In accordance with that schedule, Defendants filed their motion and supporting papers on January 21, 2021 (Dkt. #57-59); Plaintiff filed his opposition papers on March 8, 2021 (Dkt. #64); and Defendants filed their reply on April 7, 2021 (Dkt. #65). Both Plaintiff and Defendants filed notices of supplemental authority on April 27, 2021 (Dkt. #66-68), directing the Court to the same decision by the Second Circuit in *McMorris* v. *Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021). Defendants filed an additional notice of supplemental authority on June 28, 2021 (Dkt. #69), directing the Court to the Supreme Court's decision in *TransUnion LLC* v.

Ramirez, 141 S. Ct. 2190 (2021), which notice Plaintiff opposed as improper supplemental briefing (Dkt. #70). The Court accepted both Defendants' and Plaintiff's letters but barred further submissions. (Dkt. #71).

Defendants' motion is now fully briefed and ripe for decision.

DISCUSSION

A. The Court Denies Defendants' Motion to Dismiss for Lack of Subject Matter Jurisdiction

Defendants first argue that the Complaint must be dismissed under Federal Rule of Civil Procedure 12(b)(1) because Plaintiff lacks Article III standing. (Def. Br. 4-13). For the reasons that follow, the Court concludes that Plaintiff has adequately established his standing to sue and thus denies Defendants' motion on this basis.

1. Legal Standards Under Federal Rule of Civil Procedure 12(b)(1)

Plaintiff bears the burden of establishing the Court's subject matter jurisdiction by a preponderance of the evidence. *Libertarian Party of Erie Cty.* v. *Cuomo*, 970 F.3d 106, 121 (2d Cir. 2020) ("*Libertarian Party*"), *cert. denied sub nom. Libertarian Party* v. *Cuomo*, — S. Ct. — , 2021 WL 2519117 (June 21, 2021); *Makarova* v. *United States*, 201 F.3d 110, 113 (2d Cir. 2000). "In ruling on a motion to dismiss under Rule 12(b)(1) for lack of statutory or constitutional power to adjudicate the action, the district court 'may refer to evidence outside the pleadings,'" *Libertarian Party*, 970 F.3d at 120-21 (quoting *Makarova*, 201 F.3d at 113), which evidence may include affidavits submitted by the parties, *see Broidy Cap. Mgmt. LLC* v. *Benomar*, 944 F.3d 436, 441 (2d

Cir. 2019) (quoting *Kamen* v. *Am. Tel. & Tel. Co.*, 791 F.2d 1006, 1011 (2d Cir. 1986)).

2. Plaintiff Has Established Article III Standing

a. Applicable Law

Federal courts are courts of limited jurisdiction and as such may not adjudicate matters that fall outside their subject matter jurisdiction. *See McMorris*, 995 F.3d at 299; Fed. R. Civ. P. 12(h)(3). To bring a case or controversy within the subject matter jurisdiction of federal courts, a plaintiff must have standing under Article III of the Constitution, which requires "a 'personal stake' in the outcome 'throughout the life of the lawsuit.'" *Libertarian Party*, 970 F.3d at 121 (quoting *Cook* v. *Colgate Univ.*, 992 F.2d 17, 19 (2d Cir. 1993)). "In a class action, 'federal courts lack jurisdiction if no named plaintiff has standing.'" *McMorris*, 995 F.3d at 299 (quoting *Frank* v. *Gaos*, 139 S. Ct. 1041, 1046 (2019)); *see also Lewis* v. *Casey*, 518 U.S. 343, 357 (1996) ("[N]amed plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." (internal quotation marks omitted)).

To establish standing, "a plaintiff must demonstrate [i] that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, [ii] that the injury was caused by the defendant, and [iii] that the injury would likely be redressed by the requested judicial relief." *Thole* v. *U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020); *accord McMorris*, 995 F.3d at 299-

300. "The party invoking federal jurisdiction bears the burden of establishing" each element of standing, which "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of litigation." *Lujan* v. *Defs. of Wildlife*, 504 U.S. 555, 561 (1992). Defendants' motion addresses only the first element — the existence of a cognizable injury in fact — and thus the Court focuses on that element.[2]

"[T]he Supreme Court has made clear that 'allegations of possible future injury' or even an 'objectively reasonable likelihood' of future injury are insufficient to confer standing." *McMorris*, 995 F.3d at 300 (quoting *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 409-10 (2013)). Rather, a future injury may support standing only if "the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Id.* (quoting *Susan B. Anthony List* v. *Driehaus*, 573 U.S. 149, 158 (2014)).

---

[2] The Court is satisfied that Plaintiff's allegations satisfy the requirements of causation and redressability. Plaintiff adequately alleges that the injuries he suffered are "fairly traceable" to Defendants' actions in collecting and storing PII without following proper data security principles or implementing adequate cyber security measures. (*See* Compl. ¶¶ 56-65). *See, e.g.*, *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 60-61 (D.C. Cir. 2019) ("*OPM*"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) ("*Zappos*"). And the Court concludes that "it is likely and not merely speculative that the plaintiff's injury will be remedied" by the damages and other forms of relief sought. *Sprint Commc'ns Co., L.P.* v. *APCC Services, Inc.*, 554 U.S. 269, 273 (2008) (internal quotation marks omitted); *see also Zappos*, 888 F.3d at 1030 ("If Plaintiffs succeed on the merits, any proven injury could be compensated through damages. And at least some of their requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit and the like." (internal citation omitted)).

b. Analysis

Defendants argue that "[t]he Complaint contains no allegation that Plaintiff suffered any actual present injury whatsoever as a result of the Breach," and that "[b]ecause none of his sensitive financial or other information was impacted, Plaintiff does not and cannot allege that the risk of future injury is 'certainly impending,' imminent, or substantially likely." (Def. Br. 5 (quoting *Whalen* v. *Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) (summary order)); *see also* Def. Reply 1-7). Plaintiff responds that he has adequately alleged an imminent risk of identity theft as a result of the improper accessing of a document containing his name, signature, email address, mailing address, phone number, and employee identification number, which information Plaintiff claims is "precisely the type of information that can be used to commit identity theft." (Pl. Opp. 7-8, n.5).

In its recent decision in *McMorris*, the Second Circuit held for the first time that plaintiffs may establish standing based solely on an increased risk of future identity theft or fraud following the unauthorized disclosure of their data. 995 F.3d at 300-01 (citing *Susan B. Anthony List*, 573 U.S. at 158). The inciting incident in *McMorris* was the accidental disclosure of a spreadsheet containing the PII of a company's current and former employees to all current employees. *Id.* at 298. The plaintiffs were individuals whose information had been shared as a result of the disclosure, and they alleged that they were "'at imminent risk of suffering identity theft' and becoming the victims of 'unknown but certainly impending future crimes.'" *Id.* In contrast to Fowler, the

McMorris plaintiffs "did not allege that the PII in the spreadsheet was ever shared with anyone outside of [the company] or taken or misused by any third parties." *Id.*

The Second Circuit ultimately concluded that the *McMorris* plaintiffs had not established Article III standing, but in reaching that conclusion the Court clarified certain factors that should be considered when evaluating standing in the context of an unauthorized disclosure of PII. *See* 995 F.3d at 301-03 (surveying caselaw from sister circuits). Specifically, the Court held that:

> courts confronted with allegations that plaintiffs are at an increased risk of identity theft or fraud based on an unauthorized data disclosure should consider the following non-exhaustive factors in determining whether those plaintiffs have adequately alleged an Article III injury in fact: [i] whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; [ii] whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and [iii] whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Id. at 303. However, the Court also reiterated that "determining standing is an inherently fact-specific inquiry that 'requires careful judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted.'" *Id.* at 302 (quoting *Allen* v. *Wright*, 468 U.S. 737, 752 (1984)).

Here, the Court finds that the first and second *McMorris* factors point strongly in favor of finding that Plaintiff has standing. *First*, as alleged, the Data Breach was the result of a phishing attack — in other words, a "targeted

attempt to obtain" the GE employee data held by Canon. (*See* Compl. ¶ 46; *see also id.* at ¶ 44 (acknowledging that "an unauthorized party" gained access to the Canon email account containing GE employees' PII)). *Second*, although Plaintiff does not allege that he has yet experienced identity theft as a result of the Data Breach, he does allege that he has received phishing and scam emails to his personal email address and phishing and scam phone calls to his personal phone number. (Fowler Decl. ¶¶ 2-3). The Complaint further alleges that Baz and other proposed class members have already suffered identity theft, fraud, and abuse. (Compl. ¶¶ 17-20, 79, 104, 119, 125, 182).[3] These allegations satisfy the prong of misuse of the improperly obtained data. *See McMorris*, 995 F.3d at 304 (collecting cases in which some part of the exposed dataset was shown to have been compromised).

With respect to the third factor — whether the stolen data is sufficiently sensitive to create a high risk of identity or fraud — Defendants argue that the information purportedly obtained about Plaintiff is "publicly available even in

[3] Baz alleged that following the Data Breach he personally dealt with fraudulent charges to his bank account, electronic solicitations regarding his social security number and his date of birth, and the fraudulent use of his daughter's social security number, and had to expend substantial time and money to resolve the existing fraudulent activity and to detect and prevent future misuse. (Compl. ¶¶ 17-20). He further attested that "[a]part from the Data Breach, Plaintiff Baz is unaware of any other breaches where his [Personal Financial Information ('PFI')] was compromised within the last year[.]" (*Id.* at ¶ 17). However, in a declaration in support of Defendants' motion to dismiss, James Allen, Canon's Senior Director for Digital Transformation Services, asserts that "[t]he Potentially Affected Emails did not include any personal information of or relating to Maher Baz." (Allen Decl. ¶ 5). While one possible explanation for this inconsistency is that the harms Baz allegedly suffered resulted from a separate data breach of which Baz was not made aware, another possibility is that the Data Breach was more extensive than the Allen Declaration represents. The Court need not resolve this factual issue at this stage because, as discussed below, the Court concludes that Plaintiff Fowler has adequately alleged standing, even accepting that the scope of the Data Breach was as narrow as Canon claims.

the absence of any data breach" and "is not sensitive financially or otherwise." (Def. Br. 8 (citing *Antman* v. *Uber Techs., Inc.*, No. 3:15 Civ. 1175 (LB), 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015); *Rahman* v. *Marriott Int'l, Inc.*, No. SA Civ. 20-654 (DOC) (KES), 2021 WL 346421, at *2 (C.D. Cal. Jan. 12, 2021)); *see also* Def. Reply 2 (citing *Whalen*, 689 F. App'x at 90; *Jantzer* v. *Elizabethtown Cmty. Hosp.*, No. 8:19 Civ. 791 (BKS) (DJS), 2020 WL 2404764, at *2, 4-5 (N.D.N.Y. May 12, 2020); *Rudolph* v. *Hudson's Bay Co.*, No. 18 Civ. 8472 (PKC), 2019 WL 2023713, at *3-4 (S.D.N.Y. May 7, 2019))).

Plaintiff responds that the information about him that was compromised "is not publicly available all in one place," so far as he knows (Pl. Opp. 8 n.5), and that the exposure of his email address, phone number, employee identification number, and home address "provides hackers the means to commit fraud or identity theft by way of a social engineering attack" (*id.* at 9). In support, he cites several out-of-circuit decisions finding standing based on theft of this type of information, among others. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-28 (9th Cir. 2018) (finding standing where "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information" was stolen by hackers); *Bass* v. *Facebook, Inc.*, 394 F. Supp. 3d 1024, 1033-35 (N.D. Cal. 2019) (finding standing where the plaintiff's "name, email address, telephone number, date of birth, locations, work and education history, hometown, relationship status, and photographs now reside with criminals" as a result of a Facebook data breach, and the plaintiff had been "bombarded" with phishing

emails and text messages); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 454, 457-66 (D. Md. 2020) (finding injury in fact where hackers obtained "names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, payment card expiration dates, and tools needed to decrypt cardholder data"). While it is indisputable that the PII concerning Plaintiff that Canon claims was accessed is not as sensitive as social security numbers, account passwords, or bank account information, the Court agrees with its colleague in *Bass* that "information taken … need not be sensitive to weaponize hackers in their quest to commit further fraud or identity theft," and that even an individual's email address, mailing address, telephone number, and employment information can "provide further ammo" to nefarious actors. 394 F. Supp. 3d at 1034. Thus, while the third factor does not support Plaintiff's claim to standing as strongly as do the first two, it also does not undermine it.

In sum, the Court concludes that Plaintiff has made a sufficient showing at this stage of the litigation to establish his standing under Article III, based on the circumstances of the Data Breach, the allegations regarding misuse of PII exposed in the Data Breach, and the potential uses of the PII to target Plaintiff and other class members for identity theft or fraud. Accordingly, the Court denies Defendants' motion to dismiss the Complaint under Rule 12(b)(1).

B. The Court Grants in Part and Denies in Part Defendants' Motion to Dismiss for Failure to State a Claim

Plaintiff's Complaint asserts claims for negligence, negligence *per se*, breach of express contract, breach of implied contract, violation of New York's General Business Law ("GBL") Section 349, and breach of fiduciary duty. Defendants move to dismiss each of these claims under Federal Rule of Civil Procedure 12(b)(6). For the reasons that follow, the Court grants Defendants' motion in part and denies the motion in part.

1. Legal Standards Under Federal Rule of Civil Procedure 12(b)(6)

To survive a motion to dismiss pursuant to Rule 12(b)(6), a plaintiff must plead sufficient factual allegations "to state a claim to relief that is plausible on its face." *Bell Atl. Corp.* v. *Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft* v. *Iqbal*, 556 U.S. 662, 678 (2009). In determining the viability of Plaintiff's claims, the Court must accept as true all well-pleaded factual allegations in the Complaint. *Id.* at 678. Additionally, the Court may consider any written instrument attached to the Complaint as an exhibit, any statements or documents incorporated by reference in the complaint, and documents that are "integral" to the Complaint even if they are not incorporated by reference. *See Chambers* v. *Time Warner, Inc.*, 282 F.3d 147, 152-53 (2d Cir. 2002); *see generally Goel* v. *Bunge, Ltd.*, 820 F.3d 554, 559 (2d Cir. 2016) (discussing materials that may properly be considered in resolving a motion brought under Fed. R. Civ. P. 12(b)(6)).

2. Plaintiff's Claims for Negligence and Negligence *Per Se*

Plaintiff's first two claims are for negligence and negligence *per se*, raised on behalf of himself and a proposed nationwide class against both Defendants. Specifically, Plaintiff alleges, with respect to the negligence claim, that: (i) Defendants had a duty to exercise reasonable care in safeguarding and protecting the personal and financial information of GE employees; (ii) Defendants violated this duty by failing to implement appropriate data security systems and processes; (iii) Defendants' wrongful actions directly and proximately caused the Data Breach; and (iv) the Data Breach resulted in identity theft and abuse, monetary losses, reduced value of the stolen PII, time spent addressing the consequences of the Data Breach, and other economic and non-economic harms. (*See* Compl. ¶¶ 94-104). With respect to the negligence *per se* claim, Plaintiff additionally alleges that Defendants' failure to use reasonable measures to protect the personal and financial information of the proposed class members violated the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits unfair business practices. (*Id.* at ¶¶ 105-113). In their motion to dismiss, Defendants argue that "Plaintiff's two negligence-based claims are insufficient as a matter of law because he has failed to allege any cognizable damages," and that his negligence *per se* claim "fails for the additional reason that the [FTCA] … does not provide for a private right of action." (Def. Br. 13-14). For the reasons stated below, the Court denies Defendants' motion to dismiss Plaintiff's negligence claim, but grants the motion as to his negligence *per se* claim.

a. Negligence

To plead a viable negligence claim under New York law, a plaintiff must plausibly allege that "[i] the defendant owed the plaintiff a cognizable duty of care; [ii] the defendant breached that duty; and [iii] the plaintiff suffered damage as a proximate result." *Ferreira* v. *City of Binghamton*, 975 F.3d 255, 266 (2d Cir. 2020) (quoting *Williams* v. *Utica Coll. of Syracuse Univ.*, 453 F.3d 112, 116 (2d Cir. 2006)).[4] The Court addresses each of these elements in turn.

First, Plaintiff adequately alleges that Defendants owed him and proposed class members a duty to exercise reasonable care in safeguarding their PII, which duty arose out of the "special relationship that existed between GE and its employees," GE's requirement that employees "submit non-public, sensitive personal and financial information for purposes of employment with GE[,]" and Defendants' exclusive ability to implement security measures within their computer systems. (Compl. ¶¶ 95-97; *see also id.* at ¶¶ 56-57). New York courts have found a duty of care in such situations because of the asymmetries of power and capabilities between employees and employers. *See, e.g.*, *Sackin* v. *TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) ("[E]mployers have a duty to take reasonable precautions to protect the PII that they require from employees. Employees ordinarily have no means to protect

[4] Plaintiff does not identify in the Complaint the state under whose law he asserts his common law claims. However, his jurisdiction and venue allegations point towards New York (*see* Compl. ¶¶ 12-14), the remaining state statutory claim concerns a New York statute (*see id.* at ¶¶ 138-146), and he discusses New York law in his opposition to the motion to dismiss (*see* Pl. Opp. 14-25). Accordingly, the Court concludes that Plaintiff's claims are properly analyzed under New York law.

that information in the hands of the employer, nor is withholding their PII a realistic option."). Employers are "best positioned to avoid the harm in question," and thus may be expected to bear the burden of doing so. *Id.* (quoting *In re N.Y.C. Asbestos Litig.*, 27 N.Y.3d 765, 788 (2016)); *cf. Wallace* v. *Health Quest Sys., Inc.*, No. 20 Civ. 545 (VB), 2021 WL 1109727, at *9 (S.D.N.Y. Mar. 23, 2021) (finding that plaintiffs plausibly pleaded that an operator of hospitals and healthcare providers owed a duty of care to safeguard customers' and patients' sensitive personal information).

Second, the Complaint alleges that Defendants breached this duty by "failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the personal and financial information entrusted to [them]," despite a reasonably foreseeable risk that such failure "would result in the unauthorized release, disclosure, and dissemination of [Plaintiff's] and Class members' personal and financial information." (Compl. ¶ 98; *see also id.* at ¶¶ 59, 99-100). Again, this Court agrees with others that have found such allegations sufficient to sustain a negligence claim. *See Wallace*, 2021 WL 1109727, at *9; *Sackin*, 278 F. Supp. 3d at 748 (finding negligence allegations to be adequate where plaintiffs alleged that defendant "was aware of the sensitivity of PII and the need to protect it," but despite this knowledge "failed to take reasonable steps to prevent the wrongful dissemination of Plaintiffs' PII — including erecting a

digital firewall, conducting data security training and adopting retention and destruction policies").

Third, Defendants' arguments notwithstanding (*see* Def. Br. 14-15), the Court finds that Plaintiff has alleged that he and proposed class members incurred concrete damages as a proximate result of the Data Breach.[5] Specifically, Plaintiff alleges that he and proposed class members have suffered:

> ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; … loss of the confidentiality of the stolen confidential data; … expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

(Compl. ¶ 104; *see also id.* at ¶ 79). Accepted as true, these allegations are sufficient to survive Defendants' motion to dismiss. *See Sackin*, 278 F. Supp. 3d at 749 ("[T]he Complaint adequately alleges that Plaintiffs face an imminent threat of identity theft and have purchased preventive services to mitigate the threat. These mitigation expenses satisfy the injury requirements of negligence[.]"); *Wallace*, 2021 WL 1109727, at *6 (finding plausible allegations

[5] "Pleading damages to support a cause of action is distinct from pleading injury-in-fact to support standing." *Wallace* v. *Health Quest Sys., Inc.*, No. 20 Civ. 545 (VB), 2021 WL 1109727, at *5 (S.D.N.Y. Mar. 23, 2021) (citing *Doe* v. *Chao*, 540 U.S. 614, 624-25 (2004)). Consequently, the Court's determination that Plaintiff has adequately alleged an injury in fact to survive Defendants' motion to dismiss under Rule 12(b)(1) is not dispositive; the Court must separately assess whether he has pleaded cognizable damages to survive the motion under Rule 12(b)(6).

of monetary damages where plaintiffs, *inter alia*, "allege[d] they purchased credit monitoring and identity protection services to reduce the risk of future identity theft from the Data Breach"); *cf. Anderson* v. *Hannaford Bros. Co.*, 659 F.3d 151, 162-67 (1st Cir. 2011) (finding, under Maine law, that expenditures to reduce risks stemming from a data theft "are recoverable as mitigation damages so long as they are reasonable"); *Walters* v. *Kimpton Hotel & Rest. Grp., LLC*, No. 16 Civ. 5387 (VC), 2017 WL 1398660, at *2 (N.D. Cal. Apr. 13, 2017) (finding that plaintiff "sufficiently alleged actual damages flowing from the alleged breach, including having to secure and maintain credit monitoring services (which presumably come at a cost) and other out-of-pocket expenses and the value of … time reasonably incurred to remedy or mitigate the breach." (internal quotation marks omitted) (quoting *In re Anthem, Inc. Data Breach Litig.*, No. 15 MD 2617 (LHK), 2016 WL 3029783, at *16 (N.D. Cal. May 27, 2016))). *But see Wallace*, 2021 WL 1109727, at *7-8 (rejecting plaintiffs' allegations of damages based on time spent mitigating or remedying attempted fraud or monitoring their credit, the threat of future harm through fraud, and the diminished value of plaintiffs' private information).

In sum, the Court concludes that Plaintiff has sufficiently alleged the elements of a negligence claim — a duty of care, a breach of that duty, and cognizable damages resulting from the breach — to survive Defendants' motion to dismiss under Rule 12(b)(6).

b. Negligence *Per Se*

Under New York law, "the unexcused omission or violation of a duty imposed by statute for the benefit of a particular class *is* negligence itself." *Timperio* v. *Bronx-Lebanon Hosp. Ctr.*, 384 F. Supp. 3d 425, 434 (S.D.N.Y. 2019) (emphasis in original) (internal quotation marks omitted) (quoting *Chen* v. *United States*, 854 F.2d 622, 627 (2d Cir. 1988)). However, "the mere violation of a statute does not automatically constitute negligence *per se*." *Id.* (internal quotation marks and alterations omitted) (quoting *German by German* v. *Fed. Home Loan Mortg. Corp.*, 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995)). Rather, "in order to warrant a finding of negligence *per se* for a statutory violation, the statute must evidence an intention, express or implied, that from disregard of its command a liability for resultant damages shall arise which would not exist but for the statute." *Id.* (internal quotation marks omitted) (quoting *German by German*, 896 F. Supp. at 1397).

To determine whether a statute may support a claim of negligence *per se*, the Court must consider "[i] whether the plaintiff is one of the class for whose benefit the statute was enacted, [ii] whether a finding of negligence *per se* for violation of the statute would promote the legislative purpose, and [iii] whether creation of such liability would be consistent with the legislative scheme." *Timperio*, 384 F. Supp. 3d at 435 (quoting *German by German*, 896 F. Supp. at 1397); *see also Buchanan for Buchanan* v. *Hesse*, No. 18 Civ. 1566 (VB), 2021 WL 705757, at *6 (S.D.N.Y. Feb. 22, 2021) (explaining that a statute may give rise to a duty of care "when the purpose of the legislation or regulation, in

whole or in part, is '[i] to protect a class of persons which includes the one whose interest is invaded, [ii] to protect the particular interest which is invaded, [iii] to protect that interest against the kind of harm which has resulted, and [iv] to protect that interest against the particular hazard from which the harm results.'" (quoting *Signature Health Ctr., LLC* v. *State*, 902 N.Y.S.2d 893, 903 (N.Y. Ct. Cl. 2010))).

Plaintiff bases his negligence *per se* claim on Section 5 of the FTCA, which makes unlawful "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). This provision has been interpreted by courts outside this Circuit to apply to a company's failure to implement appropriate cybersecurity measures and safeguard consumers' personal data. *See, e.g.*, *F.T.C.* v. *Wyndham Worldwide Corp.*, 799 F.3d 236, 244-49 (3d Cir. 2015); *accord In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019). Defendants argue that Section 5 does not support a negligence *per se* claim because it "does not confer a private right of action, and New York courts decline to recognize negligence *per se* claims where no private right of action exists in the statute on which the claim is based." (Def. Br. 15). Plaintiff responds that courts in other districts have held that Section 5 can support a negligence *per se* claim even though it does not provide a private right of action. (Pl. Opp. 16 (citing cases from Georgia, Maryland, and Pennsylvania, applying or recognizing determinations under Georgia law)).

The Court agrees with Defendants that Plaintiff's negligence *per se* claim is not viable under New York law because Section 5 does not provide a private

right of action; instead, the FTCA confers exclusive enforcement authority on the Federal Trade Commission. *See Alfred Dunhill, Ltd.* v. *Interstate Cigar Co.*, 499 F.2d 232, 237 (2d Cir. 1974) ("[T]he provisions of the Federal Trade Commission Act may be enforced only by the Federal Trade Commission. Nowhere does the Act bestow upon either competitors or consumers standing to enforce its provisions."); *accord Dumay* v. *Episcopal Health Servs., Inc.*, No. 19 Civ. 6213 (DLI) (CLP), 2020 WL 3312116, at *2 (E.D.N.Y. June 18, 2020) ("FTCA enforcement actions … fall within the exclusive purview of the Federal Trade Commission."). *See generally* 15 U.S.C. § 45. Thus, allowing Plaintiff's negligence *per se* claim to proceed based on a violation of the FTCA would be inconsistent with the legislative scheme. In so finding, the Court joins other courts in this District and State that have dismissed negligence *per se* claims predicated upon FTCA violations. *See, e.g.*, *Cohen* v. *Ne. Radiology P.C.*, No. 20 Civ. 1202 (VB), 2021 WL 293123, at *7 (S.D.N.Y. Jan. 28, 2021) (determining that the absence of a private right of action under the FTCA "weighs heavily against implying a private right of action necessary to sustain a negligence *per se* claim" and dismissing such claim accordingly); *Smahaj* v. *Retrieval-Masters Creditors Bureau, Inc.*, 131 N.Y.S.3d 817, 827 (N.Y. Sup. Ct. 2020) (dismissing a negligence *per se* claim based on an alleged violation of the FTCA because "if mere proof of a violation of [the statute] were to establish negligence *per se*, plaintiff would effectively be afforded a private right of action that the statute does not recognize" (internal quotation marks and alterations omitted) (quoting *Lugo* v. *St. Nicholas Assoc.*, 772 N.Y.S.2d 449, 454-55 (N.Y. Sup. Ct. 2003),

aff'd, 795 N.Y.S.2d 227 (2005), and citing *Moore* v. *N.Y. Cotton Exch.*, 270 U.S. 593, 602-03 (1926))). *But see In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407-08 (E.D. Va. 2020) (holding that New York law would permit plaintiffs to assert a negligence *per se* claim premised on Section 5 of the FTCA). Accordingly, the Court dismisses Plaintiff's claim for negligence *per se*.

3. Plaintiff's Claims for Breach of Contract and Implied Breach of Contract

Plaintiff next raises claims against GE for breach of express contract and breach of implied contract. He first alleges that he and the proposed class members "entered into express contracts with GE that included GE's promise to protect nonpublic personal information given to GE from disclosure." (Compl. ¶ 115). Plaintiff specifically cites the aforementioned GE guidance document, "The Spirit & The Letter," which sets forth GE's Code of Conduct and summarizes a range of compliance policies, including policies related to data protection. (*Id.* at ¶ 116; *see generally* The Spirit and the Letter). Alternatively, Plaintiff argues that in providing personal and financial information to GE as a condition of employment, Plaintiff and proposed class members "entered into implied contracts with GE by which GE agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised, or stolen." (Compl. ¶ 122). Defendants move to dismiss both claims, arguing that Plaintiff fails to allege the existence of an enforceable agreement or cognizable damages. (Def. Br. 16).

For the reasons stated below, the Court concludes that Plaintiff has not stated a claim for breach of express contract, but has stated a viable claim for breach of implied contract.

"To state a claim in federal court for breach of contract under New York law, a complaint need only allege [i] the existence of an agreement, [ii] adequate performance of the contract by the plaintiff, [iii] breach of contract by the defendant, and [iv] damages." *Ricatto* v. *M3 Innovations Unlimited, Inc.*, No. 18 Civ. 8404 (KPF), 2019 WL 6681558, at *5 (S.D.N.Y. Dec. 6, 2019) (quoting *Harsco Corp.* v. *Segui*, 91 F.3d 337, 348 (2d Cir. 1996)). "To create a binding contract, there must be a manifestation of mutual assent sufficiently definite to assure that the parties are truly in agreement with respect to all material terms." *Sprint Commc'ns Co. L.P.* v. *Jasco Trading, Inc.*, 5 F. Supp. 3d 323, 336 (E.D.N.Y. 2014) (quoting *Tractebel Energy Mktg., Inc.* v. *AEP Power Mktg., Inc.*, 487 F.3d 89, 95 (2d Cir. 2007)). "Generally, a party alleging a breach of contract must demonstrate the existence of a contract reflecting the terms and conditions of their purported agreement." *Reznick* v. *Bluegreen Resorts Mgmt., Inc.*, 62 N.Y.S.3d 460, 462 (2d Dep't 2017) (internal quotation marks and alterations omitted) (quoting *Mandarin Trading Ltd.* v. *Wildenstein*, 16 N.Y.3d 173, 181-82 (2011)). However, "[a] contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the 'presumed' intention of the parties as indicated by their conduct." *Leibowitz* v. *Cornell Univ.*, 584 F.3d 487, 506-07

(2d Cir. 2009) (quoting *Jemzura* v. *Jemzura*, 36 N.Y.2d 496, 503-04 (1975)), *superseded by statute on other grounds*.

Defendants argue that GE's policy documents should not be construed as valid contracts because Plaintiff does not allege "that these documents contained terms that GE offered to Plaintiff, that he accepted, that consideration was exchanged, and that there was mutual assent and intent to be bound by an agreement to safeguard Plaintiff's information against third party hackers." (Def. Br. 17-18). The Court is mindful that "[r]outinely issued employee manuals, handbooks and policy statements should not lightly be converted into binding employment agreements," *Lobosco* v. *N.Y. Tel. Co./NYNEX*, 96 N.Y.2d 312, 317 (2001); *accord Azzolini* v. *Marriott Int'l, Inc.*, 417 F. Supp. 2d 243, 247-48 (S.D.N.Y. 2005), and agrees with Defendants that the documents Plaintiff references are not written with the standard trappings of express contracts, and are thus insufficient to sustain a claim for breach of express contract. Nevertheless, the Court finds that GE's policy documents create implied contracts.

"The Spirit & The Letter" states, *inter alia*: (i) that it "*must* be followed by anyone who works for or represents GE" (The Spirit & The Letter at 2 (emphasis added)); (ii) that "GE employees working with third parties … *must*: [r]equire these parties to agree to comply with relevant aspects of GE's compliance policies … [and] [t]ake action, up to and including terminating a contract, after learning that a third party failed to abide by GE's compliance policies" (*id.* (emphasis added)); (iii) that "GE is committed to collecting,

handling and protecting Personal Information responsibly, and in compliance with applicable privacy and information security laws and GE's Commitment to the Protection of Personal Information (GE's Binding Corporate Rules), where applicable" (*id.* at 17); and (iv) that "GE seeks to protect its networks, systems, devices and information in our possession" and "to maintain appropriate access controls" (*id.*). (*But* see *id.* at 21 (stating that the guidance set forth therein "is not a substitute for [employees'] good judgment, and … cannot cover every conceivable situation")). Additionally, as Plaintiff discusses in detail in the Complaint, GE further expresses its commitment to protecting its employees' sensitive data — and explains the principles to which it adheres and the measures it takes to fulfill that commitment — in its Employee Data Protection Standards and Commitment to the Protection of Personal Information documents. (Compl. ¶¶ 30-31, 34-37).

Plaintiff alleges that "[b]ased on these representations, GE's current and former employees reasonably believed that GE, and any third parties GE contracted with, would protect their Personal Financial Information ["PFI"], including the PFI of their beneficiaries." (Compl. ¶ 38). These allegations are sufficient at this stage to establish the existence of an implied contract. *See Sackin*, 278 F. Supp. 3d at 750-51 (finding an implied contract where the defendant "required and obtained [employees'] PII as part of the employment relationship, evincing an implicit promise … to act reasonably to keep its employees' PII safe," and the defendant's privacy policies and security practices manual stated that the company maintained robust data security procedures);

Enslin v. *The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) (denying a motion to dismiss breach of contract claims where "[d]efendants, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard [Plaintiff's] PII in exchange for his employment"); *cf. Castillo* v. *Seagate Tech., LLC*, No. 16 Civ. 1958 (RS), 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016) ("[I]t 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.").

The Court additionally finds that Plaintiff has adequately alleged the remaining elements of his breach of implied contract claim, *i.e.*, adequate performance of the contract by Plaintiff, breach of contract by GE, and damages. *First*, Plaintiff alleges that he and the proposed class members provided GE with their personal information as required as a condition of their employment, and thus "fully performed their obligations under the implied contracts with GE." (*See* Compl. ¶¶ 122-123). *Second*, Plaintiff alleges that GE breached the implied contracts "by failing to safeguard and protect [employees'] personal and financial information, … and by failing to provide timely and accurate notice to them that personal and financial information, along with the personal information of their beneficiaries and dependents, was compromised as a result of the data breach." (*Id.* at ¶ 124; *see also id.* at ¶ 40 ("GE failed to maintain the confidentiality of PFI, … failed to prevent the unauthorized disclosure of PFI outside of GE, and failed to provide security measures

consistent with industry standards for the protection of PFI, of its current and former employees and the beneficiaries of GE's employees.")). *Third*, as discussed previously with respect to Plaintiff's negligence claim, Plaintiff has adequately pleaded that he and proposed class members suffered cognizable damages as a result of the Data Breach. (*See id.* at ¶¶ 79, 125).

Accordingly, the Court grants Defendants' motion to dismiss Plaintiff's claim for breach of express contract, but denies the motion as to Plaintiff's claim for implied breach of contract.

4. Plaintiff's Claim Under New York General Business Law § 349

Plaintiff's fifth claim is for violation of GBL Section 349, which declares unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. N.Y. Gen. Bus. Law § 349(a). The statute authorizes "any person who has been injured by reason of any violation of this section [to] bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such actions." *Id.* § 349(h). Plaintiff alleges that Defendants violated Section 349 by: (i) misrepresenting material facts regarding Defendants' data privacy and security practices and procedures to safeguard employees' PII from unauthorized disclosure; (ii) misrepresenting material facts regarding Defendants' compliance with federal and state laws pertaining to the privacy and security of class members' PII; (iii) omitting, suppressing, and concealing material facts of the inadequacy of Defendants' data privacy and security protections; (iv) failing to maintain the privacy and

security of class members' PII; and (v) failing to disclose the Data Breach to class members in a timely and accurate manner. (Compl. ¶ 139). Defendants move to dismiss on the grounds that: "[i] Plaintiff does not have standing to bring a GBL claim as he has not alleged a sufficient nexus to New York State; [ii] Defendants' alleged conduct was not 'consumer-oriented'; and [iii] Plaintiff has not alleged any actual injury under the statute." (Def. Br. 20-21).

To maintain a cause of action under Section 349, "a plaintiff must allege that a defendant has engaged in [i] consumer-oriented conduct that is [ii] materially misleading and that [iii] plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Orlander* v. *Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (quoting *Koch* v. *Acker, Merrall & Condit Co.*, 18 N.Y.3d 940, 941 (2012)). The New York Court of Appeals has held that Section 349 "unambiguously evinces a legislative intent to address commercial misconduct occurring within New York[,]" and thus "to qualify as a prohibited act under the statute, the deception of a consumer must occur in New York." *Goshen* v. *Mut. Life Ins. Co. of N.Y.*, 98 N.Y.2d 314, 324-25 (2002). The provision "[is] not intended to police the out-of-state transactions of New York companies, nor [is] it intended to function as a *per se* bar to out-of-state plaintiffs' claims of deceptive acts leading to transactions within the state." *Id.* at 325. Thus, it is irrelevant to this analysis that Plaintiff is a citizen of Kentucky (Compl. ¶ 21), that GE is a New York corporation with its headquarters in Boston (*id.* at ¶ 22), and that Canon is a Delaware corporation with its principal place of business in New York (*id.* at ¶ 23). All that matters is where the alleged deceptive

conduct occurred. *See Cruz* v. *FXDirectDealer, LLC*, 720 F.3d 115, 122 (2d Cir. 2013) (holding that the focus of the inquiry under Section 349 is "the location of the transaction, and in particular the strength of New York's connection to the allegedly deceptive transaction").

Plaintiff alleges in conclusory terms that "the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in [the] Data Breach was likely stored and/or maintained in accordance with practices emanating from this District" (Compl. ¶ 12), but none of his specific allegations regarding GE's promises to its employees and their beneficiaries regarding protection of PII, the data protection measures Defendants did and did not take, and the manner in which Defendants notified affected persons about the Data Breach identifies the location(s) where Defendants' relevant conduct took place (*see generally id.*). The conduct could have occurred in New York — the state of which GE is a citizen and where Canon has its principal place of business — but it also could have occurred at GE's headquarters in Massachusetts or in any number of other locations, *e.g.*, where Defendants maintain servers, where employees responsible for human resource management and/or information technology work, or where those involved in the Data Breach notification processes work. The Court is unable to discern from the Complaint "the strength of New York's connection" to the allegedly deceptive conduct at issue. Given the *Goshen* Court's warning against "an unwarranted expansive reading of the statute, contrary to legislative intent, and potentially leading to the nationwide, if not

global application of General Business Law § 349," 98 N.Y.2d at 325; *accord* *Cline* v. *TouchTunes Music Corp.*, 211 F. Supp. 3d 628, 634 (S.D.N.Y. 2016), the Court concludes that Plaintiff has not established the requisite nexus between specific deceptive conduct and New York in order to support a claim under the GBL. *See Fishon* v. *Peloton Interactive, Inc.*, No. 19 Civ. 11711 (LJL), 2021 WL 2941820, at *3-5 (S.D.N.Y. July 12, 2021) (dismissing a claim under Section 349 where plaintiff's "allegations merely go to show that [defendant] is based in New York"); *Wright* v. *Publishers Clearing House, Inc.*, 439 F. Supp. 3d 102, 110 (E.D.N.Y. 2020) (denying standing under Section 349 where the facts alleged "neither individually nor cumulatively establish that some part of the underlying transaction occurred in New York State").

Because Plaintiff has not adequately pleaded facts showing cognizable deceptive conduct in New York, the Court need not address the other aspects of a Section 349 claim, *i.e.*, consumer-oriented conduct and injury to Plaintiff and the proposed class members. The Court grants Defendants' motion to dismiss Plaintiff's claim under GBL Section 349.

5. Plaintiff's Claim for Breach of Fiduciary Duty

Finally, Defendants move to dismiss Plaintiff's claim for breach of fiduciary duty. Plaintiff alleges that:

> Defendants became fiduciaries by their undertaking and guardianship of the PII, to act primarily for the benefit of GE's employee[s], former employees, and their beneficiaries, including Plaintiffs and Class Members, [i] for the safeguarding of Plaintiffs' and Class Members' PII; [ii] to timely notify Plaintiffs and Class Members of a data breach and disclosure; and [iii] maintain

> complete and accurate records of what information (and where) Defendants did and does store.

(Compl. ¶ 175). Furthermore, Plaintiff alleges that "[a]s the agent of Defendant GE for purposes of storing, maintaining, and safeguarding Plaintiffs' and Class Members' PII, Defendant GE's fiduciary duty is imputed to Defendant Canon." (*Id.* at ¶ 176). Defendants' alleged breaches include: [i] "failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time"; [ii] "failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII"; [iii] "failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach"; and [iv] "otherwise failing to safeguard Plaintiffs' and Class Members' PII." (*Id.* at ¶¶ 178-181). As a result of these breaches, Plaintiff and proposed class members allegedly suffered the various injuries previously discussed with respect to Plaintiff's other claims. (*See id.* at ¶¶ 79, 182-183). Defendants argue that this claim is not viable because Plaintiff fails to allege the required elements of such a claim, *i.e.*, "[i] a fiduciary duty; [ii] a knowing breach by Defendants; and [iii] cognizable damages as a result of such breach." (Def. Br. 24).

The Court concludes that Plaintiff's breach of fiduciary claim must be dismissed for a different reason: the claim is duplicative of his breach of implied contract claim, which survives Defendants' motion to dismiss. "A breach of fiduciary duty claim is duplicative when it is based on allegations of fiduciary wrongdoing that are expressly raised in plaintiff's breach of contract claim." *Mex. Infrastructure Fin., LLC* v. *Corp. of Hamilton*, No. 17 Civ. 6424

(VSB), 2020 WL 4572679, at *6 (S.D.N.Y. Aug. 7, 2020) (quoting *N. Shipping Funds I, LLC* v. *Icon Cap. Corp.*, 921 F. Supp. 2d 94, 105 (S.D.N.Y. 2013)). When a breach of fiduciary duty claim is "merely a restatement, albeit in slightly different language, of the 'implied' contractual obligations asserted in a cause of action for breach of contract," *Ellington Credit Fund, Ltd.* v. *Select Portfolio Servicing, Inc.*, 837 F. Supp. 2d 162, 193 (S.D.N.Y. 2011) (quoting *Clark-Fitzpatrick, Inc.* v. *Long Island R.R. Co.*, 70 N.Y.2d 382, 390 (1987)), the claim "cannot stand," *id.* (quoting *Grund* v. *Del. Charter Guar. & Tr. Co.*, 788 F. Supp. 2d 226, 249-250 (S.D.N.Y. 2011)); *accord Mex. Infrastructure*, 2020 WL 4572679, at *6; *see also Uni-World Cap., L.P.* v. *Preferred Fragrance, Inc.*, 43 F. Supp. 3d 236, 244 (S.D.N.Y. 2014) (denying leave to replead fiduciary duty claim because "plaintiffs do not allege or point to a single fact supporting the proposed breach of fiduciary duty claim that is not already included in the proposed breach of contract claim"); *Celle* v. *Barclays Bank P.L.C.*, 851 N.Y.S.2d 500, 501 (1st Dep't 2008) ("The breach of fiduciary duty claim was properly dismissed as the agreement covers the precise subject matter of the alleged fiduciary duty." (internal quotation marks and alterations omitted)). Here, the allegations in support of Plaintiff's breach of implied contract claim and breach of fiduciary duty claim are identical in all meaningful respects. (*Compare* Compl. ¶¶ 120-125, *with id.* at ¶¶ 174-183).

Accordingly, the Court grants Defendants' motion to dismiss Plaintiff's breach of fiduciary duty claim.

CONCLUSION[6]

For the foregoing reasons, Defendants' motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) is DENIED. Defendants' motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) is GRANTED with respect to Plaintiff's claims for negligence *per se*, breach of express contract, violation of GBL Section 349, and breach of fiduciary duty. Defendants' motion is DENIED with respect to Plaintiff's claims for negligence and breach of implied contract.

In his opposition brief, Plaintiff makes a cursory request for leave to amend should the Court "grant the motion in any respect." (Pl. Opp. 25). Although the Court acknowledges that Federal Rule of Civil Procedure 15(a)(2) embodies a liberal policy with respect to amendments, the Court denies the request here because Plaintiff has offered no indication as to how he would correct the deficiencies in the claims the Court now dismisses. *See Rosner* v. *Star Gas Partners, L.P.*, 344 F. App'x 642, 644-45 (2d Cir. 2009) (summary order) (finding no abuse of discretion in the district court's denial of leave to amend where plaintiffs had the opportunity to amend following both a pre-motion conference and defendants' filing of briefs in support of dismissal, but instead only informally requested leave to amend in their motion papers and did not specify proposed modifications).

---

[6] The Complaint also asserts a claim for violation of the Florida Deceptive and Unfair Trade Practices Act, on behalf of Baz and a proposed class of Florida residents. (Compl. ¶¶ 126-137). However, the Court understands that Baz's voluntary dismissal of his claims disposed of this claim (*see* Dkt. #54), and the parties do not address it in their briefing.

Defendants are hereby ORDERED to file a responsive pleading on or before **August 27, 2021**. Further, the parties are hereby ORDERED to submit a proposed case management plan to the Court on or before **September 3, 2021**.

The Clerk of Court is directed to terminate the motion at docket entry 57.

SO ORDERED.

Dated: August 4, 2021
New York, New York

Katherine Polk Failla

KATHERINE POLK FAILLA
United States District Judge