UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JENNIFER RAND, individually and on behalf of a class similarly situated, Plaintiff, v. THE TRAVELERS INDEMNITY COMPANY, Defendant.	**OPINION AND ORDER** 21 CV 10744 (VB)

Briccetti, J.:

Plaintiff Jennifer Rand brings this putative class action against defendant The Travelers Indemnity Company ("Travelers"), arising out of Travelers's disclosure of plaintiff's personal identifying information ("PII") to non-party cybercriminals. Plaintiff asserts claims under the Driver's Privacy Protection Act (the "DPPA") and Section 349 of the New York State General Business Law, as well as state law claims for negligence and negligence per se.

Now pending is Travelers's motion to dismiss the amended complaint under Rules 12(b)(1) and 12(b)(6). (Doc. #23).

For the foregoing reasons, the motion is GRANTED IN PART and DENIED IN PART.

BACKGROUND

For the purpose of the ruling on the motion, the Court accepts as true all well-pleaded allegations in the amended complaint and draws all reasonable inferences in plaintiff's favor, as summarized below.

Travelers and its related entitles provide insurance, banking, investment, retirement, and mortgage services.

Plaintiff alleges Travelers designed its website to ensure agents could generate insurance quotes for consumers as seamlessly as possible through a "'shortcut' process." (Doc. #20 ("Am.

Compl.") ¶¶ 44–46). Specifically, plaintiff contends an agent seeking to generate a quote for an individual consumer could do so by providing only "minimal information" about the consumer, such as a name, address, and date of birth. (Am. Compl. ¶¶ 44, 49). Plaintiff further alleges that once an agent requests a quote through the agency portal, Travelers provides a final insurance quote that auto-populates with PII regarding the individual, including the individual's driver's license number. This PII is allegedly drawn from the relevant state's department of motor vehicles ("DMV") or other third parties that receive the PII from DMVs.

Plaintiff contends needing minimal consumer information to generate a quote "is by design" as it "allows Defendant to employ less [agents] and handle less phone calls from consumers." (Am. Compl. ¶ 45). Plaintiff further alleges Travelers's insurance-quote application process "is easily exploitable by non-parties to obtain the PII of other individuals . . . who are not voluntary customers" of Travelers. (Am. Compl. ¶ 48).

On February 16, 2021, and again on March 30, 2021, the New York State Department of Financial Services ("NYSDFS") issued cybersecurity fraud alerts warning regulated financial entities like Travelers that cybercriminals were targeting "websites that offer instant online automobile insurance premium quotes" to steal driver's license numbers. (Am. Compl. ¶¶ 67, 71, 75). In light of the "serious risk of theft and consumer harm" posed by the instant quote system, NYSDFS recommended numerous data security measures, including redacting PII, "disabl[ing] prefill of redacted" PII, or "avoid[ing] displaying prefilled [PII] on public-facing websites" entirely. (Am. Compl. ¶¶ 73, 77–78).

Plaintiff alleges she received a December 10, 2021, notice from Travelers that an unauthorized party may have accessed her name, address, date of birth, and driver's license number by improperly using the credentials of Travelers agents to access Travelers's agency

portal (the "Travelers Notice"). Plaintiff maintains she never applied for Travelers insurance on her own and is not a voluntary customer of Travelers.

As a result, Travelers allegedly offered plaintiff and the putative class members "complimentary identity theft and credit monitoring services for a period of one year." (Am. Compl. ¶ 57).

Plaintiff claims she spent "valuable time and resources in an effort to detect and prevent any additional misuses of her PII" and protect against "the heightened risk for fraud and identity theft" for years to come. (Am. Compl. ¶¶ 39–40). Plaintiff also claims she and putative class members "face years of constant surveillance of their financial and personal records, monitoring, and loss of rights" and they "are incurring and will continue to incur such damages in addition to any fraudulent use of their PII." (Am. Compl. ¶¶ 147–148). Plaintiff further alleges she and putative class members incurred "[c]osts associated with requested credit freezes," "[c]osts associated with the detection and prevention of identity theft," "[c]osts associated with purchasing credit monitoring and identity theft protection services," and "[l]owered credit scores resulting from credit inquiries following fraudulent activities." (Am. Compl. ¶ 173).

DISCUSSION

I. Standards of Review

A. Rule 12(b)(1)

"[F]ederal courts are courts of limited jurisdiction and lack the power to disregard such limits as have been imposed by the Constitution or Congress." Durant, Nichols, Houston, Hodgson & Cortese-Costa, P.C. v. Dupont, 565 F.3d 56, 62 (2d Cir. 2009).[1] "A case is properly

[1] Unless otherwise indicated, case quotations omit all internal citations, quotation marks, footnotes, and alterations.

dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it." Nike, Inc. v. Already, LLC, 663 F.3d 89, 94 (2d Cir. 2011), aff'd, 568 U.S. 85 (2013). "The party invoking the court's jurisdiction bears the burden of establishing jurisdiction exists." Conyers v. Rossides, 558 F.3d 137, 143 (2d Cir. 2009).

"When the Rule 12(b)(1) motion is facial, i.e., based solely on the allegations of the complaint . . . , the plaintiff has no evidentiary burden," and "[t]he task of the district court is to determine whether the [complaint] alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue." Carter v. HealthPort Techs., LLC, 822 F.3d 47, 56 (2d Cir. 2016).

In deciding a motion to dismiss under Rule 12(b)(1) at the pleading stage, the court "must accept as true all material facts alleged in the complaint and draw all reasonable inferences in the plaintiff's favor." Conyers v. Rossides, 558 F.3d at 143. But "argumentative inferences favorable to the party asserting jurisdiction should not be drawn." Buday v. N.Y. Yankees P'ship, 486 F. App'x 894, 895 (2d Cir. 2012) (summary order).

When a defendant moves to dismiss for lack of subject matter jurisdiction and "on other grounds, the court should consider the Rule 12(b)(1) challenge first." Rhulen Agency, Inc. v. Ala. Ins. Guar. Ass'n, 896 F.2d 674, 678 (2d Cir. 1990).

B. Rule 12(b)(6)

In deciding a Rule 12(b)(6) motion, the Court evaluates the sufficiency of the complaint under the "two-pronged approach" articulated by the Supreme Court in Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009). First, a plaintiff's legal conclusions and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements," are not entitled to the assumption of truth and thus are not sufficient to withstand a motion to dismiss. Id. at 678;

Hayden v. Paterson, 594 F.3d 150, 161 (2d Cir. 2010). Second, "[w]hen there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." Ashcroft v. Iqbal, 556 U.S. at 679.

To survive a Rule 12(b)(6) motion, the complaint's allegations must meet a standard of "plausibility." Ashcroft v. Iqbal, 556 U.S. at 678; Bell Atl. Corp. v. Twombly, 550 U.S. 544, 564 (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. at 678. "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. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. at 556).

II. Standing

Travelers argues plaintiff does not allege an injury-in-fact to support Article III standing. The Court disagrees.

A. Legal Standard

To satisfy the "irreducible constitutional minimum of standing . . . [t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016).

An injury-in-fact is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." Spokeo, Inc. v. Robins, 578 U.S. at 339. This is "a low threshold which helps to ensure that the plaintiff has a personal stake in the outcome of the controversy." John v. Whole Foods Mkt. Grp., Inc., 858 F.3d 732, 736 (2d Cir. 2017).

To be concrete, an injury "must actually exist." Spokeo, Inc. v. Robins, 578 U.S. at 340. Further, an injury-in-fact must bear a "close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms." TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

Regarding statutory harms, it is not enough to allege a defendant violated the statute; "[o]nly those plaintiffs who have been concretely harmed by a defendant's statutory violation" will have standing. TransUnion LLC v. Ramirez, 141 S. Ct. at 2205.

"Any monetary loss suffered by the plaintiff satisfies [the injury-in-fact] element; even a small financial loss suffices." Carter v. HealthPort Techs., LLC, 822 F.3d at 55. In the data-breach context, the time and money spent to respond to a data breach may satisfy the injury-in-fact requirement. See Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *6–7 (S.D.N.Y. May 7, 2019). In addition, expenses "reasonably incurred to mitigate [the] risk" of identity theft in the future may also qualify as an injury-in-fact, but only if the plaintiff plausibly alleges a substantial risk of the future identity theft. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021).

In McMorris, the Second Circuit applied a three-factor test to determine whether a plaintiff plausibly alleges a substantial risk of identity theft as part of the injury-in-fact analysis:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

995 F.3d at 303.

Conversely, when plaintiffs "[do] not allege[] a substantial risk of future identity theft," based on the factors discussed above, "the time they spent protecting themselves against this

speculative threat cannot create an injury." McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303.

A plaintiff seeking injunctive relief to prevent future harm may plausibly allege an injury-in-fact if she demonstrates "the risk of [future] harm is sufficiently imminent and substantial." TransUnion LLC v. Ramirez, 141 S. Ct. at 2210. However, "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm." Id. at 2210–11.[2]

B. Analysis

Here, plaintiff adequately pleads injuries-in-fact in the form of a loss of privacy, as well as the harm incurred by attempting to mitigate existing and future identity theft. The Court will address each theory in turn.

1. Loss of Privacy

As an initial matter, plaintiff plausibly alleges injury-in-fact in the form of a loss of privacy protected under the DPPA.

The loss of privacy arising out of the data breach, against which the DPPA was intended to protect, bears a sufficiently "close relationship" to the tort of public disclosure of private information, recognized at common law. TransUnion LLC v. Ramirez, 141 S. Ct. at 2204 (acknowledging disclosure of private information as indicative of the type of harm sufficient to

[2] McMorris, decided before TransUnion, suggested that a sufficiently imminent risk of identity theft, standing alone, could constitute injury-in-fact, even in a suit for damages. See In re Practicefirst Data Breach Litig., 2022 WL 354544, at *4 n.7 (W.D.N.Y. Feb. 2, 2022), report and recommendation adopted, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022). TransUnion appears to have "abrogated this holding in suits for damages by requiring both an imminent risk of future harm and a concrete injury related to the risk." Id. Nevertheless, "McMorris's three-factor test is still instructive for determining whether the risk of injury is imminent, which remains part of the requirement for standing in suits for both damages and injunctive relief, pursuant to TransUnion." Id.

establish injury-in-fact). The privacy tort applies when "one gives publicity to a matter concerning the private life of another," so long as the "matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Restatement (Second) of Torts § 652(D).

Here, plaintiff plausibly alleges Travelers automatically discloses an individual's driver's license information to a third party seeking an insurance quote if the third party provides Travelers with "minimal and basic information" regarding that individual, and, here, Travelers disclosed plaintiff's driver's license number and other PII to an unauthorized third party. (Am. Compl. ¶ 49). Moreover, plaintiff alleges she received the Travelers Notice informing her of the unauthorized access, notwithstanding that she never applied for Travelers insurance on her own and is not a voluntary customer of Travelers. Accepting the allegations in the amended complaint as true and drawing all reasonable inferences in plaintiff's favor, the Court may reasonably infer that an unauthorized third party accessed sensitive information about plaintiff on Travelers's agency portal.

To be clear, it is debatable whether Travelers's disclosure to even a group of cybercriminals improperly accessing plaintiff's PII on the agency portal is sufficiently "public" under the tort, and whether the type of disclosure here is sufficiently "offensive,"[3] but the Supreme Court is clear that the common-law analogue need not be an "exact duplicate." TransUnion LLC v. Ramirez, 141 S. Ct. at 2209; see also Bohnak v. Marsh & McLennan Cos., Inc., 2022 WL 158537, at *5 (S.D.N.Y. Jan. 17, 2022) (plaintiffs had standing in data-breach

[3] Indeed, the Restatement of Torts cautions it is not enough "to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons." Restatement (Second) of Torts § 652D.

case because "disclosing [private] information to third parties without authorization or consent could plausibly be offensive to a reasonable person").

Accordingly, the Court concludes that at this early stage in the litigation, plaintiff's allegations sufficiently resemble the type of loss in privacy protected by the tort of public disclosure of private information such that the loss constitutes an injury-in-fact.

2. Costs Mitigating the Risk of Future Identity Theft

To mitigate the risk of future identity theft, plaintiff alleges she and class members have incurred costs associated with "requested credit freezes," "the detection and prevention of identity theft," and "purchasing credit monitoring and identity theft protection services." (Am. Compl. ¶¶ 142, 173).

Although plaintiff does not allege that her PII obtained from Travelers's agency portal, or that of other class members, was actually misused or that there was any attempted misuse after the data breach, "misuse is not necessarily required." Clemens v. ExecuPharm Inc., 48 F.4th 146, 154 (3d Cir. 2022) ("The Seventh Circuit has found standing despite no allegations of misuse."); see also In re Am. Med. Collection Agency, Inc. Consumer Data Sec. Breach Litig., 2021 WL 5937742, at *9–10 (D.N.J. Dec. 16, 2021) (plaintiffs need not "wait until they suffer identity theft to bring their claims"). Further, consideration of the first and third McMorris factors supports a determination that plaintiff's risk of future identity theft is sufficiently imminent and substantial such that the costs incurred to mitigate that risk constitute an independent injury-in-fact. See McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303.

Regarding the first factor, the amended complaint plausibly alleges Travelers discovered suspicious activity by an unauthorized party "us[ing] the credentials of a limited number of agents to access the portal to obtain" individuals' PII, and plaintiff received the Travelers Notice

notwithstanding that she never voluntarily accessed Travelers's system or requested a quote from Travelers. Based thereon, the Court can reasonably infer plaintiff's data was "exposed as the result of a targeted attempt" to obtain sensitive consumer data from Travelers. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303.

Regarding the third factor, plaintiff plausibly alleges her PII on Travelers's system is sufficiently "sensitive such that there is a high risk of identity theft or fraud" upon its disclosure. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303. For example, plaintiff alleges that a driver's license number, available to users of Travelers's agency portal or individuals that request insurance quotes with only minimal consumer information, can be used to file fraudulent unemployment claims, open a new account, take out a loan, or commit income tax refund fraud. Based on this allegation, and the allegation that third parties had already improperly obtained and misused plaintiff's personal information to access the agency portal in the first instance, there is an objectively reasonable likelihood that an injury will result from the data breach.

Accordingly, although it is a close call, the Court concludes plaintiff adequately pleads an imminent risk of future identity theft, and therefore the financial costs plaintiff allegedly incurred mitigating that risk constitute an independent injury-in-fact.

III. DPPA Claim

Travelers argues plaintiff cannot state a claim under the DPPA because she does not plausibly allege Travelers "knowingly or intentionally disclosed her personal information." (Doc. # 24 ("Def. Mem.") at 12).

The Court disagrees.

A. Legal Standard

The DPPA prohibits state and private individuals and entities from "knowingly

disclos[ing] or otherwise mak[ing] available to any person or entity" a range of "personal information"—including driver's license numbers—drawn from state motor vehicle records, unless the disclosure is made for one of fourteen enumerated "permissible uses," including insurance ratings. 18 U.S.C. §§ 2721(a)–(b). "The default rule is one of non-disclosure." Gordon v. Softech Int'l, Inc., 726 F.3d 42, 49 (2d Cir. 2013).

The DPPA also regulates "the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state DMV." Reno v. Condon, 528 U.S. 141, 146 (2000) (citing 18 U.S.C. § 2721(c)). Indeed, the Second Circuit has held such persons are "subject to a duty of reasonable care before disclosing DPPA-protected personal information." Gordon v. Softech Int'l, Inc., 726 F.3d at 56–57.

The DPPA creates a civil cause of action against any "[p]erson who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under" the DPPA. 18 U.S.C. § 2724.

A "knowing disclosure" is a disclosure made voluntarily, not necessarily one made with "knowledge of illegality or potential consequences." Senne v. Village of Palatine, 695 F.3d 597, 603 (7th Cir. 2012) (en banc).

A rediscloser like Travelers—which, as discussed above, is subject to a duty of reasonable care before disclosing DPPA-protected information—may be liable under the DPPA for a third-party recipient's impermissible use of the information, but only if the rediscloser knew or reasonably should have known of the third party's improper purpose before it disclosed the DPPA-protected information. See Gordon v. Softech Int'l, Inc., 726 F.3d at 54.

B. Analysis

Here, plaintiff adequately pleads a claim under the DPPA.

First, plaintiff plausibly alleges Travelers obtained driver's license numbers "from the relevant state's department of motor vehicles . . . or other third parties, such as insurers or data aggregators, who receive this information from state DMVs" (Am. Compl. ¶ 44), and thus were disclosed "from a motor vehicle record." 18 U.S.C. § 2724(a).

Second, Travelers's voluntary decision to auto-populate its quote responses with driver's license numbers constitutes a "knowing disclosure" of personal information. 18 U.S.C. § 2724(a). That is, regardless of how the cybercriminals initially obtained some of plaintiff's PII or how they obtained credentials belonging to Travelers agents, Travelers configured its agency portal to divulge driver's license numbers on insurance quotes based on "minimal and basic" personal information. (Am. Compl. ¶ 49).

Third, plaintiff adequately alleges that in light of the two separate NYSDFS data-security alerts warning Travelers of the vulnerability of its auto-populate data features, Travelers reasonably should have known its auto-populating of driver's license numbers would disclose such protected information directly to cybercriminals for impermissible purposes. See Gordon v. Softech Int'l, Inc., 726 F.3d at 54.

Accordingly, the DPPA claim may proceed.

IV. Negligence

Travelers argues plaintiff fails plausibly to state a negligence claim under New York law because Travelers did not owe a duty of care to plaintiff, who, in any event, does not allege cognizable damages.

The Court disagrees as to Travelers's duty of care.

The Court also disagrees as to plaintiff's damages based on monetary harm.

However, the Court agrees plaintiff's remaining theories of damages are not cognizable

under New York law.

A. Legal Standard

To plead a negligence claim under New York law, a plaintiff must plausibly allege "(1) the defendant owed the plaintiff a cognizable duty of care; (2) the defendant breached that duty; and (3) the plaintiff suffered damage as a proximate result of that breach." Stagl v. Delta Airlines, Inc., 52 F.3d 463, 467 (2d Cir. 1995).

1. Duty of Care

At common law, New York courts evaluate the duty of care by balancing several factors, including "the reasonable expectations of parties and society generally, the proliferation of claims, the likelihood of unlimited or insurer-like liability, disproportionate risk and reparation allocation, and public policies affecting the expansion or limitation of new channels of liability." Hamilton v. Beretta U.S.A. Corp., 96 N.Y.2d 222, 232 (2001). "Foreseeability, alone, does not define duty—it merely determines the scope of the duty once it is determined to exist." Id.

Although appellate courts in New York have yet to address the duty of care owed by custodians or disclosers of PII in this context, district courts applying New York law have determined a duty of care existed when the custodian was "in the best position to protect information on its own servers from data breach," "understood the importance of data security to its business, knew it was the target of cyber-attacks, and touted its data security to current and potential customers," and would not be subject to limitless liability, because liability would have been "limited to the individuals whose personal information it obtained while providing its services." See, e.g., Toretto v. Donnelley Fin. Sols., Inc., 2022 WL 348412, at *12 (S.D.N.Y. Feb. 4, 2022) (proxy service provider that received mutual funds investors' PII owed duty of care to protect those investors' PII, despite lacking a direct relationship with the investors).

2. Damages

It is well established that even when a plaintiff's allegations are sufficient to support standing, the plaintiff must also plead cognizable damages to survive a defendant's motion to dismiss under Rule 12(b)(6). See Doe v. Chao, 540 U.S. 614, 624–25 (2004).

"Under New York's doctrine of avoidable consequences, a plaintiff must minimize damages caused by a defendant's tortious conduct, and can recover mitigation costs for any action reasonable under the circumstances." Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (citing applicable New York law).

However, a plaintiff may only recover damages for a risk of future harm, standing alone, if he or she alleges an expense is "reasonably certain to be incurred" by virtue of the risk. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008).

Moreover, time and effort alone, without ties to lost wages, or otherwise unaccompanied by monetary loss, are not cognizable damages in common law claims for negligence. See, e.g., In re Gen. Motors LLC Ignition Switch Litig., 339 F. Supp. 3d 262, 307 (S.D.N.Y. 2018) (analyzing New York state common law and noting that, with certain exceptions not relevant here, damages for lost time are usually confined to lost wages).

Finally, a plaintiff may only recover damages for the lost value of private information if the plaintiff plausibly alleges the existence of a market for the information and how the value of such information could have decreased due to its disclosure. See Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *8.

B. Analysis

1. Duty of Care

Here, plaintiff plausibly alleges facts that, taken together, support the inference that

Travelers owed plaintiff a duty of reasonable care under New York law. First, plaintiff plausibly alleges Travelers obtained and then redisclosed her PII—without her knowledge or consent—as part of its ordinary course of business, and was thus "in the best position" as between Travelers and plaintiff to protect the information. Toretto v. Donnelley Fin. Sols., Inc., 2022 WL 348412, at *12. Second, plaintiff alleges Travelers actively marketed the strength of its cybersecurity on its website and "knew it was the target of cyber-attacks" because of the two NYSDFS alerts. Id. Third, imposing a duty on Travelers under these alleged circumstances would subject Travelers to liability only with respect to individuals whose personal information was already stolen by cybercriminals from other sources.

Thus, holding a discloser of personal information liable for its own negligence under these circumstances fits comfortably into the "duty equation" articulated by the New York Court of Appeals. See Hamilton v. Beretta U.S.A. Corp., 96 N.Y.2d at 233 (the "key" to the special relationship is that the "defendant [is] is in the best position to protect against the risk of harm" without the "specter of limitless liability"). Accordingly, fixing a duty of care under these circumstances best realizes the expectations of the parties without imposing unlimited liability.

2. Damages

Generally, fees paid to freeze credit reports and costs incurred in purchasing credit monitoring and identity theft services are cognizable expenses incurred for the purpose of avoiding further data-breach-related damages. See Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d at 749 (discussing the "doctrine of avoidable consequences").

However, the mere time and effort plaintiff allegedly expended addressing the consequences of the data breach, standing alone, are not cognizable. See In re Gen. Motors LLC Ignition Switch Litig., 339 F. Supp. 3d at 307. Nor would plaintiff's allegedly lowered credit

score suffice, absent additional allegations regarding the score's actual financial impact.

In addition, even if plaintiff plausibly alleges a substantial risk of identity fraud for the purpose of pleading injury-in-fact, she does not plausibly allege she is "reasonably certain" to incur expenses as a result of her greater exposure to the fraud. See, e.g., Caronia v. Philip Morris USA, Inc., 22 N.Y.3d 439, 446 (2013) (plaintiffs failed to allege present damages due to future risk of cancer caused by smoking). Accordingly, plaintiff falls short of alleging expenses "reasonably certain to be incurred." Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d at 281.

Finally, plaintiff offers only general allegations regarding the value of her PII, and she does not allege she could have monetized her PII or that her PII was actually monetized. Plaintiff thus does not plausibly allege damages based on her PII's lost value. Cf. In re Yahoo! Inc. Customer Data Sec. Breach Litig., 2017 WL 3727318, at *13–14 (N.D. Cal. Aug. 30, 2017) (allegations that information was "highly valuable to identity thieves" and "hackers have sold this [information]," including specific examples of sales, were sufficient to allege plaintiffs lost the value of their private information).[4]

In short, plaintiff's negligence claim may proceed, but only to the extent it is based on monetary costs incurred to mitigate the harm caused by the data breach. To the extent the negligence claim is based on the other alleged theories of damages, it must be dismissed.

[4] The Court agrees with the weight of authority applying New York law and concluding the economic loss doctrine—which prevents recovery for "purely economic losses" absent a "special relationship"—does not apply to data-breach cases. See Toretto v. Donnelley Fin. Sols., Inc., 2022 WL 348412, at *9 (collecting cases). Moreover, even if the economic loss doctrine did apply to data-breach cases, plaintiff's claims would survive because of the "special relationship" imposed by the DPPA, which, as discussed above, requires redisclosers like Travelers to protect against the risk of disclosing plaintiff's driver's license number for impermissible purposes.

V. Negligence Per Se

Travelers argues plaintiff does not state a claim for negligence per se because she does not identify an applicable statutory duty under New York law and does not allege cognizable damages.

The Court disagrees as to Travelers's duty.

For the reasons discussed above regarding plaintiff's negligence claim, the Court also disagrees as to plaintiff's damages based on monetary harm, but agrees plaintiff's remaining theories of damages are not cognizable under New York law.

A duty of care established by statute implicates the rule of negligence per se.

> Under the rule of negligence per se, if a statute is designed to protect a class of persons, in which the plaintiff is included, from the type of harm which in fact occurred as a result of its violation, the issues of the defendant's duty of care to the plaintiff and the defendant's breach of that duty are conclusively established upon proof that the statute was violated.

German by German v. Fed. Home Loan Mortg. Corp., 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995).

Here, in light of the fact that (i) the DPPA "was designed to protect a class of persons" comprising individuals whose PII has been disclosed for an impermissible purpose; (ii) plaintiff plausibly alleges she became a part of that class as a result of Travelers's data breach; and (iii) the improper disclosure of plaintiff's PII to cybercriminals is the "type of harm [that] in fact occurred as a result of [the DPPA's] violation," Travelers's duty of care to plaintiff and its breach of that duty are conclusively established upon proof that it violated the statute. German by German v. Fed. Home Loan Mortg. Corp., 896 F. Supp. at 1396.[5] And, as discussed above,

[5] Plaintiff also alleges breaches of statutory duties purportedly created by Section 5 of the Federal Trade Commission Act, 15 U.S.C § 45 (the "FTCA"), and New York's Shield Act, N.Y. Gen. Bus. Law § 899-aa (the "NY Shield Act"). However, neither statute creates or implies a private right of action, which is a prerequisite to asserting a claim for negligence per se under New York law. See, e.g., Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 131 N.Y.S.3d

plaintiff plausibly alleges Travelers violated the DPPA.

Accordingly, plaintiff's negligence per se claim may proceed, but only to the extent it is based on monetary costs incurred to mitigate the harm caused by the data breach. Plaintiff's negligence per se claim based on the other alleged theories of damages must be dismissed.

VI. General Business Law Section 349

Travelers argues plaintiff does not state a claim under Section 349 because she does not plausibly allege any deceptive conduct "caused" her injuries.

The Court agrees.

Section 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." To assert a claim under Section 349 a "plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) 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).

Although justifiable reliance on the alleged misrepresentation or omission is not a requisite element under Section 349, a plaintiff must plausibly allege she was exposed to the deceptive conduct in the first instance. See Fero v. Excellus Health Plan, Inc., 502 F. Supp. 3d 724, 740 (W.D.N.Y. 2020) (applying New York law and denying class certification in data-breach action because named plaintiff, whose PII was housed on defendant's network, failed to show sufficient evidence that he had any direct dealings with defendant at all). Put another way, "in order to have been injured by the defendant's deceptive act, a plaintiff must have been personally misled or deceived." Id.

817, 827 (Sup. Ct. Westchester Cty. 2020). Accordingly, the negligence per se claim allegedly arising out of either statute must be dismissed.

Here, plaintiff does not plausibly allege she was ever exposed to any purportedly deceptive misrepresentation or omission by Travelers. To the contrary, the well-pleaded allegations that plaintiff never applied for Travelers insurance and was not a voluntary customer of Travelers support the inference that she was not exposed to Travelers before the data breach at all. Plaintiff thus fails plausibly to allege her injuries were "caused" by any deceptive conduct on the part of Travelers.

Accordingly, plaintiff's Section 349 claim must be dismissed.

VII. Declaratory Relief

Travelers argues plaintiff's separate claim for declaratory relief must be dismissed because it is not an independent cause of action.

Travelers is correct there is no independent cause of action for a declaratory judgment, but plaintiff may nevertheless pursue declaratory relief to the extent her substantive claims survive.

The Declaratory Judgment Act, 28 U.S.C. § 2201, does not create an independent cause of action. In re Joint E. & S. Dit. Asbestos Litig., 14 F.3d 726, 231 (2d Cir. 1993). Rather, "[i]ts operation is procedural only—to provide a form of relief previously unavailable. Therefore, a court may only enter a declaratory judgment in favor of a party who has a substantive claim of right to such relief." Id. In other words, a plaintiff properly obtains declaratory relief only "based on other laws"—i.e., a law other than the Declaratory Judgment Act—"that the defendant allegedly violated." In re Methyl Tertiary Butyl Ether ("MBTE") Prods. Liab. Litig., 247 F.R.D. 420, 422–23 (S.D.N.Y. 2007).

Thus, although plaintiff styled her claim for declaratory relief as a separate count, that is not fatal to her claim. In Count V, plaintiff incorporates by reference her earlier allegations and

refers to the specific substantive provisions under which she is allegedly entitled to declaratory relief. Specifically, plaintiff claims pursuant to the Court's "authority under the Declaratory Judgment Act," it should enter a judgment declaring Travelers "owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, the NY Shield Act, and the DPPA." (Am. Compl. ¶ 243(a) (emphasis added)). Plaintiff's claim for declaratory relief is thus derivative of her substantive claims and dependent on whether her underlying claims proceed.

As the Court dismissed plaintiff's claims under Section 5 of the FTCA and the NY Shield Act, plaintiff has no right to declaratory relief related to those statutes. Any request for declaratory relief related to those statutes is dismissed.

Plaintiff may seek declaratory relief with respect to her DPPA, negligence, and negligence per se claims.

VIII. Injunctive Relief

Travelers also argues plaintiff's separate claim for injunctive relief must be dismissed because it is not an independent cause of action.

The Court agrees a request for injunctive relief is not a separate cause of action; however, the Court disagrees that plaintiff's request for injunctive relief must be dismissed.

A plaintiff seeking injunctive relief must plausibly allege "(1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

Here, plaintiff plausibly alleges entitlement to the injunctive relief she seeks. That is, plaintiff seeks injunctive relief in the form of requiring Travelers to implement certain specific security protocols, including engaging third-party auditors to test its systems for weaknesses and regularly testing its systems for security vulnerabilities. Plaintiff alleges she "will likely be subjected to substantial identity theft and other damage" if Travelers does not implement these measures. (Am. Compl. ¶ 245). She also alleges "the cost to Defendant of complying with an injunction by employing" these measures "is relatively minimal," and that an injunction will serve the public interest "by preventing another data breach at" Travelers. (Am. Compl. ¶¶ 246–247).

Thus, at this early stage of the case, plaintiff adequately alleges entitlement to the injunctive relief she seeks, and her request for injunctive relief may proceed.

CONCLUSION

The motion to dismiss under Rule 12(b)(1) is DENIED.

The motion to dismiss under Rule 12(b)(6) is GRANTED IN PART and DENIED IN PART.

Plaintiff's claim under Section 349 of the New York General Business Law is dismissed.

Plaintiff's request for declaratory relief is also dismissed to the extent it is based on Section 5 of the FTCA or the NY Shield Act.

Plaintiff's other claims may proceed.

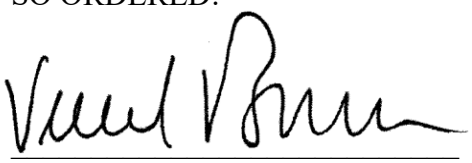
Defendant shall file an answer by November 9, 2022.

By separate order, the Court will schedule an initial pretrial conference.

The Clerk is instructed to terminate the motion. (Doc. #23).

Dated: October 26, 2022
White Plains, NY

SO ORDERED:



Vincent L. Briccetti
United States District Judge