UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In Re:	:	**OPINION AND ORDER**
	:	
USAA DATA SECURITY LITIGATION	:	21 CV 5813 (VB)

Briccetti, J.:

Plaintiffs Vincent Dolan and Christine Mapes bring this consolidated putative class action against defendant United Services Automobile Association ("USAA"), arising out of USAA's disclosure of plaintiffs' driver's license numbers to non-party cybercriminals. Plaintiffs assert 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 USAA's motion to dismiss the amended consolidated complaint under Rules 12(b)(1) and 12(b)(6). (Doc. #35).

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

BACKGROUND

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

USAA provides insurance and financial services to current and former members of the United States military and their families.

Plaintiffs allege USAA designed its website to ensure users could apply for its insurance policies as seamlessly as possible. Specifically, plaintiffs contend an individual seeking a quote for any of USAA's insurance policies could do so by first creating a USAA account, which requires providing "minimal information," such as a name, an address, and a date of birth, and

then answering "yes" to questions regarding the individual's history of military service. (Doc. #34 ("Am. Compl.") ¶¶ 37, 43). Plaintiffs further allege that once the account is made, the USAA member would then receive an online quote form pre-filled with personally identifiable information ("PII") regarding the member drawn from the relevant state's department of motor vehicles ("DMV"), including the member's driver's license number.

According to plaintiffs, a driver's license number ranks among a person's most "highly valuable" PII because it is "readily useable to commit fraud and identity theft." (Am. Compl. ¶ 15). Plaintiffs contend driver's license numbers, particularly when combined with other PII, can be used to "file fraudulent unemployment claims, to open a new account, take out a loan in someone's name, or commit income tax refund fraud," among a "host of other financial crimes." (Id. ¶ 16).

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 USAA that cybercriminals were targeting "websites that offer instant online automobile insurance premium quotes" to steal driver's license numbers. (Am. Compl. ¶ 48). In light of the "serious risk of theft and consumer harm" posed by the instant quote system, the NYSDFS recommended a number of data safety measures, including redacting PII or "avoid[ing] displaying prefilled [PII] on public-facing websites" entirely. (Id. ¶¶ 53–54).

Plaintiffs claim USAA failed to follow any of NYSDFS's recommendations, and, consequently, suffered the "type of data breach that NYSDFS predicted" on May 6, 2021. (Am. Compl. ¶ 57). Cybercriminals allegedly used certain of plaintiffs' PII—stolen from other sources—to create USAA accounts in plaintiffs' names and then steal plaintiffs' driver's license numbers that were automatically disclosed by USAA. Plaintiffs maintain they were never

members of USAA, nor did they have any relationship of any kind with USAA before the data breach.

USAA allegedly informed plaintiffs, as well as the putative class members, of the data breach in a notice dated June 2, 2021 (the "USAA Notice"). In the USAA Notice, USAA claimed that upon learning of the breach, it immediately "blocked access to driver's license information," "enhanc[ed] [its] security measures to help prevent this type of incident in the future," and would be "offering a complimentary two-year membership" to an identity theft detection and resolution program. (Doc. #36-1 ("USAA Notice")).

Plaintiffs contend that in the immediate aftermath of the USAA breach, cybercriminals fraudulently filed a claim for unemployment in plaintiff Dolan's name, and successfully took out an insurance policy from another, unrelated insurance provider in plaintiff Mape's name. Plaintiffs allege they have spent "valuable time and resources" to address the existing identity theft and to guard against the "heightened risk for fraud and identity theft" likely to occur in the future, including by purchasing additional credit monitoring and identity theft protection services. (Am. Compl. ¶¶ 17, 22–23, 26–27, 138). Plaintiffs also allege they incurred "costs associated with requested credit freezes," and also suffered lowered credit scores as a result of repeated inquiries into their credit. (Id. ¶ 138).

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 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, 567 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

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

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).

"In considering a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), a district court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint." DiFolco v. MSNBC Cable L.L.C., 622 F.3d 104, 111 (2d Cir. 2010).

II. Standing of the Named Plaintiffs

USAA argues plaintiffs do not allege an injury-in-fact sufficient 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 295, 303 (2d Cir. 2021).

Conversely, when a plaintiff "[does] 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, plaintiffs adequately plead injuries-in-fact in the form of a loss of privacy, as well

[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.

as the harm incurred by attempting to mitigate existing and future identity theft. The Court will address each theory in turn.[3]

1. Loss of Privacy

As an initial matter, plaintiffs plausibly allege 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 stablish 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, plaintiffs plausibly allege USAA automatically discloses any individual's driver's license information to any third party with "minimal information" regarding that individual, and, in this instance, disclosed plaintiffs' driver's license numbers to cybercriminals for use in further identity fraud, which plaintiffs plausibly contend would be highly offensive to a reasonable person. (Am. Compl. ¶ 38).

To be clear, it is debatable whether USAA's disclosure to even a group of cybercriminals

[3] Contrary to USAA's assertions, plaintiffs also adequately plead traceability, "which is a standard lower than that of proximate causation." Carter v. HealthPort Techs., LLC, 822 F.3d at 55. That is, plaintiffs plausibly allege that "immediately" after the data breach, they suffered the very types of fraudulent activities that are allegedly typically associated with the theft of driver's license numbers: fraudulent insurance and unemployment claims. (Am. Compl. ¶¶ 21, 25).

is sufficiently "public" under the tort, and whether the type of disclosure here is sufficiently "offensive,"[4] but the Supreme Court is equally 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 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, plaintiffs' 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. Direct Harm from Responding to Existing Identity Theft

Plaintiffs allege they have incurred "costs associated with credit freezes" as well as "lowered credit scores resulting from [their] credit inquiries following fraudulent activities." (Am. Compl. ¶ 138). Because these alleged losses implicate monetary harm directly caused by the data breach, they are sufficiently concrete to constitute an injury-in-fact.

Plaintiffs also allege they have spent significant time, effort, and resources addressing the insurance and unemployment claims taken out in their names. Even absent a risk of future identity theft, such "concrete and particularized loss[es] based on actual time spent responding to" the already-occurred identity thefts are sufficient to demonstrate a concrete injury for the purpose of Article III standing. See, e.g., Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *7 (plaintiff's alleged time and expenses incurred in obtaining a new debit card following a data

[4] Indeed, the Restatement of Torts cautions it 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.

breach constituted injury-in-fact, in part because "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective").

3. Costs Mitigating the Risk of Future Identity Theft

Plaintiffs also plausibly allege a risk of future identity theft that is sufficiently imminent and substantial such that the costs incurred to mitigate that risk constitute an independent injury-in-fact.

First, defendants do not dispute the amended consolidated complaint plausibly states plaintiffs' driver's license numbers were "exposed as the result of a targeted attempt to obtain [plaintiffs'] data" on May 16, 2021. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303.

Second, plaintiffs' allegations that cybercriminals used plaintiff Dolan's driver's license number to apply for unemployment benefits in his name, and plaintiff Mapes's driver's license number to obtain an insurance policy in her name, plausibly demonstrate that at least some portion of the at-issue data "has already been misused." McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303.

Third, plaintiffs plausibly allege their driver's license numbers are sufficiently "sensitive such that there is a high risk of identity theft or fraud" upon their disclosure. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d at 303. That is, "plaintiff[s] recognize[] that the drivers' license numbers alone would not be sufficient to forge an identity," but they nevertheless "allege[] that drivers' license numbers, in addition to other personal information already gathered from other sources, can provide an opening for fraud, including applying for credit cards or loans or opening bank accounts." Park v. Am. Fam. Life Ins. Co., 2022 WL 2230171, at *2 (W.D. Wis. June 17, 2022) (plaintiff alleged "objectively reasonable likelihood that an injury will

occur" as a result of cybercriminals' theft of driver's license numbers automatically disclosed in online quotes).[5]

Accordingly, because plaintiffs adequately plead an imminent risk of future identity theft, the costs plaintiffs allegedly incurred mitigating that risk (including fees for credit freezes, fees for credit monitoring services, and the time and resources spent monitoring credit and financial transactions), constitute an independent injury-in-fact.

III. Standing of Putative Class Members

USAA suggests that even if the Court concluded that plaintiffs plausibly alleged injury-in-fact themselves, "this says nothing about whether any unnamed putative class members suffered such an injury." (Doc. #37, at 6 n.4). However, in "a class action, a court must analyze the injuries allegedly suffered by the named plaintiffs, not unnamed members of the potential class, to determine whether the plaintiffs have Article III standing." In re Propranolol Antitrust Litig., 249 F. Supp. 3d 712, 727 (S.D.N.Y. 2017). Accordingly, the Court need not address the standing of any unnamed potential class members at this time.

IV. DPPA Claim

USAA argues plaintiff cannot state a claim under the DPPA because USAA disclosed plaintiffs' driver's license numbers for what it believed to be a permissible purpose.

The Court disagrees.

---

[5] The Court acknowledges that some courts outside this Circuit have declined to find standing in cases involving the automated disclosure of driver's license numbers based on similar "instant quote" systems. See Greenstein v. Noblr Reciprocal Exch., 2022 WL 472183, at *4 (N.D. Cal. Feb. 15, 2022); Baysal v. Midvale Indem. Co., 2022 WL 1155295, at *3 (W.D. Wis. Apr. 19, 2022). However, those decisions are not binding on this Court, did not situate the sensitivity of driver's license numbers in the context of other PII, and did not involve well-pleaded allegations of actual proof of identity theft as a result of the disclosure. Cf. Park v. Am. Fam. Life Ins. Co., 2022 WL 2230171, at *2 (distinguishing Baysal and holding victims of data breach had standing to challenge instant quote disclosure of driver's license numbers).

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 individuals 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 USAA—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, plaintiffs adequately plead a claim under the DPPA.

First, plaintiffs plausibly allege their driver's license numbers were "obtained [by USAA] from the relevant state DMVs" (Am. Compl. ¶ 71), and thus were disclosed "from a motor vehicle record." 18 U.S.C. § 2724(a).

Second, USAA's voluntary decision to automatically pre-fill its quote forms with driver's license numbers constitutes a "knowing disclosure" of personal information. 18 U.S.C. § 2724(a).

Third, plaintiffs adequately allege that in light of the two separate data-security alerts that warned USAA as to the vulnerability of its pre-fill data features, USAA reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes. See Gordon v. Softech Int'l, Inc., 726 F.3d at 54.

USAA argues the duty of reasonable care articulated by the Second Circuit in Gordon applies only to "resellers" of DPPA-protected information. But the DPPA does not make a distinction between "resale or redisclosure." 18 U.S.C. § 2721(c). Moreover, in noting it was confining its holding to resellers, the Second Circuit distinguished resellers only with "state DMVs" or other "upstream sources of DPPA-protected personal information." Gordon v. Softech Int'l, Inc., 726 F. 3d at 57 n.14. A rediscloser like USAA is neither a state DMV nor any other upstream source of DPPA-protected personal information, but rather is situated more similarly to resellers as a "downstream" entity with equal access and ability to redisclose DPPA-protected personal information received by state DMVs. The Second's Circuit's analysis of the language, structure, and legislative history of the DPPA thus applies with equal force to USAA.

Accordingly, the DPPA claim may proceed.

V. Negligence

USAA argues plaintiffs fail plausibly to state a negligence claim under New York law because USAA did not owe a duty of care to plaintiffs, who, in any event, do not allege cognizable damages.

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

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

However, the Court agrees plaintiffs' 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

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 found

that 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 as 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

Here, plaintiffs plausibly allege facts that, taken together, support the inference that USAA owed plaintiffs a duty of reasonable care under New York law. First, plaintiffs plausibly allege USAA obtained and then redisclosed plaintiffs' PII—without their knowledge or consent—as part of its ordinary course of business, and was thus "in the best position" as between USAA and plaintiffs to protect the information. Toretto v. Donnelley Fin. Sols., Inc., 2022 WL 348412, at *12. Second, plaintiffs allege USAA actively marketed the strength of its cybersecurity to the public and "knew it was the target of cyber-attacks" because of the two NYSDFS alerts. Id. Third, imposing a duty on USAA under these alleged circumstances would subject USAA to liability only with respect to individuals whose personal information had already been stolen by cybercriminals from other sources. Accordingly, fixing a duty of care under these circumstances best realizes the expectations of the parties without imposing unlimited liability.

USAA warns imposing a duty of care on it would extend liability for "negligent enablement of imposter fraud," which is not recognized in New York unless there is a "special relationship" that warrants holding the defendant responsible for the acts of a third party. See Polzer v. TRW, Inc., 256 A.D.2d 248, 248 (1st Dep't 1998). However, each of the cases upon

which USAA relies involved financial institutions negligently allowing imposters to open accounts or credit cards in those plaintiffs' names, thereby "enabling" the fraud of the third party. See, e.g., id. Here, by contrast, plaintiffs plausibly allege USAA negligently handed over additional PII—driver's license numbers—that the imposters then used to commit additional imposter fraud elsewhere. 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").

2. Damages

As an initial matter, the fees plaintiffs allegedly paid to freeze their credit reports and the costs they allegedly incurred in purchasing credit monitoring and identity theft services are all 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 plaintiffs allegedly spent 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 plaintiffs' allegedly lowered credit scores suffice, absent additional allegations regarding the scores' actual financial impact on plaintiffs.

In addition, even if plaintiffs plausibly allege a substantial risk of identity fraud for the purpose of pleading injury-in-fact, they do not plausibly allege they are "reasonably certain" to incur expenses as a result of their 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, plaintiffs fall short of alleging expenses "reasonably certain to be incurred." Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d at 281.

Finally, plaintiffs supply only general allegations regarding the value of their driver's license numbers themselves, and they do not allege they could have monetized their driver's license numbers or that their driver's license numbers were actually monetized. Plaintiffs thus do not plausibly allege damages based on the lost value of their driver's license numbers. 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).[6]

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

VI. Negligence Per Se

USAA argues plaintiffs do not state a claim for negligence per se because they do not identify an applicable statutory duty under New York law.

The Court disagrees.

[6] 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, plaintiffs' claims would survive because of the "special relationship" imposed by the DPPA, which, as discussed above, requires redisclosers like USAA to protect against the risk of disclosing plaintiffs' driver's license numbers for impermissible purposes.

> 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).

In light of the fact that (i) the DPPA "was designed to protect a class of persons" comprising individuals whose PII has been misused or disclosed for an impermissible purpose; (ii) plaintiffs plausibly allege they became a part of that class as a result of the USAA data breach; and (iii) the criminal use of plaintiffs' PII is the "type of harm [that] in fact occurred as a result of [the DPPA's] violation," USAA's duty of care to plaintiffs and its 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. at 1396.[7] And, as discussed above, plaintiffs plausibly allege the DPPA was violated.

Accordingly, plaintiffs' negligence per se claim may proceed.

VII. New York General Business Law Section 349

USAA argues plaintiffs do not state a claim under Section 349 because they do not plausibly allege that any deceptive conduct "caused" plaintiffs' injuries.

The Court agrees.

---

[7] Plaintiffs also allege 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 817, 827 (Sup. Ct. Westchester Cty. 2020). Accordingly, the negligence per se claim arising out of either statute must be dismissed.

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 for a claim under Section 349, a plaintiff must plausibly allege he or 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 the named plaintiff, whose PII was housed on the defendant's network, failed to show sufficient evidence that it had any direct dealings with the 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.

Here, plaintiffs do not plausibly allege they were ever exposed to any purportedly deceptive misrepresentation or omission by USAA. To the contrary, the well-pleaded allegations that neither plaintiff was ever a member of USAA support the inference that neither plaintiff had been exposed to USAA prior to the data breach at all. Plaintiffs thus fail plausibly to allege their injuries were "caused" by any deceptive conduct on the part of USAA.

Accordingly, plaintiffs' Section 349 claim must be dismissed.

VIII. Declaratory Judgment Relief

USAA argues plaintiffs cannot seek a declaratory judgment regarding its data-security measures because such a judgment would address past actions that have since been corrected.

The Court disagrees.

To seek relief under the Declaratory Judgment Act, a plaintiff must adequately allege a dispute that is: (1) "definite and concrete, touching the legal relations of parties having adverse legal interests"; (2) "real and substantial"; and (3) "admit[ting] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." MedImmune, Inc. v. Genentech, Inc., 549 U.S. 118, 127 (2007) (analyzing 28 U.S.C. § 2201).

Here, plaintiffs plead an ongoing, actionable dispute arising out of USAA's allegedly inadequate data-security measures, including its fraud-detection capabilities and its pre-filling of driver's license numbers, in breach of its duty of care.

USAA contends it "blocked access to the driver's license information," as it stated in the USAA Notice, but such an assurance is too vague and conclusory for the Court to conclude, at this early stage of the case, that there is no longer a live, actionable controversy regarding the adequacy of USAA's data security. For example, "blocking access" to driver's license numbers could mean any one of a range of actions, from redacting the driver's license numbers to disabling the pre-fill feature entirely, each of which may bear differently on USAA's compliance with its duty of care.

Because plaintiffs "plausibly allege[] the continued inadequacy of [USAA's] security measures," they "plausibly allege that they face a substantial risk of future harm if [USAA's] security shortcomings are not redressed, making this dispute sufficiently real and immediate with respect to the parties' legal relations, which are adverse." In re Cap. One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 414–15 (E.D. Va. 2020) (plaintiff sufficiently alleged declaratory judgment claim in data-breach case even when defendant allegedly disclosed it

corrected the alleged vulnerability).[8]

Accordingly, plaintiffs' request for declaratory relief may proceed.

IX. Injunctive Relief

USAA argues plaintiffs are not entitled to injunctive relief.

The Court disagrees, except with respect to plaintiffs' request for an injunction regarding credit monitoring services.

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, plaintiffs plausibly allege entitlement to the injunctive relief it seeks in conjunction with its request for a declaratory judgment, for the reasons discussed above.

However, plaintiffs' request for credit monitoring services is "compensable through money damages" and therefore does not concern an irreparable injury.

Accordingly, plaintiffs' request for injunctive relief in the form of credit monitoring services must be dismissed. Plaintiffs' request for injunctive relief on the remaining grounds may proceed.

---

[8] To the extent plaintiffs' request for declaratory relief arises out of apparent duties under Section 5 of the FTCA and the NY Shield Act, as asserted in the amended consolidated complaint (Am. Compl. ¶ 208), that request must be dismissed because, as discussed above, neither statute creates or implies a private right of action.

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.

Plaintiffs' claim under Section 349 is dismissed. Plaintiffs' negligence per se claim is also dismissed to the extent it is based on Section 5 of the FTCA or the NY Shield Act.

Plaintiffs' requests for injunctive relief in the form of credit monitoring, and for declaratory relief arising out of Section 5 of the FTCA and the NY Shield Act, are also dismissed.

Plaintiffs' other claims may proceed.

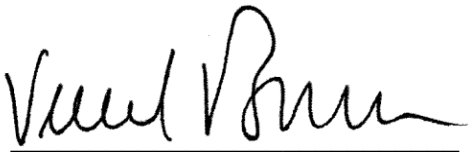
Defendant shall file an answer by August 25, 2022.

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

The Clerk is instructed to terminate the motion. (Doc. #35).

Dated: August 11, 2022
White Plains, NY

SO ORDERED:



Vincent L. Briccetti
United States District Judge