UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE WARNER MUSIC GROUP DATA BREACH

MEMORANDUM OPINION & ORDER

20 Civ. 7473 (PGG)

PAUL G. GARDEPHE, U.S.D.J.:

In 2020, websites owned by Defendant Warner Music Group suffered a cyberattack in which the perpetrators obtained payment details and other personal information of approximately 130,000 Warner Music customers. (Am. Cmplt. (Dkt. No. 74) ¶¶ 1, 5, 29 n.1, 47) In this consolidated action, Plaintiffs assert negligence and other state law causes of action on behalf of themselves, a putative nationwide class, and a putative California class against Warner Music for failing to prevent the data breach. Plaintiffs seek injunctive relief and damages for injuries they have suffered and are at risk of suffering in the future as a result of the data breach. (Id. at 92)[1]

Defendant Warner Music has moved to dismiss the Amended Complaint under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction, and under Rule 12(b)(6) for failure to state a claim. (Def. Mot. (Dkt. No. 75))

For the reasons stated below, Defendant's motion to dismiss will be granted in part and denied in part.

[1] The page numbers of documents cited in this Opinion correspond to the page numbers designated by this District's Electronic Case Files ("ECF") system.

BACKGROUND

I. FACTS[2]

A. The Parties

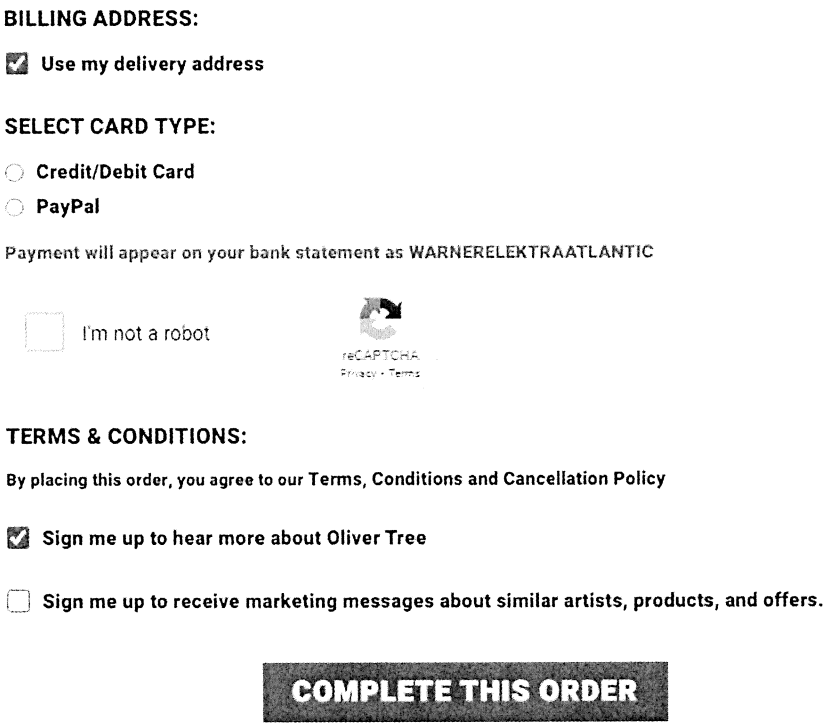
Defendant Warner Music is a media entertainment company incorporated in Delaware with its principal place of business in New York. (Am. Cmplt. (Dkt. No. 74) ¶¶ 2-3, 28, 32-33) Warner Music "operates" several websites through which it sells "exclusive music and merchandise" of the recording artists it represents. (Id. ¶¶ 3, 32, 48) These websites are "hosted" and "supported" by Magento, an "external service provider." (Id. ¶¶ 3-4, 32, 48, 64; see id., Ex. A (Dkt. No. 74-1) (Notice of Data Breach) at 2)

Plaintiffs are fourteen residents of California, Florida, Kansas, Massachusetts, New York, Ohio, Oregon, Texas, and Virginia who purchased items from websites operated by Warner Music between April 21, 2020 and August 5, 2020. (Id. ¶¶ 14-27)

In order to complete an online transaction on Warner Music's websites, a consumer is directed to the following payment webpage:

---

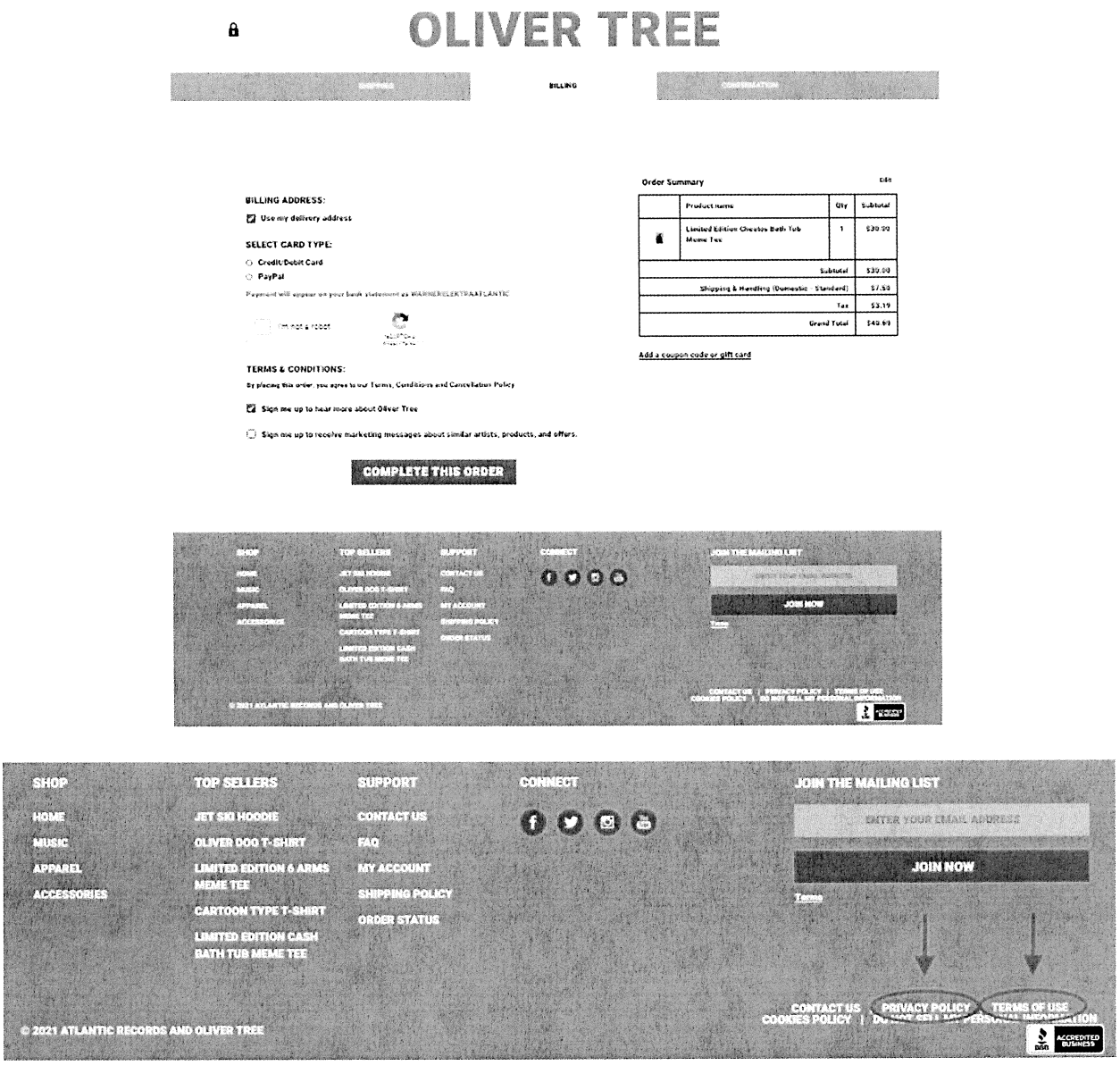
[2] The Court's factual statement is drawn from the Amended Consolidated Class Action Complaint (Dkt. No. 74). The well-pled facts in the Amended Complaint are presumed true for purposes of resolving Defendant's motion to dismiss. See Kassner v. 2nd Ave. Delicatessen Inc., 496 F.3d 229, 237 (2d Cir. 2007); Sonterra Cap. Master Fund Ltd. v. UBS AG, 954 F.3d 529, 533 (2d Cir. 2020).



(Id. (Dkt. No. 74) ¶ 239)

On this payment page, the customer is required to provide certain personal information, including his or her full name, billing address, shipping address, email address, telephone number, "name on the payment card," the card network, the "full payment card number," the card expiration date, and the card security code or verification number. (Id. ¶ 37) A pink "Complete This Order" button is displayed on the payment webpage screen. (Id. ¶ 239)

As shown above, the following language appears above the "Complete This Order" button: "TERMS & CONDITIONS: By placing this order, you agree to our Terms, Conditions and Cancellation Policy." (Id.) The "Terms, Conditions and Cancellation Policy" are not hyperlinked at this point. (Id.) Further down on the webpage there are references to "Privacy Policy" and "Terms of Use" that are hyperlinked. (Id. ¶ 241)



(Id. ¶ 241) (arrows and circles added)

As of 2020, Warner Music's Privacy Policy stated that the Company uses "reasonable physical, technical[,] and administrative measures designed to protect Personal Information under [its] control." (Id. ¶¶ 50, 248)

B. The 2017 and 2020 Data Breaches

Warner Music has suffered two cyberattacks.

In 2017, cybercriminals Warner Music was the target of a "phishing scam." (Id. ¶ 54) That attack exposed approximately 3.12 terabytes of data "relating to one of [Warner Music's] music video providers." (Id.)

A second cyberattack took place between April 25, 2020 and August 5, 2020, when "unauthorized third parties" "compromised" a number of the websites operated by Warner Music, gaining "access" to customers' "private data and payment card information," including "full names, email addresses, telephone numbers, billing addresses, shipping addresses, payment card numbers, payment card CVV security codes, and payment card expiration dates." (Id. ¶¶ 5, 6) The breach affected approximately 130,000 customers. (Id. ¶ 29 n.1)

The cyberattack "exploit[ed] weaknesses" in the platform of the "external service provider" – Magento – that Warner Music used to "host[]" and "support[]" its websites. (Id. ¶¶ 3-4, 48, 64-65) The cyberattack may have been "the result of a 'Magecart' attack" by several criminal organizations working together.[3] Such criminals target online retailers and steal customers' personal information, "especially payment card information." (Id. ¶ 57 & n.12)

A "Magecart" cyberattack generally begins with a hack of the original code on a retailer's "website or payment platform." (Id. ¶¶ 59, 62) The attacker then "inject[s] malicious code" into the original code. (Id.) When customers enter their personal information on the

---

[3] As an article cited in the Amended Complaint explains, "[t]he term 'Magecart' is comparable to something like 'Anonymous' or 'Antifa' in that it is not one large cohesive group, but rather a label and set of tactics used to describe independent smaller groups that don't necessarily associate with each other. Security researchers estimate there are at least 12 major persistent threat groups that make Magecart attacks their primary stock-in-trade, along with an uncountable number of more minor copycats." Scott Ikeda, Magecart Attacks Alive and Well as Recent Wave Hits High-End Retailers, CPO Magazine (Sept. 20, 2019), https://www.cpomagazine.com/cybersecurity/magecart-attacks-alive-and-well-as-recent-wave-hits-high-endretailers/ [https://perma.cc/5QZX-KNPX] (cited in Am. Cmplt. (Dkt. No. 57) ¶ 57 n.13).

website, the malicious code intercepts the data before it is delivered to the retailer, and transmits a copy of the information to a server controlled by the hackers. (Id. ¶¶ 62-63) The customer's "unencrypted, unredacted" personal information can then be used for criminal purposes (id. ¶¶ 7-8), or sold to other cybercriminals for such use. (Id. ¶¶ 8, 81 (stating that personal customer data is "of high value to criminals, as evidenced by the prices they will pay on the dark web": $50 to $200 for "bank details" and $5 to $110 for a credit or debit card number))

Plaintiffs allege that Magecart cyberattacks have "caused significant damage in recent years," compromising the personal customer data held by "at least 50,000 companies worldwide[.]" (Id. ¶ 58) According to Plaintiffs, Magecart cyberattacks occur because (1) "websites are not regularly updated to the latest (and most secure) software"; and (2) websites do not "obfuscate" their original code. (Id. ¶ 59)

In the Amended Complaint, Plaintiffs list several "reasonable industry standard protective measures" that could have "prevent[ed]" the cyberattack. (Id. ¶ 61) According to Plaintiffs, Warner Music "should not have pages with PII [Personally Identifiable Information] or payment information on the artists' websites" hosted by Magento, but instead "outsource the payment processing" to a secure third-party site, "such as PayPal or Stripe." (Id. ¶ 66) Warner Music also should not include on its websites code "from [external] webpages" that it "does not manage"; doing so makes the Warner Music websites more susceptible to Magecart attacks. (Id. ¶ 69) If payment information must be collected on Warner Music's artists' websites, the Company should minimize the use of code vulnerable to "possible [cyber]attacks" (id. ¶ 67), "install" a "web skimming protection" program that would "monitor" suspicious code (id. ¶ 72), and regularly update its Magento software. (Id. ¶ 65)

C. The Consequences of the 2020 Data Breach

Warner Music learned of the 2020 cyberattack and breach on August 5, 2020. (Id., Ex. A (Dkt. No. 74-1) (Notice of Data Breach) at 2) After detecting the breach, Warner Music "immediately launched a thorough forensic investigation with the assistance of . . . outside cybersecurity experts," and "notified the relevant credit card providers as well as law enforcement[.]" (Id.)

On September 2, 2020, Warner Music disclosed the cyberattack to several State Attorneys General. (Am. Cmplt. (Dkt. No. 74) ¶¶ 6, 49) On September 3, 2020, Warner Music sent notices to potentially affected customers, including Plaintiffs. (Id. ¶ 48) The notice reads as follows:

> We are writing to let you know that a cybersecurity incident involving a number of e-commerce websites operated by Warner Music Group . . . through an external service provider may have allowed an unauthorized third party to acquire a copy of personal information you entered into those websites [between April 25, 2020 and August 5, 2020]. . . .
>
> While we cannot definitively confirm that your personal information was affected, it is possible that it might have been as your transaction(s) occurred during the period of compromise. If it was, this might have exposed you to a risk of fraudulent transactions being carried out using your details.
>
> **WHAT INFORMATION WAS INVOLVED?**
>
> Any personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020 after placing an item in your shopping cart . . . . This could have included your name, email address, telephone number, billing address, shipping address, and payment card details (card number, [card security code or verification number,] and expiration date).
>
> Payments made through PayPal were not affected by this breach.

(Id., Ex. A (Dkt. No. 74-1) (Notice of Data Breach) at 2) (emphasis in original) In the notice, Warner Music offered customers free fraud and "identity monitoring services" for 12 months. (Id. at 2-3)

II. PROCEDURAL HISTORY

Nine related complaints – brought by twelve individuals who received Defendant's September 3, 2020 data breach notice – were filed against Defendant between September 2020 and November 2020. The first such complaint – captioned Combs v. Warner Music Group (20 Civ. 7473) – was filed on September 11, 2020. (Dkt. No. 1) Eight related complaints followed. See Kuhn v. Warner Music Group (20 Civ. 7608); Beardsley v. Warner Music Group (20 Civ. 7967); Cimaglio v. Warner Music Group (20 Civ. 8085); Gutierrez v. Warner Music Group (20 Civ. 8117); Watts v. Warner Music Group (20 Civ. 8644); Hart v. Warner Music Group (20 Civ. 8952); Buck v. Warner Music Group (20 Civ. 9075); and Hammett v. Warner Music Group (20 Civ. 9261).

On November 10, 2020, this Court consolidated the nine related putative class actions, as well as any cases "involving substantially related questions of law and fact hereafter filed in or transferred to this Court" under the caption In re Warner Music Group Data Breach. (Nov. 10, 2020 Order (Dkt. No. 34) at 5-7)

On February 22, 2021, this Court issued an order appointing Gayle Blatt and Jean Martin as interim co-lead counsel. (Feb. 22, 2021 Order (Dkt. No. 62))

On February 25, 2021, Stevens v. Warner Music Group (21 Civ. 1659) was transferred to this District from the Central District of California. Pursuant to the November 10, 2020 consolidation order, this Court consolidated Stevens with the related actions. (Mar. 5, 2021 Order (Dkt. No. 63) at 1)

The Amended Consolidated Class Action Complaint was filed on March 19, 2021, is brought on behalf of a nationwide class and a related California statewide subclass, and invokes this Court's jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). (Am. Cmplt. (Dkt. No. 74) ¶¶ 29-31) The putative nationwide class consists of "[a]ll

residents of the United States who made payment card purchases on [Warner Music's] e-commerce websites between April 25, 2020 and August 5, 2020." (Id. ¶ 222) The putative class encompasses a California subclass, defined as "all residents of the state of California who made payment card purchases on [Warner Music's] e-commerce websites between April 25, 2020 and August 5, 2020." (Id. ¶ 223)

The Amended Complaint alleges that Defendant (1) maintained "inadequate" "security procedures and practices" which did not "properly secure and safeguard [customers'] personal identifiable information" (id. ¶¶ 1, 5, 53); and (2) did not "provide timely and adequate notice" to all plaintiffs, the nationwide class, and the California subclass of the "full details of the [2020] Data Breach," including that their personal data "had been stolen by hackers" and that the stolen data was "unencrypted." (Id. ¶¶ 1, 52)

On behalf of Plaintiffs, the nationwide class, and the California subclass, the Amended Complaint asserts claims for (1) negligence; (2) negligent misrepresentation; (3) breach of implied contract; (4) unjust enrichment; (5) deceptive acts and practices in violation of Section 349 of the New York General Business Law ("GBL"); and (6) false advertising in violation of Section 350 of the GBL. (Id. ¶¶ 247-305) On behalf of the California subclass, the Amended Complaint asserts a claim for failure to "implement and maintain reasonable security procedures and practices," in violation of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code. § 1798.150. (Id. ¶¶ 306-17) Plaintiffs seek to enjoin Defendant's "wrongful conduct" and compel its compliance with "appropriate systems and policies to protect consumer [information]," and seek an award of compensatory and statutory damages. (Id. at 92, ad damnum clause)

On November 22, 2021, Defendant moved to dismiss all of Plaintiffs' claims under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction, and under Rule 12(b)(6) for failure to state a claim. (Def. Mot. (Dkt. No. 75))

In connection with its Rule 12(b)(1) motion, Defendant contends that the Amended Complaint does not plead facts sufficient to demonstrate standing, because Plaintiffs have not pled that they have suffered – or will suffer – a concrete injury. (Def. Br. (Dkt. No. 76) at 16-18)

In connection with its Rule 12(b)(6) motion, Defendant contends that, in any event, the Amended Complaint fails to state a claim. (Def. Br. (Dkt. No. 76) at 18-33)

DISCUSSION

I. LEGAL STANDARDS

A. Rule 12(b)(1) Motion to Dismiss

"[A] federal court generally may not rule on the merits of a case without first determining that it has jurisdiction over the category of claim in suit ([i.e.,] subject-matter jurisdiction)[.]" Sinochem Int'l Co. Ltd. v. Malay. Int'l Shipping Corp., 549 U.S. 422, 430-31 (2007). "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." Makarova v. United States, 201 F.3d 110, 113 (2d Cir. 2000).

Where, as here, a defendant challenges subject matter jurisdiction at the pleading stage "'based solely on the allegations of the complaint'" – i.e., a facial challenge – a court must "'accept[] as true all material factual allegations of the complaint' and 'draw[] all reasonable inferences in favor of the plaintiff.'" Sonterra Cap. Master Fund Ltd. v. UBS AG, 954 F.3d 529, 533 (2d Cir. 2020) (quoting Carter v. HealthPort Technologies, LLC, 822 F.3d 47, 56-57 (2d Cir. 2016)). In resolving a Rule 12(b)(1) motion, a court "'may refer to evidence outside the pleadings,'" but "it is not invariably required to consider such evidence[.]" Harty v. W. Point

Realty, Inc., 28 F.4th 435, 441 (2d Cir. 2022) (quoting Makarova, 201 F.3d at 113); see also Morrison v. Nat'l Austl. Bank Ltd., 547 F.3d 167, 170 (2d Cir. 2008), ("In resolving a motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), a district court may consider evidence outside the pleadings."), aff'd, 561 U.S. 247 (2010). A court may also consider "any matters of which judicial notice may be taken," Hirsch v. Arthur Andersen & Co., 72 F.3d 1085, 1092 (2d Cir. 1995), including publicly available materials, Kramer v. Time Warner, Inc., 937 F.2d 767, 774 (2d Cir. 1991).

B. Rule 12(b)(6) Motion to Dismiss

"To survive a [Rule 12(b)(6)] motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

"[T]he court is to accept as true all facts alleged in the complaint" and must "draw all reasonable inferences in favor of the plaintiff." Kassner v. 2nd Ave. Delicatessen Inc., 496 F.3d 229, 237 (2d Cir. 2007). "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). For documents to be incorporated by reference, "the complaint must make 'a clear, definite and substantial reference to the documents.'" Brown v. New York City Housing Auth., No. 13-CV-7599 (RJS), 2015 WL 4461558, at *2 (S.D.N.Y. July 20, 2015) (quoting Helprin v. Harcourt, Inc., 277 F. Supp. 2d 327, 330-31 (S.D.N.Y. 2003)).

II. STANDING

A. Applicable Law

To establish constitutional standing at the motion to dismiss stage, a plaintiff must plead facts showing "(i) that he [or she] suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." TransUnion LLC v. Ramirez, 594 U.S. 413, 423 (2021) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)); Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140, 145 (2d Cir. 2011) (at the pleading stage, a plaintiff "must allege facts that affirmatively and plausibly suggest that it has standing to sue"). In a class action, "[a]t least one named plaintiff" must "demonstrate the requisite injury" in order to establish standing. Hyland v. Navient Corp., 48 F.4th 110, 117 (2d Cir. 2022).

A "concrete" injury must be "'real,' and not 'abstract,'" and any alleged "particularized" injury "'must affect the plaintiff in a personal and individual way.'" Spokeo, Inc. v. Robins, 578 U.S. 330, 339-40 (2016) (quoting first Webster's Third New International Dictionary 472 (1971) and then quoting Lujan, 504 U.S. at 560 n.1). In considering whether a harm is "concrete," courts ask "whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." TransUnion, 594 U.S. at 424-25 (quoting Spokeo, 578 U.S. at 341).

An "actual or imminent" injury "need not be actualized" to satisfy Article III standing. Davis v. Fed. Election Comm'n, 554 U.S. 724, 734 (2008); see also Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (noting that the standing requirement "do[es] not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about"). But an allegation of threatened "future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk

that the harm will occur.'" McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300 (2d Cir. 2021) (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)).

Bohnak v. Marsh & McLennan Companies, Inc., 79 F.4th 276 (2d Cir. 2023) illustrates how these standards apply in data breach cases. In Bohnak, the Second Circuit considered whether a plaintiff may establish an injury in fact based on a risk of future identity theft. Plaintiff alleged that her name and Social Security number were exposed in a targeted data breach of her employer's internal network. Id. at 280. While plaintiff did not contend that her personal information had been misused after the breach, she alleged that she had (1) been harmed by "'the continued and certainly increased risk'" that her personal information would be misused, given that it "'remains unencrypted and available for unauthorized third parties to access and abuse'"; (2) incurred "'out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft'"; and (3) "'lost opportunity costs associated with attempting to mitigate the actual consequences of the [d]ata [b]reach.'" Plaintiff also claimed that the "value" of her personal information had been "'lost or diminished.'" Id. at 281-82, 286 (quoting joint appendix).

The Bohnak court concluded that plaintiff had pled two "separate and concrete harms," each of which "independently" constituted an injury in fact sufficient to demonstrate standing. Id. at 286, 289. The plaintiff's "core injury" was that that her private information – her name and Social Security number – had been disclosed "to unauthorized third parties" through a data breach. Id. at 285. The Bohnak court concluded that this type of injury is sufficiently "concrete" to demonstrate standing, noting that this type of injury bears "some relationship to a well-established common-law analog: public disclosure of private facts." Id. at 285-86 (citing Restatement (Second) Torts § 652D); see also TransUnion, 594 U.S. at 425

(noting that "disclosure of private information" is an intangible harm "traditionally recognized as providing a basis for lawsuits in American courts") (citing, inter alia, Davis v. Federal Election Comm'n, 554 U.S. 724, 733 (2008)).

The Bohnak court further concluded that "the risk of future harm occasioned by the exposure of" such information could "'itself cause[] a separate concrete harm.'" Bohnak, 79 F.4th at 285-86 (emphasis omitted) (quoting TransUnion, 594 U.S. at 436). For example, where a plaintiff plausibly alleges a "material risk of future harm," the time and money spent "attempting to mitigate the consequences of the data breach" constitute "concrete harms foreseeably arising from the exposure of [personal information] to a malign outside actor[.]" Id. at 286; see also McMorris, 995 F.3d at 303 ("[W]here plaintiffs have shown a substantial risk of future identity theft or fraud, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.") (internal quotation marks and citation omitted).

As to the "actual or imminent" requirement, the Second Circuit identified "three non-exhaustive factors" relevant to the inquiry: whether (1) "the data was compromised as the result of a targeted attack intended to get" personal information; (2) "some part of the compromised dataset has been misused[,] even if a plaintiff's own data has not" – for example, "fraudulent charges to the credit cards of other customers impacted by the same data breach"; and (3) the type of information "exposed" is "'more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.'" Bohnak, 79 F.4th at 288 (emphasis in original) (quoting McMorris, 995 F.3d at 302). The Bohnak court concluded that plaintiff had pled a "'substantial risk that the harm will occur,'" even though she had merely

alleged that her personal information was "compromised but not yet misused." Bohnak, 79 F.4th at 288-89 (quoting McMorris, 995 F.3d at 300).[4]

In connection with the "type of information exposed" factor, courts have noted that it is "more likely that . . . victims will be subject to future identity theft or fraud" where the information "disseminat[ed]" is "high-risk," such as "Social Security numbers and dates of birth[,] . . . especially when accompanied by victims' names," McMorris, 995 F.3d at 302; see Bohnak, 79 F.4th at 280 (compromised "name and Social Security number"); "credit or debit card numbers, card security or access codes, card expiration dates, and billing addresses," Jones v. Sturm, Ruger & Co., Inc., No. 22 Civ. 1233 (KAD), 2024 WL 1307148, at *2 (D. Conn. Mar. 27, 2024); "Medicare Health Insurance Claim Numbers, . . . treatment and diagnosis information, . . . health insurance claims information," Wallace v. Health Quest Sys., Inc., No. 20 Civ. 545 (VB), 2021 WL 1109727, at *2 (S.D.N.Y. Mar. 23, 2021); or "driver's license number[s]." Rand v. Travelers Indem. Co., 637 F. Supp. 3d 55, 67 (S.D.N.Y. 2022) (noting that a "driver's license number" can readily be "used to file fraudulent unemployment claims" or "take out a loan," with "only minimal consumer information").

"[L]ess sensitive data" – such as "basic publicly available information, or data that can be rendered useless to cybercriminals" – "do[] not pose the same risk of future identity theft or fraud[.]" McMorris, 995 F.3d at 302. For example, courts have found that "where a plaintiff's credit card was stolen as part of a data breach, but she promptly canceled her credit card 'and no other [personal information] – such as her birth date or Social Security number – was alleged to have been stolen,'" plaintiff has "failed to allege 'how she could plausibly face a

[4] In ruling that plaintiff satisfied the "actual or imminent" harm requirement, the Second Circuit cited plaintiff's allegation "of a targeted hack that exposed [her] name and [Social Security number] to an unauthorized actor[.]" Id. at 289.

threat of future fraud.'" Id. (quoting Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (finding no standing where plaintiff promptly canceled her credit card after a data breach "and no other personally identifying information – such as her birth date or Social Security number – is alleged to have been stolen")).

In sum, allegations demonstrating "a risk of future harm" may be sufficient to plead an injury in fact. Bohnak, 79 F.4th at 285, 290.

B. Analysis

In moving to dismiss, Defendant argues that the Amended Complaint does not plead facts demonstrating that Plaintiffs have suffered – or will suffer – any concrete or imminent injury in fact, because allegations of "future identity theft" and "risks" are too "speculative" and "hypothetical" to support Article III standing. (See Def. Br. (Dkt. No. 76) at 16-18)

All fourteen named Plaintiffs allege that – as a result of the 2020 Data Breach – they suffered the following injuries:

(1) "substantially increased risk of fraud, identity theft, and misuse" of their personal information (Am. Cmplt. (Dkt. No. 74) ¶¶ 96, 106, 115, 123, 133, 142, 151, 161, 171, 180, 190, 200, 210, 219);

(2) "annoyance, interference," and "increased concerns for the loss" of private information (id. ¶¶ 95, 105, 114, 122, 132, 142, 150, 160, 170, 179, 189, 199, 209, 219).

(3) loss of "time dealing with the consequences of the [2020] Data Breach," including "monitoring" and "reviewing" accounts for any fraudulent charges, "contacting" their bank to remediate any fraudulent charges, and "exploring credit monitoring and identity theft insurance options" (id. ¶¶ 91, 102, 111, 119, 128, 139, 147, 157, 167, 176, 186, 196, 206, 216);

(4) loss of money spent on "purchasing products from" Warner Music's websites – purchases that Plaintiffs "would not have made had [Warner Music] disclosed that it lacked consumer systems and data security practices adequate to safeguard customers' [personal information]" (id. ¶¶ 93, 103, 112, 120, 130, 140, 148, 158, 168, 177, 187, 197, 207, 217); and

(5) "diminution in the value" of their personal information (id. ¶¶ 94, 104, 113, 121, 131, 141, 149, 159, 169, 178, 188, 198, 208, 218).

Eleven named Plaintiffs further allege that they suffered financial fraud as a result of the data breach, including unauthorized charges to payment cards they had used to make purchases on the Warner Music websites. (See id. ¶ 90 ($197.90 fraudulent charge withdrawn from Plaintiff Combs's checking account, later reimbursed by his bank); id. ¶ 101 ($86.11 attempted fraudulent charge on Plaintiff Trujillo's card, declined by his bank); id. ¶ 108 ("more than" $500 in "numerous unauthorized charges" on Plaintiff Kuhn's debit card, for which she was not reimbursed); id. ¶¶ 138-39 ($300 in fraudulent charges on Plaintiff Cimaglio's debit card, later reimbursed by his bank); id. ¶ 146 ($3,000 in fraudulent withdrawals from Plaintiff Gutierrez's bank account, later reimbursed by her bank); id. ¶ 156 ($2,500 in fraudulent charges on Plaintiff Foster's card, later reimbursed by her bank); id. ¶ 166 (several fraudulent charges on Plaintiff Watts' credit card for, inter alia, a plane ticket and hotel room, later reimbursed by his bank); id. ¶ 185 ($2,254 in "numerous unauthorized purchases" on Plaintiff Buck's debit card, partially reimbursed by his bank); id. ¶ 195 ("at least $2,800" in "unauthorized purchases" on Plaintiff Hammett's card, partially reimbursed by her bank); id. ¶ 205 ($240 in fraudulent charges on Plaintiff Stevens' credit card, later reimbursed by her bank); id. ¶ 215 ($90 fraudulent charge on Plaintiff Blank's debit card, later reimbursed by her bank))

Three of the named Plaintiffs who suffered financial fraud were not fully reimbursed for unauthorized charges made to their cards and bank accounts. (See id. ¶¶ 108, 185, 195; see also id. ¶ 146 (alleging that – because of $3,000 in fraudulent charges made to her debit card and withdrawn from her bank account – Plaintiff Gutierrez was "forced to place her apartment rent on her credit card, causing her to incur convenience fees and interest charges of approximately $300," for which she was not reimbursed))

Some of the Plaintiffs who were fraud victims further allege that they were unable to use their credit or debit cards for a period of time, because their cards had been suspended. (See, e.g., id. ¶ 109 (alleging that Plaintiff Kuhn's card was frozen while the unauthorized charges were being investigated)) Three of these Plaintiffs canceled their existing payment cards and ordered a replacement card. (See id. ¶¶ 156, 185, 205)

Three Plaintiffs who do not allege fraud state that they remain concerned that they may be victimized in the future. (See id. ¶¶ 115, 123, 200)

The Court concludes that all of the named Plaintiffs have alleged a "concrete" injury sufficient to demonstrate standing.

Here, as in Bohnak, Plaintiffs have alleged that their private information – their "full names, email addresses, telephone numbers, billing addresses, shipping addresses, payment card numbers, payment card CVV security codes, and payment card expiration dates" (Am. Cmplt. (Dkt. No. 74) ¶¶ 5, 6, 46-48) – was exposed "to unauthorized third parties" through a data breach. Bohnak, 79 F.4th at 285. Plaintiffs have also alleged that there is a "risk of future harm occasioned by the exposure of [their private information]." (Am. Cmplt. (Dkt. No. 74) ¶¶ 8, 10, 91, 96, 102, 106, 111, 115, 119, 123, 128, 133, 139, 142, 147, 151, 157, 161, 167, 171, 176, 180, 186, 190, 196, 200, 206, 210, 216, 219); see Bohnak 79 F.4th at 286. Plaintiffs have also pled facts demonstrating that they expended time and money to remediate and mitigate the risks that "foreseeably aris[e]" from the data breach. (Am. Cmplt. (Dkt. No. 74) ¶¶ 91, 95, 102, 105, 111, 114, 119, 122, 128, 132, 139, 142, 147, 150, 157, 160, 167, 170, 176, 179, 186, 189, 196, 199, 206, 209, 216, 219) These allegations demonstrate a "separate concrete harm." Bohnak, 79 F.4th at 285-86; see also McMorris, 995 F.3d at 303 (holding that "'any expenses [plaintiffs] have reasonably

incurred to mitigate [a] risk'" of future identity theft "'qualify as injury in fact'") (internal quotation marks and citation omitted).

As to an "actual or imminent" injury, Plaintiffs have also pled facts sufficient to demonstrate both that an actual injury has occurred as to certain Plaintiffs, and that there is a "'substantial risk [that future] harm will occur.'" Bohnak, 79 F.4th at 288 (quoting McMorris, 995 F.3d at 300).

As discussed above, the Second Circuit has instructed that – in considering whether an "actual or imminent" injury has been pled – courts should consider whether (1) "the data was compromised as the result of a targeted attack intended to get [personal identifying information]"; (2) "some part of the compromised dataset has been misused[,] even if a plaintiff's own data has not" – for example, "fraudulent charges to the credit cards of other customers impacted by the same data breach"; and (3) the type of information "exposed" is "'more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.'" Bohnak, 79 F.4th at 288 (emphasis in original) (quoting McMorris, 995 F.3d at 302).

Consideration of these factors here indicates that Plaintiffs have demonstrated standing. With respect to the "targeted attack" factor – the "most important[]" factor, see McMorris, 995 F.3d at 301 – the Amended Complaint alleges that the 2020 data breach was the result of a "Magecart-style attack[]" that targeted "payment platform[s]" with the intention to "steal individuals' [personal identifying information], especially payment card information." (Am. Cmplt. (Dkt. No. 74) ¶¶ 57, 62-64) The "intentional[] target[ing of] a defendant's system and . . . st[ealing of] a plaintiff's data stored on that system" gives rise to a plausible inference that the data may be misused. Bohnak, 79 F.4th at 288; see also McMorris, 995 F.3d at 301

(where a complaint alleges a targeted attack to obtain plaintiffs' data, courts may "'presume[]'" that "'the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities'") (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).

As to the second factor – whether "some part of the compromised data set has been misused" – eleven named Plaintiffs allege that they have already suffered fraud or identity theft as a result of the 2020 data breach, including unauthorized charges made to existing payment cards and other financial accounts. (Am. Cmplt. (Dkt. No. 74) ¶¶ 90, 101, 108, 138, 146, 156, 166, 185, 195, 205, 215) Although three named Plaintiffs have not alleged that they have suffered fraud or identity theft, allegations that some portion of the compromised dataset has already been misused make it more likely that other portions of the dataset will be similarly misused. See McMorris, 995 F.3d at 301-02.

Finally, here – as in Bohnak – the type of information exposed is "'likely to subject plaintiffs to a perpetual risk of identity theft or fraud[.]'" Bohnak, 79 F.4th at 288 (quoting McMorris 995 F.3d at 302). The compromised information includes "full names, email addresses, telephone numbers, billing addresses, shipping addresses, payment card numbers, payment card CVV security codes, and payment card expiration dates." (Am. Cmplt. (Dkt. No. 74) ¶¶ 5, 6, 46-48) This is the type of personal information that is highly susceptible to misuse.

Defendant points out, however, that Plaintiffs do not allege that Social Security numbers have been stolen. (Def. Br. (Dkt. No. 76) at 18; Def. Reply (Dkt. No. 77) at 7) But Plaintiffs are not required at this stage to demonstrate that the most sensitive personal information was stolen. It is instead sufficient for them to plead facts showing that the personal information that was stolen is sufficiently "sensitive such that there is a high risk of identity theft

or fraud." McMorris, 995 F.3d at 303. The payment information accessed on Defendant's website is sufficiently sensitive so as to expose Plaintiffs to a substantial risk of financial fraud. See, e.g., Jones, 2024 WL 1307148, at *4 (finding standing at motion to dismiss where plaintiffs' "payment card information" was stolen; concluding that "the type of data stolen is more likely to subject [plaintiffs] to a perpetual risk of identity theft or fraud"). Such information may be used to steal a cardholder's identity and make unauthorized payments in her name. That risk, of course, is compounded where the hack targeted customers' financial information. (See Am. Cmplt. (Dkt. No. 74) ¶ 57 (alleging that Magecart hackers "use a certain set of tactics to hack into websites and steal individuals' . . . payment card information"); see id. ¶ 64 ("Magecart attackers frequently target a payment platform[.]"))

In this context, it is hardly surprising that a number of the named Plaintiffs have alleged that the payment information they used to make their Warner Music purchases has been misused to make unauthorized purchases. (See, e.g., id. ¶ 90 (alleging that an unauthorized purchase was made on "the same payment card" Plaintiff Combs used on Warner Music's "hacked e-commerce platform"); id. ¶ 138 (same as to Plaintiff Cimaglio); id. ¶ 146 (same as to Plaintiff Gutierrez))

The Court concludes that Plaintiffs have demonstrated a concrete, actual, and imminent injury in fact. Given that the other components of Article III standing are not disputed, Defendant's Rule 12(b)(1) motion to dismiss will be denied.

III. WHETHER PLAINTIFFS HAVE STATED A CLAIM

As discussed above, the Amended Complaint asserts claims for negligence, negligent misrepresentation, breach of implied contract, unjust enrichment, deceptive acts or practices in violation of GBL § 349, false advertising in violation of GBL § 350, and failure to

implement and maintain reasonable cybersecurity practices under the CCPA.[5] (Am. Cmplt. (Dkt. No. 74) ¶¶ 247-317) Defendant Warner Music moves to dismiss the Amended Complaint on the grounds that it fails to state a claim. (Def. Br. (Dkt. No. 76) at 18-33)

A. Negligence

1. Applicable Law

To allege a negligence claim under New York law, a plaintiff must plead: "'(1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof.'" Borley v. United States, 22 F.4th 75, 78 (2d Cir. 2021) (quoting Akins v. Glens Falls City Sch. Dist., 53 N.Y.2d 325, 333 (1981)). "[T]he definition, and hence the existence, of a duty relationship is usually a question for the court[.]" Id.

In determining what duty is owed in the data breach context, courts consider several factors, including whether a custodian of personal information (1) "received [p]laintiffs' personal information while providing its services and stored that information on its servers"; (2) was "in the best position to protect information on its own servers from data breach"; (3)

---

[5] In this diversity action, the parties do not dispute that the law of New York – where Defendant maintains its principal place of business – governs all claims in this case other than Plaintiffs' CCPA claim. The Amended Complaint asserts that New York law applies (Am. Cmplt. (Dkt. No. 74) ¶ 238 ("New York law applies to the claims of all the Class Members regardless of their state of residence."), and both sides cite to New York law in their briefing concerning the non-CCPA claims. (Pltf. Opp. (Dkt. No. 80) at 14-25 (citing to New York law); Def. Br. (Dkt. No. 76) at 18-30 (same)) Given these circumstances, this Court will apply New York law in resolving the motion to dismiss the non-CCPA claims. See, e.g., Farrakhan v. Anti-Defamation League, No. 23 Civ. 9110 (DLC), 2024 WL 1484449, at *7 n.3 (S.D.N.Y. Apr. 5, 2024) (applying New York law when parties "do not dispute that New York law applies to this action"); Krumme v. WestPoint Stevens Inc., 238 F.3d 133, 138 (2d Cir. 2000) (explaining that "the parties' briefs assume that New York law controls, and such implied consent . . . is sufficient to establish choice of law") (citation and internal quotation marks omitted). The parties similarly do not dispute that the law of California governs Plaintiffs' CCPA claim. (Pltf. Opp. (Dkt. No. 80) 26-29 (citing to California law); Def. Br. (Dkt. No. 76) at 30-32 (same)) Accordingly, this Court will apply California law in resolving the motion to dismiss the CCPA claim.

"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 (4) would not be subject to "limitless liability," because its potential liability was "limited to the individuals whose personal information it obtained while providing its services." Toretto v. Donnelley Fin. Sols., Inc., 583 F. Supp. 3d 570, 594 (S.D.N.Y. 2022) (finding that proxy service provider that obtained stockholders' personal information "while providing its services" owed a duty of care to protect that information); see also In re USAA Data Sec. Litig., 621 F. Supp. 3d 454, 469-70 (S.D.N.Y. 2022) (citing Toretto factors in concluding that USAA – an automobile insurance company that had obtained drivers' personal information from state agencies and then populated that information on its own portal – owed a duty to the drivers to protect that information); Wallace, 2021 WL 1109727, at *9 (finding that healthcare provider that stored its patients' personal information on a portal owed a duty to the patients to protect that information).

2. Analysis

In moving to dismiss Plaintiffs' claim that Warner Music "negligently or recklessly fail[ed] . . . to take available steps to prevent [the 2020 data breach]" (see Am. Cmplt. (Dkt. No. 74) ¶¶ 13, 247-54), Defendant contends that it did not breach any duty it owed to Plaintiffs. In the alternative, Defendant argues that any negligence claim is barred by the economic loss rule. (See Def. Br. (Dkt. No. 76) at 18-23)

a. Duty

Plaintiffs allege that Warner Music owed them and proposed class members a duty of reasonable care "to safeguard and protect" their personal information. (Am. Cmplt. (Dkt. No. 74) ¶ 248; see also id. ¶ 35 (alleging that Defendant owed a "duty to adopt reasonable measures to protect [Plaintiffs' personal information] from involuntary disclosure to third parties")) According to Plaintiffs, this duty required Defendant to, inter alia, "adequately

design[], employ[], and maintain[]" "cybersecurity systems . . . sufficient to protect the[ir customers' personal information] from unauthorized access and to promptly alert Defendant to any such access[.]" (Id. ¶¶ 249-50)

In asserting that Warner Music owes its customers a duty of care, the Amended Complaint alleges that the Company "requires" consumers to submit their personal information – payment information and contact details – to "purchase items on [its] websites" (id. ¶ 37), and later "stor[es]" the information for "commercial gain." (Id. ¶¶ 7, 248) Warner Music's customers cannot withhold their payment information at the time of purchase. (Id. ¶ 37)

As to Warner Music's knowledge that it was a target for cyber attack, the Amended Complaint asserts that Defendant was "on notice of the very real risks of security breaches like the [2020] Data Breach," given its history of data security failures, including in connection with "a phishing scam" in 2017. (Id. ¶ 54) And given that it operates an online commerce platform, Warner Music should be particularly aware of the "numerous instances" of recent Magecart attacks to similar platforms. (Id. ¶¶ 55-56, 58 & n.17 (listing media reports of Magecart attacks on "50,000 companies worldwide," and alleging that Warner Music "should have been well aware of the risk of falling victim to the [2020] Data Breach, and should have properly secured itself against such an attack"); id. ¶ 4 (alleging that it is "common knowledge in [online] commerce" that "platforms" such as Defendant's "are frequently subjected to payment card skimming attacks and other similar data theft efforts"))

The Amended Complaint further notes that Warner Music "has acknowledged the sensitive and confidential nature of [the personal information it obtains from customers]" (id. ¶ 78), "emphasize[d]" that "keeping personal information safe and secure is very important" (id., Ex. A (Dkt. No. 74-1) (Notice of Data Breach) at 2), and made "representations in its Privacy

Policy [referenced on its websites] that it uses 'reasonable physical, technical, and administrative measures designed to protect [customers'] Personal Information under [its] control.'" (Id. ¶ 248; see also id. ¶¶ 35-36 (alleging that Defendant "touts the secure nature of its websites with the image of a combination lock displayed on the upper left corner of the [web]page"))

The Court concludes that the Amended Complaint pleads facts demonstrating that Warner Music sought and obtained Plaintiffs' personal information in the course of selling its music and related merchandise; that Warner Music was "in the best position to protect [customer] information on [the websites it operates] from data breach"; that Warner Music "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 that Warner Music's potential liability is "limited to the individuals whose personal information it obtained [in the course of selling music and related merchandise online]." Toretto, 583 F. Supp. 3d at 594. Accordingly, the Amended Complaint pleads facts demonstrating that Warner Music owes Plaintiffs "a duty to exercise reasonable care in safeguarding [the] personal information" that it obtains from customers. Id.

b. Breach of Duty of Care

Plaintiffs allege that Defendant breached its duty by failing to take reasonable measures to protect its customers' personal information. (Am. Cmplt. (Dkt. No. 74) ¶ 251) (alleging that "Defendant breached its duties" by "failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to minimize the [personal information] that any intrusion could compromise, and failing to detect the [2020] Data Breach in a timely manner"))

The Amended Complaint further alleges that Warner Music was aware of the sensitivity of the personal information it collected and stored and the importance of protecting it.

(Id., Ex. A (Dkt. No. 74-1) (Notice of Data Breach) at 2) (Warner Music acknowledging that "keeping personal information safe and secure is very important"); see also id. (Dkt. No. 74) ¶¶ 55-56 (given that "security breaches . . . have been frequent and garnered significant media attention," it is "apparent that any e-commerce provider," such as Warner Music, "is well aware of the risk of security breaches and the need to ensure a robust system of safeguarding against security breaches"); id. ¶ 54 (alleging that Warner Music "was on notice of the very real risks of security breaches like the [2020] Data Breach," because it was previously "involved in a phishing scam"))

According to Plaintiffs – despite this knowledge – Warner Music did not take reasonable steps to protect against cyberattacks, including the "reasonable industry standard protective measures" set forth below (id. ¶ 61):

(1) Warner Music did not "outsource the payment process[]" to a secure "third-party site such as PayPal or Stripe," but instead directed customers to enter their personal information directly "on artists' websites," which are more susceptible to cyberattack (id. ¶ 66);

(2) in including on its "payment processing page and payment iframe . . . JavaScript from several non-WMG domains," Warner Music created a risk that hackers would "use those scripts to gain access to other parts of the website or alter the script to create fake but convincing replicas of payments pages that steal the data entered" (id. ¶¶ 69, 71);

(3) Warner Music did not install a "web skimming protection program" that would "monitor JavaScript codes and automatically block access to all form field or cookies unless the JavaScript has been given express permission to access them" (id. ¶ 72); and

(4) the Magento software Warner Music utilized "is out of date," "and Magecart-style hackers have been able to exploit weaknesses or gain access to websites running it through malicious third-party scripts." (Id. ¶ 65)

These allegations are sufficient at this stage of the proceedings to demonstrate that Defendant breached its duty of care. See, e.g., Toretto, 583 F. Supp. 3d at 595 (finding breach of duty of care adequately pled where plaintiff alleged that defendant "maintained deficient controls

to prevent and monitor for unauthorized access," "failed to encrypt the personal information stored on its servers," and was "aware[] that it was a target of cybersecurity threats") (internal quotation marks and citation omitted); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) (finding breach of duty of care adequately pled where plaintiff alleged that defendant failed to "erect[] a digital firewall, conduct[] data security training[,] adopt[] retention and destruction policies," or take other "reasonable steps to prevent the wrongful dissemination of [p]laintiffs' [personal information]"); In re GE/CBPS Data Breach Litig., No. 20 Civ. 2903 (KPF), 2021 WL 3406374, at *8 (S.D.N.Y. Aug. 4, 2021) (same where complaint alleged that defendants "fail[ed] to design, adopt, [and] implement, . . . appropriate data security processes") (internal quotations marks and citation omitted).

c. Economic Loss Doctrine

In moving to dismiss, Defendant contends that Plaintiffs' negligence claim is precluded by "the economic loss rule," because the Amended Complaint does not allege that Defendant had (1) a "special relationship" with its customers; or (2) a tort duty distinct from its contractual duty under the Terms of Use. (Def. Br. (Dkt. No. 76) at 19, 22)

The economic loss doctrine "originate[s]" from products liability cases, and "'prevents [an end-purchaser of a product] from recovering purely economic losses in a negligence action [against a product's manufacturer].'" Toretto, 583 F. Supp. 3d at 590 (quoting Cruz v. TD Bank, N.A., 855 F. Supp. 2d 157, 178 (S.D.N.Y. 2012), aff'd, 742 F.3d 520 (2d Cir. 2013)); see 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 96 N.Y.2d 280, 292 (2001) (noting that the economic loss doctrine reflects "[p]olicy-driven line-drawing"). The economic loss rule requires a plaintiff end-purchaser to plead (1) "'a special relationship that requires the defendant to protect against the risk of harm to plaintiff,'" and (2) that the defendant's legal duty is "'in the nature of a . . . tort,'" and not duplicative of a duty under

"'breach of contract.'" Toretto, 583 F. Supp. 3d at 590 (quoting first Cruz, 855 F. Supp. 2d at 178, and then quoting Hydro Invs., Inc. v. Trafalgar Power Inc., 227 F.3d 8, 16 (2d Cir. 2000)); see also 532 Madison Ave., 96 N.Y.2d at 288 n.1 (the economic loss rule "stands for the proposition that an end-purchaser of a product is limited to contract remedies and may not seek damages in tort for economic loss against a manufacturer").

Courts applying New York law have uniformly concluded that "the economic loss doctrine does not bar negligence claims in data breach cases." Toretto, 583 F. Supp. 3d at 590 (collecting cases); see also USAA Data Sec. Litig., 621 F. Supp. 3d at 471 n.6 (joining "the weight of authority applying New York law and concluding [that] the economic loss doctrine . . . does not apply to data-breach cases"); Sackin, 278 F. Supp. 3d at 749 (finding that the economic loss doctrine was "inapplicable" in data breach case "because the [c]omplaint does not allege a products liability claim"); Rudolph v. Hudson's Bay Co., No. 18 Civ. 8472 (PKC), 2019 WL 2023713, at *9 (S.D.N.Y. May 7, 2019) (rejecting application of economic loss doctrine in data breach case, and noting that "[d]efendants have not explained how [the economic loss doctrine] limitation on negligence liability could apply to the data breach alleged"); Ambac Assurance Corp. v. U.S. Bank Nat'l Ass'n, 328 F. Supp. 3d 141, 159 (S.D.N.Y. 2018) (finding that "the applicability of the economic loss rule outside the product-liability context from which it originated is doubtful").

Because the purpose of the economic loss doctrine is to ensure that manufacturers of defective products do not face "unlimited or insurer-like liability" to "an indeterminate class of [users] conceivably injured by any negligence in a defendant's act," the doctrine has no application here. 532 Madison Ave., 96 N.Y.2d at 288-89; see also Travelers Cas. & Sur. Co. v. Dormitory Auth., 734 F. Supp. 2d 368, 379 (S.D.N.Y. 2010) (the economic loss doctrine "reflects

a policy interest in protecting defendants from disproportionate, and potentially limitless, liability"). Plaintiffs do not allege that the "music and related merchandise" they purchased on the Warner Music websites was defective. Plaintiffs instead complain that Defendant "fail[ed] to undertake appropriate and adequate measures to protect [their personal information]." (Id. ¶ 253; see also id. ¶ 251 (alleging that "Defendant breached its duties of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access")) Given these circumstances, the economic loss doctrine presents no obstacle to Plaintiffs' negligence claim.

Defendant's motion to dismiss Plaintiffs' negligence claim will be denied.

B. Negligent Misrepresentation

1. Applicable Law

To plead negligent misrepresentation under New York law, a plaintiff must allege that

> (1) the defendant had a duty, as a result of a special relationship, to give correct information; (2) the defendant made a false representation that [it] should have known was incorrect; (3) the information supplied in the representation was known by the defendant to be desired by the plaintiff for a serious purpose; (4) the plaintiff intended to rely and act upon it; and (5) the plaintiff reasonably relied on it to his or her detriment.

Anschutz Corp. v. Merrill Lynch & Co., 690 F.3d 98, 114 (2d Cir. 2012) (quotation marks and citations omitted).

The "strictures" of "Rule 9(b) may or may not apply to a state law claim for negligent misrepresentation," Eternity Glob. Master Fund Ltd. v. Morgan Guar. Tr. Co. of N.Y., 375 F.3d 168, 188 (2d Cir. 2004), depending on whether the negligent misrepresentation claim sounds in negligence or fraud. Tyman v. Pfizer, Inc., No. 16 Civ. 6941 (LTS) (BCM), 2017 WL 6988936, at *8 (S.D.N.Y. Dec. 27, 2017) (Rule 9(b) "must be applied where 'the claim sounds in

fraud'") (quoting Riker v. Premier Capital, LLC, No. 15 Civ. 8293 (ALC), 2016 WL 5334980, at *5 (S.D.N.Y. Sept. 22, 2016)), report and recommendation adopted, 2018 WL 481890 (S.D.N.Y. Jan. 18, 2018).

> A claim "sound[s] in fraud" if "the wording and imputations of the complaint are classically associated with fraud," Rombach, 355 F.3d at 167, 172 (internal citations and quotations omitted). In applying this "pragmatic standard," courts "reject plaintiffs' efforts to 'characterize claims by the label used in the[ir] pleading,'" Matsumura, 542 F. Supp. at 251 (quoting Rombach, 355 F.3d at 172), and apply Rule 9(b) "to any cause of action that bears a close relationship to fraud or mistake." Id. (collecting cases). See also Levy v. Young Adult Inst., Inc., 103 F. Supp. 3d 426, 443 (S.D.N.Y. 2015) ("Courts have found non-fraud claims to sound in fraud where the underlying conduct alleged has been fraud or closely linked with fraudulent behavior, such as claims for which fraud is a necessary element or claims that the other party has attempted to induce action through misrepresentations or material omissions.").
>
> To determine whether Rule 9(b) applies, courts conduct a "case-by-case analysis of particular pleadings to determine whether 'the gravamen of the complaint is plainly fraud.'" In re Refco, Inc. Sec. Litig., 503 F. Supp. 2d 611, 632 (S.D.N.Y. 2007) (quoting Rombach, 355 F.3d at 172). In the consumer fraud context, as elsewhere, courts "tend to take a holistic approach." Miller v. Hyundia Motor Am., 2016 WL 5476000, at *14 (S.D.N.Y. Sept. 28, 2016) (collecting cases). "As part of this inquiry, courts look for references to 'specific misrepresentations' in the complaint . . . [and] allegations of 'fraudulent concealment,' 'fraudulent misrepresentations,' and 'deceptive practices,' based on a defendant's 'knowing acts.'" Id. at *14 (internal citations omitted).

Tyman, 2017 WL 6988936, at *8 (alterations in original), report and recommendation adopted, 2018 WL 481890 (S.D.N.Y. Jan. 18, 2018).[6]

Applying this analysis here, the Court concludes that the Amended Complaint's negligent misrepresentation claim sounds in negligence rather than fraud. The focus of Plaintiffs' grievance is that Defendant had a duty to Plaintiffs and other class members to

[6] Neither side has addressed whether Plaintiffs' negligent misrepresentation claim sounds in negligence or fraud. (Def. Br. (Dkt. No. 76) at 23; Pltf. Opp. (Dkt. No. 80) at 19-21) Defendants merely state that "[n]egligent misrepresentation claims must . . . be pled with particularity pursuant to Fed. R. Civ. P. 9(b)," without analyzing whether the negligent misrepresentation claim here sounds in negligence or fraud. (Def. Br. (Dkt. No. 76) at 23)

safeguard and protect their personal information, and that Defendant breached that duty, knowing that doing so would put Plaintiffs at risk of fraud committed by third parties. Because the negligent misrepresentation claim sounds in negligence, the more "liberal pleading standards of Rule 8 [apply]." Eternity, 375 F.3d at 188.

Even under Rule 8 pleading standards, however, Plaintiffs must plead facts sufficient to demonstrate that they "reasonably or justifiably relied on [Defendant's alleged] misrepresentation[s]." PHL Variable Ins. Co. v. Town of Oyster Bay, 929 F.3d 79, 94 (2d Cir. 2019); see Olson v. Major League Baseball, 29 F.4th 59, 76 (2d Cir. 2022) ("[E]ven under the liberal pleading standard of Rule 8," a plaintiff must "plausibly plead actual or reasonable reliance as to any of the alleged specific misrepresentations[.]"). "In assessing the reasonableness of a plaintiff's alleged reliance," courts "consider the entire context of the transaction, including factors such as its complexity and magnitude, the sophistication of the parties, and the content of any agreements between them." Emergent Capital Inv. Mgmt., LLC v. Stonepath Group, Inc., 343 F.3d 189, 195 (2d Cir. 2003).

2. Analysis

In connection with Plaintiffs' negligent misrepresentation claim, Defendant contends that the Amended Complaint does not plausibly allege reliance. (Def. Br. (Dkt. No. 76) at 24-26)

According to the Amended Complaint, Warner Music made the following misrepresentations:

(1) displaying an "image of a combination lock . . . on the upper left corner of [Warner Music's websites], giving the consumer the false hope that their transaction will be secure" (Am. Cmplt. (Dkt. No. 74) ¶¶ 35, 256);

(2) displaying the "image of a lock . . . in the URL," "giving the consumer indication that the website, and the payment transactions made . . . are secure" (id. ¶¶ 36, 256); and

(3) stating in its Privacy Policy that Warner Music uses "reasonable physical, technical and administrative measures to protect Personal Information under [its] control" (id. ¶ 50).

As to reliance, the Amended Complaint states that "Plaintiffs and members of the Classes justifiably relied on Defendant's representations regarding the security of their [personal information] in choosing to provide their [personal information] to Defendant." (Am. Cmplt. (Dkt. No. 74) ¶ 260; see id. ¶ 34 (asserting that Plaintiffs "relied on this sophisticated Defendant to keep their [personal information] confidential and securely maintained"); id. ¶ 76 (asserting that Plaintiffs "relied on [Warner Music], a major, multi-billion dollar company, to have implemented and maintained systems that would keep their [personal information] safe"))

While asserting that they "justifiably relied" on Defendant's alleged misrepresentations (see id. ¶ 260), Plaintiffs do not plead facts demonstrating that they actually saw, read, or otherwise noticed the image of the combination lock or the Privacy Policy when completing their transactions. Indeed, at other points in the Amended Complaint, Plaintiffs complain that the link to the Privacy Policy is contained "[i]n the extreme bottom right borders of the website pages," is "not emphasized in any way," and is "inconspicuous at best," and that at no point is a purchaser "asked to acknowledge [Warner Music's] Privacy Policy[.]" (Am. Cmplt. (Dkt. No. 74) ¶¶ 239, 241, 243) And the lock images cited by Plaintiffs are found in the "upper left corner" of the Warner Music websites, and "in the URL." (Id. ¶¶ 35-36)

In sum, Plaintiffs do not allege that they ever "saw, read, or otherwise noticed" the alleged misrepresentations. In re Fyre Festival Litig., 399 F. Supp. 3d 203, 217 (S.D.N.Y. 2019). Absent such "specific[] alleg[ations]," the Amended Complaint's conclusory assertions of reliance are not sufficient to state a claim for negligent misrepresentation. Olson, 29 F.4th at 76-77 (affirming dismissal of fraud and negligent misrepresentation claims where the complaint "contained no allegation that plaintiffs 'saw, read, [heard,] or otherwise noticed' any of the

actionable misrepresentations"); Rider v. Uphold HQ Inc., 657 F. Supp. 3d 491, 503-04 (S.D.N.Y. 2023) (dismissing negligent misrepresentation claim under New York law where the complaint "contains only conclusory allegations that plaintiffs relied on defendants' statements"); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 772 (W.D.N.Y. 2017) (dismissing negligent misrepresentation claim because plaintiffs "failed to allege . . . that they actually read or saw the notices concerning [defendants'] privacy policies and practices").

Accordingly, Plaintiffs' negligent misrepresentation claim will be dismissed pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a claim.

C. Breach of Implied Contract

1. Applicable Law

To allege an implied contract under New York law, a plaintiff must plead the same elements as an express contract: "'consideration, mutual assent, legal capacity and legal subject matter.'" Sackin, 278 F. Supp. 3d at 750 (quoting Leibowitz v. Cornell Univ., 584 F.3d 487, 507 (2d Cir. 2009), superseded by statute on other grounds as recognized in Vogel v. CA, Inc., 662 F. App'x 72, 75 (2d Cir. 2016)); Forest Park Pictures v. Universal Television Network, Inc., 683 F.3d 424, 432 (2d Cir. 2012) ("[U]nder New York law, proof of an implied-in-fact contract requires proof of the same elements as an express contract[.]").

An implied contract "'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.'" Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of New Jersey, Inc., 448 F.3d 573, 582 (2d Cir. 2006) (quoting Jemzura v. Jemzura, 36 N.Y.2d 496, 503-04 (1975)). Such "facts and circumstances" include the "specific conduct of the parties, industry custom, and course of dealing." Nadel v. Play-By-Play Toys & Novelties, Inc., 208 F.3d 368, 376 n.5 (2d Cir. 2000) (citation omitted).

2. Analysis

In moving to dismiss, Defendant contends that "Plaintiffs fail to allege an implied contract," because allegations concerning Warner Music's "representations of security in its Privacy Policy" do not "give rise to contract claims." (Def. Br. (Dkt. No. 76) at 26-27) And even if the Court were to conclude that Plaintiffs have adequately alleged an implied contract, Plaintiffs "fail to offer non-conclusory allegations that [Warner Music] breached any such agreement." (Id. at 27)

The Amended Complaint alleges that (1) Defendant "solicited Plaintiffs . . . to make purchases through [its] e-commerce platforms," and that Defendant's solicitation "implied" a "promise" to Plaintiffs to keep their personal information "safe and secure"; (2) Plaintiffs "accepted" Defendant's offer, when they provided personal information required as a condition of their purchase of "goods or service[s]" from Defendant; (3) Defendant "breached these implied contracts by failing to keep the [personal information Plaintiffs] provided . . . safe and secure"; and (4) "[a]s a result of the breach of these implied contracts by [Defendant], Plaintiffs . . . suffered [] economic damages[.]" (Am. Cmplt. (Dkt. No. 74) ¶¶ 266-69)

In alleging the "mutual assent" element of an implied contract, Plaintiffs do not rely on the Warner Music Privacy Policy. Plaintiffs instead cite Warner Music's "operation of [online] commerce platforms" that required Plaintiffs to "enter" certain personal information "onto the website[s]" as a prerequisite to making a purchase. (Am. Cmplt. (Dkt. No. 74) ¶¶ 37, 266-67) Plaintiffs further allege that they provided the personal information Warner Music requested, and paid for music and related merchandise from Warner Music, and thus "adequate[ly] perform[ed]" their obligations under the implied contract." GE/CBPS Data Breach Litig., 2021 WL 3406374, at *12.

Courts have had little difficulty in concluding that an implied contract arises in such circumstances: "'it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of . . . sensitive personal information would not imply the recipient's assent to protect the information sufficiently,'" even where the recipient "may not have explicitly promised" to protect such information. Sackin, 278 F. Supp. 3d at 750-51 (quoting Castillo v. Seagate Tech., LLC, No. 16 Civ. 1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016)) (finding implied contract sufficiently pled where employer "required and obtained" its employees' personal information as part of a "course of dealing," thus "evincing an implicit promise . . . to keep its employees' [personal information] safe"); Miller v. Syracuse Univ., 662 F. Supp. 3d 338, 365 (N.D.N.Y. 2023) (finding implied contract sufficiently pled where defendant required plaintiff to "provide[] [s]ensitive information . . . to [d]efendant in connection with . . . obtaining . . . services from [d]efendant"); GE/CBPS Data Breach Litig., 2021 WL 3406374, at *12 (finding implied contract sufficiently pled where he "provided [his employer] with [his] personal information as required as a condition of [his] employment"). This Court finds that the Amended Complaint has alleged conduct evincing mutual assent.

The Amended Complaint also alleges facts demonstrating that Defendant breached the implied contract by failing to take reasonable measures "to keep the [personal information] provided by Plaintiffs . . . safe and secure[.]" (Am. Cmplt. (Dkt. No. 74) ¶ 268; id. ¶¶ 66-67, 69-70, 72, 74 (listing "reasonable industry standard protective measures" that Warner Music "failed to have in place")); see GE/CBPS Data Breach Litig., 2021 WL 3406374, at *12 (complaint adequately alleged breach of implied contract where it asserted that employer "'fail[ed] to safeguard and protect employees' personal and financial information . . . and . . .

fail[ed] to provide timely and accurate notice to [employees] that personal and financial information . . . was compromised as a result of the data breach'").

Accordingly, Defendant's motion to dismiss Plaintiffs' breach of implied contract claim will be denied.

D. Unjust Enrichment

1. Applicable Law

Unjust enrichment is a "quasi-contract cause of action." Under New York law, a plaintiff alleging unjust enrichment must plead facts showing that "'(1) the defendant benefitted; (2) at the plaintiff's expense; and (3) that equity and good conscience require restitution.'" Myun-Uk Choi v. Tower Research Capital LLC, 890 F.3d 60, 69 (2d Cir. 2018) (quoting Kaye v. Grossman, 202 F.3d 611, 616 (2d Cir. 2000)).

An unjust enrichment claim "is not available where it simply duplicates, or replaces, a conventional contract or tort claim[.]" Corsello v. Verizon N.Y., Inc., 18 N.Y.3d 777, 790 (2012) ("[U]njust enrichment is not a catchall cause of action to be used when others fail.") (collecting cases). In practice, such a claim is "available only in unusual situations when, though the defendant has not breached a contract nor committed a recognized tort, circumstances create an equitable obligation running from the defendant to the plaintiff," such as where a defendant, "though guilty of no wrongdoing, has received money to which he or she is not entitled." Id. at 790. In connection with unjust enrichment claims made in data breach cases, courts have acknowledged that it is generally the "third-party hacker [who] benefit[s] at the expense of" the entity whose system was breached and the individuals whose information was stolen, and as such, it is the hacker who "in equity and good conscience owes restitution." In re Waste Mgmt. Data Breach Litig., No. 21 Civ. 6147 (DLC), 2022 WL 561734, at *6 (S.D.N.Y. Feb. 24, 2022).

2. Analysis

Defendant argues that Plaintiffs' unjust enrichment claim should be dismissed because it "is a mere restatement" of Plaintiffs' other claims. (Def. Br. (Dkt. No. 76) at 33)

Plaintiffs' unjust enrichment claim is premised on the allegation that Defendant "profited from [Plaintiffs'] purchases" on its websites, and should have "used" part of its profits "to pay for the administrative costs of data management and security." (Am. Cmplt. (Dkt. No. 74) ¶¶ 271-273) Given these circumstances, Plaintiffs argue, "equity requires restitution of Defendant's ill-gotten gains" – the money it saved by "fail[ing] to implement" the "security measures that are mandated by industry standards." (Id. ¶ 274)

In their negligence claim, however, Plaintiffs allege that "Defendant breached its duties of care [to Plaintiffs]" by "failing to maintain appropriate technological and other systems to prevent unauthorized access[.]" (Id. ¶ 251) The duty of care that Defendant allegedly breached and the reasonable care that it failed to exercise relate to the same alleged failure to "use" its profits to "implement" "security measures" that Plaintiffs claim that they were entitled to as customers. (Id. ¶¶ 271-74)

The Amended Complaint's unjust enrichment and negligence claims are thus premised on the same facts, arise from the same 2020 data breach, and present "the same theories of harm." Rider, 657 F. Supp. 3d at 502-03 (dismissing – as "duplicative" of plaintiffs' contract claim – unjust enrichment claim alleging that "it would be inequitable to let [defendant] keep the profit it saved by maintaining allegedly inadequate data protection measures").

Because Plaintiffs' unjust enrichment claim is duplicative of their negligence claim, Warner Music's motion to dismiss the Amended Complaint's unjust enrichment claim will be granted.

E. New York General Business Law §§ 349, 350

1. Applicable Law

GBL § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce," while GBL § 350 prohibits "[f]alse advertising in the conduct of any business, trade or commerce[.]" N.Y. Gen Bus. Law §§ 349, 350. In order to state a claim under either section, "'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) (quoting Koch v. Acker, Merrall & Condit Co., 18 N.Y.3d 940, 944 (2012)).

To establish the "requisite causal connection between the alleged misrepresentation and the resulting injury," a plaintiff must plead facts showing that he or she "'actually viewed the misleading statement[s] prior to making [the] decision to purchase [defendant's product or service], and must set forth where, when and how [they] came to view it.'" Troy v. Am. Bar Ass'n, No. 23 Civ. 3053 (NGG) (VMS), 2024 WL 1886753, at *6 (E.D.N.Y. Apr. 30, 2024) (quoting In re GEICO Customer Data Breach Litig., No. 21 Civ. 2210 (KAM) (SJB), 2023 WL 4778646, at *17 (E.D.N.Y. July 21, 2023)). Absent such specific allegations a plaintiff has not pled causation, and such a deficiency is "fatal to [a GBL § 349] claim." Id.; see Oden v. Bos. Sci. Corp., 330 F. Supp. 3d 877, 902 (E.D.N.Y. 2018) (analyzing GBL § 350 claim under the same pleading standard as GBL § 349 claim, and dismissing both GBL § 349 and § 350 claims because "none of the[] allegations provides any indication . . . [of] where, when and how [p]laintiff came to view [the allegedly deceptive statements]").

2. Analysis

Defendant argues that Plaintiffs' GBL claims should be dismissed because Plaintiffs do not allege that "[Warner Music's] statements regarding its data security practices

had any effect on their decisions to make purchases on [Warner Music's] websites." (Def. Br. (Dkt. No. 76) at 29)

As discussed in connection with Plaintiffs' negligent misrepresentation claim, the Amended Complaint alleges that the assertion in Warner Music's Privacy Policy that Defendant uses "reasonable physical, technical and administrative measures to protect Personal Information under [its] control" is false. (See Am. Cmplt. (Dkt. No. 74) ¶ 287) (characterizing the Privacy Policy as a "misleading act and practice[]" or "misrepresent[ation]")

As to causation, the Amended Complaint asserts that when Plaintiffs entered their personal information on Warner Music's websites in order to purchase Defendant's music and related merchandise, they "relied" on Warner Music's false representation that it would "safeguard" their personal information. (Am. Cmplt. (Dkt. No. 74) ¶ 290) Plaintiffs further assert that they "would not have provided their [personal information] to Defendant had they known Defendant did not use 'reasonable physical, technical and administrative measures to protect Personal Information under [its] control.'" (Id. ¶¶ 293, 304)

However, the Amended Complaint does not plead facts demonstrating that Plaintiffs saw or read the Privacy Policy containing the representation that Warner Music uses "'reasonable physical, technical and administrative measures to protect [customers'] Personal Information under [its] control.'" Because Plaintiffs do not plead facts establishing "where, when and how [they] came to view'" the Privacy Policy containing the alleged misrepresentation, their GBL claims must be dismissed. See Troy, 2024 WL 1886753, at *6 (dismissing GBL § 349 claim because "Plaintiffs do not allege that they saw or read [defendant's] privacy policy prior to the alleged harm"); see also Oden, 330 F. Supp. 3d at 902 (dismissing GBL §§ 349, 350 claims; although the complaint "sets forth certain statements

contained on [d]efendant's website," "these allegations neither explicitly state nor permit the plausible inference that [p]laintiff actually saw these statements prior to making the determination . . . to purchase the [product at issue]"); Turk v. Rubbermaid Inc., No. 21 Civ. 270 (KMK), 2022 WL 836894, at *9 (S.D.N.Y. Mar. 21, 2022) (dismissing GBL §§ 349, 350 claims because plaintiffs merely "allege[d] in a conclusory fashion that they 'relied on representations . . . on [defendant's websites],'" without alleging "that they actually saw or were aware of the statements in question . . . before buying' products [at issue]"); Gale v. Int'l Bus. Machines Corp., 9 A.D. 3d 446, 447 (2d Dept. 2004) (dismissing GBL §§ 349, 350 claims; "[a]lthough the plaintiff cites particular misleading statements," he "nowhere states in his complaint that he saw any of these statements before he purchased" the product at issue).

In seeking to avoid this result, Plaintiffs point to the Amended Complaint's allegation that "they would not have made purchases from Defendant had Defendant 'disclosed that it lacked computer systems and data security practices adequate to safeguard customers' [personal information] from theft.'" (Pltf. Opp. (Dkt. No. 80) at 24 (quoting Am. Cmplt. (Dkt. No. 74) ¶ 93))

While "[r]eliance is not an element under [GBL] § 349," a plaintiff must nonetheless show – under both GBL § 349 and GBL § 350 – that the "defendant's material deceptive act caused [plaintiff] injury." Gale, 9 A.D. 3d at 447; see also Koch, 18 N.Y.3d at 941 (same). And a plaintiff cannot have been injured by an alleged misrepresentation that the plaintiff never saw. Here, the Amended Complaint provides only broad conclusory allegations as

to causation. Plaintiffs have not plausibly alleged the requisite element of causation "with sufficient specificity to withstand dismissal."[7] Gale, 9 A.D. 3d at 447.

Accordingly, Warner Music's motion to dismiss the Amended Complaint's GBL §§ 349, 350 claims will be granted.

F. California Consumer Privacy Act

1. Applicable Law

The California Consumer Privacy Act ("CCPA") authorizes an award of damages, injunctive relief, and declaratory relief for "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of [a] business's violation of the duty to implement and maintain reasonable security procedures and practices[.]" Cal. Civ. Code § 1798.150(a)(1); see Waste Mgmt. Data Breach, 2022 WL 561734, at *6.[8]

For purposes of the CCPA, "[p]ersonal information" is defined as, inter alia, an "[a]ccount number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

To plead a CCPA violation, a plaintiff must allege that defendant breached its "duty to implement and maintain reasonable security procedures and practices[.]" Cal. Civ.

---

[7] Having found that Plaintiffs have not adequately pled causation, the Court does not reach Defendant's additional arguments for dismissal of Plaintiffs' GBL claims, including that Plaintiffs have not plausibly alleged that the Privacy Policy was materially misleading. (Def. Br. (Dkt. No. 76) at 28-29)

[8] The CCPA claim is brought on behalf of a California subclass. (See Am. Cmplt. (Dkt. No. 74) ¶¶ 223, 307) Because Defendant has not disputed the applicability of the CCPA (or that Warner Music is a "business" that is covered by the statute, see Cal. Civ. Code § 1798.140(d)(1)); Def. Br. (Dkt. No. 76) at 30-32), the Court considers below whether the CCPA claim is adequately pled.

Code § 1798.150(a)(1). The statute does not define the term "reasonable security procedures and practices," and because "the CCPA only applies to data breaches that occurred after January 1, 2020, courts have had few opportunities to dissect the Act's provisions." In re Blackbaud, Inc., Customer Data Breach Litig., No. 20 MDL 2972 (JMC), 2021 WL 3568394, at *4 (D.S.C. Aug. 12, 2021). Accordingly, the pleading standard for CCPA claims is not entirely clear.

Some courts have permitted CCPA claims to proceed where plaintiff merely "alleg[es] that unauthorized parties were able to access plaintiffs' personal information." Doe v. MKS Instruments, Inc., No. 23 Civ. 868 (CJC), 2023 WL 9421115, at *3 (C.D. Cal. Nov. 3, 2023); see also Kirsten v. California Pizza Kitchen, Inc., 21 Civ. 9578 (DOC), 2022 WL 16894503, at *3 (C.D. Cal. July 29, 2022) ("[W]hen plaintiffs alleged that defendants allowed unauthorized parties on the internet to access plaintiffs' [personal information], plaintiffs [have] plausibly alleged that defendant failed to maintain reasonable security procedures") (collecting cases); Mehta v. Robinhood Fin. LLC, No. 21 Civ. 1013 (SVK), 2021 WL 6882377, at *8 (N.D. Cal. May 6, 2021) (permitting CCPA claim to proceed where complaint alleged that defendant "allow[ed] unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal information of [p]laintiffs and other customers, including their personal and financial information"); Ramos v. Wells Fargo Bank, N.A., No. 23-CV-0757 (BGS), 2023 WL 5310540, at *2 (S.D. Cal. Aug. 17, 2023) (plaintiff plausibly alleged that defendant did not maintain adequate security measures when he pled that "unknown individuals accessed information regarding his savings account").

The cases cited above indicate that where a hacker has breached a business's database, it necessarily follows – at least for pleading purposes – that that business did not employ "reasonable security procedures and practices." In this regard, one court has explained

that – at the pleading stage – "a plaintiff ordinarily will have few facts in his possession to allege precisely how a data breach occurred and how a defendant's security procedures were inadequate to prevent the data breach." MKS Instruments, 2023 WL 9421115, at *3.

Other courts have required CCPA plaintiffs to plead facts demonstrating not only that there was a data breach, but also that the breach occurred "as a result of" the defendant's failure "to implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.150(a)(1); see, e.g., Waste Mgmt. Data Breach Litig., 2022 WL 561734, at *6 (dismissing CCPA claim where plaintiff "allege[d] that an unauthorized actor hacked into and stole the plaintiffs' [personal information] from [defendant's] systems," but not did not explain what security practices "need to be remedied"); Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 57 (D. Ariz. 2021) (dismissing CCPA claim regarding data breach because complaint "did not allege sufficient facts to establish how or why [defendant's] systems were inadequate or unreasonable or how or why [defendant] knew or should have known its systems were inadequate or unreasonable"); Tian v. Bank of Am., N.A., No. 2:24-CV-09877-MCS-PD, 2025 WL 1377767, at *3 (C.D. Cal. Apr. 2, 2025) (same); Danfer-Klaben v. JPMorgan Chase Bank, N.A., No. 2:12-cv-62, 2022 WL 3012528, at *7 (C.D. Cal. Jan. 24, 2022) (dismissing CCPA claim where plaintiff did not allege that data breach was the result of a failure "to implement and maintain reasonable security measures"); see also In re Bank of Am. California Unemployment Benefits Litig., 674 F. Supp. 3d 884, 916 (S.D. Cal. 2023) (dismissing CCPA claim where plaintiff alleged that defendant "collected, stored, and/or transmitted Plaintiffs' . . . personal information in a nonencrypted and nonredacted form . . . that permitted unauthorized third parties to access that information"; "[w]hile [plaintiff's] allegations certainly suggest a possibility that inadequately secure collection, transmission, and storage may be the reason

[plaintiff's] data was stolen, they aren't the only or even the most plausible inference supported by the allegations") (emphasis in original).

The Court concludes that this line of authority is more consistent with the applicable statutory language, see Cal. Civ. Code § 1798.150(a)(1), and with general pleading standards requiring plaintiffs to "plead[] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678. Accordingly, for purposes of their CCPA claim, Plaintiffs must plead facts (1) identifying "reasonable security procedures and practices" that would have prevented disclosure of their private information, which (2) Defendant did not take, and as a result, (3) Plaintiffs' "personal information" was "subject[ed]" to an "unauthorized access."[9] Cal. Civ. Code § 1798.150(a)(1).

2. Analysis

In moving to dismiss, Defendants argue that Plaintiffs have not alleged (1) disclosure of any actionable "personal information" as defined by the CCPA; or (2) that Warner Music's "security was deficient." (Def. Br. (Dkt. No. 76) at 30-32)

As to personal information, the Amended Complaint alleges that the compromised information includes "payment card numbers, payment card . . . security codes [or verification

[9] This approach is also consistent with how California courts have treated other California statutes that require businesses to employ "reasonable security procedures and practices" to protect customer information. For example, the California Customer Records Act requires businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the [customer] information [owned, licensed, or maintained]." Cal. Civ. Code § 1798.81.5. A plaintiff alleging a violation of this statute is required to plead in his or her complaint "facts about [the business's] protocols or actions it took when choosing appropriate security measures," and "what made [the business's] security measures unreasonable by comparison to what other companies are doing[.]" Razuki v. Caliber Home Loans, Inc., No. 17 Civ. 1718 (LAB), 2018 WL 6018361, at *1-2 (S.D. Cal. Nov. 15, 2018) (acknowledging that while "it may be difficult to definitively show [a business's practices] were insufficient prior to discovery," a plaintiff is nonetheless required to plead "basic" answers to "[w]hat facts le[d] him to believe [the defendant] didn't comply with industry standards? What are other companies doing that [defendant] isn't?").

numbers,] and payment card expiration dates." (Am. Cmplt. (Dkt. No. 74) ¶¶ 1, 37; see id. ¶ 310 (alleging that the compromised personal information "was unencrypted and unredacted and included names and account numbers of payment cards combined with the security codes); id. ¶ 308 (alleging that Plaintiffs "provided to Defendant their nonencrypted and nonredacted personal information")) These allegations are adequate for purposes of a CCPA claim, given that the statute defines "personal information" to include a "credit or debit card number, in combination with any required security code . . . that would permit access to an individual's financial account." Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

As to reasonable security procedures – and as discussed above – the Amended Complaint cites a number of "reasonable industry standard protective measures" and practices that Defendant "failed to have in place" (see Am. Cmplt. (Dkt. No. 74) ¶¶ 61, 66-67, 69-70, 72, 74), which "result[ed]" in the "unauthorized access and exfiltration, theft, or disclosure of" Plaintiffs' personal information. (Id. ¶¶ 309, 311; see also id. ¶¶ 4-5 ("Because of [Warner Music's] inadequate data security practices, for more than three months, unauthorized third parties compromised a number of [Warner Music's] . . . websites . . . and exfiltrated private data and payment card information . . . from the Plaintiffs' and the Class Members' browser."))

While Defendant asserts that Plaintiffs merely assume that "because [Warner Music] issued a breach notification, its security was deficient" (Def. Br. (Dkt. No. 76) at 32), that is not a fair characterization of what is pled in the Amended Complaint. As discussed above, Plaintiffs have described reasonable policies and practices Warner Music should have implemented to protect their personal information, including, inter alia, "outsourc[ing] the payment processing to a . . . third-party site," and "not hav[ing] pages with [customers' personal information] or payment information on the artists' websites[.]" (Am. Cmplt. (Dkt. No. 74) ¶ 66)

According to the Amended Complaint, such security measures are "reasonable" and "industry standard" (id. ¶ 61), but Warner Music "failed to have [such measures] in place," thus permitting "Magecart-style hackers" to "exploit weaknesses or gain access to" Plaintiffs' personal information. (Id. ¶¶ 61, 65-68)

The Court concludes that Plaintiffs' allegations are sufficient for purposes of their CCPA claim. Accordingly, Defendant's motion to dismiss will be denied as to the Amended Complaint's CCPA claim.

IV. LEAVE TO AMEND

Although Plaintiffs have not requested leave to re-plead, the Court has considered whether they should be given an opportunity to do so. Leave to amend should be "freely give[n] . . . when justice so requires." Fed. R. Civ. P. 15(a)(2). District courts "ha[ve] broad discretion in determining whether to grant leave to amend." Gurary v. Winehouse, 235 F.3d 792, 801 (2d Cir. 2000). Leave to amend may properly be denied in cases of "'undue delay, bad faith, or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of amendment, etc.'" Ruotolo v. City of N.Y., 514 F.3d 184, 191 (2d Cir. 2008) (quoting Foman v. Davis, 371 U.S. 178, 182 (1962)).

"Where the possibility exists that [a] defect can be cured," leave to amend "should normally be granted" at least once. Wright v. Ernst & Young LLP, 97 Civ. 2189 (SAS), 1997 WL 563782, at *3 (S.D.N.Y. Sept. 10, 1997), aff'd, 152 F.3d 169 (2d Cir. 1998) (citing Oliver Schs., Inc. v. Foley, 930 F.2d 248, 253 (2d Cir. 1991)). Moreover, where a claim is dismissed on the grounds that it is "inadequate[ly] [pled]," there is "a strong preference for allowing plaintiffs to amend." In re Bear Stearns Cos., Inc. Sec., Derivative, & ERISA Litig., 08 MDL 1963 (RWS),

2011 WL 4072027, at *2 (S.D.N.Y. Sept. 13, 2011) (citing Ronzani v. Sanofi S.A., 899 F.2d 195, 198 (2d Cir. 1990)).

Leave to amend is denied as to Plaintiffs' unjust enrichment claim, which is duplicative of Plaintiffs' negligence claim. As to Plaintiffs' negligent misrepresentation and GBL claims, this Court cannot find – at this stage of the proceedings – that it is impossible to cure the pleading defects identified above. Accordingly, leave to move to amend is granted as to the Amended Complaint's negligent misrepresentation and GBL §§ 349, 350 claims.

CONCLUSION

For the reasons stated above, Defendant's motion to dismiss the Amended Complaint's negligent misrepresentation, unjust enrichment, and GBL §§ 349, 350 claims is granted. The motion to dismiss is otherwise denied. Leave to move to amend is granted as to the negligent misrepresentation and GBL §§ 349, 350 claims, but denied as to the unjust enrichment claim.

Any motion for leave to amend will be filed by **September 17, 2025**. The proposed Second Amended Consolidated Class Action Complaint is to be attached as an exhibit to the motion papers.

The Clerk of Court is directed to terminate the motion (Dkt. No. 75).

Dated: New York, New York
September 3, 2025

SO ORDERED.

Paul G. Gardephe
United States District Judge

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.nysd.544071/go
on 2026-11-21 and is hosted, unaltered, for reference at
https://dev.chimo.ai/class-action/warner-music-group

Court: U.S. District Court for the Southern District of New York
Case number: 1:20-cv-07473-PGG
Filed: 2025-09-03

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.