UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In re Stryker Corporation Cyberattack Litigation

Case No. 1:26-CV-00832-HYJ-PJG

Hon. Hala Y. Jarbou
Hon. Phillip J. Green

Stryker Corporation's Brief in Support of Its Motion To Dismiss

DLA PIPER LLP (US)
Colleen Carey Gulliver
1251 Avenue of the Americas
New York, New York 10020
Tel: 212-335-4500
colleen.gulliver@us.dlapiper.com

MILLER JOHNSON PLC
D. Andrew Portinga
Amy E. Murphy
45 Ottawa Avenue SW
Suite 1100
Grand Rapids, Michigan 49503
Tel: 616-831-1700
portingaa@millerjohnson.com
murphya@millerjohnson.com

Table of Contents

Table of Authorities

Page(s)

Cases

Statutes

Other Authorities

I. Introduction

Merely 48 hours after Stryker Corporation ("Stryker") announced on March 11, 2026, that it had experienced a cyberattack (the "Cyberattack"), plaintiffs Tom Mesmer, Dax Dodge, Joseph Fredrickson, Scott Mangold, Maurice Primer, Tristan Tanner, Belva Thompson, and Stacy Trepanier ("Plaintiffs") began filing lawsuits, each speculating that their personally identifiable information ("PII") was accessed. Stryker respectfully submits this memorandum of law in support of its motion to dismiss Plaintiffs' Consolidated Amended Complaint ("CAC") in its entirety under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) ("Motion").

As an initial matter, this case must be dismissed because the Court does not have subject matter jurisdiction. Plaintiffs' allegations of Article III standing cannot survive Stryker's factual challenge. Plaintiffs bear the burden of establishing, *as a factual matter* and not simply as a matter of conclusory allegations afforded a presumption of truthfulness, that subject matter jurisdiction exists. When, as here, Stryker submits evidence that "Stryker's investigation into the Cyberattack did not uncover any evidence that Plaintiffs' PII was accessed in the Cyberattack" (June 22, 2026 Declaration of Juan Pablo Calderon ("Calderon Decl.") ¶ 5), Plaintiffs bear the burden of *proving* this Court has subject matter jurisdiction. They cannot do so.

Plaintiffs have not alleged (nor can they allege) that Stryker notified them that their PII was accessed in the Cyberattack, even though notifications would be required under the governing legal framework in various jurisdictions and is typically used to allege standing. Notably, Plaintiffs have each had their data

exposed in numerous prior breaches having nothing to do with Stryker. For example, Thompson experienced identity theft *multiple times* before the Cyberattack, and Tanner sued another former employer just a week *before* filing the CAC, claiming that the same information was accessed.

Even if Plaintiffs could establish standing, which they cannot, the CAC must still be dismissed because it fails to state a claim. At "the motion-to-dismiss stage, [a plaintiff] must plead specific facts beyond speculation." *Romero v. City of Lansing Mich.*, 159 F.4th 1002, 1015 (6th Cir. 2025), *petition for cert. filed*, No. 25-1295 (U.S. May 13, 2026). They have not done so. Plaintiffs' allegations fail to state a claim for any of their seven claims, as outlined below.

Accordingly, the Court should grant Stryker's Motion.

II. Factual Background

A. Stryker Was the Victim of a Major Cyberattack.

Stryker is a global medical technology company that develops products and services used in medical and surgical care. *See* CAC PageID.87 ¶ 2, PageID.90 ¶ 20. Stryker is incorporated and has its principal place of business in Michigan. *Id.* PageID.89 ¶ 16. On March 11, 2026, Stryker announced that it had experienced a Cyberattack, "[which] caused disruption[] to [its] business operations." Calderon Decl. ¶ 3. Plaintiffs allege that Stryker experienced a "wipe[r]" attack, which wiped certain data from Stryker systems and that an Iranian nation-state cybercriminal group, called "Handala," claimed credit. CAC PageID.96 ¶ 42, PageID.94 ¶ 38.[1]

[1] Plaintiffs allege that Stryker has a "Privacy Policy," whereby Stryker "represented that it had a legal duty to protect Plaintiffs' . . . PII." (CAC PageID.90 ¶ 25, PageID.133

B. Plaintiffs Sued Stryker 48 Hours After the Cyberattack.

48 hours after the announcement, Plaintiffs began to sue. *See* ECF No. 1 (Mesmer Complaint, dated March 13, 2026). Plaintiffs alleged that PII and protected health information ("PHI") had been accessed during the Cyberattack. However, no Plaintiffs alleged that they had received a notice from Stryker informing them that their PII had been accessed (nor could they).

On May 8, 2026, Plaintiffs filed the CAC and alleged that PII was disclosed, purportedly including names, social security numbers, unspecified financial account information, unspecified health insurance information, and unspecified driver's license information. CAC PageID.160 ¶ 28. Plaintiffs assert seven claims: negligence, negligence *per se*, breach of implied contract, intrusion upon seclusion, unjust enrichment, breach of confidence, and declaratory judgment. *Id.* PageID.128-141 ¶¶ 246-334. Despite Plaintiffs all being current or former Stryker employees, they seek to represent: "[a]ll *individuals* residing in the United States whose PII was compromised … including all those individuals who received notice of the Data Breach." *Id.* PageID.125 ¶ 236 (emphasis added).

¶ 283). This is incorrect. Stryker has a "Privacy Statement," which applies "to the personal information of consumers." June 22, 2026 Declaration of Colleen M. Gulliver ("Gulliver Decl."), Ex. B. Plaintiffs, however, are all current or former *employees* of Stryker. Because this document is a "public record" that is "central to the claims" in the CAC, the Court may consider it on a motion to dismiss. *Elec. Merch. Sys. LLC v. Gaal*, 58 F.4th 877, 883 (6th Cir. 2023) (citations omitted).

C. Plaintiffs Only Vaguely Allege that They Were Injured.

The CAC does not allege that any Plaintiff received a notice from Stryker stating that their PII was accessed. Instead, Plaintiffs repeat vague allegations of a host of theoretical injuries comprised of:

- "exposure and theft of [their] PII" (*See, e.g.*, CAC PageID.99 ¶ 60, PageID.101 ¶ 82);
- "fear[] for [their] personal financial security" and "anxiety" (*see, e.g.*, *id.* PageID.99 ¶¶ 58-59, PageID.101 ¶¶ 80-81);
- "diminution in the value of [their] PII" (*see, e.g.*, *id.* PageID.99 ¶ 61; PageID.102 ¶83);
- "[o]n information and belief" that their PII "ha[d] already been published—or w[ould] be published imminently—by cybercriminals on the dark web" (*see, e.g.*, *id.* PageID.131 ¶ 265; PageID.101 ¶ 76); and
- that they "anticipate[] spending considerable amounts of time and money to try to mitigate [their] injuries" (*see, e.g.*, *id.* PageID.99 ¶ 63, PageID.102 ¶ 85, PageID.104 ¶103).

Moreover, six Plaintiffs vaguely allege purported misuse of their PII that they speculate is tied to the Cyberattack, apparently simply because it occurred "around the time" of the Cyberattack, as detailed below:

Plaintiff	Allegation
Mesmer	"[A]round the time of the Data Breach, Plaintiff received a LinkedIn invitation and message from a fraudulent actor posing as a Stryker employee in an attempt to commit social-engineering fraud." CAC PageID.98 ¶ 56.
Primer	"Plaintiff experienced fraudulent activity associated with his Apple account shortly after the Data Breach." *Id.* PageID.107 ¶ 133.
Mangold	"[A]round the time of the Data Breach, Plaintiff received a dark

Plaintiff	Allegation
	web alert . . . alerting him that his PII, including an email and password he used during his time he [sic] worked with Stryker, was found on the dark web." *Id.* PageID.105 ¶ 114.
Thompson	"[R]ight after the Data Breach, she had multiple instances of account openings/attempts." *Id.* PageID.111 ¶ 167. "Plaintiff received a denial notice for a credit application she did not submit, and an unauthorized account was opened in her name." *Id.* ¶ 168. "Plaintiff's credit score dropped by 46 points." *Id.* ¶ 169. "On or about March 17, 2026, Plaintiff began receiving multiple alerts ,. . . indicating her login credentials had been found on the dark web. That same day, she was locked out of her bank account twice after an unknown actor repeatedly changed her password." *Id.* ¶ 170. "[I]n the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls." *Id.* ¶ 172.
Trepanier	"[I]n the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam emails and phone calls." *Id.* PageID.113 ¶ 189.
Dodge	"[I]n the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam emails, text messages and phone calls." *Id.* PageID.101 ¶ 79.

These Plaintiffs, however, do not allege sufficient detail to link these incidents to the Cyberattack. *See* Declaration of William Hardin ("Hardin Decl.") ¶ 13. For example, much of the data necessary for these occurrences has not even been alleged to have been accessed in the Cyberattack. *Compare* CAC PageID.92 ¶ 28, PageID.98-114 ¶¶ 47-196, *with* Hardin Decl. ¶¶ 16-23, 25-35, 37-38. Finally, despite seeking to represent individuals who were damaged when their PII was accessed, Dodge also asserts that he "was not paid for at least 34 hours because Defendant was not operational after the [Cyberattack]." CAC PageID.101 ¶ 75.

D. Plaintiffs' Allegations of Injury are Unfounded.

While Plaintiffs allege in conclusory fashion both that they were injured and that their alleged injuries are due to the Cyberattack, Plaintiffs' allegations are demonstrably untrue. In fact, Stryker does not have any evidence that Plaintiffs' PII was accessed. Calderon Decl. ¶ 5. Stryker, with the help of independent experts, "reviewed files and data that were identified as potentially being accessed by the threat actor during the Cyberattack" and "determined as a purely factual matter that … the Plaintiffs' PII [does not] exist[] in those files and data." *Id.* ¶ 5. The only information relating to Plaintiffs identified were the business email addresses of Dodge and Fredrickson. *Id.* Significantly, although Stryker is required by governing legal frameworks in various jurisdictions to make written notifications to any individual whose PII was accessed during an incident like the Cyberattack, Stryker has not notified any of these eight individuals that their PII was accessed. *Id.* ¶ 6.

Moreover, each Plaintiff has been impacted by numerous prior data breaches, including potential exposure of their social security numbers. *See* Hardin Decl. ¶¶ 12, 20, 31, 35, 38. For example, Thompson and Tanner's data was implicated in at least 20 prior data breaches. *Id.* ¶¶ 20, 42. Plaintiffs concede that in 2024 *alone* data breaches "expos[ed] approximately 1,350,835,988 sensitive records." CAC PageID.121-122 ¶ 222.

The evidence otherwise refutes Plaintiffs' conclusory allegations. For example, while Mangold alleges that he is a "former employee" and that Stryker "continues to maintain [his] PII" (CAC PageID.104-105 ¶¶ 105, 110), he does not acknowledge that his employment ended in "July 2007," *19 years ago*. June 21, 2026 Declaration of Michael Puca ("Puca Decl.") ¶ 5. Stryker "did not locate any files for Mr. Mangold," which is not surprising given that "Stryker's retention period for an employee's personnel file is a period of six years after their employment ends" and "Stryker would have … ceased retaining [Mangold's] physical personnel file [in or around 2013]", or more than a decade before the Cyberattack." Puca Decl. ¶¶ 5, 6.

Similarly, while Thompson claims that her PII was "compromised" in the Cyberattack (CAC PageID.111 ¶ 166), she fails to disclose that she experienced at least *three* prior instances of her identity being stolen: (1) in October 2017, she "checked her Experian credit bureau report" and saw "an apparent attempt by somebody to change her personal data" (Hardin Decl. Ex. C); (2) in September 2020, she was "defrauded out of unemployment compensation and [her] identity stolen

along with [her] social security information [and she did] not know what else could have been taken or compromised" (*id.* Ex. D); and (3) in September 2021, "[her] unemployment insurance was stolen, someone took over [her] platform and put their information in and changed the banking details … prevent[ing her] from appl[y]ing or having access to [her] account" (*id.* Ex. E).

Furthermore, Tanner alleges his PII was "compromised" (CAC PageID.107 ¶ 132), but does not acknowledge that he sued another former employer, Medtronic, alleging that the *same* PII "has presumably been compromised" in a Medtronic cyber-breach incident purportedly suffered on April 17, 2026. *Compare* Gulliver Decl. Ex. A at ¶ 27 ("likely includ[ing]" his name, social security number, and driver's license information), *with* CAC PageID.92 ¶ 28, PageID.107 ¶ 132.

Dodge, Thompson, and Trepanier also allege "a spike in spam and scam [] text messages and phone calls." CAC PageID.101 ¶ 79, PageID.111¶ 172, PageID.113 ¶ 189. Yet, Plaintiffs do not allege that the information needed to send spam—their phone number or email address—was accessed during the Cyberattack. CAC PageID.92 ¶ 28. Regardless, they experienced numerous prior breaches where their phone number or email address *was* disclosed. Hardin Decl. ¶¶ 16, 19-20, 25-26, 37-38. Moreover, Mesmer alleges that he "received a LinkedIn invitation … from a fraudulent actor posing as a Stryker employee" (CAC PageID.99 ¶ 56), but does not allege that he suffered any resulting injuries or otherwise explain how this could be related to the Cyberattack. *Id.* PageID.98-100 ¶¶ 47-64.

Finally, while Dodge alleges that he "was not paid for at least 34 hours" of work after the Cyberattack (CAC PageID.101 ¶ 75), he *was* in fact paid. Dodge was informed twice, more than two months before he filed the CAC, that he would receive "facility closure pay" for any regular hours he did not work. *See* Puca Decl. ¶ 7, Exs. B, C. Dodge was paid his full 40 hours at his regular hourly rate during the week of the Cyberattack and the two weeks after, including 55.5 hours of Facility Closure pay. *Id.* ¶ 8.

III. Legal Standard

A. Fed. R. Civ. P. 12(b)(1).

"The standard for evaluating a Rule 12(b)(1) motion depends on the nature of the 'attack' on subject matter jurisdiction." *Miedel v. Ally Bank*, No. 1:25-cv-406, 2025 WL 2751533, at *2 (W.D. Mich. Sep. 29, 2025) (Jarbou C.J.). "No presumption of truth applies in a 'factual attack' on subject matter jurisdiction." *Id.* "The plaintiff bears the burden of proof of jurisdiction when a factual attack is made. And the Court has 'broad discretion with respect to what evidence to consider[.]'" *Id.* (citations omitted); *see also Shepherd v. Cancer & Hematology Ctrs. of W. Michigan,* 2023 WL 4056342, at *4-5 (W.D. Mich. 2023) (courts have "wide discretion" to consider evidence outside the pleadings when resolving a factual attack on standing); *Polkowski v. Jack Doheny Cos., Inc.*, No. 2:25-cv-10516, 2025 WL 3079358, at *6 (E.D. Mich. Nov. 4, 2025). "'[T]he trial court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case [and t]he existence of disputed material facts will not preclude the trial court from evaluating

for itself the merits of jurisdictional claims.'" *Miedel*, 2025 WL 2751533, at *2 (citation omitted).

B. Fed. R. Civ. P. 12(b)(6).

"Under Rule 12(b)(6) … a complaint may be dismissed for failure to state a claim if it fails to give the defendant fair notice of what the [] claim is and the grounds upon which it rests." *Babbin v. Muirhead*, No. 1:25-cv-1794, 2026 WL 935893, at *2 (W.D. Mich. Apr. 7, 2026) (Jarbou C.J.) (citation omitted). "The court must determine whether the complaint contains 'enough facts to state a claim to relief that is plausible on its face.'" *Id.* (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim is facially plausible 'when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Fulton v. Lilly Township*, No. 1:24-cv-1168, 2025 WL 2601914, at *5 (W.D. Mich. Sep. 9, 2025) (Jarbou C.J.) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). "[A] plaintiff's allegations must include more than labels and conclusions." *Id.* at *4. "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—that the pleader is entitled to relief." *Id.* at *5 (alterations in original) (citations omitted).

IV. Argument

A. Plaintiffs Do Not Have Article III Standing.

Plaintiffs do not have Article III standing, and this Court does not have subject matter jurisdiction. "Whether a party has Article III standing is an issue of the court's subject matter jurisdiction under [FRCP] 12(b)(1). A plaintiff must have

standing for each claim pursued[.]" *Fedorova v. Foley*, No. 1:22-cv-991, 2023 WL 3484430, at *2 (W.D. Mich. May 16, 2023) (Jarbou, C.J.) (citation modified & omitted) (dismissing complaint for lack of subject matter jurisdiction).

A factual challenge to standing "contests the factual predicate for jurisdiction." *Shepherd*, 2023 WL 4056342, at *2. "In a factual attack, the allegations in the complaint are not afforded a presumption of truthfulness and the district court weighs competing evidence to determine whether subject matter jurisdiction exists." *Id.* "The burden remains with the Plaintiff to establish that jurisdiction exists." *Polkwoski*, 2025 WL 3079358, at *2.

To establish standing, Plaintiffs *must* "show they '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.'" *Miedel*, 2025 WL 2751533, at *3 (citation omitted) (dismissing for lack of standing). "[T]he plaintiff must 'clearly … allege facts demonstrating' each element … If no plaintiff has standing, then the court lacks subject-matter jurisdiction." *Id.* (citations omitted).

Here, Plaintiffs do not have standing because they have: (1) no cognizable injury; and (2) any putative injury is not fairly traceable to Stryker.

1. *Plaintiffs Have Not Been Injured Because They Have Not Suffered Concrete Harm.*

Plaintiffs cannot demonstrate that they suffered cognizable injuries. "Even at the motion-to-dismiss stage, [a plaintiff] must plead specific facts beyond speculation[.]" *Romero*, 159 F.4th at 1015. The Supreme Court reinforced that plaintiffs "must demonstrate … that they suffered a concrete harm. No concrete

harm, no standing." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021). In *TransUnion*, the Supreme Court found that although the defendant had applied inaccurate Office of Foreign Assets Control alerts to over 8,000 consumers' credit files, only those consumers whose potential creditors received the alerts suffered concrete injury sufficient to establish standing. *See id.* at 432-33. In contrast, those consumers whose "credit files were not disseminated …" did not suffer a concrete harm" and "risk of future harm" that the credit files could be disseminated were insufficient for standing. *Id.* at 437-39.

Prior to *Transunion,* the Sixth Circuit considered the necessary showing for Article III standing in a data breach context in an unpublished, non-binding decision, *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384 (6th Cir. 2016). There, the Sixth Circuit found standing only where the plaintiffs' PII had "already been stolen and [wa]s now in the hands of ill-intentioned criminals." *Id.* at 388. The court expressly distinguished cases where, as here, no "identifiable taking" occurred. *Id.* at 389-90.

District courts have similarly and repeatedly distinguished *Galaria* where a plaintiff's allegations "indicate only that the data was accessed, *i.e.*, breached," that "alone does not demonstrate a cognizable injury." *See, e.g.*, *Muniz v. Bronson Health Care Grp.*, No. 1:25-cv-693, 2026 WL 1649197, at *4 (W.D. Mich. Jan. 20, 2026); *Shepherd*, 2023 WL 4056342, at *6-7 (distinguishing *Galaria*). Here, as shown below, Plaintiffs cannot even establish that their data was accessed—let

alone establish an "identifiable taking"—or that their purported injuries are fairly traceable to Stryker.

A plaintiff does not have standing by "simply claim[ing] the existence of a breach" and then "speculat[ing] a parade of horribles." *Sifuentes v. Pluto TV*, No. 1:23-cv-1013, 2023 WL 7319434, at *3 (W.D. Mich. Nov. 7, 2023) (dismissing on standing). Instead, employees typically support standing by alleging they received employer notice that their data was accessed and then demonstrating misuse of that accessed data. *See*, *e.g.*, *Polkowski*, 2025 WL 3079358, at *1, *3-4 (plaintiff who was "informed" by the defendant of access had pled injuries to sustain a facial attack on standing).[2]

In *Muniz*, for example, the plaintiff, who received a notice indicating her PII was "potentially accessed," alleged she was injured because her PII was "wrongfully 'obtained,' 'accessed and acquired,' 'misused,' and/or 'accessed and stolen.'" 2026 WL 1649197, at *3. The Court found that "the fact of a data breach alone does not demonstrate a cognizable injury" and "without some plausible supporting factual allegations describing misuse or theft, [the plaintiff's] bare allegation that the [PII] was merely accessed and only *might* be sold or otherwise fraudulently used is too speculative to satisfy Article III standing." *Id.* at *4.

So too here. Plaintiffs do not allege Stryker notified them that their data was accessed (*see generally* CAC), nor could they, as Stryker does not have any evidence

[2] Plaintiffs tacitly acknowledge this by including in their class definition "individuals who received notice of the Data Breach." *See* CAC PageID.125 ¶ 236.

that their PII was exposed and never sent them any such notices. Calderon Decl. ¶¶ 5, 6. Only Dodge and Fredrickson's Stryker business emails were contained in the files and data potentially accessed in the Cyberattack (*id.* ¶ 5), but business emails are not PII (Mich. Compl. Laws Ann. § 445.63 ("'Personal identifying information' means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts[.]"). Without this, they are forced to allege in a conclusory fashion "exposure and theft of [their] PII." (*See, e.g.*, CAC PageID.99 ¶ 60, PageID.101 ¶ 82, PageID.103 ¶ 100). These vague and speculative allegations of access do not establish concrete harm.[3]

Moreover, Mangold similarly does not have a concrete harm because Stryker was not in possession of his employee file at the time of the Cyberattack, thus his PII was not accessed. Mangold's employment with Stryker appears to have ended in July 2007 and at that time, and for "more than a decade thereafter," Stryker "maintained personnel files as physical paper files" and Stryker's "retention period for an employee's personnel file is a period of six years after their employment ends." Puca Decl. ¶¶ 5, 6, Ex. A.

[3] Plaintiffs also assert that Stryker's "Bring Your Own Device" policy caused employees' "personal phones and laptops" to be "wiped as part of the Data Breach." CAC ¶ 29. "It is well settled that … class representatives without personal standing cannot predicate standing on injuries suffered by members of the class … which they themselves have not or will not suffer." *Rosen v. Tenn. Com'r of Fin. & Admin.*, 288 F.3d 918, 928 (6th Cir. 2002). As the CAC is entirely devoid of claims that Plaintiffs personally suffered any data loss, they do not have standing to assert such claims. *See generally* CAC PageID.98 ¶ 47– PageID.114 ¶ 196.

Finally, Dodge alleges that he suffered injury because he "was not paid for at least 34 hours because [Stryker] was not operational after the data breach." CAC PageID.101 ¶ 75. This is untrue. "Stryker notified employees," including Dodge, approximately two months before the CAC was filed "that they would be made whole for their hours through facility closure pay." Puca Decl. ¶ 7, Exs. B, C. Dodge's pay records confirm "he was paid for at least his full 40 hours at his regularly hourly rate during the week of the Cyberattack … and the two weeks after." *Id.* ¶ 8. Thus, Thus, Dodge did not experience lost wages.[4]

2. *Plaintiffs Cannot Show That Any Injury is Fairly Traceable to Stryker.*

Even if Plaintiffs' PII had been accessed in the Cyberattack (and Stryker does not have any evidence that it was), Plaintiffs must show—and they cannot—that their injury "is fairly traceable to the challenged conduct of the defendant." *Miedel*, 2025 WL 2751533, at *3. Plaintiffs cannot show traceability here because: (1) they cannot show that their PII was accessed in the Cyberattack; (2) their PII was exposed in data breaches predating the Cyberattack; and (3) certain of their alleged injuries are self-inflicted.

[4] Even if Dodge had a claim for lost wages (he does not), it is subject to arbitration, as the Arbitration Agreement he executed on January 16, 2024 provides that all claims he may have against Stryker "related to wages … compensation … [and/or] hours worked" "will be brought, heard, and adjudicated exclusively through final and binding arbitration." Puca Decl. ¶¶ 7-8, Exs. D at § 3 & E.

a. *Stryker Does Not Have Any Evidence That Plaintiffs' PII Was Accessed in the Cyberattack.*

"[C]onclusory, broad, and speculative allegations that [a plaintiff's] injury is fairly traceable to the data breach" do not suffice to establish traceability. *Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-cv-4036, 2022 WL 11745549, at *3 (D. Kan. Oct. 20, 2022). For example, a plaintiff's injury is not fairly traceable when "[t]he Complaint provides no information linking the" injuries to the "data breach." *Williams v. Bienville Orthopaedic Specialists*, LLC, 737 F. Supp. 3d 411, 424 (S.D. Miss. 2024) (granting motion to dismiss). There, the plaintiff did not have standing despite his allegation that he received a "dark web" alert after the breach because "[t]he mere fact that [plaintiffs] experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII [wa]s fairly traceable to the [defendant's] data breach." *Id.* at 425.

Similarly, in *Shepherd* the Court found traceability lacking after a factual challenge to standing "[b]ecause Plaintiff's information was not accessed by the data breachers," and thus "Plaintiff's receipt of spam and phishing communication is not a harm that is a consequence of [the defendant's] actions." 2023 WL 4056342, at *6. In *Muniz*, likewise, the Court found no traceability after a factual challenge to standing where the plaintiff "relie[d] on a speculative chain of events that belie[d] that the data accessed in the Privacy Incident *alone* [wa]s sufficient to" establish injury. 2026 WL 1649197, at *5. Plaintiff's "claimed harms arising from the

current necessity to monitor her financial and personal records are self-inflicted," based entirely on speculation. *Id.*

So too here. As in *Shepherd* and *Muniz*, because Plaintiffs have only speculated that their PII was accessed and misused, they cannot demonstrate that any injury is fairly traceable to Stryker. *See, e.g.*, CAC PageID.99 ¶ 60, PageID.101 ¶ 82, PageID.103 ¶ 100 (alleging "exposure and theft of [their] PII"). Even if their allegations were not speculative, they still would fail as Stryker's investigation did not reveal any evidence that Plaintiffs' PII was accessed in the Cyberattack. Calderon Decl. ¶ 5. Thus, Plaintiffs' purported injuries are not traceable to the Cyberattack.

b. *Plaintiffs' PII Was Exposed in Prior Data Breaches.*

Because each Plaintiff's PII was exposed in earlier unrelated data breaches, none of their alleged injuries are traceable to Stryker. "It is a bedrock principle that a federal court cannot redress 'injury that results from the independent action of some third party not before the court.'" *Murthy v. Missouri*, 603 U.S. 43, 57 (2024) (citation omitted). "In today's society, an individual's PII and PHI can be stolen in myriad ways …. Data breaches and other forms of data theft are so prevalent that it is seemingly impossible to trace the misuse of personal information to one particular breach." *Williams*, 737 F. Supp. 3d at 425. Indeed, Plaintiffs concede that "[t]he exposure of one's PII to cybercriminals is a bell that cannot be unrung[,]" as after a data breach a person's "private information is forever exposed and unsecure" and acknowledge that "[i]n 2024, a record 3,158 data breaches occurred—

exposing approximately 1,350,835,988 sensitive records." CAC PageID.88 ¶ 7, PageID.121-122 ¶ 222.

Even if Plaintiffs had pleaded traceability (they did not), Plaintiffs' numerous prior data breaches are more likely to be the impetus for their purported injuries than Stryker, which does not have any evidence Plaintiffs' PII was accessed in the Cyberattack. *See* Hardin Decl. ¶¶ 16-23, 26, 28, 31, 35, 38, 40, 42; Calderon Decl. ¶ 5. Each Plaintiff's purported injuries involve third-parties not before this Court as outlined below:

- ***Mesmer***: Mesmer's information was impacted by "4 previously reported data breaches," including potential exposure of his name, Social Security number, date of birth, physical address, phone number, email address, password information, and usernames. Hardin Decl. ¶ 35.
- ***Dodge***: Dodge's information was impacted by "six previously reported data breaches," including potential exposure of his name, date of birth, email address, and usernames. *Id.* ¶ 26.
- ***Fredrickson***: Fredrickson's information was impacted by "7 previously reported data breaches," including potential exposure of his name, date of birth, physical address, phone number, email address, and password information. *Id.* ¶ 40.
- ***Mangold***: At the time of the Cyberattack, Stryker had not retained files for Mangold for nearly 13 years. Puca Decl. ¶ 6. Additionally, Mangold's information was impacted by "18 previously reported data breaches," including potential exposure of his name, Social Security number, date of birth, physical address, phone number, email address, password information, user identification numbers, and usernames. Hardin Decl. ¶ 31.
- ***Primer***: Primer's information was impacted by "eight previously reported data breaches," including potential exposure of his name, physical address, phone number, and email address. *Id.* ¶ 28.
- ***Tanner***: Tanner has claimed that the exact same PII he speculatively claims was accessed here was accessed in another incident involving another former employer, Medtronic. *See* Gulliver Decl. Ex. A; Hardin Decl. ¶¶ 36-37. Additionally, Tanner's information was impacted by "20 previously reported

data breaches," including potential exposure of his physical address, phone number, email address, password information, and user identification numbers. Hardin Decl. ¶ 42.

- ***Thompson***: Thompson has experienced three incidents of identity theft prior to the Cyberattack, including misuse of her financial information and "social security information." *See* Section II.D; Hardin Decl. ¶ 21, Exs. C, D, E. Thompson's PII also was exposed in "20 previously reported data breaches," including potential exposure of her name, Social Security number, date of birth, physical address, phone number, email address, password information, user IDs, and usernames. Hardin Decl. ¶ 20.

- ***Trepanier***: Trepanier's information was impacted by "18 previously reported data breaches," including potential exposure of her name, Social Security number, date of birth, physical address, phone number, email address, and password information. *Id.* ¶ 38.

Since Plaintiffs' PII was previously exposed and they cannot demonstrate their PII was accessed in the Cyberattack, their allegations that they suffered injury in the form of "time and effort monitoring [their] accounts" and "time and money to try to mitigate [their] injuries" (*See, e.g.*, CAC PageID.99 ¶¶ 57 & 63, PageID.101-102 ¶¶ 78 & 85, PageID.103-104 ¶¶ 97 & 103), "fear for [their] personal financial security" and "worr[y] about what information was exposed" (*see e.g.*, *id.* PageID.99 ¶¶ 58 & 59, PageID.101 ¶¶ 80 & 81), "exposure and theft of [their] PII" (*see, e.g.*, *id.* PageID.99 ¶ 60, PageID.101 ¶82, PageID.103 ¶100), "diminution in the value of [their] PII" (*see, e.g.*, *id.* PageID.99 ¶ 61, PageID.102 ¶ 83, PageID.104 ¶ 101), "increased risk of fraud, misuse, and identity theft" (*see, e.g.*, *id.* PageID.99 ¶ 62, PageID.102 ¶ 84, PageID.104 ¶102), and that their PII "has already been published—or will be published imminently" on the dark web (*see, e.g.*, *id.* PageID.97 ¶ 46) all are not fairly traceable to Stryker.

Thompson, Trepanier, Dodge, Mesmer, Primer, and Mangold's allegations that their PII was purportedly misused after the Cyberattack fail for the same reasons, as well as because:

- While Dodge, Thompson, and Trepanier each allege increased spam communications following the Cyberattack (CAC PageID.101 ¶ 79, PageID.111 ¶ 172, PageID.113 ¶189), they do not allege that phone numbers or email addresses were among the PII purportedly compromised (*see* CAC PageID.92 ¶ 28). Additionally, their email addresses and/or phone numbers were exposed in prior cyber incidents. *Compare* CAC PageID.101 ¶ 79, PageID.111 ¶ 172, PageID.113 ¶ 189, *with* Hardin Decl. ¶¶ 19, 25, 37.

- Mesmer alleges that he "received a LinkedIn invitation and message from a fraudulent actor posing as a Stryker employee" (CAC PageID.99 ¶ 56), but does not explain how that was connected to the Cyberattack or any purported exposure of his PII, and in Stryker's expert's opinion, it was not (*see* Hardin Decl. ¶¶ 32-33).

- Dodge alleges he "was not paid for at least 34 hours" of work due to the Cyberattack. CAC PageID.101 ¶ 75. Setting aside the fact that that allegation is wrong (*see* Section II.C), Dodge also does not explain how that alleged injury is traceable to his alleged exposure of PII.

- Primer alleges that he experienced unspecified "fraudulent activity associated with his Apple Account shortly after" the Cyberattack (CAC PageID.107 ¶ 133), but he does not allege that his Apple account information was among the PII purportedly accessed (*see id.* PageID.92 ¶ 28). Regardless, "Apple accounts can be setup with an email address or phone number" and "can be logged into with an email address or phone number and password." Hardin Decl. ¶ 27. Primer's email addresses, phone numbers, and passwords were exposed in prior cyber events. *Id.*

- Mangold alleges that "around the time of" the Cyberattack he "received a dark web alert from LifeLock alerting him that his PII, including an email and password he used during the time he worked with Stryker, was found on the dark web." CAC PageID.105 ¶ 114. However he does not allege that his email address and password were accessed in the Cyberattack. *See* CAC PageID.92 ¶ 28. Regardless, due to how LifeLock scans the dark web, receipt of an alert "does not mean that it is newly accessible data or necessarily related to" the Cyberattack. Hardin Decl. ¶ 30. Additionally, Mangold's email addresses and passwords were exposed in prior cyber events. *Id.*

- Thompson alleges that she experienced "multiple instances of account openings/attempts" after the Cyberattack. CAC PageID.111 ¶ 167. However, "[n]ormally to open an account, a person would need a name, Social Security number, email, phone number, [and] address, amongst other items" and "[a]ll of this information was identified on the dark web from previously cyber security incidents." Hardin Decl. ¶ 16. Thompson also alleges she received a notice that unspecified "login credentials had been found on the dark web" and she was "locked out of her bank account twice after an unknown actor repeatedly changed her password" (CAC PageID.111 ¶¶ 170), but (1) she does not allege that "login credentials" were among the PII purportedly accessed (*see id.* PageID.92 ¶ 28), and (2) in any event, Stryker's expert "identified numerous usernames and passwords" for Thompson on the dark web "associated with previous cyber security incidents." Hardin Decl. ¶¶ 17, 18.

c. *Plaintiffs Cannot Manufacture Standing Due to Speculative Fear of Future Injury.*

Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Muniz*, 2026 WL 1649197, at *4 (citation omitted); *accord Buchholz v. Meyer Njus Tanick, PA*, 946 F.3d 855, 865-66 (6th Cir. 2020) ("[A] plaintiff cannot create an injury by taking precautionary measures against a speculative fear."). Moreover, "[a] self-inflicted injury, by definition, is not traceable to anyone but the plaintiff." *Buchholz*, 946 F.3d at 866.

In *Muniz*, the plaintiff speculated that her information had been accessed and thus "her … necessity to monitor her financial and personal records [we]re self-inflicted injuries that fail[ed] to demonstrate traceability to [the defendant]." 2026 WL 1649197, at *5. In *Shepherd*, the Court held that the plaintiff's "choice to spend time and money mitigating her risk of identity theft was a harm caused by Plaintiff herself" and thus not traceable to the defendant. 2023 WL 4056342, at *6.

For the same reason, Plaintiffs' time or money spent monitoring or attempting to prevent some future injury and fear of same (*See, e.g.*, CAC PageID.99 ¶ 57 & 63, PageID.101-102 ¶¶78 & 85, PageID.103-104 ¶¶ 97 & 103) are self-inflicted and not traceable to Stryker.

Thus, Plaintiffs lack standing.

B. Plaintiffs Fail to State a Claim Under Michigan Law.

While Plaintiffs assert seven claims, none state a claim. As a preliminary matter, Michigan law applies to Plaintiffs' claims. The Sixth Circuit has held that "[w]e generally apply the substantive law of the forum state to actions brought pursuant to our diversity jurisdiction." *Savedoff v. Access Grp.*, 524 F.3d 754, 762 (6th Cir. 2008). "In a tort action, Michigan courts recognize a presumption in favor of the application of Michigan law unless a rational reason to do otherwise exists." *Smartrend Mfg. Grp. (SMG) v. Opti-Luxx, Inc.*, Nos. 1:21-cv-1009, 1:22-cv-915, 2023 WL 6304912, at *32 (W.D. Mich. Sep. 28, 2023) (Jarbou C.J.) (citation modified & omitted) (reversed in part on other grounds); *see also Sutherland v. Kennington Truck Serv., Ltd.*, 454 Mich. 274, 286 (1997). Thus, courts routinely apply Michigan law when cyber incidents involve Michigan companies. *Polkowski,* 2025 WL 3079358, at *1, *8 (applying Michigan law; defendant "is a Michigan corporation"); *In re Grede Holdings LLC Data Breach Litig.*, No. 25-cv-10831, 2026 WL 396292, at *1, *2 (E.D. Mich. Feb. 12, 2026) (applying Michigan law; defendant is "located in Southfield, Michigan"). So too here. Stryker is incorporated and has its principal place of business in Michigan. CAC PageID.89 ¶ 16.

1. *Plaintiffs Have Not Alleged a Present Injury.*

Plaintiffs' alleged injuries do not state a claim for their tort causes of action (negligence, intrusion upon seclusion, and breach of confidence) and their breach of implied contract claim. "To establish a tort claim under Michigan law, the plaintiff must demonstrate a present injury[.]" *Rakyta v. Munson Healthcare*, No. 354831, 2021 WL 4808339, at *6 (Mich. Ct. App. Oct. 14, 2021) (citing *Henry v. Dow Chem. Co.*, 473 Mich. 63, 78-79 (2005)). Likewise, a claim for "breach of implied contract … require[s] damages based on a present injury." *Polkowski.*, 2025 WL 3079358, at *8. Plaintiffs here allege a number of injuries, the majority of which fail to state a claim.

a. *Publication of PII to the Dark Web Is Not Cognizable.*

Plaintiffs' allegation that their PII was posted to the dark web fails. To allege a cognizable injury, Plaintiffs must "allege a present injury to 'credit or identity.'" *Id.* at *8 (citation omitted). This may include "financial costs" or "loss of time … due to *actual* identity theft." *Grede*, 2026 WL 396292, at *2 (emphasis added). Thus, "Michigan does not recognize … 'the publication' of [PII] alone as [a] form[] of compensable injury." *Id.* (citation omitted). "[T]he fact that PII is posted to the dark web, while unsettling, cannot be remedied under Michigan law[.]" *Polkowski*, 2025 WL 3079358, at *8.

In *Polkowski*, "the Complaint allege[d] Plaintiff's PII has been published on … the dark web," but the plaintiffs had "not allege[d] a present injury to 'credit or identity.'" 2025 WL 3079358, at *8 (citation omitted). Thus, the Court dismissed the plaintiffs' negligence and breach of implied contract claims.

The same result is compelled here. Plaintiffs' allegations that their PII "has … been published [] or will be published" on the dark web (*See, e.g.*, CAC PageID.101 ¶ 76, PageID.103 ¶ 95), that Mangold "received a dark web alert" (*id.* PageID.105 ¶ 114), and that Thompson "receiv[ed] multiple alerts" *(id.* PageID.111 ¶ 170) are not compensable injuries.

b. *Purported Unauthorized Account Activity Is Not a Present Injury to Credit or Identity.*

Certain Plaintiffs allege that they experienced unauthorized account activity, but such activities do not rise to a credit or identity injury. Indeed, such a "loss of privacy" is not a "form[] of compensable injury" "under Michigan law." *See Grede*, 2026 WL 396292, at *2. In *Grede*, a plaintiff's allegation that "'a fraudulent charge was made to [his] bank account' … nearly a month after the alleged data breach" was insufficient because it did not "raise[] a plausible inference that [the plaintiff was a] victim[] of 'actual identity theft or fraud.'" *Id.* at *3.

The same is true of Plaintiffs' allegations here, which do not amount to identity theft or credit fraud and are not cognizable: Primer's allegations that he "experienced fraudulent activity associated with his Apple account" (CAC PageID.107 ¶ 133) and Thompson's allegations that she "had multiple instances of account openings/attempts," "received a denial notice for a credit application she did not submit," "an unauthorized account was opened in her name," and "she was

locked out of her bank account twice after an unknown actor repeatedly changed her password" fail. CAC PageID.111 ¶¶ 167-170.[5]

c. *Risk of Future Injury or Mitigation Is Not Cognizable.*

Plaintiffs' purported injuries of time and effort monitoring and future mitigation efforts fail as a matter of law because they are not a present injury. "[I]njuries associated with the 'risk' or 'imminent threat' of future harm … are not cognizable under Michigan law because they 'are wholly derivative of a possible, future injury rather than an actual present injury.'" *Grede*, 2026 WL 396292, at *2 (citation omitted). "[B]are allegations of damages arising from the expenditure of resources to mitigate or prevent a future harm to not establish a present injury." *Rakyta*, 2021 WL 4808339, at *4 (affirming dismissal where the "allegations involved possible future injuries and the prophylactic measures that [plaintiff] and the potential class members might reasonably take to prevent or mitigate the potential future injuries."); *Henry*, 473 Mich. at 68 (ordering dismissal "[b]ecause plaintiffs do not allege a present injury").

The Eastern District of Michigan recently dismissed a tort claim over a cyber incident, rejecting the plaintiffs' allegations of "risk" of future harm. *Grede*, 2026 WL 396292, at *3. Specifically, the plaintiffs alleged injuries including: "loss of time" and "financial costs incurred mitigating the materialized risk and imminent threat of identity theft;" and "the continued risk to their sensitive Private

[5] Stryker does not challenge Thompson's allegation that her "credit score dropped by 46 points" CAC PageID.111 ¶¶ 169-70 as a plausibly pled credit injury. However, these allegations cannot survive Stryker's factual challenge to standing (*see* Section IV.A), nor do they plausibly allege causation under Rule 12(b)(6) (*see* Section IV.B.2).

Information." *Id.* at *2. The Court held that such injuries "are wholly derivative of a *possible, future* injury rather than an *actual, present* injury." *Id.* (citation omitted).

The same is true here. Plaintiffs allege the same deficient "risk" and anticipated injuries that the *Grede* Court rejected. Plaintiffs allege they "*will continue* to spend … significant time and effort monitoring [their] accounts" (*see, e.g.*, CAC PageID.99 ¶ 57, PageID.101 ¶ 78, PageID.103 ¶ 97) (emphasis added); "*anticipate*[] spending … time and money to try to mitigate [their] injuries" (*see, e.g., id.* PageID.99 ¶ 63, PageID.102 ¶85, PageID.104 ¶ 103) (emphasis added), and face "substantially increased *risk* of fraud, misuse, and identity theft" (*see, e.g.*, *id.* PageID.99 ¶ 62, PageID.102 ¶ 84, PageID.104 ¶ 102) (emphasis added). Such speculative injuries and allegations amount, at most, to a "'risk' or 'imminent threat' of future harm" and a "*possible, future* injury rather than an *actual, present* injury." *Grede*, 2026 WL 396292, at *2 (citations omitted).

d. *Fear and Anxiety Are Insufficient to Allege Injury.*

Under Michigan law "fear of future … injury" is "not enough to state a claim." *Henry*, 473 Mich. at 79; *Grede*, 2026 WL 396292, at *2 ("emotional distress including anxiety and stress in dealing with the Data Breach" was insufficient).

In *Rakyta*, the Court affirmed that the plaintiff's allegations that she "suffered damages in the form of anxiety, embarrassment, and emotional distress as a result of defendant's failure to protect their confidential information" were insufficient. 2021 WL 4808339, at *5. The Court explained that the Michigan Supreme Court has "rejected … allegations of damages arising from emotional

distress or anxiety about a potential future injury." *Id.* "Michigan law only recognize[s] emotional distress as the basis for a negligence claim when the emotional distress involved present physical manifestations of the distress." *Id.* Relying on *Rakyta*, both *Grede* and *In re A-Line Staffing Solutions Data Security Incident Litigation* reject purported injuries of fear and anxiety as sufficient to state a claim. 2026 WL 396292, at *2; 2026 WL 1480273, at *10 (E.D. Mich. May 27, 2026), *appeal docketed*, No. 26-1522 (6th Cir. June 12, 2026).

The same result is compelled here. Plaintiffs' allegations that they "fear[] for [their] personal financial security," "worr[y] about what information was" accessed, and experienced "anxiety" and "stress" do not allege a present injury cognizable under Michigan law. *See, e.g.*, CAC PageID.99 ¶ 58-59, PageID.101 ¶ 80-81, PageID.103 ¶ 98-99, PageID.105 ¶ 116-117, PageID.107 ¶ 135-36, PageID.113 ¶ 190-91.

e. *Diminution in Value of Plaintiffs' PII Is Insufficient.*

Plaintiffs' alleged diminution in the value of their PII fails. "[T]he unauthorized viewing of confidential information does not by itself reduce the value of the information" and a plaintiff must "allege that anyone actually used [their] confidential information in a way that devalued it." *Rakyta*, 2021 WL 4808339, at *5. "[M]erely assert[ing] that the exposure of the information caused a loss of value without explaining how it did so" is a "[c]onclusory allegation[] [that] will not suffice to state a cause of action." *Id.*

In *Rakyta*, the plaintiff alleged "that her confidential information lost value as a result of the exposure to third parties." *Id.* The Court disagreed, explaining

that "the unauthorized viewing of confidential information" was insufficient, requiring instead that "the information [is used] in some harmful way that devalues" it. *Id.* As the plaintiff "merely asserted that the exposure of the information caused a loss of value without explaining how it did so," it failed to state a claim. *Id.*

Here, Plaintiffs' CAC offers no more than a singular paragraph that somehow there was a "diminution in the value of [their] PII" without explaining how it lost value. *See, e.g.*, CAC PageID.99 ¶ 61, PageID.102 ¶ 83, PageID.104 ¶ 101. This conclusory allegation is insufficient. Regardless, absent Thompson's credit drop, Plaintiffs do not allege misuse of their PII to support a present injury. In sum, diminution of PII is insufficient to state a claim.

f. *Violation of Right to Privacy Does Not Allege Injury.*

Plaintiffs allege that they were injured when their "right[] to privacy" was violated (*see, e.g.*, CAC PageID.99 ¶ 60, PageID.101 ¶ 82, PageID.103 ¶ 100, PageID.105 ¶ 118), but "Michigan does not recognize plaintiffs' current 'loss of privacy' … alone as [a] form[] of compensable injury." *Grede*, 2026 WL 396292, at *2 (dismissing claim). "Michigan courts reject" an injury premised on "invasion of privacy" where "the plaintiff does not allege a present injury to 'credit or identity.'" *Polkowski* 2025 WL 3079358, at *8 (citations omitted) (dismissing claim). As Plaintiffs have not alleged a present injury to credit or identity, their alleged violation of the "right to privacy" is insufficient. *See* Section IV.B.1.b.

g. *Spam Communications Are Insufficient to Allege Injury.*

Plaintiffs' allegations that they experienced an increase in spam communications after the Cyberattack also do not establish a compensable injury. Courts have held that a plaintiff must allege "actual identity theft or fraud," not merely spam or fraudulent communications.

In *Grede*, the Court found the plaintiff's allegation that he "experienced a sharp uptick in suspicious spam calls and texts using his [PII]" was insufficient to allege an injury because it did not "raise[] a plausible inference that [the plaintiff was a] victim[] of 'actual identity theft or fraud.'" 2026 WL 396292, at *3.

Here, Plaintiffs' allegations that they "suffered from a spike in spam and scam text messages and phone calls" (CAC PageID.101 ¶ 79, PageID.111 ¶ 172, PageID.113 ¶ 189) and that Plaintiff Mesmer "received a LinkedIn invitation and message" (*id.* at PageID.99 ¶ 56) fail because these allegations do not establish "actual identity theft or fraud." *Grede*, 2026 WL 396292, at *3.

In summary, Plaintiffs have not plausibly alleged an injury.

2. *Plaintiffs Have Not Sufficiently Alleged Causation.*

Plaintiffs' negligence claims[6] and their implied contract claim also fail because they have not plausibly alleged the Cyberattack caused their injuries. For negligence claims, "a plaintiff must establish both factual []and legal causation." *A-Line,* 2026 WL 1480273, at *12 (citation omitted) (dismissing claim). Similarly,

[6] "[N]egligence per se is not an independent cause of action" under Michigan law, and thus Plaintiffs' negligence per se claim fails for the same reasons as the negligence claim. *Polkowski*, 2025 WL 3079358, at *9 (citation omitted); *see also Grede*, 2026 WL 396292, at *3-4.

"[c]ausation is an essential element in all breach-of-contract claims." *JRR Props. Westland, LLC v. Westland Mall Realty, LLC*, No. 364334, 2023 WL 6931924, at *3 (Mich. App. 2023); *see also Grede*, 2026 WL 396292, at *4 ("Under Michigan law, the breach of an implied contract comprises the same elements as the breach of an express contract"). The "plaintiff must establish a causal link between the asserted breach of contract and the claimed damages." *JRR Props.*, 2023 WL 6931924, at *3 (citation omitted).

"Factual causation requires a 'showing that "*but for*" the defendant's actions, the plaintiff's injury would not have occurred.'" *Grede*, 2026 WL 396292, at *3 (emphasis added) (citation omitted). "Proximate causation 'involves examining the foreseeability of consequences, and whether a defendant should be held legally responsible[.]'" *Id.* (citation omitted). Allegations of "mere temporal proximity and correlation … do not suffice to plausibly establish the element of causation for negligence claims." *A-Line,* 2026 WL 1480273, at *12.

Grede is on point. There, the plaintiffs alleged that they experienced a "fraudulent bank charge" and "unsolicited spam communications" after the data breach. 2026 WL 396292, at *3. The Court held that "Plaintiffs cannot satisfy the factual causation prong" because the "complaint omits any plausible allegations that 'but for' the data breach those injuries 'would not have occurred.'" *Id.* (citation omitted). A mere "alleged temporal proximity between the data breach" and these events is "insufficient to plausibly establish a causal link." *Id.* In so holding, the Court rejected the complaint's allegations that causation was plausible because they

were "targeted by a ransomware group" that sought to misuse PII and plaintiff's allegation that he had never experienced another data breach. *See A-Line*, 2026 WL 1480273, at *11-12 (discussing how *Grede* rejected causation allegations).

The same result occurred in *A-Line*. There, plaintiffs alleged that they had been targeted by a ransomware group and that a plaintiff "allegedly took steps to protect his PII prior to the data breach." 2026 WL 1480273 at *12. The Court held that the allegations were "analogous" to *Grede* and because the complaint "essentially relies on mere temporal proximity and correlation," it did not "plausibly establish the element of causation for negligence claims." *Id*.

The same result is warranted here because the CAC alleges even less than *Grede* or *A-Line*. Plaintiffs' causation allegations are entirely conclusory. *See, e.g.*, CAC PageID.131 ¶ 264 ("As a direct and traceable result of Defendant's negligence … Plaintiffs and Class Members have suffered[.]"); PageID.135 ¶ 291 ("Defendant's material breaches were the direct and proximate cause of Plaintiffs' … injuries[.]"). Instead, Plaintiffs seek to rely on allegations of alleged misuse that occurred "shortly after," "around the time of" or in the "aftermath" of the Cyberattack, which are insufficient to plausibly allege causation. *See, e.g.*, CAC PageID.99 ¶ 56, PageID.101 ¶ 79, PageID.111 ¶¶ 167 &172, PageID.113 ¶ 189, PageID.107 ¶ 133.[7] Moreover, Dodge's allegation that he lost wages after the Cyberattack (*id.* PageID.101 ¶ 75) likewise fails because he cannot plausibly allege

[7] Plaintiffs also state without any factual support that Stryker "has admitted that the PII of Plaintiffs" was "wrongfully lost and disclosed" due to the Cyberattack (CAC PageID.131 ¶ 263), but they provide no support for their bald assertion.

that "but for" the purported access of *his* PII, he would not have lost time from work. *See Grede*, 2026 WL 396292, at *3. The Cyberattack's disruption to business operations is entirely independent of whether Dodge's PII was accessed, and thus his lost-time theory does not satisfy causation.

In addition, many of Plaintiffs' alleged injuries are not plausibly alleged to be caused by the Cyberattack because Plaintiffs do not allege that the PII required for such unauthorized activity was "compromised." First, Thompson, Trepanier, and Dodge allege that they experienced an increase in spam emails, text messages and phone calls (CAC PageID.101 ¶ 79, PageID.111 ¶ 172, PageID.113 ¶ 189), but they do not allege that their telephone numbers or email addresses were compromised (CAC PageID.92 ¶ 28). Primer similarly alleges that he experienced fraudulent activity "associated with his Apple account" (*id.* PageID.107 ¶ 133), which was not alleged to be compromised (*see id.* PageID.92 ¶ 28). Mesmer claims he was targeted when he "received a LinkedIn invitation," but the CAC does not contain any allegations tying this purported social engineering attack to the Cyberattack. *Id.* PageID.99 ¶ 56. Finally, Thompson vaguely alleges that she suffered multiple account openings and closings (*id.* PageID.111 ¶¶ 167-68) but does not allege how these instances are linked to the PII purportedly accessed. Thus, Plaintiffs' negligence claims fail as a matter of law.

3. *Plaintiffs Also Fail to State Their Negligence Claims Because They Have Not Alleged Stryker Breached Its Duty.*

Plaintiffs' negligence claims also fail because they have not plausibly alleged a breach of duty. While "'[c]ompanies have a duty to take reasonable precautions' to

protect [] PII 'due to the reasonably foreseeable risk of danger of a data breach incident,'" to state a negligence claim, Plaintiff must establish "the defendant breached the legal duty." *Polkowski*, 2025 WL 3079358, at *9 (citations omitted). Plaintiffs have not done so here.

Plaintiffs asserting negligence must allege *facts* demonstrating how the defendant allegedly breached its duty to safeguard their information. *See id.* "[M]ere recitation of industry standards and conclusory statements [as to a breach of duty] are insufficient." *Id.* "And although complaints grounding claims on 'information and belief' can survive a motion to dismiss, they 'must set forth a factual basis for such belief[.]" *Smith v. Gen. Motors LLC*, 988 F.3d 873, 885 (6th Cir. 2021) (affirming dismissal of claim based on information and belief allegations); *see also Sunrise Foods Int'l, Inc. v. Agridient, Inc.*, No. 24-cv-10212, 2025 WL 1643741, at *10 (E.D. Mich. Jan. 24, 2025) ("[T]o open the doors of discovery, allegations 'on information and belief' must still be supported by enough facts to support the inference[.]" (citation omitted)). Moreover, courts have "never held that delayed notice [of data access] alone supports a negligence claim." *Polkowski*, 2025 WL 3079358, at *9.

In *Polkowski*, the Court dismissed the negligence claim because the plaintiff "offered a conclusory assertion that Defendant failed to 'sufficiently encrypt' their PII, without further specifying how or why [the defendant's] encryption fell short of industry standards. Even full compliance with industry standards does not necessarily guarantee complete security against cyberattacks; so without more, the

Court cannot plausibly conclude that Defendant breached its duty to the Plaintiff." *Id.* The Court rejected the plaintiff's "'delayed notice' theory" as well "because he has not alleged that the delay itself caused a present, compensable injury." *Id.*

Here, Plaintiffs have pleaded far less than was held insufficient in *Polkowski*. Plaintiffs allege only that "[u]pon information and belief" Stryker's security measures did not comport with "industry standards." CAC PageID.125 ¶ 234. Merely, alleging that Stryker did not follow industry standards without specifying *how* Stryker purportedly failed those standards is insufficient. *Id.* Regardless, as the allegation was on information and belief, Plaintiffs were required to allege the factual basis for this belief, which they did not do. Though Plaintiffs allege that Stryker "fail[ed] to provide reasonably timely notice of the [Cyberattack]" (*id.* PageId.130 ¶ 262), such delayed notice allegations alone fail. 2025 WL 3079358, at *9. Plaintiffs' allegations do not plausibly allege a breach of duty.

4. *Plaintiffs' Breach of Implied Contract Claim Also Fails for Lack of Consideration.*

Plaintiffs' breach of implied contract claim also fails because they do not adequately allege separate consideration for the protection of their PII. A "contract will be implied only if there is no express contract covering the same subject matter." *Belle Isle Grill Corp. v. City of Detroit*, 256 Mich. App. 463, 478 (2003). Thus, "[a]n implied contract must still 'satisfy the elements of mutual assent and consideration.'" *Polkowski,* 2025 WL 3079358, at *10 (citation omitted).

"A contract for employment is typically formed when the employee accepts the employer's promised terms of employment through performance." *AFT Mich. v.*

State, 497 Mich. 197, 236 (2015). Where, as here, employees bring claims against their employers over purported breaches of their PII, courts routinely find that implied contract claims fail for lack of "independent consideration" beyond the consideration provided through the express employment agreement. *See*, *e.g.*, *Polkowski*, 2025 WL 3079358, at *10 (dismissing implied contract claim); *Grede*, 2026 WL 396292, at *4 (same); *A-Line,* 2026 WL 1480273, at *13 (same).

In *Polkowski*, the plaintiffs alleged that their employer breached the implied contract to "safeguard their PII" because (1) they were required to provide their PII to Defendant as a condition of receiving employment; (2) they "provided their PII … in exchange for employment" and "reasonabl[y] underst[ood] that Defendant would use a portion of the funds from their employment to pay for adequate cybersecurity." 2025 WL 3079358, at *1, *4. The Court concluded that "employees do not provide Defendant with their PII in exchange for employment; they perform their employment duties in exchange for employment (and compensation) pursuant to a valid employment agreement." *Id.* Thus, "[a]ny purported implied contract would be duplicative of the parties' express employment relationship and unsupported by independent consideration. Plaintiff's provision of PII was merely incidental to their employment and cannot serve as consideration for a separate agreement to safeguard that data." *Id.* at *10.

Grede is in accord. There, former employees sued alleging that they "provided their personal identifying information to Grede 'as a condition of and in exchange for … employment.'" *Grede*, 2026 WL 396292 at *1. The Court dismissed

the claim because "plaintiffs cannot point to an independent source of consideration for this promise beyond their 'express employment relationship.'" *Id.* at *4 (citation omitted). *Grede* agreed that "Plaintiffs' 'provision of [PII] was merely incidental to their employment'" such that it "cannot serve as consideration for a separate agreement to safeguard that data." *Id.* (citation omitted)

So too here. Plaintiffs' allegations are almost identical to *Polkowski*'s deficient allegations. Plaintiffs allege they (1) "were required to provide their PII to Defendant as a condition of receiving employment;" (2) they "reasonably understood that a portion of the funds they derived from their labor would be used to pay for adequate cybersecurity measures" and (3) "accepted Defendant's offers by disclosing their PII." *Compare* CAC at PageID.133 ¶¶ 278-81, *with Polkowski*, 2025 WL 3079358, at *1, *4. Thus, "Plaintiffs' 'provision of [PII] was merely incidental to their employment'" (*Grede*, 2026 WL 396292, at *4 (citation omitted)), and they fail to allege any separate consideration for their alleged implied contract for the protection of their PII, dooming that claim.

5. *The Unjust Enrichment Claim Also Lacks Separate Consideration.*

For the same reason that Plaintiffs cannot plead a breach of implied contract claim, their unjust enrichment claim (pled in the alternative) fails—Plaintiffs cannot allege their PII was provided as a benefit separate from "the parties' employment relationship." *Grede*, 2026 WL 396292, at *4 (citation omitted). "A Michigan unjust enrichment claim requires the plaintiff to plausibly demonstrate: '(1) the receipt of a benefit by defendant from plaintiff, and (2) an inequity resulting

to plaintiff because of the retention of the benefit by defendant.'" *A-Line*, 2026 WL 1480273, at *13 (citation omitted). "In the employment setting, the benefit received must be independent from the consideration underlying an existing employer-employee relationship. The benefit received cannot be 'incidental to the parties' employment relationship.'" *Id.* (citation omitted). In *A-Line*, the plaintiffs "allege[d] that they were required to provide their PII as a condition of contracting." *Id.* As such, the benefit was "incidental" to the employment relationship. *Id.* at *14 (citation omitted).

Similarly, in *Polkowski*, the Court dismissed the unjust enrichment claim, finding that "[a]ny benefit [the defendant] received from maintaining or using Plaintiff's PII was merely incidental to the parties' employment relationship … Rather, the alleged benefit, cost savings from underinvesting in cybersecurity, is derivative of Defendant's internal business decisions, not a transfer of value from Plaintiff himself. 2025 WL 3079358, at *11.

The same result follows here. Plaintiffs allege that "[a]s a condition of [their] employment … Plaintiff[s] provided [Stryker] with [their] PII." *See, e.g.*, CAC PageID.98 ¶ 51, PageID.100 ¶ 69. They further allege that they "conferred a benefit upon [Stryker]" because Stryker "benefitted from (1) using their PII to facilitate employment, and (2) using their labor to derive profit" (CAC PageID.137 ¶ 312). The unjust enrichment claim thus must be dismissed.

6. *The Intrusion Upon Seclusion Claim Also Fails for Additional Reasons.*

Plaintiffs' intrusion upon seclusion claim also fails because: (1) Stryker did not obtain Plaintiffs' PII through an objectionable method; and (2) Stryker did not intentionally publicize Plaintiffs' PII. "The three elements establishing Invasion of Privacy by intrusion upon seclusion are: '(1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man.'" *Polkowski*, 2025 WL 3079358, at *11 (citation omitted).[8] "An action for intrusion focuses on the manner in which information is obtained, not its publication." *Doe v. Peterson*, 784 F. Supp. 2d 831, 842 (E.D. Mich. 2011).

a. *Stryker Did Not Obtain Plaintiffs' PII Through an Objectionable Method.*

Because Plaintiffs admit that they provided their PII to Stryker "as a condition of [their] employment" their intrusion upon seclusion claim fails. *See, e.g.*, CAC PageID.98 ¶ 51. A claim for intrusion upon seclusion "does not exist where 'the only aspect of the contemplated disclosure offensive to the plaintiffs is the fact of disclosure, not the method by which it was obtained.'" *Doe,* 784 F. Supp. 2d at 842 (citation modified & omitted). "Michigan courts recognize that the objectionable obtaining of the information must be done *by the defendant*[.]" *Polkowski*, 2025 WL

[8] Moreover, names and driver's license information are not sufficiently sensitive to constitute an invasion of privacy claim. "Contrary to plaintiff's arguments, the disclosure of his name and home address is not an actionable invasion of a cognizable right to privacy." *Bennett v. U.S. Dept. of Army*, 842 F.2d 330, at *1 (6th Cir. 1988).

3079358, at *11 (emphasis added). Thus, courts routinely dismiss invasion of privacy claims where, as here, the employer did not obtain the PII by objectionable methods. *See*, *e.g.*, *id.* (dismissing claim); *Doe v. Mills,* 212 Mich. App. 73, 88-89 (1995) (affirming dismissal of intrusion upon seclusion claim because plaintiffs complained about "publicizing" the private information).

In *Polkowski*, the court explained that "Plaintiff does not allege any facts showing that [the defendant] obtained its PII via an objectionable method. In fact, Plaintiff concedes that he and the proposed class *willingly provided* their PII to [the defendant] …. Thus, the Court finds Plaintiff has not stated a claim for Invasion of Privacy." 2025 WL 3079358, at *11 (emphasis added).

The same result is warranted here. Plaintiffs admit they willingly "provided Defendant with [their] PII" as a "condition of [their] employment" and thus cannot allege that Stryker obtained their PII through an objectionable method. *See* CAC PageID.98 ¶ 51; *see also id.* PageID.135 ¶ 298 ("Plaintiffs … disclosed their sensitive and confidential information to Defendant[.]").

b. *Stryker Did Not Intentionally Publicize Plaintiffs' PII.*

Plaintiffs' intrusion upon seclusion claim also fails because they fail to allege that Stryker intentionally intruded on their seclusion. Michigan courts have held that invasion of privacy is an "intentional tort." *Doe v. Henry Ford Health Sys.*, 308 Mich. App. 592, 598 (2014). For example, "to establish an invasion of privacy through the disclosure of private facts, a plaintiff must show that the disclosure of those facts was intentional." *Id.* at 599. There, the court dismissed the invasion of

privacy claim because a "negligent disclosure" of PII is insufficient to maintain an invasion of privacy claim. *Id.*

The same result should follow here. While Plaintiffs allege in an entirely conclusory manner that the Cyberattack "constitute[d] an intentional interference" (CAC PageID.136 ¶ 299), the CAC makes plain that they are alleging Stryker was negligent in its cybersecurity controls. Thus, the intrusion upon seclusion claim must be dismissed.

7. *The Breach of Confidence Claim Also Fails Because Stryker Did Not Make an Affirmative Disclosure.*

Plaintiffs' breach of confidence claim also fails because they do not—and could not—allege that Stryker affirmatively disclosed their PII to a third party. "A breach of confidence claim involves 'the unconsented, unprivileged *disclosure* to a third party of nonpublic information that the defendant has learned[.]'." *A-Line*, 2026 WL 1480273, at *14 (citation omitted).

In *A-Line*, the Court dismissed the breach of confidence claim because "[c]ritically, courts have repeatedly found the disclosure element lacking" when the dispute involves a third-party exploiting a purported security weakness. *Id.* As "a third party allegedly stole Plaintiffs' PII due to Defendant's purportedly insufficient security practices rather than any affirmative disclosure by Defendant," the claim failed to state a claim. *Id.* at 15.

The same must be said about the CAC. Plaintiffs allege that "[o]n information and belief, cybercriminals were able to breach Defendant's systems."

CAC PageID.88 ¶ 5. Plaintiffs do not allege that Stryker themselves disseminated the PII, and the claim fails as a matter of law.

8. *The Plaintiffs' Requests for Declaratory and Injunctive Relief Must Be Dismissed.*

Because Plaintiffs' underlying claims fail, so should their requests for declaratory and injunctive relief. *Grede*, 2026 WL 396292, at *5-6. "[I]njunctive and declaratory relief claims are both implausible" when Plaintiffs "cannot prevail on any of their underlying substantive claims." *Id*. That is the case here.

V. Conclusion

Stryker respectfully requests that this Court grant Stryker's Motion to Dismiss in its entirety.

Dated: June 22, 2026

Respectfully submitted,

DLA PIPER LLP (US)

/s/Colleen Carey Gulliver
Colleen Carey Gulliver
1251 Avenue of the Americas
New York, New York 10020
Tel: 212-335-4500
colleen.gulliver@us.dlapiper.com

MILLER JOHNSON PLC
D. Andrew Portinga
Amy E. Murphy
45 Ottawa Avenue SW
Suite 1100
Grand Rapids, Michigan 49503
Tel: 616-831-1700
portingaa@millerjohnson.com
murphya@millerjohnson.com

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to LCivR 7.2(b)(i), I certify that the foregoing, including the headings, footnotes, citations and quotations, but excluding the case caption, cover sheets, table of contents, table of authorities, and the signature block, contains 10,753 words, and is therefore in compliance with the word limit set in LCivR 7.3(b)(i). The word count was generated by Microsoft® Word for Microsoft 365 MSO (Version 2604 Build 16.0.19929.20172) 64-bit.

Dated: June 22, 2026

/s/ Colleen Carey Gulliver
Colleen Carey Gulliver