

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
PENNSYLVANIA

**Jerry M. Adair, et al. v. Cigna Corporate Services, LLC and The
Cigna Group**

Civil Action No. 25-2384 · No. 2:25-cv-02384 · Decided February 4, 2026

OPINION

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA JERRY M. ADAIR, et al., CIVIL ACTION Plaintiffs, v. CIGNA CORPORATE SERVICES, LLC, NO. 25-2384 and THE CIGNA GROUP, Defendants. OPINION In recent years, the proliferation of Internet tracking technologies has flooded federal courts with invasion-of-privacy cases. This is one of them.

Five individuals have filed a complaint on behalf of a class, bringing claims under federal and state laws and alleging that their insurance carrier and its subsidiary enabled the unconsented interception of insureds' medical information. Specifically, Plaintiffs allege that Defendants The Cigna Group ("Cigna") and Cigna Corporate Services ("CCS") traded insureds' privacy for commercial gain by embedding third-party tracking technologies throughout Cigna's website (www.cigna.com) and secure member portals.

Defendants have moved to dismiss the Amended Complaint in its entirety pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). For the reasons explained below, Defendants' Motion will be granted in part and denied in part. FACTUAL BACKGROUND¹ Defendant Cigna is a multibillion-dollar conglomerate, one of the nation's largest providers of health insurance and health services.

Defendant CCS is Cigna's wholly owned subsidiary that operates and maintains Cigna's digital infrastructure, including the Cigna- branded website and member portals. Cigna and CCS are subject to the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320d et seq., and its implementing regulations,² which, among other things, prohibit "any use or disclosure of protected health information for marketing" absent a specific, dated, written authorization, see 45 C.F.R. §§ 164.508(a)(3), (c)(1)-(2).

The Department of Health and Human Services has issued a bulletin which states that HIPAA-regulated entities "are not [permitted] to use tracking technologies in a manner that would result in impermissible disclosures of [protected health information] to tracking technology vendors or any other violations of the HIPAA rules." Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, U.S. Dep't of Health & Hum.

Servs. (June 26, 2024), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>. It continues: “For example, disclosures of [protected health information] to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.” Id. 1 The well-pleaded allegations in Plaintiffs’ Amended Complaint are taken as true at this stage.

Fowler v. UPMC Shadyside, 578 F.3d 203, 210-11 (3d Cir. 2009). 2 Cigna, as a provider of health plans, is a “covered entity” under HIPAA. 45 C.F.R. § 160.102(a). CCS, as an entity that “creates, receives, maintains, or transmits protected health information for a function or activity” on behalf of Cigna, is a “business associate” under HIPAA and thus also subject to its requirements and regulations.

45 C.F.R. § 160.103. Plaintiffs are five individuals who were or are insured under Cigna health, dental, or vision plans. Between May 2023 and the present, they accessed various webpages on Defendants’ website to manage their healthcare coverage, review benefit information, and obtain materials associated with medical care, including information related to prescriptions, providers, procedures, and medical conditions.

Plaintiffs allege that, in the ordinary course of obtaining these services, third-party tracking technologies embedded within the webpages—namely, tracking pixels and session replay code³—intercepted their website interactions. They describe how, upon a user loading Cigna’s unauthenticated website and subpages, the tracking technologies of eight third-party vendors⁴ captured and transmitted in real time users’ mouse movements, clicks, keystrokes (including text entered into search boxes), page-specific URLs, and other electronic communications.

Meanwhile, within Defendants’ authenticated⁵ “myCigna” medical and dental portals, additional code transmitted users’ portal interactions to “smetrics.cigna.com”—a domain that belongs to Adobe. According to Plaintiffs, the third-party vendors profited from the captured information, using insureds’ health-related information to create or bolster advertising profiles, target advertising, and sell insureds’ information to other entities.

Likewise, Defendants used the harvested data to track visits, enabling them to add new customers and avoid advertising costs. 3 A tracking pixel is “a piece of code that tracks users’ interactions with a website, including their pages visited, any buttons clicked, and the full text of any search queries entered.” Session replay code “logs and tracks everything a user does on a webpage, including mouse movements, clicks, scrolls, and taps, and can actually track every single key stroke, creating a complete reproduction of the user’s visit to the website.” 4 The vendors are Google, Meta, Pinterest, Snapchat, The Trade Desk, LiveRamp, Demandbase, and MediaMath.

5 As explained in the Amended Complaint, “authenticated” websites “require a user to log in before gaining access to the site.” Meanwhile, “unauthenticated” webpages do not. Plaintiffs

allege that the widespread collection of the insureds' information remains ongoing and occurs without notice, consent, or an opportunity to opt out. At the same time, they acknowledge that they agreed to Cigna's Terms of Use, thereby forming a "direct agreement" with Defendants.

The Terms of Use apply to "a user of any portion" of Defendants' website and set forth various user agreements, obligations, and restrictions. They also incorporate Defendants' privacy notices and other site-specific terms.

As described in the Amended Complaint, Defendants' Privacy Notice discloses that they and "third-party ad companies may use cookies, pixel tags, and other tools to collect browsing and activity information within our Services[6] (as well as on third-party websites and services), as well as IP addresses, unique ID, cookie and advertising IDs, and other online identifiers." Similarly, the Privacy Notice communicates Defendants' utilization of third-party tools that "use cookies, pixels, and other tracking technologies to collect usage data about [Defendants'] Services to... enhance performance and user experiences." Plaintiffs allege that Defendants' and the third parties' conduct have resulted in numerous injuries, including "loss of privacy, embarrassment, and greatly increased vulnerability to identity theft and fraud, as well as having their confidential information used for the benefit of Defendants and others." On behalf of themselves and a putative class,⁷ they now bring claims under the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. § 2510 et seq., and the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. 6 The Privacy Notice defines "Services" as the "Cigna Healthcare website," including cigna.com and the authenticated portal.

⁷ Plaintiffs propose a class consisting of "[e]very current and former insured of Cigna whose Website Communications were captured from May 9, 2023 through the use of Tracking Pixels and/or Session Replay Code embedded in Defendants' Website, www.cigna.com, subpages, including medical and dental portals to the date of judgment herein." C.S.A. § 5701 et seq., as well as common law claims for invasion of privacy (specifically, intrusion upon seclusion), breach of fiduciary duty, and unjust enrichment.

SCOPE OF THE PLEADINGS Before turning to the parties' arguments on the Motion, a threshold procedural question is what materials can be relied upon in deciding Defendants' Motion. They attach to it ten exhibits, arguing that each is incorporated by reference in the Amended Complaint and subject to judicial notice. Three exhibits are user-facing policies and agreements: Cigna's Terms of Use (Exhibit D); its Website Privacy Notice (Exhibit E) ("Privacy Notice"); and, its HIPAA Notice of Privacy Practices (Exhibit H) ("HIPAA Notice").

The remaining seven exhibits depict various Cigna webpages (Exhibits A, B, C, F, and J), a "consent banner" (Exhibit I), and an informational webpage about Adobe-supplied tracking technology (Exhibit G). "As a general matter, a district court ruling on a motion to dismiss may

not consider matters extraneous to the pleadings.” In *re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir.

1997) (citation omitted). However, matters incorporated by reference, as well as items subject to judicial notice, may be considered without converting the motion to dismiss into one for summary judgment. *Id.* (citation omitted); *Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006) (citing 5B Wright & Miller’s Federal Practice & Procedure § 1357 (3d ed.

2004)). Defendants argue their exhibits fall within the ambit of both exceptions, permitting the Court to consider them when ruling on their Motion. A. Incorporation by Reference Under the incorporation-by-reference doctrine, a court deciding a motion to dismiss may consider any “undisputedly authentic document,” *Pension Benefit Guar. Corp. v. White Consol.*

Indus., Inc., 998 F.2d 1192, 1196 (3d Cir. 1993), that is “integral to or explicitly relied upon in the complaint,” *Burlington Coat*, 114 F.3d at 1426 (citation omitted); see also *Pryor v. NCAA*, 288 F.3d 548, 560 (3d Cir. 2002) (“[D]ocuments whose contents are alleged in the complaint and whose authenticity no party questions, but which are not physically attached to the pleading, may be considered.” (citation omitted)).

The doctrine holds plaintiffs accountable for a document’s full text, preventing them from maintaining a claim “‘based’ on an extrinsic document” that they selectively quote and fail to attach to the complaint. *Burlington Coat*, 114 F.3d at 1426 (citation omitted); see also *Tomaszewski v. Trevena, Inc.*, 482 F. Supp.3d 317, 328 (E.D. Pa. 2020) (“The purpose of the integral documents exception is to avoid the situation where a plaintiff ‘selected only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims.’” (quoting *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir.

2018), cert. denied sub nom. *Hagan v. Khoja*, 587 U.S. 1014 (2019))). *Burlington Coat* illustrates the doctrine’s utility and proper use. There, plaintiffs brought claims under the Securities Exchange Act of 1934, alleging that a publicly traded coat retailer omitted material information about supplier discounts in its annual report. *Burlington Coat*, 114 F.3d at 1414-15, 1425-26.

At the motion to dismiss stage, the district court had relied upon the report to determine the alleged omission’s materiality. *Id.* at 1426. On appeal, the plaintiffs argued this was procedurally improper because they had not attached the report to their complaint. *Id.* The Third Circuit, however, found no error. *Id.* It first considered whether the complaint referred to or cited the report, because either pleading strategy would have justified the district court’s reliance on the “extrinsic document.” *Id.* The complaint did neither, so the Third Circuit contemplated a third possibility: whether plaintiffs’ securities claim was “based” on the report.

See *id.* (“Plaintiffs cannot prevent a court from looking at the texts of the documents on which its claim is based by failing to attach or explicitly cite them.”). The plaintiffs had alleged that the supplier-discount data was material, and therefore should have been disclosed, by “unambiguous[ly] referenc[ing]” full-year cost data published within the annual report.

Id. Accordingly, the Third Circuit held that the claim was “based” on the report and affirmed the district court’s reliance on it. *Id.*; see also, e.g., *Fallon v. Mercy Cath. Med. Ctr. of Se. Pa.*, 877 F.3d 487, 493 (3d Cir. 2017) (permitting full consideration of an essay that was quoted in the complaint); *CardioNet, Inc. v. Cigna Health Corp.*, 751 F.3d 165, 168 n.2 (3d Cir.

2017) (permitting, in a contract dispute, consideration of the underlying contracts referenced in the complaint); *Schmidt v. Skolas*, 770 F.3d 241, 249-50 (3d Cir. 2014) (holding press releases and updates were not integral to a complaint alleging a breach of fiduciary duty in connection with the sale of corporate assets, because the claim was “‘based’ on” the transactions, not those corporate documents).

Here, Plaintiffs’ Amended Complaint relies on selective quotes from Defendants’ Terms of Use (Defs.’ Ex. D) and Privacy Notice (Defs.’ Ex. E). Moreover, it “explicitly refer[s] to,” *Burlington Coat*, 114 F.3d at 1426, four Cigna webpages: *www.cigna.com* (Defs.’ Ex. A), *my.cigna.com* (Defs.’ Ex. B), *plans.cigna.com* (Defs.’ Ex. C), and the “Knowledge Center” webpage (Defs.’ Ex. F).

Notably, Plaintiffs do not dispute the authenticity of these exhibits. Accordingly, it is appropriate to consider on this Motion to Dismiss all of these exhibits. By contrast, consideration of Defendants’ other exhibits would be improper. These exhibits are a registration page for the myCigna portal (Defs.’ Ex. J), Cigna’s HIPAA Notice 8 Although not mentioned by name, *my.cigna.com* represents the landing page for Cigna’s authenticated environment, which Plaintiffs explicitly refer to throughout the Amended Complaint.

(Defs.’ Ex. H), a consent banner shown to website users with a California IP address (Defs.’ Ex. I), and an informational webpage from Adobe (Defs.’ Ex. G). With the exception of the Adobe webpage, the Amended Complaint does not “explicitly” quote from or refer to these sources. *Id.* Moreover, properly understood, Plaintiffs’ claims are not “based” on these documents.

The Amended Complaint alleges that Defendants enabled third parties to covertly harvest insureds’ personal health information through tracking technologies embedded within the source code of various Cigna’s webpages. While those allegations implicate HIPAA- and consent- related issues, Plaintiffs’ claims do not arise from their “texts” and, accordingly, are not “based” on them.

Id. Defendants argue that the myCigna registration page and HIPAA Notice should be incorporated by reference because, in order for Plaintiffs to log in to the myCigna portal, as they alleged, they would need to create an account and agree to the HIPAA Notice. Similarly,

Defendants contend the consent banner is incorporated because the Amended Complaint alleges that the website “does not display a pop-up, banner, or consent prompt.” But those arguments are for summary judgment in that they inject new facts contradicting Plaintiffs’ allegations.

Their consideration at this stage would “short-circuit the resolution of a well-pleaded claim.” *Khoja*, 899 F.3d at 1003. Finally, Defendants’ exhibit concerning the Adobe informational webpage merits special attention.

The Amended Complaint quotes from an Adobe webpage to explain how entities like Defendants use Adobe’s tracking technology. Defendants’ exhibit purports to represent that page, but the exhibit’s URL does not match that cited in the Amended Complaint.

In fact, Plaintiffs’ quotation appears nowhere in Defendants’ exhibit. It is therefore not “an undisputedly authentic document” and is beyond the scope of the incorporation-by-reference doctrine. *Pension Benefit*, 998 F.2d at 1196; see also Fed. R. Evid. 901 (“To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” (emphasis added)).

B. Judicial Notice Nevertheless, Defendants urge the Court to take judicial notice of these exhibits. Judicial notice is an “evidentiary doctrine that permits the court to consider as established in a case a matter of law or fact without the necessity of formal proof of the matter by any party.” 21B Wright & Miller’s Federal Practice & Procedure Evidence § 5102 (2d ed.

2025) (alteration omitted). Federal Rule of Evidence 201 authorizes judicial notice of facts that are: (1) adjudicative, not legislative; and, (2) not subject to reasonable dispute because they are either (i) “generally known within the trial court’s territorial jurisdiction” or (ii) “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” Fed.

R. Evid. 201. A court “may take judicial notice on its own,” but it “must take judicial notice if a party requests it and the court is supplied with the necessary information.” Fed. R. Evid. 201(c). Although the rule permits noticing of a fact at any stage of the proceeding, Fed. R. Evid. 201(d), the Third Circuit has cautioned that courts should do so “sparingly at the pleadings stage.” *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir.

2007), as amended (Nov. 20, 2007). “Only in the clearest of cases should a district court reach outside the pleadings for facts necessary to resolve a case at that point.” *Id.* In assessing motions to dismiss, the Third Circuit has taken judicial notice of publicly available documents on government websites. See, e.g., *Skolas*, 770 F.3d at 249 (taking judicial notice of SEC filings); *In re NAHC, Inc. Sec. Litig.*, 306 F.3d 1314, 1331 (3d Cir.

2002) (same); *Oran v. Stafford*, 226 F.3d 275, 289 (3d Cir. 2000) (same); see also *Pension Benefit*, 998 F.2d at 1197 (explaining that “public record[s], for purposes of what properly may be considered on a motion to dismiss,” includes criminal convictions, letter decisions of government agencies, and published reports of administrative bodies). Defendants argue for an expansion of this practice to the content and policies on a commercial website, contending such sources are analogous to government documents.

They do not provide any precedential authority to support their position, which strongly counsels against noticing non-governmental, publicly available web sources. And, in fact, *Skolas*, cited by Defendants, significantly undermines their position.

In that case, the Third Circuit held that ordinary business documents, such as press releases, were not subject to judicial notice because they were not “records of a government agency.” *Skolas*, 770 F.3d at 250 (citing *Pension Benefit*, 998 F.2d at 1197). Similarly, in *Victaulic*, the Third Circuit described “private corporate websites, particularly when describing their own business,” as generally “not the sorts of ‘sources whose accuracy cannot reasonably be questioned.’” *Victaulic*, 499 F.3d at 236 (quoting *Fed.*

R. Evid. 201(b)). * * * In sum, Defendants’ Exhibits G, H, I, and J are neither incorporated by reference in the Amended Complaint nor the proper subject of judicial notice. They will not be considered here.⁹ DISCUSSION A. Standing Pursuant to Federal Rule of Civil Procedure 12(b) (1), Defendants move to dismiss the entirety of the Amended Complaint for lack of standing, arguing that Plaintiffs have failed to 9 Defendants’ interrogatory responses, relied upon by Plaintiffs in their briefing, will also be ignored.

See *In re BYJU’s Alpha, Inc.*, 2025 WL 659092, at *16 n.56 (D. Del. Feb. 27, 2025) (“Interrogatory responses are generally considered beyond the scope of the record on a motion to dismiss.”). allege an injury for each claim and their request for injunctive relief. Rule 12(b)(1) requires dismissal of claims over which a federal court lacks subject-matter jurisdiction.

Fed. R. Civ. P. 12(b)(1). “A motion to dismiss for want of standing is... properly brought pursuant to Rule 12(b)(1), because standing is a jurisdictional matter.” *Ballentine v. United States*, 486 F.3d 806, 810 (3d Cir. 2007). Article III standing consists of three components: (1) an injury-in-fact; (2) a sufficient causal connection between the injury and the conduct complained of; and, (3) a likelihood that the injury will be redressed by a favorable decision.

Finkelman v. NFL, 810 F.3d 187, 193 (3d Cir. 2016) (citing *Neale v. Volvo Cars of N. Am., LLC*, 794 F.3d 353, 358-59 (3d Cir. 2015)). Defendants challenge the injury-in-fact component only. In this posture, it is the Court’s “duty to ‘examine the allegations in the complaint from a number of different angles’ in order to see if the ‘purported injury can be framed in a way that satisfies Article III.’” *In re Johnson & Johnson Talcum Power Prods.*

Mtkg., Sales Pracs. & Liab. Litig., 903 F.3d 278, 282 (quoting Finkelman, 810 F.3d at 197). Specifically, the question is whether the Amended Complaint alleges “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks and citations omitted). “[S]tanding is not dispensed in gross.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021).

Rather, Plaintiffs, as the party invoking federal jurisdiction, bear the burden of “demonstrat[ing] standing for each claim that they press and for each form of relief that they seek.” *Id.* at 430-31. In other words, the Amended Complaint must allege a cognizable injury- in-fact with respect to each claim raised and form of relief sought.

In a putative class action such as this, standing is satisfied “so long as a class representative has standing” to press a claim or form of relief. *Neale*, 794 F.3d at 362; see also *McNair v. Synapse Grp. Inc.*, 672 F.3d 213, 223 (3d Cir. 2012) (“In the class action context, [the standing] requirement must be satisfied by at least one named plaintiff.”). “[U]nnamed, putative class members need not establish Article III standing.” *Neale*, 794 F.3d at 362.10 A challenge to standing may be either a facial or a factual attack, with the distinction determining how the pleadings must be reviewed.

Const. Party of Pa. v. Aichele, 757 F.3d 347, 357 (3d Cir. 2014) (citing *In re Schering Ploug Corp. Intron*, 678 F.3d 235, 243 (3d Cir. 2012)). “A facial attack, as the adjective indicates, is an argument that considers a claim on its face and asserts that it is insufficient to invoke the subject matter jurisdiction of the court because, for example, it does not present a question of federal law, or because there is no indication of a diversity of citizenship among the parties, or because some other jurisdictional defect is present,” such as the lack of an injury-in-fact.

Id. at 358. A factual attack, on the other hand, is an argument that there is no subject matter jurisdiction because, though jurisdiction may have been adequately pleaded, the actual facts of the case do not support the asserted jurisdiction. *Id.* A factual attack requires a factual dispute—the presentation of “competing facts.” *Id.*; see also *Davis v. Wells Fargo*, 824 F.3d 333, 346 (3d Cir.

2016) (“[B]ecause it submitted a signed declaration disputing Davis’s factual allegations, Assurant has mounted a factual challenge to subject matter jurisdiction.” (citation omitted)). Here, Defendants raise both types of challenges, 10 Defendants assert that “[e]very class member must have Article III standing in order to recover individual damages.” *TransUnion*, 594 U.S. at 431.

That is a correct statement of the law: every member of a certified class action must establish their standing to recover individual damages. *Huber v. Simon’s Agency, Inc.*, 84 F.4th 132, 155 (3d Cir. 2023). But before then, and even at class certification, the focus of the standing inquiry is exclusively on the named plaintiffs. *Id.*; see also *TransUnion*, 594 U.S. at 431 n.4 (declining to

address “the distinct question” of “whether every class member must demonstrate standing before a court certifies a class” (emphasis in original)).

The Court lacks subject matter jurisdiction only if no named Plaintiff has standing. See Finkelman, 810 F.3d at 195 (“Absent standing on the part of the named plaintiffs, we must dismiss a putative class action for lack of subject matter jurisdiction.”); Frank v. Gaos, 586 U.S. 485, 492 (2019) (“[F]ederal courts lack jurisdiction if no named plaintiff has standing.” (citation omitted)).

varying their approach by claim and relief. i. Factual Attack a. Legal Standard With respect to Plaintiffs’ ECPA, WESCA, and invasion-of-privacy claims, Defendants’ standing arguments rely in part on “evidence outside the pleadings,” Aichele, 757 F.3d at 358— Cigna’s HIPAA Notice, accompanied by a sworn declaration stating it is a true and correct copy.

This means, as to these three claims, Defendants mount a factual attack. See Davis, 824 F.3d at 346 (classifying a challenge as factual where the Rule 12(b)(1) motion was accompanied by a signed declaration disputing the complaint’s factual allegations); Int’l Ass’n of Machinists & Aerospace Workers v. Nw. Airlines, Inc., 673 F.2d 700, 711 (3d Cir. 1982) (holding that a 12(b)(1) motion supported by a sworn statement of facts “must be construed as a factual” attack).

When faced with a factual attack, plaintiffs “‘ha[ve] the burden of proof that jurisdiction does in fact exist,’ the court ‘is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case,’ and ‘no presumptive truthfulness attaches to the plaintiff’s allegations.’” Hartig Drug Co. v. Senju Pharm. Co., 836 F.3d 261, 268 (3d Cir.

2016) (internal brackets omitted) (quoting Mortensen v. First Fed. Sav. & Loan Ass’n, 549 F.2d 884, 891 (3d Cir. 1977)). b. ECPA, WESCA, and Intrusion Upon Seclusion Defendants argue that Plaintiffs lack standing to bring their ECPA and WESCA claims, asserting that Plaintiffs fail to allege a “concrete” harm resulting from the alleged statutory violations.¹¹ 11 For the reasons explained below, Plaintiffs’ standing to bring their claim for intrusion upon seclusion is co-extensive with their standing to pursue their statutory wiretapping claims.

Concreteness is an integral component of Article III standing. See TransUnion, 594 U.S. at 417 (“No concrete harm, no standing.”). It ensures that a plaintiff has suffered an injury that is “real, and not abstract,” which in turn prevents federal courts from adjudicating “hypothetical or abstract disputes” and from exceeding “their proper function in a limited and separated government.” Id. at 423-24 (citations omitted). “Article III standing requires a concrete injury even in the context of a statutory violation,” Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016), but a statutory violation does not necessarily result in a concrete harm, see TransUnion, 594 U.S. at 427 (“[U]nder Article III, an injury in law is not an injury in fact.”).

So federal courts have an obligation to make certain that “[o]nly those plaintiffs who have been concretely harmed by a defendant’s statutory violation may sue that private defendant over that

violation in federal court.” *Id.* at 426-27 (emphasis in original). Some harms, particularly physical and monetary ones, “readily qualify as concrete injuries.” *Id.* at 425.

But when a statutory violation causes an “intangible harm[],” concreteness turns on whether the alleged injury bears “a ‘close relationship’ to a harm ‘traditionally’ recognized as providing a basis for lawsuits in American courts.” *Id.* at 424-25 (citing *Spokeo*, 578 U.S. at 341). “That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury.” *Id.* at 424.

The injury need not “exact[ly] duplicate” a traditionally recognized harm, *id.*, but it must be “‘of the same character,’” *Barclift v. Keystone Credit Serv., LLC*, 93 F.4th 136, 146 (3d Cir. 2024) (quoting *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019)). That “close relationship” can exist even when “the conduct alleged would not have ‘given rise to a cause of action under common law.’” *Susinno v. Work Out World Inc.*, 862 F.3d 346, 351 (3d Cir.

2017) (quoting *In re Horizon Healthcare Serv. Inc. Data Breach Litig.*, 846 F.3d 625, 639 (3d Cir. 2017)). In this case, Plaintiffs assert wiretapping claims under the ECPA and its state counterpart, the WESCA. Both statutes “emphasize[] the protection of privacy,” *Commonwealth v. Spangler*, 809 A.2d 234, 237 (Pa. 2002), by “prohibit[ing] the interception of electronic communications without prior consent,” *Cook v. GameStop, Inc.*, 148 F.4th 153, 157 (3d Cir.

2025) (citation omitted). Plaintiffs allege that Defendants invaded their privacy—an intangible harm—by installing third-party tracking technologies throughout an insurance website. Accordingly, under TransUnion’s history-based framework, privacy torts provide the common-law analogues for assessing the concreteness of Plaintiffs’ injury. See *id.* at 159-60 (analyzing standing for a WESCA violation by reference to the harms caused by intrusion upon seclusion and public disclosure of private facts); see also *Barclift*, 93 F.4th at 145 (identifying four torts that can serve as a comparator for a privacy-related statutory violation: intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light).

Here, Plaintiffs analogize their injury to “the kind[s] of privacy harm traditionally associated with” public disclosure of private facts and intrusion upon seclusion. *Barclift*, 93 F.4th at 146. “Intrusion upon seclusion is an intentional intrusion, ‘physical or otherwise, upon the solitude or seclusion of another or his private affairs or concerns if the intrusion would be highly offensive to a reasonable person.’” *Cook*, 148 F.4th at 160 (internal brackets and alteration omitted) (quoting *Kline v. Sec. Guards, Inc.*, 386 F.3d 246, 260 (3d Cir.

2004)). The harm for this tort “‘consists solely of an intentional interference with the plaintiff’s interest in solitude or seclusion, either as to his person or as to his private affairs or concerns.’” *Id.* (internal brackets omitted) (quoting Restatement (Second) of Torts § 652B cmt. a (1977)). Unlike other privacy torts, the injury does not turn on the exposure or the use of private information.

Id. Nor does it “depend upon any publicity given to the person whose interest is invaded or to his affairs.” Restatement (Second) of Torts § 652B cmt. a (1977). An alleged harm has the “same character” as the harm of intrusion upon seclusion where there is an even marginal invasion of another’s private sphere or disturbance of another’s interest in solitude or seclusion.

See *Susinno*, 862 F.3d at 351-52. In *Susinno*, the plaintiff sued a fitness company for leaving a prerecorded voicemail on her phone, alleging that conduct violated the Telephone Consumer Protection Act’s “prohibition of prerecorded calls to cellular telephones.” Id. at 348; see also 47 U.S.C. § 227(b)(1)(A)(iii).

On appeal, the Third Circuit reversed the district court’s determination that the voicemail caused her no concrete injury. *Susinno*, 862 F.3d at 348. While acknowledging that receipt of a single unsolicited call fails to state a claim for intrusion upon seclusion, the court held that the “nuisance and invasion of privacy resulting from a single prerecorded telephone call” was “of the same character” as a “highly offensive” intrusion upon seclusion.

Id. at 351-52 (internal quotation marks and citation omitted). The court also emphasized that standing requires only “some specific, identifiable trifle of injury.” Id. (quoting *Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 278 (3d Cir. 2014)).

In this case, Plaintiffs allege that their health insurer and its subsidiary have installed third-party tracking pixels and session replay code on their public-facing webpages and within their password-protected member portals, enabling the unconsented, real-time disclosure of insureds’ website interactions. It is plausible that these captured interactions—including clicks, queries, and the URLs of visited webpages—reveal insureds’ medical and insurance information.

In turn, the third parties harvest the health data and combine it with other aggregated data to create bespoke digital dossiers for advertising purposes. Plaintiffs aver that Defendants’ wiretapping violations have caused them “embarrassment” and a “loss of privacy.” In light of *Susinno*, Plaintiffs’ alleged loss of privacy in their private affairs, caused by the unconsented interception of their healthcare-related data, is “analogous to the harm associated with intrusion upon seclusion,” *Cook*, 148 F.4th at 160; see *Susinno*, 862 F.3d at 350-51 (holding that the harm of a single unsolicited robocall had a “close relationship” to an “invasion of privacy” (quoting *Horizon*, 846 F.3d at 639-40)).

Accordingly, Plaintiffs allege an Article III injury that, though intangible, is concrete. See *TransUnion*, 594 U.S. 424-25. The Third Circuit’s recent decision in *Cook v. GameStop* does not undermine this conclusion.

In that case, *Cook* alleged that an online retailer, GameStop, captured users’ every interaction with its website through third-party session replay code. *Cook*, 148 F.4th at 156-57. *Cook* brought WESCA and common law claims, arguing she had standing because the technology caused an

invasion of privacy similar in “kind” to intrusion upon seclusion. *Id.* at 156, 159 (citation omitted).

In her view, the technology was the “electronic equivalent of ‘looking over the shoulder’ of each visitor to the GameStop website for the entire duration of [her] website interaction,” which she “presumed” was private. *Id.* at 160.

The court held that her injury was not equivalent to intrusion upon seclusion, reasoning that she did not allege that the code captured “website activity involv[ing] her private affairs” or that it tracked her while she was “secluded” or “in solitude.” *Id.* Stressing that “most of us understand that what we do on the Internet is not completely private,” the court noted that the technology tracked her product preferences, not any “sensitive or personal” data like her contact or billing information.

Id. (internal brackets omitted). Moreover, GameStop did not create an expectation of privacy where it otherwise would not have existed by explicitly “promis[ing] to refrain from collecting information.” *Id.* at 162-63; see also, e.g., *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 274, 292 (3d Cir. 2016) (holding that plaintiffs had standing to bring claims under the ECPA, the Video Privacy Protection Act, and other privacy statutes where they alleged that a website collected children’s online browsing habits, video history, and profile information, despite promising not to do so); *In re Google Inc. Cookie Placement Cons.*

Privacy Litig., 934 F.3d 316, 325 (3d Cir. 2019) (*Google II*) (holding that allegations of unauthorized data tracking—allegations “indistinguishable from those in *Nickelodeon*”—conferred standing to sue under federal privacy and fraud statutes). *Cook* is materially distinguishable. Whereas the data collected there revealed users’ product preferences—information which is not considered private¹²—this case alleges that Defendants and third parties surreptitiously collect data that discloses insureds’ personal medical history.

Few things are more sensitive and personal than information about one’s health. Indeed, the Third Circuit has long recognized that “[i]nformation about one’s body and state of health is matter which the individual is ordinarily entitled to retain within the private enclave where he may lead a private life.” *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir.

1980) (internal quotation marks and citation omitted). And, in various ways, the law reflects that special regard for personal health information. See, e.g., *Doe v. Delie*, 257 F.3d 309, 315-17 (3d Cir. 2001) (recognizing a right to privacy in one’s medical information, and extending that right to prison inmates); 42 U.S.C. § 1320d et seq. (codifying HIPAA’s privacy and disclosure requirements for personal health information); 5 U.S.C. § 552(b)(6) (exempting medical files from the Freedom of Information Act); Fed.

R. Civ. P. 35 (establishing a higher burden for discovery of medical information than for discovery generally). 12 As another court has explained: “[W]hile a customer might not like to have his online shopping activity tracked..., there is no meaningful privacy distinction between shopping online and shopping in retail stores.” *DeLong v. PHE, Inc.*, 2025 WL 2447787, at *7 (E.D.

Pa. Aug. 25, 2025) (citations omitted). In any brick-and-mortar store, employees and other consumers can readily glean a consumer’s product preferences based on what she looks for and purchases. *Id.* By extension, it is not a cognizable invasion of privacy for a retailer to learn those preferences through digital tracking on its commercial website. See *id.* Persuasively, in finding a lack of standing in invasion-of-privacy cases involving online retail behavior, courts in this District have widely noted that the interception of health information would give rise to standing.

See, e.g., *DeLong*, 2025 WL 2447787, at *6 (“While a third party collecting certain data like credit card, banking, or medical information may constitute concrete harm, that is... only because such information is private.” (emphasis added)); *In re BPS Direct, LLC*, 705 F. Supp.3d 333, 347 (E.D. Pa. 2023) (holding plaintiffs lacked standing “because they do not allege they made purchases on the Websites or engaged in activity which would cause their browsers to send highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards” (emphasis added)); *Hartley v. Urban Outfitters, Inc.*, 740 F. Supp.3d 410, 420-21 (E.D.

Pa. 2024) (noting standing may have existed if the “spy pixels” embedded within a retailer’s promotional emails had collected “highly sensitive categories of personal information,” including “medical history”). And courts elsewhere have found standing in cases alleging the unauthorized digital tracking of medical information. See, e.g., *Rodriguez v. FastMed Urgent Care, P.C.*, 741 F. Supp.3d 352, 360-61 (E.D.N.C.

2024) (“Disclosing Rodriguez’s private medical information without the meaningful opportunity to prevent the disclosure satisfies Article III’s injury requirement.”); *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp.3d 928, 939-40 (N.D. Cal. 2023) (holding plaintiffs alleged a cognizable invasion of privacy based on the defendant’s nonconsensual online collection of multiple “categories of sensitive information,” including “race, location, politics, and medical information”).

Moreover, unlike in *Cook*, Plaintiffs allege that the technologies capture data not just on Defendants’ public-facing webpages but also from within the myCigna medical and dental portals. These purportedly secure environments require a username and password, measures that underscore and reinforce an expectation of privacy. Yet according to the Amended Complaint, Defendants have installed Adobe code that tracks users’ portal interactions from the moment they log in.

Adobe then uses the data “to help its clients obtain marketing insights” by building “behavioral profiles tied to users’ searches and health conditions.” In short, Defendants’ invasion of a private domain stands in sharp distinction to the allegations in *Cook*. *Cook* suffered no meaningful injury from GameStop’s collection of her product preferences. But by contrast, there is an acute loss of privacy that closely resembles the harm of intrusion upon seclusion when tracking code secretly harvests an individual’s medical information.

Such a loss is concrete, a conclusion that upholds “a recognition that information concerning one’s body has a special character.” *Westinghouse*, 638 F.2d at 577. In addition to their challenge to concreteness, Defendants also argue that Plaintiffs lack standing because they never allege the interception of their information. “Instead,” Defendants contend, “[Plaintiffs’] theory rests on a two-step chain of inferences that do not intersect: (1) they interacted with certain Cigna-hosted webpages; and (2) Cigna deployed [tracking technologies] on certain webpages, but not necessarily those that Plaintiffs used, that could have captured Plaintiffs’ unidentified ‘private’ information.” This argument, although still bearing on Article III’s injury-in-fact prong, concerns whether Plaintiffs’ injury is “particularized”—that is, whether it affects them “in a personal and individual way.” *Lujan*, 504 U.S. at 560 n.1.

Plaintiffs have met their burden. After explaining how the third-party tracking code captures sensitive information, including from within the authenticated portals, the Amended Complaint goes on to allege that each Plaintiff used the portals to “search for in-network providers,” “review [insurance] claims,” and research “medical issues.” It buttresses this allegation with Plaintiff-specific descriptions of how they used Defendants’ website: • Plaintiff Adair “used the medical portal... to confirm whether his employer- sponsored health savings contributions had been applied after completing preventive health activities such as blood sugar screenings”; • Plaintiff Emrick “used the medical portal... to find a provider for an intestinal screening, which required her to navigate providers and this specific medical procedure”; • Plaintiff Recchia “used the medical portal to find a new primary care physician and used the dental portal after undergoing a surgical dental procedure”; • Plaintiff Pham “used the portal to search for prescriptions and to research health conditions”; and, • Plaintiff Danielson “used the portal to review her health issues, and the public- facing portions of the [w]ebsite to research health topics as well.” Although additional examples would fortify the Amended Complaint, Plaintiffs have sufficiently alleged that the technologies captured information pertaining to their patient status, medical conditions, procedures, medications, providers, and insurance benefits.

Finally, Defendants contend that Plaintiffs fail to allege an injury because they agreed to Cigna policies that disclosed the data collection and sharing practices they now challenge. In other words, they argue that Plaintiffs were unharmed because they consented to the data tracking. That argument, however, imports a merits-based defense into the standing inquiry.

It is prematurely raised. Whether an individual has suffered a cognizable harm and whether that harm may have been legally justified are distinct inquiries. See *Falcone v. Dickstein*, 92 F.4th 193, 203 (3d Cir. 2024) (“[W]e must not ‘confuse weakness on the merits with absence of Article III standing.’” (quoting *Ariz. State Legislature v. Ariz. Indep. Redistricting Comm’n*, 576 U.S. 787, 800 (2015))); see also, e.g., *Hall v. Smosh Dot Com, Inc.*, 72 F.4th 983, 991 (9th Cir.

2023) (holding, in a TCPA case, that the questions of whether Hall’s “son in fact solicited the messages, and whether his consent would be legally sufficient under the TCPA, are relevant only to the merits of Hall’s claim, not to her standing to litigate it”). “[A] district court must take care not to reach the merits of a case when deciding a Rule 12(b)(1) motion,” *CNA v. United States*, 535 F.3d 132, 144 (3d Cir.

2008), so when, as here, “a factual challenge to jurisdiction attacks facts at the core of the merits of the underlying cause of action, ‘the proper procedure for the district court is to find that jurisdiction exists and to deal with the objection as a direct attack on the merits of the plaintiff’s case.’” *Davis*, 824 F.3d at 348 (quoting *Kulick v. Pocono Downs Racing Ass’n*, 816 F.2d 895, 898 n.5 (3d Cir.

1987)). In light of that directive, and based on the foregoing, Plaintiffs have standing to bring their ECPA, WESCA, and intrusion-upon-seclusion claims. ii. Facial Attack a. Legal Standard Defendants’ challenge to Plaintiffs’ standing to request injunctive relief and to raise each of their other claims—that is, for unjust enrichment and breach of fiduciary duty—does not rely on extraneous materials.

Instead, they argue that “Plaintiffs’ theory of injury fails to satisfy Article III on the face of the pleadings.” Insofar as they “contest[] the sufficiency of the pleadings” for these claims and relief, they raise a facial challenge.

In *re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 243 (3d Cir. 2012). In evaluating a facial attack, “the same standard of review” as a motion to dismiss for failure to state a claim is applied. *Finkelman*, 810 F.3d at 194.

In other words, the “well-pleaded factual allegations” in the complaint are presumed to be true, “conclusory statements” are ignored, and then a determination is made as to whether the allegations—viewed in the light most favorable to the plaintiff—“plausibly” establish standing. *Id.*; In *re Schering*, 678 F.3d at 243. b. Unjust Enrichment Turning first to Plaintiffs’ unjust enrichment claim, Defendants argue that Plaintiffs again fail to allege a concrete, personal harm.

In response, Plaintiffs raise two different theories of economic injury. See *TransUnion*, 594 U.S. at 425 (observing that monetary harms “readily qualify as concrete injuries under Article III”); *Huertas v. Bayer US LLC*, 120 F.4th 1169, 1174 (3d Cir. 2024) (“While it is difficult to reduce

injury-in-fact to a simple formula, economic injury is one of its paradigmatic forms.’” (quoting *Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 291 (3d Cir.

2005))). Under their first theory, Plaintiffs argue that Defendants derived economic benefits from their private health-related information. At face value, that contention has an obvious problem: one person’s gain is not necessarily another’s loss.

In other words, that Defendants and third parties profited from the collection and sale of Plaintiffs’ information is not sufficient, standing alone, to plead an injury to Plaintiffs. See *Ne. Fence & Iron Works, Inc. v. Murphy Quigley Co.*, 933 A.2d 664, 669 (Pa. Super. 2007) (“The most significant element of the doctrine is whether the enrichment of the defendant is unjust; the doctrine does not apply simply because the defendant may have benefited as a result of the actions of the plaintiff.” (quoting *Lackner v. Glosser*, 892 A.2d 21, 34 (Pa.

Super. 2006))). Thus, implicit within Plaintiffs’ theory are two propositions: (1) Plaintiffs’ information has economic value; and, (2) the acquisition and subsequent use of that information has diminished that economic value, to Plaintiffs’ detriment. This is known as the diminution-in-value or loss-of-value theory. See, e.g., *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp.3d 735, 755 (W.D.N.Y.

2017); *In re SAIC Backup Tape Data Theft Litig.*, 45 F. Supp.3d 14, 30 (D.D.C. 2014). And it reflects the “[o]rdinar[y]” case of unjust enrichment whereby “the benefit to the one and the loss to the other are co-extensive.” Restatement (First) of Restitution § 1 cmt. d (1937).

The facts within the Amended Complaint sufficiently support the first premise of the diminution-in-value theory—that an individual’s health data, like other personal information, has monetary value. Describing individuals’ personal data as “new oil,” the Amended Complaint alleges there is a market of brokers who compile personal health data from providers and other health-care organizations to sell it.

And it alleges that both Defendants and the third-party vendors in this case used the harvested data for their own commercial gain, including by bolstering advertising services and by selling the data to others. However, the Amended Complaint lacks well-pleaded facts supporting the theory’s second premise—that Defendants have deprived Plaintiffs of the data’s value.

For one thing, Defendants have not literally taken Plaintiffs’ data away such that it is no longer available to them. See *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 913 (7th Cir. 2017) (rejecting the argument that a cable provider’s retention of its customer’s personal information deprived the customer of the data’s value, because the provider “did not take the plaintiff’s personal information away from him; he still has it”).

The data still exists, and it remains at Plaintiffs' disposal. Moreover, there are no factual allegations suggesting that the data is less valuable because of Defendants' or the third parties' use of it, let alone allegations indicating that Plaintiffs themselves intended to sell their information (which seems a highly unlikely proposition given their overarching privacy concerns).

See *Fero*, 236 F. Supp.3d at 755 (holding that the complaint "lacks factual allegations to support the proposition that their personal information was made less valuable to them as a result of the breach, or that the data breach negatively impacted the value of their data such that Plaintiffs could not use or sell it"); *Khan v. Childs. Nat'l Health Syst.*, 188 F. Supp.3d 524, 533 (D.

Md. 2016) ("Khan alleges that the value of her personally identifiable information has been diminished by the data breach. She does not, however, explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information."); *In re SAIC*, 45 F. Supp.3d at 30 ("As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss.

Even if the service members did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach." (emphasis in original)). At best, the harm alleged is "having their confidential financial information used for the benefit of Defendants and others." Because that does not actually describe a personalized injury to Plaintiffs, their diminution-in-value theory is unsuccessful.

Plaintiffs' second theory is that they suffered an actual monetary loss by receiving less than the bargained-for-value of their insurance premiums. In their briefing, they maintain that they paid for insurance services marketed as private, secure, and compliant with federal confidentiality requirements while in reality their insurer enabled covert tracking of their personal data.

The difference in value between what was promised and what was provided, they contend, is an economic injury that should give rise to standing. See *Huertas*, 120 F.4th at 1174 ("One way a plaintiff might successfully plead an economic injury is by alleging that she bargained for a product worth a given value but received a product worth less than that value." (internal quotation marks, internal brackets, and citation omitted)).

This is known as the benefit- of-the-bargain theory. *Id.* Under it, a plaintiff is not required to allege "exact value of her economic injury at the pleading stage." *Johnson & Johnson*, 903 F.3d at 287 (emphasis in original). "But even at the pleading stage, a plaintiff must set forth sufficient factual allegations that, if proven true, would permit a factfinder to determine," without resorting to conjecture, "that she suffered at least some economic injury." *Id.* (emphasis in original) (citing *Danvers*, 432 F.3d at 294).

Plaintiffs are also unsuccessful under this theory. The Amended Complaint lacks any allegation that Defendants provided Plaintiffs with an “economic benefit worth one penny less than what [they] paid.” *Id.* at 288. In fact, there are no allegations whatsoever about insurance premiums and whether some indeterminate portion of them went toward providing the security and confidentiality that Defendants promised.

Nor are there allegations that Plaintiffs relied on those promises when choosing Cigna as their insurer. Moreover, the Court cannot conclude it has jurisdiction by assuming that Plaintiffs would spend more for data security.

In the absence of any allegations to that effect, such an assumption “would turn the standing question on its head” because “we presume that federal courts lack jurisdiction unless the contrary appears affirmatively from the record.” *Id.* (internal brackets omitted) (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 n.3 (2006)).¹³ Because neither theory of economic injury is sufficient, Plaintiffs have failed to demonstrate they have standing for their claim of unjust enrichment.

See *TransUnion*, 594 U.S. at 430-31. The claim will therefore be dismissed without prejudice. ¹³ *Boelter v. Hearst Commc’ns, Inc.*, 192 F. Supp.3d 427 (S.N.D.Y. 2016), relied upon by Plaintiffs, is easily distinguishable. There, plaintiffs sued their magazine provider for selling their demographic information to third parties. *Id.* at 435-36.

The court held that this conduct caused an economic injury sufficient to give them standing to bring their state law claims, including for unjust enrichment. *Id.* at 438. In contrast to the Plaintiffs here, the *Boelter* plaintiffs specifically alleged that the disclosure reduced the value of their magazine subscriptions and that, had they known their information would be sold, “they would not have been willing to pay as much, if at all, for their magazine subscriptions.” *Id.* at 436, 438 (internal quotation marks and brackets omitted).

In addition, the complaint included several paragraphs explaining that the magazine profited from selling consumer data, a benefit that was not reflected in the magazine subscription price. *Id.* c. Breach of Fiduciary Duty Defendants’ standing challenge to Plaintiffs’ breach-of-fiduciary-duty claim is also facial.

The essence of Plaintiffs’ claim is that Defendants violated a fiduciary duty to maintain the confidentiality and privacy of their insureds’ personal information. In contending that Plaintiffs lack standing, Defendants argue only that they did not owe a fiduciary duty: they merely operated a website and hosted an online member portal, ordinary commercial activities that they contend do not give rise to such a duty.

But that argument is not appropriately raised under Rule 12(b)(1). Whether a fiduciary relationship existed between the parties is a merits question. See *Harold ex rel. Harold v. McGann*,

406 F. Supp.2d 562 (E.D. Pa. 2005) (“In order to plead a violation of fiduciary duty or confidential relationship, Plaintiff must show that such a relationship existed.”).

Under Pennsylvania law, a confidential relationship “exists whenever one occupies toward another such a position of advisor or counselor as reasonably to inspire confidence that he will act in good faith for the other’s interest.” *Silver v. Silver*, 219 A.2d 659, 662 (Pa. 1966). Defendants do not contend that Plaintiffs are the “wrong” people to bring this claim—the concern at the heart of standing doctrine—but rather that the claim is “without merit” because there was no duty owed.

Davis, 824 F.3d at 348. Yet, as noted above, the Third Circuit has “repeatedly cautioned against allowing a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction to be turned into an attack on the merits.” *Id.* (citations omitted).

Because “it is well settled that the failure to state a proper cause of action calls for a judgment on the merits and not for a dismissal for want of jurisdiction,” *id.* (citing *Bell v. Hood*, 327 U.S. 678, 682 (1946)), a conclusion that Plaintiffs have standing to bring their fiduciary duty claim is warranted. *d.* Injunctive Relief Lastly, to have standing to obtain forward-looking (prospective) injunctive relief, Plaintiffs must plausibly allege that they face an ongoing or future injury.

O’Shea v. Littleton, 414 U.S. 488, 495-96 (1974) (“Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief... if unaccompanied by any continuing, present adverse effects.”); *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983) (holding that standing to seek injunctive relief depended on whether the plaintiff “was likely to suffer future injury”).

Past harms, standing alone, are insufficient. *O’Shea*, 414 U.S. at 496. Where the allegations concern a future injury, the threatened harm must be “certainly impending” or have a “substantial risk” of occurring. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 401, 414 n.5 (2013)).

The Amended Complaint alleges that Defendants continue to intercept and disclose insureds’ communications every time they use the website. In other words, it alleges that the technologies remain embedded. And it further avers that some of the named Plaintiffs have ongoing or future interactions with Defendants’ website. Specifically, Plaintiff Danielson alleges that she continues to use the website regularly, and Plaintiffs Adair and Emrick allege that they remain insured by Defendants.

Thus, given the allegations of the Amended Complaint, further interceptions of their private information is virtually assured. See *McNair*, 672 F.3d at 224-26 (holding that plaintiffs lacked standing to enjoin their former magazine provider’s “allegedly deceptive” marketing techniques because, as former customers, they failed to establish any likelihood of a future injury); *id.* at 226

n.16 (“Appellants only needed to demonstrate that they were ‘likely to suffer future injury’ from the Synapse’s conduct.

Lyons, 461 U.S. at 105. The best way to do that, of course, would have been to show they were Synapse customers....”). They have standing to seek injunctive relief on behalf of themselves and the putative class. See Finkelman, 810 F.3d at 195 (“Absent standing on the part of the named plaintiffs, we must dismiss a putative class action for lack of subject matter jurisdiction.”).14 B. Sufficiency of the Allegations Defendants also challenge the merits of Plaintiffs’ surviving claims under Rule 12(b)(6). i. Legal Standard To survive a motion to dismiss brought pursuant to Rule 12(b)(6), “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)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. “Threadbare” recitations of the elements of a claim supported only by “conclusory statements” will not suffice. Id. at 683.

Rather, a plaintiff must allege some facts to raise the allegation above the level of mere speculation. Great W. Mining & Min. Co. v. Fox Rothschild, LLP, 615 F.3d 159, 176 (3d Cir. 2010) (citing Twombly, 550 U.S. at 555). Furthermore, a court may grant a motion to dismiss under Rule 12(b)(6) if there is a dispositive issue of law. Neitzke v. Williams, 490 U.S. 319, 326-27 (1989).

When analyzing a motion to dismiss, a complaint must be construed “in the light most favorable to the plaintiff,” with the question being “whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.” Fowler, 578 F.3d at 210 (citation omitted). 14 At this stage of the proceedings, whether Plaintiffs Pham and Recchia have standing to obtain an injunction is not relevant.

See Huber, 84 F.4th at 154-55. Legal conclusions are disregarded, well-pleaded facts are taken as true, and a determination is made as to whether those facts state a “plausible claim for relief.” Id. at 210-11. And, as noted above, a court may consider—as appropriate—documents “incorporated by reference or integral to the claim” in making this determination.

Buck, 452 F.3d at 260. ii. Consent Defendants invoke consent as a defense to Plaintiffs’ ECPA, WESCA, and intrusion- upon-seclusion claims.15 a. Procedural Propriety As a threshold procedural matter, the parties dispute whether consent is an issue appropriately raised and decided in a 12(b)(6) motion. Plaintiffs posit that consent is a fact- based defense that would be “fundamentally improper” to resolve at the motion-to-dismiss stage.

Defendants retort that courts have long dismissed wiretapping claims on consent grounds at the pleading stage. Rule 12(b)(6) tests the factual sufficiency of a complaint to state a claim. Fed. R.

Civ. P. 12(b)(6). Generally, that calls for an account of a claim's elements, followed by a determination of whether "the complaint alleges 'enough facts to raise a reasonable expectation that discovery will reveal evidence of' the necessary elements." *Lutz v. Portfolio Recovery Assocs.*, 49 F.4th 323, 327-28 (3d Cir.

2022) (internal brackets omitted). Here, consent is an element of Plaintiffs' intrusion-upon-seclusion claim and is thus appropriately raised at this stage. Pennsylvania follows the Second Restatement of Torts' 15 Defendants, citing *Grimminger v. Maitra*, 887 A.2d 276 (Pa. Super. 2005), also contend that consent is dispositive of Plaintiffs' breach-of-fiduciary-duty claim.

Grimminger, however, recognized that consent is an affirmative defense to an action for breach of physician-patient confidentiality, *Grimminger*, 887 A.2d at 279 (citation omitted), which is an altogether different claim, see *Haddad v. Gopal*, 787 A.2d 975, 981 (Pa. Super. 2001) (reasoning that the claim arises from doctors' "obligation to their patients to keep communications, diagnosis, and treatment completely confidential").

Thus, the Court will address the breach-of-fiduciary-duty claim separately. definition of intrusion upon seclusion, providing a cause of action where there is an: (1) intentional intrusion, physical or otherwise; (2) upon the solitude or seclusion of another or his private affairs or concerns; (3) that is substantial; and, (4) would be highly offensive to a reasonable person.

Chicarella v. Passant, 494 A.2d 1109, 1114 (Pa. Super. 1985). The Third Circuit, predicting the view of the Supreme Court of Pennsylvania on this issue, has held that consent is relevant to the first element: whether there is an "intentional intrusion" turns on whether the tortfeasor believes or is substantially certain that he lacks the necessary legal or personal permission to commit an intrusive act.

O'Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989); see also, e.g., *Nickelodeon*, 827 F.3d at 293 (adopting *O'Donnell*'s interpretation in a data tracking case, and observing that other "[c]ourts applying *O'Donnell* have appropriately treated the presence or absence of consent as a key factor" in assessing the first element); *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp.3d 108, 120-21 (W.D.

Pa. 2019) (noting that "intrusion of seclusion allegations in the realm of digital privacy... turn[] on the consent" of the complaining party). To put it more succinctly, "[o]ne cannot intrude when one has permission," *Popa*, 426 F. Supp.3d at 121 (quoting *Jevic v. Coca Cola Bottling Co. of N.Y.*, 1990 WL 109851, at *9 (D.N.J. June 6, 1990)), so Plaintiffs' intrusion claim will fail if they gave Defendants permission to track, collect, and, share their data.

Meanwhile, consent is not an element of ECPA and WESCA claims.¹⁶ Instead, under both statutes, it is a statutory exception to liability. The ECPA contains a one-party consent ¹⁶ "A plaintiff pleads a prima facie case under the [ECPA] by showing that the defendant (1)

intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.” Nickelodeon, 827 F.3d at 274 (internal quotation marks and citation omitted).

Similarly, the prima facie case for a WESCA violation requires a plaintiff to allege: “(1) that he engaged in a communication; (2) that he possessed an expectation that the communication would not be intercepted; (3) that his expectation was justifiable under the circumstances; and (4) that the defendant attempted to, or successfully exception, permitting interceptions where one “person is a party to the communication or where one of the parties to the communication has given prior consent to such interception.” 18 U.S.C. § 2511(2)(d); see also *In re Google Inc. Cookie Placement Cons.*

Privacy Litig., 806 F.3d 125, 136 (3d Cir. 2015) (Google I) (referring to § 2511(2)(d) as a one “[o]f several statutory exceptions”). Similarly, the WESCA provides: “It shall not be unlawful... for: [a] person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.” 18 Pa. C.S.A. § 5704(4); see also *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir.

2022) (observing that the WESCA, like the ECPA, “includes many exceptions from liability”). It is not, as Plaintiffs suggest it would be, “fundamentally improper” to resolve a 12(b)(6) motion on the grounds of a statutory exception.

To the contrary, where a plaintiff’s allegations trigger one of the exceptions, dismissal of the wiretapping claim is warranted.¹⁷ See, e.g., *Google I*, 806 F.3d at 145 (affirming the dismissal of an ECPA claim because, “[b]ased on the facts alleged in the pleadings, the defendants were parties to any communications that they acquired, such that their conduct [was] within the § 2511(2)(d) exception”); *Nickelodeon*, 827 F.3d at 275 (following *Google I* in holding that § 2511(2)(d) was “fatal” to the plaintiffs’ ECPA wiretapping claim at the 12(b)(6) stage); *Vonbergen v. Liberty Mutual Ins.*

Co., 705 F. Supp.3d 440, 458-60 (E.D. Pa. 2023) (sustaining a intercepted the communication, or encouraged another to do so.” *Agnew v. Dupler*, 717 A.2d 519, 522 (Pa. 1998). ¹⁷ The practice seems to be a logical outgrowth of the so-called “Third Circuit Rule,” which permits defendants to raise “affirmative defenses” under Rule 12(b)(6). See *Robinson v. Johnson*, 313 F.3d 128, 135 & n.3 (3d Cir.

2002) (documenting the history of the rule, which dates back to at least 1948). Instead of contesting the sufficiency of the allegations, a 12(b)(6) motion asserting an affirmative defense posits that the allegations, by their own terms, “effectively vitiate the pleader’s ability to recover on the claim.” 5B *Wright & Miller’s Federal Practice & Procedure* § 1357 (4th ed.

2025). Put differently, the allegations are “self-defeating.” *Id.* Critically, dismissal is appropriate only where the affirmative defense is “‘apparent on the face of the complaint’ and documents relied on in the complaint.” *Lupian v. Joseph Cory Holdings LLC*, 905 F.3d 130, 130 (3d Cir. 2018) (quoting *Bohus v. Restaurant.com, Inc.*, 784 F.3d 918, 923 n.2 (3d Cir.

2015)); see also *Bethel v. Jendoco Const. Corp.*, 570 F.2d 1168, 1174 (3d Cir. 1978) (“[A]n affirmative defense may be raised on a 12(b) (6) motion if the predicate establishing the defense is apparent from the face of the complaint.”). WESCA claim where the plaintiff sufficiently pleaded that she did not provide consent under § 5704(4)’s mutual-consent exception); *M.D. v. Google LLC*, 2025 WL 2710095, at *4-5 (N.D.

Cal. Sept. 23, 2025) (dismissing a WESCA claim under § 5704(4) where the plaintiffs conceded that they had consented to the challenged data collection practices). For these reasons, Defendants appropriately raise the issue of consent in their Motion. Whether this argument disposes of Plaintiffs’ intrusion-upon-seclusion, ECPA, and WESCA claims is addressed in the next section. b. Substantive Law Defendants argue that their data collection and sharing practices were expressly disclosed in their Privacy Notice.

Specifically, they point to the following provisions: • “We may collect information that describes or relates to you and is classified as Personal Information or Personal Data,” including “name, contact information, online identifiers,” “government-issued ID numbers,” “age,” “medical conditions,” “browsing history, interactions with our website, Internet Protocol (IP) address, Media Access Control (MAC) address[,] operating system and version[,] Internet browser type and version,” “device location,” “place of employment[,] and job title.

We may collect this Personal Information directly from you and automatically when you use our Services. We also may collect this Personal Information from our affiliates, vendors, joint marketing partners, and social media platforms.” • “We may disclose Personal Information to third-party ad network providers, sponsors and/or traffic measurement services. These third parties may use cookies, JavaScript, web beacons (including clear GIFs), and other tracking technologies to measure the effectiveness of their ads and to personalize advertising content to you.” • “We use third-party tools, such as Google Analytics, which are operated by third- party companies, to evaluate usage of our Services.

These third-party analytics companies use cookies, pixels, and other tracking technologies to collect usage data about our Services to provide us with reports and metrics that help us evaluate usage of our Services, improve our Services, and enhance performance and user experiences.” • “We work with third-party ad networks, analytics, marketing partners, and others (‘third-party ad companies’) to personalize content and display advertising within our Services, as well as to manage our advertising on third-party Websites.

We and these third-party ad companies may use cookies, pixel tags, and other tools to collect browsing and activity information within our Services (as well as on third-party websites and services), as well as IP addresses, unique ID, cookie and advertising IDs, and other online identifiers.

We and these third-party ad companies use this information to provide you more relevant ads and content within our Services and on third-party websites, and to evaluate the success of such ads and content.” Plaintiffs do not deny that these disclosures encompass the conduct they challenge.¹⁸ Instead, they maintain in their brief that they did not agree to the terms because the interception “began immediately upon the loading of the [w]ebsite and before Plaintiffs had any opportunity to review, much less affirmatively understand and consent to, Defendants’ statements.” In other words, they argue that could not have “consented to something they did not see.” Their position is irreconcilable with their allegations.

The Amended Complaint certainly alleges that “[u]sers are not asked to consent prior to browsing Defendants’ [w]ebsite, and they are wiretapped from the moment they load the site, regardless of whether they eventually navigate to, download, read, or understand the disclosures in the privacy notice.” It characterizes Defendants’ integration of the tracking technologies as “unauthorized.” Yet it simultaneously and unambiguously alleges that Plaintiffs “agreed” to Cigna’s Terms of Use, thereby “enter[ing] into a direct agreement with Defendants.” In Plaintiffs’ own words, they manifested their assent by “us[ing] the [w]ebsite.” Although courts are normally “reticent to find mutual assent when a website ‘offers terms that are disclosed only through a hyperlink and the user manifests assent to those terms simply by continuing to use the website,’” *Checchia v. SoLo Funds, Inc.*, 771 F. 18 The Amended Complaint contends that the Privacy Notice is “vague, incomplete, and misleading,” and offers several reasons why, in Plaintiffs’ view, it fails to apprise users that Defendants collect and share insureds’ personal information.

But these assertions amount to nothing more than “legal conclusions disguised as factual allegations” about how the Privacy Notice should be interpreted. *Baraka v. McGreevey*, 481 F.3d 187, 211 (3d Cir. 2007). Such conclusory allegations are not entitled to a presumption of truth and should be disregarded in a 12(b)(6) motion. *Id.*; see also *McTernan v. City of York*, 577 F.3d 521, 531 (3d Cir.

2009) (“The tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions.”). Furthermore, in their briefing, Plaintiffs forfeited any argument about whether Defendants’ conduct exceeded the scope of the disclosures by failing to raise and develop that issue. See *N.J. Dep’t of Env’t Prot. v. Am. Thermoplastics Corp.*, 974 F.3d 486, 493 n.2 (3d Cir.

2020) (“As this argument was vaguely presented without factual or legal support, it is forfeited for lack of development.”). Supp.3d 594, 607 (E.D. Pa. 2025) (quoting *Berman v. Freedom Fin.*

Network, 30 F.4th 849, 856 (9th Cir. 2022)), it is Plaintiffs who have conceded their assent to the Terms of Use, which expressly incorporate the Privacy Notice.

Thus, the unassailable conclusion is that Plaintiffs agreed to Defendants' Privacy Notice in addition to their Terms of Use, thereby giving Defendants permission to use the third-party tracking technologies. At least as currently alleged and argued, consent is dispositive of Plaintiffs' ECPA, WESCA, and invasion of privacy claims.¹⁹ iii. Breach of Fiduciary Duty The remaining issue to be addressed is whether Plaintiffs have sufficiently alleged a fiduciary duty.

That claim is premised on the assertion that Defendants failed to protect and maintain the confidentiality of insureds' personal health information. A fiduciary duty is the "highest duty implied by law," requiring "a party to act with the utmost good faith in furthering and advancing the other person's interests." *Yenchi v. Ameriprise Fin., Inc.*, 161 A.3d 811, 819- 20 (Pa.

2017). Under Pennsylvania law, the elements of a breach-of-fiduciary-duty claim are: (1) the existence of a fiduciary relationship; (2) that the defendant negligently or intentionally failed to act in good faith and solely for the plaintiff's benefit; and, (3) that the plaintiff suffered 19 The Court also notes that, even if the Amended Complaint did not establish consent, Plaintiffs' argument that they never had "any opportunity to review, much less affirmatively understand and consent to, [the Privacy Notice]" incorrectly implies that actual knowledge is a prerequisite to assent.

To the contrary, Internet users can also assent to website agreements under an inquiry notice theory where: "(1) the website provides reasonably conspicuous notice of the terms to which the consumer will be bound; and (2) the consumer takes some action, such as clicking a button or checking a box, that unambiguously manifests his or her assent to those terms." *Berman*, 30 F.4th at 856 (citations omitted); accord *Specht v. Netscape Comms.*

Corp., 306 F.3d 17, 35 (2d Cir. 2002) ("Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility."); *Popa*, 52 F.4th at 132 (observing that "prior consent" under the WESCA does not require actual knowledge and, instead, "can be demonstrated when the person being recorded knew or should have known that the conversation was being recorded" (internal brackets omitted) (citing *Commonwealth v. Byrd*, 235 A.3d 311, 319 (Pa.

2020))). Thus, as a purely legal matter, Plaintiffs' argument is partially nonresponsive because it treats actual knowledge as a necessary condition of assent rather than as a sufficient one. an injury caused by the defendant's breach of its fiduciary duty. *Marion v. Bryn Mawr Tr. Co.*, 288 A.3d 76, 88 (Pa. 2023) (citing *Snyder v. Crusader Servicing Corp.*, 231 A.3d 20, 31 (Pa.

Super. 2020)). The parties dispute the first prong: whether Defendants owed Plaintiffs and other Cigna insureds a fiduciary duty.²⁰ A fiduciary duty is imposed “only where the attendant conditions make it certain that a fiduciary relationship exists.” *Yenchi*, 161 A.3d at 820 (citing *Leedom v. Palmer*, 117 A. 410, 412 (Pa. 1922)).

For some relationships, such as an attorney-client or guardian-ward relationship, the duty is imposed as a matter of law. *Id.* Insurer-insured relationships fall outside that categorical rule. See *id.* at 819 (“[U]nder Pennsylvania law, typically the insurer/insured relationship is viewed as an arm’s-length relationship and fails to create a fiduciary duty.”); see also *Slapikas v. First American Title Ins.*

Co., 298 F.R.D. 285, 293 (W.D. Pa. 2014) (“The general rule in Pennsylvania is that insurers do not owe consumers a fiduciary duty.”). So, in this case, Plaintiffs argue that a duty arose by virtue of a fact-specific “confidential relationship,” where “the circumstances make it certain the parties do not deal on equal terms” either because there is “an overmastering influence” on one side or a “weakness, dependence or trust, justifiably reposed” on the other.

Yenchi, 161 A.3d at 820 (citing *Frowen v. Blank*, 425 A.2d 412, 416-17 (Pa. 1981)). What defines a confidential (or fiduciary) relationship “cannot be reduced to a particular set of facts or circumstances.” *Id.* But, at a minimum, the relationship must go beyond “mere reliance on superior skill” or “an arm’s-length consumer transaction” and instead reflect that one party has ceded decision-making control to the other.

Id. at 823 (citing 20 Defendants also argue that Plaintiffs fail to allege that they suffered an injury caused by the breach of a fiduciary duty. This contention, however, merely recasts their argument on standing’s particularity requirement. It is unsuccessful for the reasons stated above. *eToll, Inc. v. Elias/Savion Advertising, Inc.*, 811 A.2d 10, 23 (Pa.

Super. 2002)). Plaintiffs argue that by entering medical information on Defendants’ website, they relinquished control over how that information would be handled, which they posit gave rise to a fiduciary relationship. Defendants respond that several courts have rejected a similar argument, and they further suggest that, as a matter of law, ceding control over private information cannot create a confidential relationship.

But the cases they cite are nonprecedential and, in any event, do not actually reflect such a rule. In *Zimmerman v. Highmark, Inc.*, the court rejected a breach-of-fiduciary duty claim that was predicated solely on the existence of an insurer-insured relationship. 780 F. Supp.3d 588, 596 (W.D. Pa. 2025).

Here, by contrast, Plaintiffs argue that Defendants owed them a duty because of a confidential relationship. If anything, *Zimmerman* supports Plaintiffs’ position. The court acknowledged that a fiduciary relationship could exist even in an “insurer-insured setting,” and it granted plaintiffs

leave to amend so they could “plead additional facts to support the existence of a fiduciary relationship.” *Id.* That reasoning affirms Plaintiffs’ point that fact- specific circumstances created a confidential relationship with Defendants.

Defendants also rely on *Perloff v. Transamerica Life Insurance Co.*, 393 F. Supp.3d 404 (E.D. Pa. 2019). In that case, the plaintiff sued her insurer for mishandling a nonpayment notice, arguing she had a confidential relationship with the insurer because it “held itself out as guard keeper of its policyowner’s private personal and sensitive information by including affirmative promises and representations about protecting the [p]laintiff’s privacy.” *Id.* at 411.

But she failed to go one step further by alleging she ceded decision-making authority over her private information, so the court dismissed her fiduciary duty claim. *Id.* Accordingly, *Perloff* is a straightforward application of the confidential relationship standard to specific allegations; Defendants err by reading the decision to mean that ceding decision-making control over one’s private information is legally insufficient to create a confidential relationship.

Accordingly, Plaintiffs’ breach-of-fiduciary-duty claim will not be dismissed. See *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005) (“The defendant bears the burden of showing that no claim has been presented.” (citing *Kehr Packages, Inc. v. Fidelcor, Inc.*, 926 F.2d 1406, 1409 (3d Cir. 1991))). An appropriate order follows. BY THE COURT: S/ WENDY BEETLESTONE
_____ WENDY BEETLESTONE, C.J.