UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re ALLSTATE and ARITY *consumer privacy litigation*	Master Docket No. 25 CV 407 Judge Jeremy C. Daniel

MEMORANDUM OPINION AND ORDER

This matter is before the Court on the defendant insurance and technology companies' motion to dismiss the complaint. In this putative class action, the plaintiff insurance consumers allege that the defendants surreptitiously acquired detailed information tracking the plaintiffs' phone location and use. They further allege that this information was sold or used to make decisions concerning the plaintiffs' insurance coverage and premiums, resulting in coverage denials or higher premiums. For the reasons stated and as outlined in this order, the defendants' motion is granted in part and denied in part.

BACKGROUND

The following facts are derived from the complaint[1] and taken as true for purposes of the present motion. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The plaintiffs are thirty-nine individuals who purchased auto insurance. (R. 46 ¶¶ 17—376.)[2] Defendants Allstate Insurance Company (AIC), Allstate Vehicle and Property

[1] The operative complaint is the "Corrected Consolidated Amended Complaint." (R. 46.) The Court refers to it simply as "the complaint."

[2] For ECF filings, the Court cites to the page number(s) in the document's ECF header unless citing to a particular paragraph or other page designation is more appropriate.

Insurance Company ("AVPIC"), and The Allstate Corporation ("AllCorp") (collectively "Allstate") "sell vehicle insurance policies to individual consumers." (*Id.* ¶¶ 2.) Defendants Arity LLC, Arity 875, LLC, and Arity Services, LLC (collectively "the Arity Defendants") are technology companies that "are subsidiaries of and owned by" AllCorp. (*Id.* ¶ 3.) At a high level, the plaintiffs allege that the defendants used a software development kit (SDK) to track the plaintiffs' movements and phone usage and then used this information to make insurance coverage and rate decisions. (*Id.* ¶¶ 1–2.)

According to the complaint, the defendants paid owners of certain third-party applications ("apps") to install the SDK within those apps. (*Id.*¶ 6.) These apps include Drivewise—which is owned by Allstate, and other apps that require location information to function properly. (*Id.* ¶¶ 419, 423–27.) Once installed on the plaintiffs' phones or vehicles via these third-party apps, the SDK would collect certain real-time data, such as "geolocation, route history, driving schedule, fuel or charging levels, phone usage, hard braking events, hard acceleration events, tailgating, time spent idle, speeds over 80 miles per hour, vehicle speed, average speed, late night driving, [and] driver attention." (*Id.* ¶¶ 1, 5.) The SDK also "harvested additional identifying information, including first and last name, phone number, address, zip code, mobile ad-ID ('MAID'), and device ID." (*Id.*¶ 8.)

This information was transmitted to the defendants in real time. (*Id.* ¶ 455.) The defendants used the information "to make insurance coverage decisions for consumers who sought vehicle insurance," "sell this data to other insurers, enabling

those insurers to make their own coverage decisions," and "to decide whether to market insurance products to individual consumers, how much to increase a consumer's insurance premium or whether to provide them with insurance at all." (*Id.* ¶ 14.) However, the SDK "had no way to reliably determine whether a person was driving at the time" and recorded data as driving data even when a plaintiff, for example, "was a passenger in a bus, a taxi, or a friend's car." (*Id.* ¶¶ 435–38.) As a result, the plaintiffs "faced adverse insurance outcomes, such as denied coverage, increased rates, dropped coverage, and excessively high quotes." (*Id.* ¶ 457.) The plaintiffs allege that they did not consent to this collection and use. (*Id.* ¶¶ 444–54.)

The plaintiffs, on behalf of themselves and other similarly situated, allege a litany of claims—thirty-eight in total—against the defendants under federal law and the laws of twenty states. The claims allege violations of laws concerning wiretapping, consumer fraud, credit reporting, deceptive trade practices, and various state common law claims. The defendants move to dismiss all claims.

LEGAL STANDARD

"[A] motion to dismiss for failure to state a claim tests the sufficiency of the complaint . . . ." *McReynolds v. Merrill Lynch & Co., Inc.*, 694 F.3d 873, 879 n.4 (7th Cir. 2012). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The Court "construe[s] the complaint in the light most favorable to the plaintiffs, accepting as true all well-pleaded facts, and drawing reasonable inferences in the plaintiffs' favor." *McReynolds*, 694 F.3d at 879. "Where a complaint pleads facts that

are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of 'entitlement to relief.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557).

ANALYSIS

I. INCORPORATION BY REFERENCE

Before addressing the defendants' arguments for dismissal, there is the threshold issue of whether the Court may consider certain materials extrinsic to the complaint. In support of their motion to dismiss, the defendants filed as exhibits "(1) relevant Privacy Policies, Terms and Conditions and/or Terms of Use for the mobile applications ('Apps') referenced in the Complaint (collectively, 'App Agreements'), and (2) mobile phone screenshots showing the user registration screens related to those Apps and typical permission screens presented to users by their smartphone's iOS or Android system ('User Flows')." (R. 62 at 1.) The defendants move for the Court to hold that these materials are incorporated by reference into the complaint. (R. 62.)

When ruling on a motion to dismiss under Rule 12(b)(6), the Court ordinarily considers only the complaint and its attached exhibits. *Burke v. 401 N. Wabash Venture, LLC*, 714 F.3d 501, 505 (7th Cir. 2013). However, "the incorporation-by-reference doctrine provides that if a plaintiff mentions a document in his complaint, the defendant may then submit the document to the court without converting defendant[s'] 12(b)(6) motion to a motion for summary judgment." *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690 (7th Cir. 2012). It is meant to prevent a plaintiff from "evad[ing] dismissal under Rule 12(b)(6) simply by failing to attach to his complaint a document that proved that his claim had no merit." *Tierney v. Vahle*,

304 F.3d 734, 738 (7th Cir. 2002). Accordingly, the Court may also consider "documents that are attached to the complaint, documents that are central to the complaint and are referred to in it, and information that is properly subject to judicial notice." *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013). But Courts "caution[] against inclusion of tenuously connected materials supplied by [d]efendants." *See Polley v. Nw. Univ.*, 560 F. Supp. 3d 1197, 1205–06 (N.D. Ill. 2021) (collecting cases).

The defendants argue the Court should consider the App Agreements because the plaintiffs "affirmatively allege that they 'reviewed the prominent information about the nature and function of the'" apps at issue, (R. 62 at 2 (quoting, *e.g.*, R. 46 ¶ 27)), and because those agreements are central to deciding whether the plaintiffs consented to those functions (*Id.*). They likewise argue that the Court should consider the User Flows based on the complaint's repeated allegations that they "'did not consent' to the collection and use of their personal data," and the User Flows establish the steps of the user registration process where they would have consented. (*Id.* at 3 (quoting, *e.g.*, R. 46 ¶ 16).) The plaintiffs counter that these materials are central only to the defendants' potential affirmative defense, not to the complaint, and that there are too many factual issues to dispose of the case based on these documents at this stage. (R. 67 at 1–2.)

The Court withholds judgment on whether the documents are central to the complaint. The complaint contains thirty-eight different causes of action, and the legal nuances vary from claim to claim. For some, the consent issue is an element of

the claim; for others, it is an affirmative defense. (*See* R. 61-2 (Defendants' "Summary of How Consent Arguments Apply Across Counts").) In any event, the Court agrees with the plaintiffs that considering the defendants' proposed exhibits at this stage would be premature.

The plaintiffs identify factual disputes with the proposed exhibits, such as whether they were the versions in effect at the relevant times and whether each of the plaintiffs actually took the steps necessary to accept those terms. (*See* R. 67 at 8–8.) The defendants' response is to shift the burden to the plaintiffs, arguing "they omitted necessary detail[and] unfairly disadvantaged [d]efendants and this Court." (R. 70 at 8.) That may be true, but at this stage, the plaintiffs are entitled to all reasonable inferences. *White v. Keely*, 814 F.3d 883, 887–88 (7th Cir. 2016). Presuming the proposed exhibits' authenticity and relevance inverts this requirement.

This approach is consistent with the cases the defendants cited in their argument on centrality. For example, the defendants cite *Rodriguez v. ByteDance, Inc.*, No. 23 C 4953, 2025 WL 672951 (N.D. Ill. Mar. 3, 2025), where they say the court "*granted* the defendant's motion to incorporate by reference." (R. 70 at 6 (emphasis in original).) There is only one problem: the court in *Rodriguez* did *not* grant that motion. Though the court did conclude that "the requirements for incorporation by reference have been met," it negated this conclusion in the very next paragraph. *Rodriguez*, No. 23 C 4953, 2025 WL 672951, at *2–3. The court continued, "Even so, whether plaintiffs waived their rights to bring suit based on their alleged consent . . . is an

affirmative defense that cannot be resolved via this Rule 12(b)(6) motion." *Id.* at *3. It explained that "several outstanding questions prevent[ed] a determination, as a matter of law, that the attached [policies] 'conclusively establish[ed] consent.'" *Id.* (quoting *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020)); *see also In re TikTok, Inc. In-App Brower Priv. Litig.*, No. 24 C 2110, 2024 WL 4367849, at *8–9 (N.D. Ill. Oct. 1, 2024) (denying motion to incorporate by reference because factual issues surrounding the relevant time period and steps needed to accept the privacy policy precluded reviewing the exhibits).

Finally, the defendants claim, "At minimum, [the p]laintiffs must replead to properly allege the predicate facts they themselves admit are required to determine what each individual [p]laintiff agreed to and when," (R. 70 at 10), but they cite no authority for this requirement. *See United States v. Cisneros*, 846 F.3d 972, 978 (7th Cir. 2017) ("We have repeatedly and consistently held that perfunctory and undeveloped arguments, and arguments that are unsupported by pertinent authority, are waived.") (citation modified). The defendants' motion for incorporation by reference is therefore denied.

II. DISMISSAL

A. Rule 9(b)

The defendants' first argument for dismissal is that the complaint does not provide the level of detail required by either Rule 8 or 9(b). (R. 61 at 5–8.) The first issue here is the relevant standard. Rule 8 is the general pleading standard, requiring only "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Rule 9(b) is an exception; it imposes a heightened

standard, requiring that "the circumstances constituting" allegations of "fraud" or "mistake" be "state[d] with particularity." Fed. R. Civ. P. 9(b); *Lachmund v. ADM Inv. Servs., Inc.*, 191 F.3d 777, 783 (7th Cir. 1999) ("It is a special pleading requirement that contrasts significantly with the general standard enunciated in Rule 8.").

"Rule 9(b) applies to 'averments of fraud,' not claims of fraud, so whether the rule applies will depend on the plaintiffs' factual allegations." *Borsellino v. Goldman Sachs Grp., Inc.*, 477 F.3d 502, 507 (7th Cir. 2007); *see also Kahn v. Walmart Inc.*, 107 F.4th 585, 601–02 (7th Cir. 2024). "A claim that 'sounds in fraud'—in other words, one that is premised upon a course of fraudulent conduct—can implicate Rule 9(b)'s heightened pleading requirements." *Borsellino*, 477 F.3d at 507. This includes allegations of deceptive conduct. *Vanzant v. Hill's Pet Nutrition, Inc.*, 934 F.3d 730, 738 (7th Cir. 2019).

Here, Rule 9(b)'s heightened pleading standard applies because the complaint sounds in fraud. This is not a close call because the complaint directly alleges fraud. Specifically, regarding the California plaintiffs' claims under the California Unfair Competition Law ("UCL"), the complaint alleges, "[the d]efendants violated, and continue to violate, the 'fraudulent' prong of the UCL because they failed to inform [the plaintiffs] that [the d]efendants were collecting their Personal Data, or purported to do so in a manner so misleading, confusing, deceptive, and opaque that no reasonable consumer would have understood the extent of the Personal Data collection." (R. 46 ¶ 662; *see also id.* ¶ 445.) The complaint includes similar allegations at several other points. (*See, e.g.*, *id.* ¶ 693 ("[The d]efendants engaged in . . . deceptive

acts and practices . . . by . . . [r]epresenting that goods or services have characteristics that they do not have . . . ."); *id.* ¶ 704 ("[The d]efendants engaged in . . . deceptive trade practices in the conduct of its business . . . , including . . . [r]epresenting that goods or services have characteristics that they do not have . . . ."); *id.* ¶ 760 ([The d]efendants engaged in . . . deceptive acts and practices in . . . [o]mitting, suppressing, and concealing the material fact that [the d]efendants were intercepting, collecting, using, and selling [the plaintiffs'] data to third parties . . . ."). It also alleges the defendants' "knowing and active concealment" tolls the statute of limitations, (*id.* ¶ 468), further confirming that the complaint sounds in fraud.

Smith v. Google, LLC, 735 F. Supp. 3d 1188 (N.D. Cal. 2024), a case from the Northern District of California that the plaintiffs cite in support, is distinguishable. There, even though the complaint alleged Google "misrepresented its true intent" in receiving data, the complaint did not sound in fraud because the plaintiffs were "directly challenging Google's alleged data collection rather than challenging any potentially fraudulent or misleading representations about this collection." *Id.* at 1198. The plaintiffs in this case are challenging both the defendants' data collection and their representations about the collection. Therefore, Rule 9(b)'s heightened pleading standard applies.

Though Rule 9(b) does apply, the Court disagrees with the defendants' arguments that the complaint falls short of that standard. The defendants argue the complaint is insufficient under Rule 9(b) because it "fail[s] to include any particularized allegation that their own personal data was disclosed to third parties,

much less used to make underwriting decisions." (R. 61 at 26 (emphasis omitted).) However, Rule 9(b) does not require that all allegations in the complaint be stated with particularity, only "the circumstances constituting fraud or mistake." Although "Rule 9(b) requires that the circumstances constituting fraud be stated with particularity, it does not require factual pleadings that demonstrate the probability of wrongdoing." *Appvion, Inc. Re. Sav. & Emp. Stock Ownership Plan v. Buth*, 99 F.4th 928, 945 (7th Cir. 2024) (quoting *Loreley Fin. No. 3 Ltd. v. Wells Fargo Sec., LLC*, 797 F.3d 160, 174 (2d Cir. 2015)). The circumstances constituting the fraud are the defendants' alleged misrepresentations and the plaintiffs' actions based on those misrepresentations, not the alleged later disclosure and use of the plaintiffs' personal data. *See Windy City Metal Fabricators & Supply, Inc. v. CIT Tech. Fin. Servs., Inc.*, 536 F.3d 663, 668 (7th Cir. 2008). The complaint need only "plead sufficient facts to notify each defendant of [its] alleged participation in the scheme." *See Sindelar v. Essig*, No. 25 C 7991, 2026 WL 93123, at *3 (N.D. Ill. Jan. 13, 2026) (quoting *Goren v. New Vision Int'l, Inc.*, 156 F.3d 721, 726 (7th Cir. 1998)). Because the complaint achieves this, the Court disagrees with the defendants' argument for dismissal under Rule 9(b).

B. Rule 8

Next the Court turns to whether the complaint satisfies Rule 8. Under Rule 8(a)(2), "A pleading that states a claim for relief must contain . . . a short and plain statement of the claim showing that the pleader is entitled to relief . . . ." The defendants argue the complaint are too vague and conjectural to provide sufficient notice under Rule 8 because it pleads only "hypothetical scenarios in which data

might be gathered and where disclosures *might* occur and *could* affect insurance pricing," not "that *their own data*—rather than theoretical or aggregated data—was improperly collected, disclosed, and used." (R. 61 at 23, 26.) In other words, the defendants argue that plaintiffs do not plausibly allege their claims.

The complaint alleges the defendants integrated the SDK into their own app as well as several third-party apps, which the complaint lists, some of which the defendants paid to have installed. (R. 46 ¶¶ 405, 419.) It further alleges the SDK, once installed on a device through an integrated app, "siphons, collects, and diverts in real time substantial amounts of data concerning users." (*Id.* ¶ 406.) Each of the named plaintiffs allege that they downloaded and used at least one of the SDK-integrated apps.[3] Accepting these allegations as true, and making all reasonable inferences in the plaintiffs' favor, it is plausible that the defendants collected the plaintiffs' personal data. If the SDK collects and diverts the substantial amounts of personal data alleged, and the defendants paid third parties to install the SDK in their apps, it is reasonable to infer that the defendants did use the SDK to collect personal data. It is also reasonable to infer that the defendants monetized the data to earn a return on their investment.

The cases the defendants cite in support are not persuasive. *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117 (S.D. Cal. 2023), involved a third-party program installed on a hospital website that allegedly "collected patients' sensitive health and

[3] (R. 46 ¶¶ 18, 27, 36, 45, 54, 64, 73, 82, 91, 100, 109, 118, 127, 136, 145, 155, 164, 173, 182, 191, 201, 210, 219, 228, 237, 246, 255, 265, 275, 285, 295, 305, 314, 323, 332, 341, 351, 360, 369.)

personal information from [the hospital's] appointment scheduling page and shared it with [the third party]." *Id.* at 1121. The court found the allegations "conclusory and devoid of any factual support" because the plaintiffs failed to provide any facts supporting the allegation that their own personal data was collected and disclosed. *Id.* at 1123. There is no similar deficiency here; the plaintiffs allege that the SDK collects all manner of personal data regardless of how one uses the device, (R. 46 ¶¶ 7–10), and they each allege that they downloaded an SDK-integrated app. Likewise, *B.K. v. Eisenhower Medical Center*, 721 F. Supp. 3d 1056 (C.D. Cal. 2024), which the defendants cite for the same assertion, is also unpersuasive. And the decision by another court in this district in *Kurowski v. Rush System for Health*, 683 F. Supp. 3d 839 (N.D. Ill. 2023), required more detail because the claim dealt specifically with individual identifiable health information, *id.* at 843, which is not true here. The Court therefore rejects the defendants' arguments for dismissal under Rule 8.

C. Failure to Plead Lack of Consent

Next, the defendants argue for dismissal because the complaint fails to plead lack of consent in three ways: (1) the allegations "*sound* like a lack of consent, but are not"; (2) the plaintiffs admit that all but one of them consented because they "reviewed the prominent [app] information"; and (3) the plaintiffs incorporated the terms and conditions, which show that they consented. (R. 61 at 26–27.) For the reasons discussed above, the Court rejects the third argument and addresses only the first two.

There are two problems with the defendants' remaining arguments. First, as noted above, consent is an element of some claims, but an affirmative defense for

others. And "courts should usually refrain from granting Rule 12(b)(6) motions on affirmative defenses" unless "all relevant facts are present." *Brownmark Films, LLC*, 682 F.3d at 690. Second, the complaint sufficiently alleges a lack of consent to survive a motion to dismiss. The defendants point to allegations in the complaint that the plaintiffs "downloaded and used [the relevant apps]," "reviewed the prominent information about the nature and function of the apps," "[were] not provided *meaningful* notice" of data collection and sharing, and "[were] unaware that *Allstate and Arity's SDK* had been integrated into the apps." (R. 61 at 9 (quoting R. 46) (emphases in original).) According to the defendants, this falls short of alleging that the plaintiffs "did not know or were not on notice that they consented to the collection and use of their data." (*Id.*) The plaintiffs counter that the complaint neither concedes consent nor needs to address the issue at this stage. (R. 66 at 23–24.)

Regardless of whether it needs to, the complaint adequately pleads lack of consent to survive a motion to dismiss. It alleges that "neither [the d]efendants nor the apps . . . informed [the p]laintiffs . . . of the various ways that [the d]efendants would collect, use, and ultimately monetize the Personal Data collected." (R. 46 ¶ 446.) The complaint provides several examples of apps and the warnings they provided. The Life360 app requested permission to access users' location and motion sensor data to support the app's functions, and it also warned, "your location data will be used in accordance with our Privacy Policy and your preferences which may include sharing with third parties for purposes such as research, tailored advertising, and analytics." (*Id.* ¶ 447.) Similarly, the Fuel Rewards app requested location

information "to help find the best gas prices near you" and warned that "[w]e will also share or disclose your location with third parties, including or business partners as described in our privacy policy, to provide you with personalized offers." (*Id.* ¶ 448.) Read in the plaintiffs' favor, these warnings represented that the plaintiffs' data would be used for only operational, marketing, and advertising purposes, not for adjusting their insurance premiums. And because the Court is not considering the privacy policies referenced in these warnings, the question of whether those policies provided adequate notice is an issue for summary judgment. *See In re TikTok, Inc. In-App Browser Priv. Litig.*, No. 24 C 2110, 2024 WL 4367849, at *9.

D. Failure to Allege Harm

The defendants make two arguments attacking the plaintiffs' harm allegations. First, they argue the allegations that the plaintiffs "experienced a substantial increase in insurance premiums compared to the steady and regular increases they would otherwise expect" is improperly pled purely on "information and belief." (R. 61 at 36 (quoting R. 46 ¶ 464).) This is improper, the defendants say, because the complaint does not allege "how much [the plaintiffs] paid in premiums *before* or *after* the alleged misattribution of their data." (*Id.* at 37.) "While a complaint must contain more than a general recitation of the elements for a cause of action, the complaint need not contain every single fact that would support the claim." *See Pruitt v. Par-A-Dice Hotel Casino*, No. 20 C 1084, 2020 WL 5118035, at *3 (C.D. Ill. Aug. 31, 2020) (citing *Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010)); *see also Roldan v. Stroud*, 52 F.4th 335, 339 (7th Cir. 2022) ("[P]laintiffs do not have to recite every detail related to their allegations."). The plaintiffs allege that they suffered

increases in their insurance premiums; there is no requirement that they be any more specific as to the amount. *See Emirates v. Assaf*, No. 20 C 7655, 2023 WL 3172626, at *4 n.5 (N.D. Ill. May 1, 2023) ("A plaintiff is not required to plead the exact amount of its damages.") (citation modified).

Second, the defendants argue that most of the state law claims should be dismissed under the filed rate doctrine.[4] (R. 61 at 38–40.) "In the insurance context, the 'filed rate doctrine' provides that any filed rate, a rate filed with and approved by the governing regulatory agency, is per se reasonable and cannot be the subject of a legal action against the private entity that filed it." 1 Couch on Ins. § 2:33. "Numerous federal district courts have applied the filed rate doctrine to actions against insurers subject to such comprehensive regulation." *Winn v. Alamo Title Ins. Co.*, No. A-09-CA-214-SS, 2009 WL 7099484, at *5 (W.D. Tex. May 13, 2009) (collecting cases). Under this doctrine, courts have dismissed claims that "complain the rates [plaintiffs] were charged were artificially inflated by the improper actions of the defendants." *Id.* at *1, *5–7 (dismissing claims under state deceptive trade practices and antitrust laws); *see also McCarthy Fin., Inc. v. Premera*, 347 P.3d 872, 876 (Wash. 2015) (applying the doctrine where "the court would need to determine what health insurance premiums would have been reasonable for the Policyholders to pay as a baseline for calculating the amount of damages"); *Francese v. Am. Modern Ins. Grp.,*

[4] This argument applies to Counts VII (Alabama), XIII (California), XXI–XXVI (Kentucky, Mississippi, Michigan, New Jersey, and New York), XXVIII (North Carolina), XXIX (Ohio), XXXI (Pennsylvania), XXXV (South Carolina), XXXVI (Texas), and XXXVIII (Washington). (R. 61 at 39 n.12.)

Inc., 383 F. Supp. 3d 336, 341–42 (D.N.J. 2019) (applying the doctrine to allegations that defendants "acted collectively to inflate premiums" via a kickback scheme).

The defendants argue the filed rate doctrine applies because the complaint "challenge[s] *how* insurers calculated their rates." (R. 61 at 40.) The plaintiffs respond that "[t]he claim is not grounded in the rate itself" but instead targets the defendants' conduct, alleging that "but for [the d]efendants' misuse and sale of [the p]laintiffs' Personal Data, the amount charged by their insurer would have been lower." (R. 66 at 36.) The Court agrees with the defendants that this argument is just a difference in semantics. The plaintiffs' allegation is that the defendants inflated their rates by improper means; that is a challenge to the rate. The Court is also not persuaded that this case is similar the Eastern District of Michigan's decision in *Trzeciak v. Allstate Property & Casualty Insurance Co.*, 569 F. Supp. 3d 640 (E.D. Mich. 2021), where the court concluded the filed rate doctrine did not preclude claims that "center[ed] on whether Allstate properly disclosed [certain] rating elements in their contract" rather than whether those elements were lawful. *Id.* at 650. Here, the claim is that the conduct underpinning the rates was unlawful, not just undisclosed. That "implicate[s] 'the reasonableness or propriety of the rate.'" *Id.* (quoting *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 765 (3d Cir. 2009)).

The plaintiffs do, however, request other relief that does not implicate the filed rate doctrine, including statutory damages. Where plaintiffs do not "seek[] damages tied to the amount of an alleged overcharge," such as statutory damages, the doctrine does not apply. *Leo v. Nationstar Mortg. LLC*, 964 F.3d 213, 216 (3d Cir. 2020). The

plaintiffs raise this point in their response brief, (R. 66 at 36–37), but the defendants do not respond to it in their reply, (*see* R. 68 at 18–20.) This constitutes waiver. *Bradley v. Village of University Park*, 59 F.4th 887, 897 (2023) (stating a party "may waive a non-jurisdictional issue or argument . . . by failing to respond in a reply brief to a new argument"). The Court therefore denies the defendants' motion as to any counts discussed in this section where statutory damages are available. To the extent that statutory damages are not available for any counts discussed in this section, the defendants' motion is granted.

E. Preemption of State Law Claims

The defendants next argue that the plaintiffs' state law claims are preempted by the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.* (R. 61 at 40.) FCRA's preemption provision states that it

> does not annul, alter, affect, or exempt any person subject to the provisions of this subchapter from complying with the laws of any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this subchapter, and then only to the extent of the inconsistency.

15 U.S.C. § 1681t(a). The defendants argue that the plaintiffs' state law claims "directly conflict with the FCRA's limited consent requirements," and that the claims against the Arity Defendants are expressly preempted under § 1681t(b)(1)(F). (R. 61 at 41–42.) That section preempts any state "requirement or prohibition . . . relating to the responsibilities of persons who furnish information to consumer reporting agencies." § 1681t(b)(1)(F).

As to the first issue, whether the state law claims conflict with FCRA's limited consent requirements, the defendants argue that "Congress chose *not* to require consumer reporting agencies ('CRAs') to notify and obtain consumer consent before collecting and reporting information [or before sharing reports to third parties for insurance underwriting purposes], but instead only require consent in limited scenarios inapplicable here." (R. 61 at 40–41.) According to the defendants, requiring them to do so under state law creates a conflict with FCRA. (*Id.*) The plaintiffs respond that the claims "are not in conflict with FCRA because they challenge conduct beyond that contemplated by FCRA." (R. 66 at 37.)

The Court agrees with the plaintiffs only in part. The defendants do not identify a provision explicitly preempting notice requirements beyond those enumerated in FCRA. Absent any provision making FCRA's notice requirements exhaustive, additional notice requirements under state law are not "inconsistent" with FCRA. The plaintiffs cite several cases that are persuasive on this point. In *Davenport v. Farmers Insurance Group*, 378 F.3d 839 (8th Cir. 2004), policyholders sued their insurer under Minnesota state law for "collecting and disclosing their personal information without first providing them notice and securing their written authorization." *Id.* at 841. The Eighth Circuit observed that "FCRA does not . . . specifically require insurance companies to notify consumers before obtaining their personal information, nor does it affirmatively permit the procurement of such information without first providing notice to consumers." *Id.* at 843 (emphasis omitted). The court then "decline[d] to interpret Congress's silence with regard to any

notice requirement to signify its intent to prohibit states from enacting their own regulations on the issue." *Id.* at 842. A court in the Southern District of New York similarly concluded that FCRA did not preempt "a notice requirement on persons who request consumer information . . . prior to their attaining it," known as a "pre-pull" notice requirement. *Aghaeepour v. N. Leasing Sys., Inc.*, 378 F. Supp. 3d 254, 259 (S.D.N.Y. 2019). FCRA, on the other hand, "imposes notice requirements on users taking adverse actions before taking such actions," known as a "post-pull" notice requirement." *Id.* at 260. Because FCRA "is silent as to whether seekers of credit reports who do not intend to take any adverse actions have pre-pull notice obligations," the court concluded that FCRA did not preempt New York's notice requirement. *Id.* at 260–61. FCRA therefore does not preempt the plaintiffs' state law claims premised on lack of notice because it is not inconsistent with those claims.

However, the Court agrees that FCRA preempts any state law claims against the Arity Defendants based on consent to furnish information. Because "FCRA allows consumer reporting agencies to furnish consumer reports to insurance companies for the purpose of underwriting insurance involving that consumer without first getting the consumer's permission," *Davenport*, 378 F.3d at 843 (emphasis omitted) (citing 15 U.S.C. § 1681b(a)(3)(C)), requiring permission would conflict with FCRA. *See also id.* at 844 ("FCRA permits furnishers of consumer reports to release them to third parties without obtaining consumers' written authorization."). The plaintiffs allege that the Arity Defendants are consumer reporting agencies, (R. 46 ¶ 517), so any state law claims against them based on lack of consent to furnish information are

preempted. The same is not true for Allstate. "The fact that the FCRA does not require consumer reporting agencies to notify insurance consumers that their reports may be examined is irrelevant to the issue of whether states may require insurance companies, as users of the reports, to provide notice before obtaining those reports." *Davenport*, 378 F.3d at 843. The Court therefore finds no conflict preemption as to Allstate.

Moving to the defendants' express-preemption argument, that the state law claims are expressly preempted under 15 U.S.C. § 16881t(b)(1)(F), the Court disagrees with the defendants. Again, that section preempts any state "requirement or prohibition . . . relating to the responsibilities of persons who furnish information to consumer reporting agencies." *Id.* The defendants argue that the state law claims "improperly presume a double standard where furnishers could provide information to the Arity Defendants without consumer consent, but then the Arity Defendants would be prohibited from reporting that information to third parties without consent." (R. 61 at 43.) The plaintiffs respond that "[t]he duties imposed on furnishers . . . concern reporting information the furnisher 'knows or has reasonable cause to believe' is inaccurate, . . . [and] none of [the p]laintiffs' state law claims require as an element that [the d]efendants reported or failed to correct inaccurate information." (R. 66 at 38 (quoting 15 U.S.C. § 1681s-2(a)(1)(A)).)

There is a threshold problem with the defendants' argument. Section 1681t(b)(1)(F) applies to claims "relating to the responsibilities of persons who furnish information to [CRAs]." But the plaintiffs do not allege that the Arity Defendants

furnish information to CRAs; rather, they allege that the Arity Defendants "[a]t all relevant times . . . were [CRAs]." (R. 46 ¶ 517.) "[C]redit reporting agencies are not 'furnishers of information' and therefore, § 1681t(b)(1)(F) does not apply to them." *See Singh v. Discover Bank*, No. 14 C 5496, 2015 WL 1089443, at *8 (N.D. Cal. Mar. 4, 2015). "Section 1681t(b)(1)(F) limits its preemptive effect to . . . the requirements imposed by § 1681s-2," which outline's furnishers' responsibilities when furnishing information to CRAs. *Aargon Agency, Inc. v. O'Laughlin*, 70 F.4th 1224, 1235 (9th Cir. 2023) (citing *Dan's City Used Cars, Inc. v. Pelkey*, 569 U.S. 251 (2013)). It preempts state law claims "against a defendant who happens to be a furnisher of information to a [CRA]" if the claims "also concern that defendant's legal responsibilities as a furnisher of information under the FCRA." *Id.* (quoting *Galper v. JP Morgan Chase Bank, N.A.*, 802 F.3d 437, 446 (2d Cir. 2015)). This provision is therefore "limited to entities that furnish information to consumer reporting agencies, and does not apply to consumer reporting agencies themselves." *See Shannon v. Equifax Info. Servs., LLC*, 764 F. Supp. 2d 714, 727 n.9 (E.D. Pa. 2011); *see, e.g.*, *Aleshire v. Harris, N.A.*, 586 Fed. App'x 668, 671 (7th Cir. 2013) (holding that § 1681t(b)(1)(F) preempts claims against furnisher to CRA); *Todd v. Franklin Collection Serv., Inc.*, 694 F.3d 849, 851 (7th Cir. 2012) (same). Because the complaint alleges the Arity Defendants were themselves CRAs, not furnishers, § 1681t(b)(1)(F) does not preempt the state law claims against the Arity Defendants.

F. Wiretapping Claims

1. Federal Wiretap Act (Count I)

a. The "Party Exception"

Count I is a claim under the Federal Wiretap Act (FWA), 18 U.S.C. § 2510 *et seq*. According to the complaint, the defendants "intercepted, in real time, contemporaneously, and as it was transmitted, the contents of electronic communications transmitted within and from [the p]laintiffs' mobile devices, and diverted those communications to themselves without consent." (R. 46 ¶ 493.) The defendants argue this count should be dismissed because of the FWA's "party exception" under 18 U.S.C. § 2511(2)(d) (R. 61 at 43–45.) Under that section, it is not unlawful for a person to interception a communication in one of two circumstances: (1) "where such person is a party to the communication"; or (2) "where one of the parties to the communication has given prior consent to such interception." § 2511(2)(d). The defendants argue this case falls within the second circumstance "[b]ecause [the p]laintiffs allege that the Apps consented to the purported disclosures via their integration of the SDK." (R. 61 at 44.)

The plaintiffs counter that the exception does not apply because the defendants "were surreptitious collectors, not intended recipients." (R. 66 at 39.) This misunderstands the defendants' argument. The defendants are not asserting that they were the intended recipients; they assert that the intended recipients consented to the interceptions. If true, the exception applies. The plaintiffs' cited authorities to the contrary are inapposite. Several of those cases concern only state law claims, not the Federal Wiretap Act. *See, e.g.*, *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891

(N.D. Cal. 2023); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021). One of the plaintiffs' cited cases, *Katz-Lacabe v. Oracle America, Inc.*, 668 F. Supp. 3d 928 (N.D. Cal. 2023), supports the defendants' position. The plaintiffs in *Katz-Lacabe* sued Oracle, alleging it collected consumer data from technologies embedded in third-party websites. *Id.* at 935–36. The Court concluded that the exception under § 2511(2)(d) applied: "As Defendant's customers[, the websites,] must have chosen to deploy Oracle's tools on their websites, it necessarily follows that 'one of the parties to the communication'—the websites themselves—gave 'prior consent to such interception.'" *Id.*at 945. In other words, because the consumers and websites were parties to the communications, and the websites consented to Oracle's interceptions, the exception applied.

That is the case here. The plaintiffs allege the defendants "developed software to embed in third-party apps that require consumers to communicate location data." (R. 46 ¶ 402.) They also allege that the defendants "have paid third-party app developers millions of dollars to integrate the Arity SDK into their respective mobile apps." (*Id.* ¶ 419.) The communications allegedly intercepted are between the plaintiffs and third-party apps, and the plaintiffs allege an agreement between the defendants and the third-party apps to intercept those communications. Accordingly, one of the parties to the communication—the third-party apps—consented to the interception, and the exception under § 2511(2)(d) applies.

The plaintiffs' citation to the Ninth Circuit's decision in *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020), is of no help. There the

Ninth Circuit, relying on decisions from the First and Seventh Circuits, concluded "that simultaneous, unknown duplication and [transmission of intercepted communications] do not exempt a defendant from liability under the party exception." *Id.* at 608. However, the Court does not find the Ninth Circuit's reasoning persuasive. The Ninth Circuit relied in part on the Seventh Circuit's decision in *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). But the cited portions of that case delt with the question of whether an "interception" occurred at all, not the party exception. *See id.* at 703–07. The same is true for the First Circuit case that the Ninth Circuit relied on. *See In re Pharmatrak, Inc. Priv. Litig.*, 329 F.3d 9, 21–22 (1st Cir. 2003); *see also Kurowski v. Rush Sys. for Health*, 659 F. Supp. 3d 931, 937 (N.D. Ill. 2023) (finding the Ninth Circuit's decision unpersuasive for the same reasons).

However, that is not the end of the analysis. The plaintiffs also argue that the party exception does not apply because the interceptions were "for the purpose of committing [a] criminal or tortious act in violation of the Constitution or laws of the United States or of any State." (R. 66 at 40–42 (quoting § 2511(2)(d)).) They argue this "crime/tort" exemption to the exception applies because "the further use of the intercepted data was in violation of the right to privacy." (R. 66 at 42.) Courts interpreting this exemption apply it only where there is "a criminal or tortious act that is independent from the intentional interception." *See Allen v. Midwest Express Care, Inc.*, No. 24 C 5348, 2025 WL 2240253, at *2 (N.D. Ill. Aug. 6, 2025); *see, e.g.*, *Doe 1 v. Chestnut Health Sys., Inc.*, No. 24 C 1475, 2025 WL 1616635, at *12 (C.D. Ill. June 6, 2025); *Riganian v. LiveRamp Holdings, Inc.*, 791 F. Supp. 3d 1075, 1091 (N.D.

Cal. 2025). Courts differ, however, on whether the exemption applies where, as the defendants put it, the defendants "did what they did for business purposes, *i.e.*, *to make money*." (R. 61 at 45.)

The Court agrees with the plaintiffs that a monetary motive does not foreclose the crime/tort exemption. The Court is particularly persuaded by the reasoning of another court in this district in *Stein v. Edward-Elmhurst Health*, No. 23 C 14515, 2025 WL 580556, at *6 (N.D. Ill. Feb. 21, 2025). There, the court focused on the phrase, "purpose of committing any criminal or tortious act" and observed that "[t]he placement of 'criminal or tortious' . . . modifies 'act,' not 'purpose.'" *Id.* Accordingly, "[t]he purpose must be to commit an act, and that act must be criminal or tortious." *Id.* "A desire to commit a crime *qua* crime, or a tort *qua* tort, isn't necessary." *Id.* "The 'act' must be criminal or tortious, but the 'purpose' does not need to be criminal or tortious." *Id.* The *Stein* court also observed, and this Court agrees, that "[t]he existence of a financial motivation (on the one hand) and a criminal or tortious motivation (on the other hand) are not mutually exclusive. After all, lots of crimes and torts are money-makers." *Id.* The Court therefore concludes that the crime/tort exemption applies so long as the interception is intended to further an act, separate and apart from the interception, which happens to be criminal or tortious.

That is the case here. One example is the plaintiffs' allegation under Count III that, after intercepting their communications, the Arity Defendants furnished the intercepted information to third parties and therefore "knowingly and willfully engaged in the . . . production of inaccurate data metrics" in violation of the Fair

Credit Reporting Act (FCRA). (R. 46 ¶ 524.) As discussed below, the plaintiffs state a claim under the FCRA, and this satisfies the crime/tort exemption. This means Count I cannot be dismissed under § 2511(2)(d).

b. Failure to Plead Elements

The defendants argue that the complaint fails to plead the elements of an FWA claim for three reasons. First, they argue that the complaint alleges use of a tracking device, which is excluded from the definition of an "electronic communication." (R. 61 at 45–46 (citing 18 U.S.C. § 2510(12)(c)).) The FWA imposes liability for, among other things, intercepting an "electronic communication," § 2511(1)(a), (c)–(e), which "does not include . . . any communication from a tracking device," § 2510(12)(c). A "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." § 3117(b). According to the defendants, "The Apps built with the Arity SDK—coupled with the hardware capabilities of the smartphones in which they are installed—render Plaintiffs' phones 'tracking devices.'" (R. 61 at 45.)

The case law the plaintiffs cite recognizes that cell phones do fall within the definition of "tracking devices" insofar as they transmit real-time location information. *See In re Application of the U.S. of Am. for an Ord. Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 577 (D. Md. 2011) (footnote omitted) ("[C]ell phones, to the extent that they provide prospective, real time location information, regardless of the specificity of that location information, are tracking devices."); *In re Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 756 (S.D. Tex.

2005) ("It would surely make no sense to impose the wiretap requirements upon a pen/trap application merely because the cell phone can be used to intercept live conversations; it makes no more sense to impose the tracking device requirements for access to other types of cell phone communications unrelated to physical location."). The plaintiffs argue, however, that the complaint "described the massive amounts of data [the d]efendants intercept, beyond location data." (R. 66 at 46.)

The complaint alleges that the defendants collected "telemetric information about trip distance, trip duration, phone usage, driver attention, acceleration, hard braking, and GPS coordinates," as well as:

> a. a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;
> b. how a user interacts with their device including whether the user locks and unlocks their phone;
> c. whether the phone is in the user's hand;
> d. the amount of time the user spends using the app in which it is embedded;
> e. "Trip attributes," which includes information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;
> f. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone;
> g. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and
> h. Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, Mobile Advertising ID ("MAID"), device type, app version, and OS version.

(R. 46 ¶¶ 410–11.) Nearly all of this information tracks location with different degrees of specificity. The only possible exceptions are the information concerning phone

usage and driver attention, and those described above in paragraphs b–d and h. These categories would allow the FWA claim to proceed.

Second, the defendants argue that the complaint "fail[s] to allege that the data purportedly intercepted constitutes 'content,' *i.e.*, '[any] information concerning the substance, purport, or meaning' of a communication." (R. 61 at 46 (quoting § 2510(8)).) The weight of authority supports the defendants' argument. Though the Seventh Circuit has not, other circuits have had the opportunity to examine the "content" requirement, and "[t]he touchstone of each decision has been that the 'content' of a communication is the substance that the speaker intended to communicate, and does not include automatically generated 'record' data—for example, information about a telephone call's origination, length, and time." *See Vasil v. Kiip, Inc.*, No. 16 C 9937, 2018 WL 1156328, at *2 (N.D. Ill. Mar. 5, 2018). "[D]ata that is incidental to the use of a communication device and contains no 'content' or information that the parties intended to communicate" is not considered "content" under the FWA. *See United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009). This is because the "data is generated automatically, rather than through the intent of the user, and therefore does not constitute 'content' susceptible to interception." *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). Accordingly, "record information regarding the characteristics of the message that is generated in the course of the communication" is not "content." *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).

In addition to the data described above, the complaint alleges that the defendants collected "information about the mobile device on which the app is installed, like IP addresses, browser and device information, user IDs, geolocation data, and other data," which the defendants used in conjunction with personal identifiable information to "fingerprint" the plaintiffs. (R. 46 ¶ 412.) Most of the information described is data that is either generated automatically in the course of using a device or likely stored. This includes the IP addresses, device information, and geolocation data. However, some of the information may reflect communications between users' devices and third-party websites or applications. *See, e.g.*, *Saleh*, 562 F. Supp. 3d at 518 (concluding that real-time keystrokes and website interactions constitute "contents"). This may include browser information and user IDs. These allegations too permit the claim to proceed.

Third, the defendants argue that the complaint "fail[s] to plead allegations showing that the contents of their communications were 'intercepted' contemporaneously during their 'transmission.'" (R. 61 at 47–48.) This is because "the Arity SDK is inherent to the App and collects data in real time, and not by *intercepting* any information." (R. 61 at 48.) In support, the defendants cite *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001), which concluded that a website's sending to a third party information a consumer entered on its website did not constitute an interception because the consumer "sent his information to [the defendant] electronically; [and the defendant] did not gain access to [the consumer's] computer in order to obtain the personal information at issue." *Id.* at 1271–72. That

is not the situation here. The plaintiffs allege that their communications were between them and the third-party applications, not between them and the defendants. The fact that the defendants allegedly accomplished this interception using a tool embedded in the applications themselves does not change this fact.[5] *See, e.g.*, *Szymuszkiewicz*, 622 F.3d at 703–07 (concluding that placing an auto-forwarding rule on an email system constituted an interception). Alternatively, the defendants argue "the Arity SDK within the App receives the purportedly disclosed information and then separately discloses it to [the d]efendants, [which] is not a 'contemporaneous' interception." (R. 61 at 48.) The Court sees no difference between the Arity SDK, which is the defendants' tool, receiving the information, and the defendants receiving the information.

The upshot here is that none of the defendants' arguments, either individually or in combination, completely defeat the plaintiffs' FWA claim. This means the claim may proceed. *See BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015). For this reason, the defendants' motion to dismiss Count I is denied.

2. Analogous State Law Claims (Counts XI, XIV, XIX, & XXXIV)

The defendants move to dismiss the claims under analogous state wiretapping statutes, Counts XI (California), XIV (Florida), XIX (Illinois), and XXXIV (Pennsylvania), for the same reasons. (R. 61 at 48–49.) The defendants acknowledge

[5] The Court notes that the complaint alleges the "[d]efendants also harvested additional identifying information, including first and last name, phone number, address, zip code, mobile ad-ID ('MAID'), and device ID (together, 'Identity Information.)." (R. 46 ¶ 8.) The Court cannot discern from the complaint whether the Arity SDK takes this category of information from communications with third-party applications or from static device storage.

that the state claims track the FWA except for the fact that they are from two-party consent states. (R. 66 at 46–47 (citing *Brown v. Google, LLC*, 685 F. Supp. 3d 909, 937 n.33 (N.D. Cal. 2023); Fla. Stat. § 934.03(3); 720 ILCS 5/14-2(a)(3); 18 Pa. Stat. § 5704(4)).) This distinction does not affect the Court's ultimate conclusions. Accordingly, the Court denies the defendants' motion to dismiss Counts XI, XIV, XIX, and XXXIV.

3. California's Pen Register Statute (Count XII)

The defendants' sole argument for dismissing Count XII, the claim under California's pen register statute, Cal. Penal Code. § 638.51, is that the plaintiffs consented to the collection. (R. 61 at 50.) For the reasons discussed *supra* Section II.C of this order, the Court denies the defendants motion with respect to Count XII.

G. Computer Hacking (Counts II, IX, & XXXII)

The defendants address the computer hacking related claims collectively: Count II under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, *et seq.*, Count IX under California's Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, and Count XXXII for unlawful use of computer under Pennsylvania law, 18 Pa. Cons. Stat. § 7611. (*Id.* at 50–53.) Their first argument for dismissing these counts is, again, that the plaintiffs consented to the conduct. (*Id.* at 51–52.) For the reasons discussed *supra* Section II.C of this order, the Court rejects this argument. The defendants' remaining arguments address only Counts II and IX, (*see id.* at 51–52), so the Court denies the defendants' motion to dismiss Count XXXII.

With respect to the CFAA (Count II) and CDAFA (Count IX) claims, the defendants argue the "[p]laintiffs separately fail to allege 'damage' or 'loss.'" (*Id.* at

52.) According to the defendants, the plaintiffs' alleged damages do not constitute "damage" or "loss" under these statutes because they do not include "any impairment in the integrity of their data or devices," nor do they include "any monetary costs 'responding to a violation' or consequential damages 'because of interruption of service.'" (R. 61 at 52 (quoting *Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1174 (11th Cir. 2017)).

The plaintiffs do not advance a theory that they suffered "damage"; rather, they argue they suffered "loss." (R. 66 at 49.) In this context, "'loss' has been defined to encompass costs related to fixing a computer, lost revenue, or other consequential damages incurred due to an interruption of computer services." *See Rodriguez*, No. 23 C 4953, 2025 WL 672951, at *6 (quoting *Pratt v. Higgins*, No. 22 C 4228, 2023 WL 4564551, at *9 (N.D. Cal. July 17, 2023)). The complaint contains no allegations of any such loss. The plaintiff points to examples of loss such as lost time, expenditure of investigative and remedial resources, and increased litigation costs. (R. 66 at 49.) But each of these can be traced back to some interruption in service. Additionally, courts have rejected the theory advanced by other plaintiffs, which the plaintiffs here argue, that "the loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data" constitutes "damage" or "loss" in this context. *See, e.g.*, *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021); *Nowak v. Xapo, Inc.*, No. 20 C 3643, 2020 WL 6822888, at *4–5 (N.D. Cal. Nov. 20, 2020). Because the complaint does not plausibly allege "loss" or "damage," the Court grants the defendants' motion to dismiss Counts II and IX.

H. Fair Credit Reporting Act (Count III)

Count III is a FCRA claim against the Arity Defendants. (R. 46 ¶¶ 514–528.) The crux of this claim is that the Arity Defendants willfully reported inaccurate information concerning the plaintiffs' driving behavior in violation of FCRA.

The defendants first argue that this claim fails because the plaintiffs do not identify any inaccuracy in their credit reports, and that any such allegation is conclusory. (R. 61 at 54–55.) "Courts have long understood that, when it comes to the FCRA, 'accurate' means more than just 'technically correct.'" *Chaitoff v. Experian Info. Sols., Inc.*, 79 F.4th 800, 812 (7th Cir. 2023). FCRA "requires a showing that the information the data furnisher provided was (1) patently incorrect, or (2) materially misleading, including by omission." *Frazier v. Dovenmuehler Mortg., Inc.*, 72 F.4th 769, 776 (7th Cir. 2023). "Materially misleading" means "misleading in such a way and to such an extent that it can be expected to adversely affect credit decisions." *Id.* (quoting *Gorman v. Wolpoff & Abramson, LLP*, 584 F.3d 1147, 1163 (9th Cir. 2009)). The complaint alleges that the Arity Defendants reported information that "is prone to errors, does not correctly report Driver Data, [and] provides no context for certain Driver Data." (R. 46 ¶ 524(b).) This is based on, for example, the allegation that the defendants "collected and reported data as reflecting an individual's driving behavior even when the individual was riding as a passenger in a motor vehicle, or even riding a roller coaster." (*Id.* ¶ 11.) First, this is not conclusory. Second, the allegation that reports purported to reflect individuals' driving behavior—but omitted the important context that they were not driving—certainly falls within the definition of "misleading." And it is not difficult to see how this could negatively impact an auto-

insurer's decision-making. For these reasons, the complaint sufficiently alleges an inaccuracy.

Second, the defendants argue the plaintiffs "do not plead that they were injured *as a result* of any alleged inaccuracies." (R. 61 at 56.) "Negligent violations [of FCRA] expose companies to 'actual damages,' while willful violations may result in punitive or statutory damages." *Aldaco v. RentGrow, Inc.*, 921 F.3d 685, 689 (7th Cir. 2019) (citation modified). A bare procedural violation of FCRA does not alone establish an injury sufficient to sustain a claim. *Crabtree v. Experian Info. Sols., Inc.*, 948 F.3d 872, 879 (7th Cir. 2020) (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342–43 (2016)). "An FCRA violation may inflict pecuniary harm, like lost income or out-of-pocket expenses caused by denials of credit, housing, or insurance," or "[n]onpecuniary harms, including reputational damage and emotional distress." *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1194 (7th Cir. 2021). "[T]he consumer must also show that [the consumer] suffered injury as a result of any inaccurate information." *Aldaco*, 921 F.3d at 689. "Without a causal relation between the violation of the statute and the loss of credit, or some other harm, a plaintiff cannot obtain an award of 'actual damages.'" *Id.* (quoting *Crabill v. Trans Union, L.L.C.*, 259 F.3d 662, 664 (7th Cir. 2001)). The plaintiffs allege that they downloaded applications containing the SDK, that Allstate pays the Arity Defendants to aggregate and report that data to Allstate and other insurers, and that insurers use this information in evaluating insurance premiums and coverage. The plaintiffs further allege that they suffered coverage losses, coverage denials, or rate increases

without any preceding driving accident or infraction that could explain the change. This is sufficient to plausibly allege that the alleged FCRA violation caused their harm.

Third, the defendants argue the plaintiffs failed to allege a willful violation. "A willful violation entitles a consumer to actual damages or statutory damages, with punitive damages left to the court's discretion." *Persinger*, 20 F.4th at 1194 (citing 15 U.S.C. § 1681n(a)). "A willful violation is one committed with actual knowledge or reckless disregard for the FCRA's requirements." *Id.* at 1195. "A company recklessly violates the FCRA when it commits 'a violation under a reasonable reading of the statute's terms,' and its erroneous reading '[runs] a risk of violating the law substantially greater than the risk associated with a reading that was merely careless.'" *Id.* (alteration in original) (quoting *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 69 (2007)). In *Killingsworth v. HSBC Bank Nevada, N.A.*, 507 F.3d 614, 624 (7th Cir. 2007), the Seventh Circuit concluded a consumer adequately pled a willful FCRA violation "by alleging that the defendant charged a higher interest rate based on information it should have known was false." *See Johnson v. US Bank Home Mortg.*, No. 20 C 3433, 2020 WL 6801847, at *3 (N.D. Ill. Nov. 19, 2020) (citing *Killingsworth*, 507 F.3d at 623). The plaintiffs have done the same here. They allege that the defendants were aware that the information collected and reported was deficient and therefore misleading. (R. 46 ¶ 524.) This allegation of knowledge is sufficient to allege a willful FCRA violation. For these reasons, the defendants' motion to dismiss Count III is denied.

I. Statutory Consumer Protection Claims

Next, the defendants make several arguments for dismissing the state consumer protection claims. Their first argument addresses the Alabama (Count VII), Indiana (Count XX), Texas (Count XXXVI), Utah (Count XXXVII), Mississippi (Count XXII), and Ohio (Count XXIX) claims. (R. 61 at 57–61.) They argue the plaintiffs "fail[ed] to adequately allege compliance with pre-suit requirements" established by state law. (*Id.* at 57–58.) These include requirements that the plaintiffs provide pre-suit notice (Alabama, Indiana, Texas, and Utah), that the state's attorney general or a court first find the practice "deceptive or unconscionable" (Ohio), or that they first attempt to resolve the claim through a state-approved program (Mississippi). (*Id.*)

The plaintiffs argue, among other things, that these are procedural rules that do not apply to federal courts. (R. 66 at 56–57.) The Court agrees, but for somewhat different reasons. Though the parties characterize the state pre-suit requirements as procedural, they are substantive. They are "imposed only upon a specific class of plaintiffs" and are "rooted in policies very much related to, and to a large extent directly contrary to, the substantive cause of action provided those plaintiffs." *Felder v. Casey*, 487 U.S. 131, 145 (1988) (holding a state notice-of-claim provision applying to suits under § 1983 was substantive). The general rule is that "federal courts applying state law [must] use state substantive law and federal procedural rules." *Sumrall v. LeSea, Inc.*, 104 F.4th 622, 629 (7th Cir. 2024). However, "a valid Rule of Civil Procedure displaces contrary state law even if the state law would qualify as substantive." *Berk v. Choy*, No. 24-440, 2026 WL 135974, at *3 (U.S. Jan. 20, 2026). For example, the Supreme Court has found that Rule 8 "prescribes the information a

plaintiff must present about the merits of his claim at the outset of litigation" and therefore displaces a state requirement to attach an affidavit of merit to a medical malpractice complaint. *Id.* at *3–4. "Unless the Federal Rules single out a claim for special treatment, . . . Rule 8 sets a ceiling on the information that plaintiffs can be required to provide about the merits of their claim." *Id.* The defendants' issue with these state law claims is that the complaint fails to "allege[] proper compliance" with the state requirements. (R. 61 at 58.) At least at the pleadings stage, requiring the plaintiffs to plead around the state pre-suit requirements conflicts with Rule 8, and the Court rejects this argument for dismissal.

The defendants make two additional arguments regarding the state consumer protection claims that largely rehash arguments raised earlier in their brief. First, they argue that the plaintiffs fail to allege actual harm sufficient to support the fifteen of the state unfair or deceptive trade practices statutes.[6] (R. 61 at 59–61.) The Court rejects this argument for the reasons discussed previously in this order. *See supra* Section II.D ("The plaintiffs allege that they suffered increases in their insurance premiums; there is no requirement that they be any more specific as to the amount."). Second, they argue that the complaint fails to satisfy Rule 9(b)'s heightened pleading standard.[7] (R. 61 at 61–63.) The Court also rejects this argument for the reasons

[6] This argument applies to the following counts: VII, VIII, XIII, XV, XVI, XVIII, XXI, XXII, XXV, XXVI, XXIX, XXX, XXXIII, XXXV, & XXXVII. (R. 61 at 59.)

[7] This argument applies to the following counts: VII, VIII, XIII, XV, XVI, XVIII, XX–XXX, XXXIII, & XXXV–XXXVIII. (*Id.* at 62.)

discussed *supra* Section II.A of this order. The Court therefore denies the defendants' motion to dismiss those counts discussed in this section.[8]

J. Remaining Privacy Tort Claims (Counts IV–VI, X, XXVII, & XXXI)

Moving to the defendants' arguments for dismissing the privacy tort claims, the Court first addresses Count XXVII, the claim under New York's Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, N.Y. Gen. Bus. Law §§ 899-aa, 899-bb. The defendants argue that the SHIELD Act does not provide a private right of action. (R. 61 at 65.) The plaintiffs do not respond to this argument. (*See generally* R. 66.) This constitutes waiver, and Count XXVII is dismissed. *See Bradley*, 59 F.4th at 897; *accord In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 471 n.7 (S.D.N.Y. 2022) ("New York's Shield Act . . . neither . . . creates [n]or implies a private right of action . . . .").

Next, the Court addresses the defendants' arguments for dismissing the invasion of privacy and intrusion upon seclusion claims (Counts IV–VI & XXXI). The Court first notes that, although the defendants' section headings for this argument include Count VI, the unjust enrichment claim, (R. 61 at 63; R. 46 ¶¶ 554–62), the defendants' do not include any argument providing a basis for dismissing this claim. (*See* R. 61 at 63–66.) The Court therefore denies the motion to dismiss Count VI.

The defendants make the same arguments for dismissing the Illinois Invasion of Privacy claim (Count IV), the Illinois Intrusion Upon Seclusion claim (Count V),

[8] The defendants also move to dismiss Count XVII, the claim for recovery of litigation expenses under Georgia's deceptive trade practices act. (R. 61 at 66.) Because the Court does not dismiss the underlying claim, Count XVI, the Court also declines to dismiss Count XVII.

the California Invasion of Privacy claim (Count X), and the Pennsylvania Invasion of Privacy claim (Count XXXI). (*Id.* at 63–65.) They argue that each of these claims fail because the complaint does not allege that the defendants' intrusion was "highly offensive" or that they violated the plaintiffs' "reasonable expectation of privacy." (*Id.*) Each claim requires proof of these elements.[9] The Court has no trouble concluding that the plaintiffs sufficiently allege that the defendants violated their reasonable expectation of privacy. They allege that the defendants recorded detailed location tracking information, and the plaintiffs have a reasonable expectation of privacy in such information. *See, e.g.*, *Carpenter v. United States*, 585 U.S. 296, 310 (2018) ("[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [a cell-site location information].").

As for whether the intrusion was "highly offensive," meaning "sufficiently serious and unwarranted so as to constitute an egregious breach of the social norms," *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606 (citation modified), the Court cannot resolve this issue at this stage. "While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable," taking into consideration "factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and

[9] *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004) (Illinois Intrusion Upon Seclusion and Invasion of Privacy); *Spinks v. Equity Residential Briarwood Apartments*, 90 Cal. Rptr. 3d 453, 485 (Cal. Ct. App. 2009) (California Invasion of Privacy); *W. Glob. Lending Servs., LLC*, No. 24-6726, 2025 WL 1534967, at *6 (E.D. Pa. May 28, 2025) (Pennsylvania Invasion of Privacy; collecting Pennsylvania state cases).

whether countervailing interests or social norms render the intrusion inoffensive." *Id.* This is a fact-intensive inquiry that is typically inappropriate at the motion to dismiss stage, and courts should only dismiss such claims where no reasonable person could consider the alleged intrusion highly offensive. *See Bogie v. Rosenberg*, 705 F.3d 603, 608, 610–14 (7th Cir. 2013). Given the allegations that the defendants, without consent, collected detailed tracking information that was used to increase insurance premiums or deny coverage, the Court cannot conclude at this stage that no reasonable person would consider the alleged conduct highly offensive. The Court denies the motion to dismiss Counts IV, V, and X.

However, the Court reaches a different conclusion for Count XXXI, the claim under Pennsylvania law. Pennsylvania law further defines "highly offensive to a reasonable person" as requiring "sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of ordinary sensibilities." *Pro Golf Mfg., Inc. v. Trib. Rev. Newspaper Co.*, 809 A.2d 243, 247 (Pa. 2002). None of the alleged disclosures are of this character. At worst, the information could stitch together information about an individual plaintiff that might cause shame or humiliation, such as particular locations visited, but there are no allegations to this effect. For this reason, the Court grants the motion to dismiss Count XXXI.

K. Claims Against AllCorp, AIC, AVPIC, Arity 875, & Arity Services

Finally, the defendants make several arguments for dismissing the claims against AllCorp, AIC, AVPIC, Arity 875, and Arity Services. (R. 61 at 67.) They first

argue that the complaint engages in improper group pleading and contains "no facts showing any conduct by AVPIC, Arity 875, nor Arity Services." (*Id.* at 66.) "There is no group pleading doctrine." *See Walgreen Co. v. Peters*, No. 21 C 2522, 2024 WL 50379, at *7 n.8 (N.D. Ill. Jan. 4, 2024). A complaint need only comply with Rule 8 by "provid[ing] sufficient detail to put the defendants on notice of the claims." *See Lattimore v. Village of Streamwood*, No. 17 C 8683, 2018 WL 2183991, at *4 (N.D. Ill. May 11, 2018). "[A]t some point the factual detail in a complaint may be so sketchy that the complaint does not provide the type of notice of the claim to which the defendant is entitled under Rule 8." *Airborne Beepers & Video, Inc. v. AT & T Mobility LLC*, 499 F.3d 663, 667 (7th Cir. 2007).

The Court already concluded that the complaint complies with Rule 8, *see supra* Section II.B, and it sufficiently alleges how each of these defendants played a role. (*See* R. 46 ¶¶ 2, 380–87.) The complaint also refers to these defendants as parts of collectives, such as the "Allstate Defendants" and the "Arity Defendants," (*id.* ¶¶ 2–3), and it makes allegations attributed to those collectives. This is a permissible practice that puts the defendants on notice of the allegations against them. *See, e.g.*, *Brooks v. Ross*, 578 F.3d 574, 582 (7th Cir. 2009) ("Brooks adequately pleads personal involvement, because he specifies that he is directing this allegation at all of the defendants."). The defendants similarly argue that the "plaintiffs do not allege that certain defendants even *operate* in some of the states in which [the p]laintiffs allegedly were harmed," instead alleging only that AIC and AVPIC operate "throughout the United States." (R. 61 at 67 (quoting R. 46 ¶¶ 78–79).) But this too

is permissible. The allegation that the defendants operate "throughout the United States" plausibly implies that they operate in each of the plaintiffs' states, and the defendants do not cite any authority to the contrary, (*see* R. 61 at 67; R. 68 at 33–34).

Finally, concerning AllCorp specifically, the defendants argue it should be dismissed because the plaintiffs "incorrectly plead that AllCorp 'provides insurance products,'" but AllCorp is actually "a non-operating holding company that does not even have authority to issue, write, or sell insurance products." (R. 61 at 67 (quoting R. 46 ¶ 377).) They cite *Shannon v. Allstate Corp.*, No. 20 C 448, 2021 WL 8083333 (W.D. Tex. May 24, 2021), *report and recommendation adopted*, 2021 WL 8083341 (W.D. Tex. Aug. 6, 2021), which dismissed AllCorp for this reason. However, *Shannon* was in a different posture. The *Shannon* court made that finding as part of a personal jurisdiction analysis under Rule 12(b)(2), *id.* at *5–7, which shifts the burden to the plaintiff and permits the Court to take additional evidence, *see Meynart-Hanzel v. Turner Broad. Sys.*, No. 17 C 6308, 2018 WL 4467147, at *3 (N.D. Ill. Sept. 18, 2018). The defendants are not challenging personal jurisdiction under Rule 12(b)(2), (*see* R. 60 at 1), and they provide no other reason that AllCorp's purported status warrants dismissal. The Court therefore denies the motion to dismiss these defendants.

CONCLUSION

The defendants' motion to dismiss [60] is granted in part and denied in part. The defendants' motion for incorporation by reference [62] is denied. Any amended complaint is due March 20, 2026. The defendants shall answer the operative complaint on or before April 17, 2026.

Date: March 3, 2026

JEREMY C. DANIEL
United States District Judge