IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

| | |
|---|---|
| IN RE: CONSUMER VEHICLE DRIVING DATA TRACKING COLLECTION | MDL DOCKET NO. 3115<br>1:24-md-3115-TWT<br><br>ALL CASES |

**OPINION AND ORDER**

This is a consumer privacy case. It is before the Court on Defendant LexisNexis Risk Solutions Inc.'s ("LNRS") Motion to Dismiss [Doc. 140], Defendant Verisk Analytics, Inc.'s ("Verisk") Motion to Dismiss [Doc. 141], and Defendants General Motors LLC ("GM") and OnStar LLC's (collectively, the "GM Defendants") Motion to Dismiss [Doc. 142]. For the reasons stated below, Defendant LNRS' Motion to Dismiss [Doc. 140] is GRANTED in part and DENIED in part, Defendant Verisk's Motion to Dismiss [Doc. 141] is GRANTED in part and DENIED in part, and the GM Defendants' Motion to Dismiss is GRANTED in part and DENIED in part [Doc. 142].

## I. Background[1]

### A. The Defendants

Defendant GM manufactures and sells vehicles globally. (Am. Compl. ¶ 655 [Doc. 109]). Defendant OnStar is a subsidiary of GM and provides communications, security, emergency services, navigation, diagnostics, and

[1] The Court accepts the facts as alleged in the Amended Complaint as true for purposes of the present Motion to Dismiss. *Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1122 (11th Cir. 2019).

information services to GM vehicles. (*Id.* ¶ 656). Defendant Verisk is a corporation formed to gather statistical data and other information from insurers and report to regulators. (*Id.* ¶ 659). Defendant LNRS is a global data and analytics company that provides data and technology services, analytics, predictive insights, and fraud prevention for a wide range of industries, including the automotive industry. (*Id.* ¶ 658).

**B. The GM Defendants' Acquisition of Customer Driving Data**

In 1996, GM launched OnStar as the automotive manufacturing industry's first embedded telematics[2] system. (*Id.*). From 2010, GM introduced internet connectivity within its vehicles to supplement OnStar's capabilities. (*Id.* ¶ 824). Since 2015, GM has manufactured its vehicles with OnStar hardware and software installed as original, standard equipment in all GM vehicles before distribution to dealerships. (*Id.* ¶ 662). OnStar provides drivers of GM vehicles with a plethora of capabilities, including but not limited to connecting drivers to first responders after an accident, generating vehicle diagnostics, voice recognition technology, integrated steering wheel controls, Bluetooth connectivity, and stolen vehicle failsafe technology. (*Id.* ¶ 663).

From the time that GM marketed its model year 2015 vehicles, OnStar's functionality expanded to collect and transmit the driving data of every

[2] "Telematics" is a term derived from the words "telecommunication" and "informatics." (*Id.* ¶ 661). The word is used to describe vehicle systems that combine Global Positioning System ("GPS") and cellular technologies with onboard electronics to generate and collect data. (*Id.*)

consumer who purchased a GM vehicle. (*Id.* ¶ 664). The driving data collected by the GM Defendants has been used to create detailed profiles on both the cars and their drivers. (*Id.*). With its model year 2015 vehicles, GM also introduced a new OnStar Basic Plan that came free with every purchase. (*Id.* ¶ 826). The OnStar Basic Plan provided drivers with vehicle diagnostic reports, dealer maintenance notifications, and remote start and stop control for five years after their purchase at no additional charge. (*Id.*). With this plan, GM was able to access the driving data of GM consumers for at least five years without interruption. (*Id.*).

Then, to maximize OnStar's ability to harvest customer driving data, GM launched the Smart Driver program in 2016. (*Id.* ¶ 823). Smart Driver was marketed as a new service that provided consumers information about their driving behavior through a "gamified" format. (*Id.* ¶¶ 828-29). GM was able to access more driver information through this program, obtaining data on every instance of "hard braking," "hard acceleration," driving without a seatbelt, driving over 80 miles per hour, and "late night driving." (*Id.* ¶ 833). GM collected this data at every ignition cycle and transmitted it from vehicles to GM's servers using the vehicle's cellular network. (*Id.* ¶ 834).

The GM Defendants were able to collect and process the data acquired by Smart Driver by equipping vehicles with technology that allows them to do so. (*Id.* ¶ 844). Each vehicle is equipped with a number of sensors that work together to gather specific information on the consumer's driving habits. (*Id.*

¶¶ 846-48). The technology within the vehicle then processes this information and transmits it to the GM Defendants through its cellular network connection, some of which is done in "real time" while other information is transmitted only periodically. (*Id.* ¶¶ 849-55). As of 2020, GM boasted that their "Vehicle Intelligence Platform" powers an electronic system capable of managing up to 4.5 terabytes of data processing power per hour. (*Id.* ¶ 845).

### C. The GM Defendants' Use and Sale of Customer Data

#### 1. The Partnership with Verisk

In 2005, GM began utilizing driver data collected by OnStar through a voluntary, opt-in system. (*Id.* ¶ 681). Two years later, OnStar began actively soliciting insurers to partner with them with the intention of creating a centralized exchange for sharing car data with insurers. (*Id.* ¶ 682). Although unsuccessful at the time, GM ultimately partnered directly with several insurers to offer mileage discount plans. (*Id.* ¶ 683).

Sometime later, GM renewed its efforts to create an exchange for sharing its car data. (*See id.* ¶ 697). This time, a number of prominent data vendors were interested in partnering with GM. (*Id.*). After negotiations, GM ultimately contracted with Verisk in order to share its amassed driving data. (*Id.* ¶¶ 695, 697). Pursuant to this agreement, GM sold Verisk the driving data of its customers and routinely funneled the data from its vehicles to Verisk without the vehicle owners' knowledge or consent. (*Id.* ¶ 702). Driving data sold to Verisk included each vehicle's location, speed, trip mileage, hard braking

and acceleration, unique trip identifiers, and other information on how the drivers drove their vehicle each time they drove it. (*Id.* ¶ 703). The driving data sold by GM also included information that permitted Verisk to personally identify each customer, such as each customer's identification number, name, home address, Vehicle Identification Number ("VIN"), vehicle year, vehicle make, vehicle model, OnStar Vehicle Diagnostics ("OVD") enrollment date, and OVD unenrollment date. (*Id.*).

Verisk utilized the information to develop a "Driving Score" for each of the customers and prepared Driving Behavior Data History Reports, which were then sold to auto insurance companies. (*Id.* ¶ 704). Verisk also developed a database called the "Verisk Data Exchange" to store the data. (*Id.* ¶ 705). Verisk marketed and sold licenses to insurance companies to access its exchange. (*Id.*). Verisk was also required by contract to solicit other vehicle manufacturers, telecom carriers, and other third parties who had similar driving data to GM for inclusion in the Verisk Data Exchange. (*Id.* ¶ 711). Verisk then shared part of the revenue gained from the operation with OnStar and paid GM royalties based on revenue generated from the license sales. (*Id.* ¶¶ 705, 710).

By the end of 2016, Verisk anticipated the growth rate of its database to average 5,000 to 6,000 vehicles and 3 million miles a day. (*Id.* ¶ 713). By 2021, Verisk had licensed its exchange to "5 of the top 10 insurers in North America," along with "numerous other midmarket, regional, and [I]nsurtech customers."

(*Id.* ¶ 709). By 2023, Verisk claimed that its database contained information on more than 270 million insured drivers and 270 million registered vehicles, along with 2 billion traffic court records and 500 billion miles of telematics data. (*Id.* ¶ 718). Verisk continues to innovate uses for the driver data within its database and continues to partner with other insurers, vehicle manufacturers, and other interested third parties to expand and improve the Verisk Data Exchange. (*See id.* ¶¶ 722-737).

**2. The Partnership with LNRS**

In 2019, GM sold its consumers' driving data collected between 2017 and 2019 to LNRS, without the consumers' knowledge or consent, in exchange for a multi-million-dollar payment. (*Id.* ¶¶ 742-43). The data provided by GM to LNRS was the same type of data provided to Verisk. (*Id.* ¶ 745). LNRS used this data to compute driving scores for each of GM's customers. (*Id.* ¶ 746). GM continued to funnel such data to LNRS on a routine basis from 2019 to 2024. (*Id.* ¶ 744). In return, LNRS agreed to annually pay GM a guaranteed minimum amount if GM provided LNRS with data from a certain percentage of the vehicles it sold that year. (*Id.* ¶ 746). LNRS further agreed to pay GM additional royalty payments if LNRS successfully contracted with certain specified vehicle manufacturers, based on GM's influence in the vehicle manufacturing industry. (*Id.* ¶ 750).

Like Verisk, LNRS also utilized a database where they charged insurance companies for access to the data provided by GM and other

companies. (*Id.* ¶ 749). Insurance companies would utilize the information provided by LNRS to obtain information about individuals who inquire about car insurance and make decisions accordingly. (*Id.* ¶¶ 749-50). LNRS also used the data to market and deliver Fair Credit Reporting Act ("FCRA") and non-FCRA products and solutions to Insurers. (*Id.* ¶ 751).

Since announcing its partnership with GM, LNRS has contracted with 5 of the top 10 insurers for access to its database, along with 42 percent of the automotive insurance market within the United States, as of 2022. (*Id.* ¶ 752). As of that time, the LNRS exchange had data collected from 10 million vehicles driven over 252 billion miles. (*Id.*).

**3. Other Partnerships**

Over time, GM has also sold billions of miles of customer data to other third parties. (*Id.* ¶ 769). The data sold not only encompassed the driving data of its consumers but also included non-driving data, such as AM/FM frequency, time zone identifiers, radio station call signs, and channel genres. (*Id.* ¶ 771).

GM also used customer driving data for its own purposes. (*Id.* ¶ 786). In November 2020, GM re-launched its auto insurance division as OnStar Insurance. (*Id.* ¶ 787, 790). OnStar Insurance utilized the driving data collected by OnStar to provide a quote for those seeking auto insurance. (*Id.* ¶ 787). OnStar Insurance operated out of thirty-eight states within the United States within 10 months of its introduction. (*Id.* ¶ 790).

### D. Consumer Lack of Notice and Consent

From 2015 on, GM marketed OnStar as a subscription-based service that was provided as part of the sale or lease of certain vehicles. (*Id.* ¶ 877). This included the OnStar Basic Plan, which lasted for five years. (*Id.*). In 2018, Smart Driver was added to the rebranded Basic Plan, which then lasted ten years. (*Id.* ¶ 878). GM would also offer free trials of the paid OnStar plans where, at the conclusion of the trials, customers would automatically be enrolled in the Basic Plan without any notice. (*Id.* ¶ 880).

From 2022 on, GM made OnStar a mandatory part of any GM vehicle purchase. (*Id.* ¶ 881). GM began including a three-year pre-paid OnStar plan within the list price of any GM vehicle. (*Id.*). Customers still had the option not to activate OnStar, but the purchase price included the subscription regardless. (*Id.* ¶ 882). In any case, GM mandated that its partnered dealers activate OnStar for buyers and lessees of cars model year 2015 or newer, imposing penalties when a dealer failed to activate OnStar at the point of sale and financial rewards for those that complied. (*Id.* ¶ 884). This induced many dealers to sign up as many customers as possible, "clicking through screens and agreements without obtaining customer consent, and rushing through the process so that consumers were unable to review any terms that might be applicable to the program." (*Id.* ¶ 885). Accordingly, many customers reported that dealers never took them through any online enrollment process for OnStar

and that they had never heard of Smart Driver. (*Id.* ¶¶ 886-87). GM was aware of such dealer practices. (*Id.* ¶ 890).

In addition, GM customers who personally went through the terms and conditions of OnStar were consistently deterred from declining OnStar and Smart Driver. (*Id.* ¶¶ 896-904). Customers who accessed the terms were confronted with a small box that only showed the first paragraph of the User Terms and the first paragraph of the Privacy Statement, requiring them to alter the window in order to read the whole documents. (*Id.* ¶ 897). Furthermore, customers declining the services were repeatedly displayed misleading messages that declining would result in the deactivation of all OnStar services, despite never accepting the services in the first place. (*Id.* ¶¶ 900-04). When signing up for Smart Driver, GM provided warnings to customers that certain services already provided by OnStar would not be available if they chose not to sign up for the program. (*Id.* ¶ 907-11). Once enrolled, the GM Defendants only allowed a consumer to opt-out of OnStar by calling GM. (*Id.* ¶ 915).

**E. Procedural History**

Several Plaintiffs brought suit against some or all of the Defendants in several districts. On motion to the Judicial Panel on Multidistrict Litigation under 28 U.S.C. § 1407, the panel saw fit to transfer these actions to this Court for centralization and consolidation of related actions across the nation for pretrial proceedings. *See generally In re Consumer Vehicle Driving Data*

*Tracking Litig.*, 737 F. Supp. 3d 1355 (J.P.M.L. 2024). In order to facilitate the pretrial proceedings, the Plaintiffs filed their Master Consolidated Class Action Complaint (the "Amended Complaint"), consisting of 65 causes of action, before this Court. In response, the GM Defendants, Verisk, and LNRS have filed Motions to Dismiss for failure to state a claim. (GM Defs.' Mot. to Dismiss [Doc.142]; Verisk's Mot. to Dismiss [Doc. 141]; LNRS Mot. to Dismiss [Doc. 140]). On September 5, 2025, the Court held oral argument on these Motions to Dismiss. The Court declined to rule from the bench, instead taking the arguments under advisement.

## II. Legal Standards

A complaint should be dismissed under Rule 12(b)(1) only where the court lacks jurisdiction over the subject matter of the dispute. Fed. R. Civ. P. 12(b)(1). Attacks on subject matter jurisdiction come in two forms: "facial attacks" and "factual attacks." *Garcia v. Copenhaver, Bell & Assocs., M.D.'s, P.A.*, 104 F.3d 1256, 1260 (11th Cir. 1997). Facial attacks on the complaint "require the court merely to look and see if the plaintiff has sufficiently alleged a basis of subject matter jurisdiction, and the allegations in his complaint are taken as true for the purposes of the motion." *Id.* at 1261 (citation modified). On a facial attack, therefore, a plaintiff is afforded safeguards similar to those provided in opposing a Rule 12(b)(6) motion. *Lawrence v. Dunbar*, 919 F.2d 1525, 1529 (11th Cir. 1990). "Factual attacks, on the other hand, challenge the existence of subject matter jurisdiction in fact, irrespective of the pleadings,

and matters outside the pleadings, such as testimony and affidavits, are considered." *Garcia*, 104 F.3d at 1261 (quotation marks omitted). On a factual attack, "no presumptive truthfulness attaches to plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the merits of jurisdictional claims." *Scarfo v. Ginsberg*, 175 F.3d 957, 960–61 (11th Cir. 1999) (quotation marks and citation omitted).

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); Fed. R. Civ. P. 12(b)(6). A complaint may survive a motion to dismiss for failure to state a claim; however, even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). In ruling on a motion to dismiss, the Court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff. *See Quality Foods de Centro Am., S.A. v. Latin Am. Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); *see also Sanjuan v. Am. Bd. of Psychiatry & Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff "receives the benefit of imagination"). Generally, notice pleading is all that is required for a valid complaint. *See Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985). Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon

which it rests. *See Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (citing *Twombly*, 550 U.S. at 555).

## III. Discussion

The GM Defendants, Verisk, and LNRS make several arguments in support of their Motions to Dismiss. The Court will address each of the Defendants' arguments.

### A. Shotgun Pleadings

"A shotgun pleading is a complaint that violates either Federal Rule of Civil Procedure 8(a)(2) or Rule 10(b), or both." *Barmapov v. Amuial*, 986 F.3d 1321, 1324 (11th Cir. 2021) (citation omitted). "Shotgun pleadings are flatly forbidden by the spirit, if not the letter, of these rules because they are calculated to confuse the enemy, and the court, so that theories for relief not provided by law and which can prejudice an opponent's case, especially before the jury, can be masked." *Id.* (citation modified). There are four rough categories of shotgun pleadings. *Weiland v. Palm Beach Cnty. Sheriff's Off.*, 792 F.3d 1313, 1321 (11th Cir. 2015).

> The most common type—by a long shot—is a complaint containing multiple counts where each count adopts the allegations of all preceding counts, causing each successive count to carry all that came before and the last count to be a combination of the entire complaint. The next most common type, at least as far as our published opinions on the subject reflect, is a complaint that does not commit the mortal sin of re-alleging all preceding counts but is guilty of the venial sin of being replete with conclusory, vague, and immaterial facts not obviously connected to any particular cause of action. The third type of shotgun pleading is one that commits the sin of not separating into a different count each cause of action or claim for relief.

> Fourth, and finally, there is the relatively rare sin of asserting multiple claims against multiple defendants without specifying which of the defendants are responsible for which acts or omissions, or which of the defendants the claim is brought against. The unifying characteristic of all types of shotgun pleadings is that they fail to one degree or another, and in one way or another, to give the defendants adequate notice of the claims against them and the grounds upon which each claim rests.

*Id.* at 1321-23.

Defendants Verisk and LNRS (the "CRA Defendants") argue that the Amended Complaint is an improper shotgun pleading. (Br. in Supp. of Verisk's Mot. to Dismiss, at 6 [Doc. 141-1]). Specifically, the CRA Defendants argue that the pleading fails to differentiate the factual statements applicable to each count and improperly treats all defendants as a group. (*Id.* at 6-7). The CRA Defendants point to the fact that each of the 65 counts within the Amended Complaint incorporates all 973 paragraphs of factual allegations—over hundreds of pages—without differentiating the factual statements that are applicable to each count, depriving the CRA Defendants of notice. (*Id.* at 6). However, the argument is unpersuasive because the complaint does not contain any "sins" of a shotgun complaint.

Although each count in the Amended Complaint incorporates 973 paragraphs of factual allegations, nowhere in the complaint does each count systematically adopt the allegations contained in a previous count. *See Weiland*, F.3d at 1321. The Amended Complaint does not have conclusory, vague, or immaterial facts, instead properly detailing the factual background

for the Plaintiffs' claims. *Id.* at 1321-22. Each cause of action or claim for relief is separated into separate counts and specifically lists which defendant is liable for each count. *Id* at 1322-23.

The CRA Defendants' ask the Court to look to *Barmapov*, but *Barmapov* is easily distinguishable. (*See* Br. in Supp. of Verisk's Mot. to Dismiss, at 6-7). Although the Eleventh Circuit took issue with the fact that the complaint incorporated and repeated hundreds of paragraphs of factual allegations within the majority of the counts, the Eleventh Circuit did not determine that the pleading was a shotgun pleading on that basis alone. *See Barmapov*, 986 F.3d at 1325. The court specifically found that the pleading was a shotgun pleading because it contained conclusory, immaterial, and vague facts within each count, which the CRA Defendants do not allege here. *Id.* In fact, the Eleventh Circuit specifically went through each category in *Weiland* and found that every other category of shotgun pleading did not apply to the complaint despite the factual section being 249 paragraphs long and realleged in the majority of the complaint. *Id.* Thus, *Barmapov* cuts against the CRA Defendants' argument.

The CRA Defendants also ask the Court to look to *Clifford v. Federman*, 855 F. App'x 525 (11th Cir. 2021), in support of the proposition that treating all defendants as a group within the factual allegations is prohibited. (Br. in Supp. of Verisk's Mot. to Dismiss, at 7). However, *Clifford* is also easily distinguishable because there the Eleventh Circuit's ultimate reasoning met

three of the four categories of impermissible shotgun pleading. *See Clifford*, 855 F. App'x at 529. When the Eleventh Circuit listed the five reasons why the district court did not abuse its discretion, it highlighted that "each cause of action incorporated by reference each and every prior cause of action," "each enumerated cause of action was asserted against multiple defendants," and the plaintiff "essentially accused all defendants of being responsible for all acts and omissions, so that no individual defendant could identify exactly what he or she did wrong." *Id.* None of these categories apply here. Accordingly, the Amended Complaint is not a shotgun pleading.

### B. Wiretap Claims

The Defendants argue that all claims related to the Federal Wiretap Act ("FWA") (Counts 1 and 2) and state wiretap statutes (Counts 14, 23, 25, 30, 35, 38, 41, 43, and 55) should be dismissed. The Court will first address the Federal Wiretap Act claims, then turn to the state wiretap statutes.

#### 1. Federal Wiretap Act (Counts 1, 2)

To state a claim under the FWA, a plaintiff must show 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." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). The FWA authorizes civil damages as a remedy for any person found to have engaged in a violation of the statute. 18 U.S.C. § 2520(a). Accordingly, the Plaintiffs bring forth two claims under the FWA

against Defendants GM, Verisk, and LNRS. (*See* Am. Compl. ¶¶ 974-1011). The Defendants move to dismiss these counts for several reasons. The Court will address each argument in turn.

**a. Electronic Communication**

The Defendants argue that the FWA does not apply because operating a vehicle does not create an "electronic communication" under the meaning of the statute. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 15-17 [Doc. 142-1]; Br. in Supp. of Verisk's Mot. to Dismiss, at 10). They point to the fact that a communication under the FWA requires at least two parties to a conversation and the Plaintiffs alleged that they "did not intend to send any Driving Data to GM–only to themselves," which only alleges a singular party for the communication. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 15-16; Br. in Supp. of Verisk's Mot. to Dismiss, at 10; Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 17 [Doc. 153]).

When engaging in statutory interpretation, "we begin where all such inquiries must begin: with the language of the statute itself." *Republic of Sudan v. Harrison*, 587 U.S. 1, 8 (2019) (citation modified). Under the FWA, any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or *electronic communication*" may be criminally and civilly liable, subject to certain exceptions. 18 U.S.C. § 2511(1)(a) (emphasis added); *see* 18 U.S.C. § 2520. An "electronic communication" is defined as "any transfer of signs,

signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

The Defendants direct this Court to the "party exception" in support of its assertion that an "electronic communication" under the FWA implicitly requires at least two individuals to be communicating. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 15). The "party exception" to the FWA states that "it shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication where such 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).

Indeed, "statutes must be read as a whole" and must not be evaluated in a piecemeal manner. *Territory of Guam v. United States*, 593 U.S. 310, 316 (2021) (citation modified). However, the Defendants are attempting to use an exception to create a rule for the overarching statute in order to effectively reconstruct the meaning of the statute from the ground up. While "electronic communications" can certainly involve two parties, no such requirement is imposed within either the statute imposing liability or within the definition of "electronic communication." *See* 18 U.S.C. §§ 2510(12), 2511(1)(a). "Electronic communication" under the FWA is solely defined as a "transfer" of data. 18 U.S.C. § 2510(12). While the FWA is intentional with its use of "person" or

"entity" throughout the statute, there is no such language present within the definition of "electronic communication." *See Conner v. Tate*, 130 F. Supp. 2d 1370 (N.D. Ga. 2001) (discussing Congress's intentional use of "person" in some parts of the FWA while using "entity" in other parts).

The Eleventh Circuit has also rejected the notion that "electronic communications" must involve at least two individuals and only impliedly requires that there be an origin and a destination. In *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003), a defendant in a criminal proceeding moved to suppress incriminating pictures and videos obtained from an anonymous informant under the FWA, arguing that a Trojan Horse virus that accessed his personal computer and collected evidence was an impermissible wiretap. *Id.* at 1043-44, 1046. As a threshold matter, the Court held that the data intercepted by the informant was an "electronic communication," even though the files remained on the computer prior to the interception, based on a plain text interpretation of the definition of the term. *Id.* at 1047. The Ninth Circuit has also held similarly, finding no requirement that an "electronic communication" must be contemporaneously delivered to an intended recipient. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002) ("Although the website owner's document does not go directly or immediately to the user, once a user accesses a website, information is transferred from the website owner to the user via one of the specified mediums. We therefore conclude that Konop's website fits the definition of "electronic communication.").

Ignoring precedent within the Eleventh Circuit, the Defendants cite *Jurgens v. Build.com, Inc.*, 2017 WL 5277679 (E.D. Mo. Nov. 13, 2017), in support of their proposition that an "electronic communication" requires two parties. However, *Jurgens* is easily distinguishable. In *Jurgens*, the plaintiff used the defendant's website to purchase kitchen plumbing hardware and entered her credit card information into the website to pay for the equipment. *Jurgens*, 2017 WL 5277679, at *1. The defendant allegedly intercepted the information entered into the website through the use of JavaScript commands within the payment page, which disclosed the information to other third parties. *Id.* at *1-*2. The plaintiff argued that her own computer was the intended recipient of her "electronic communications" (the credit card information) and that the defendant violated the FWA by intercepting such communications. *Id.* at *6. The court disagreed, finding that "electronic communications" under the FWA do not include interactions with one's own computer. *Id.*

However, the facts underlying the *Jurgens* court's analysis are largely different than the ones presented here. In *Jurgens*, the plaintiff's interactions with her own computer were for the ultimate purpose of paying the defendant through the defendant's website. *See id.* at *1-2. Such a situation does not exist here. The information acquired by GM was not entered by the Plaintiffs for the purpose of sending the information to GM. Instead, the Plaintiffs used OnStar

and Smart Driver for the purposes of facilitating their own driving experience within the vehicle, as marketed.

The two cases *Jurgens* cites as support for its position, *United States v. Barrington*, 648 F.3d 1178 (11th Cir. 2011), and *United States v. Ropp*, 347 F. Supp. 2d 831 (C.D. Cal. 2004), highlight the difference in facts underlying the *Jurgens* decision. *See Jurgens*, 2017 WL 5277679 at *6. The cite to *Barrington* stands for the proposition that the use of a keylogger would not violate the FWA if the transmission was not contemporaneous at the time the strokes were made. *Id.* The cite to *Ropp* stands for the proposition that internal computer signals sent in order to transmit a message were not "electronic communications." *Id.* Here, the Plaintiffs do allege that GM intercepted the data sent by the consumer contemporaneously. Furthermore, because the information was not intended for transmission to GM, but rather to the OnStar system and Smart Driver program for the Plaintiffs' benefit, *Ropp* and *Barrington* are inapplicable here, as is *Jurgens*. Therefore, the consumer driving data does constitute "electronic communication."

**b. Tracking Device Exception**

Even if the driving data satisfies the definition of "electronic communication," the Defendants argue that the tracking device exception applies, excepting the driving data an "electronic communication" under the FWA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 16; Br. in Supp. of Verisk's Mot. to Dismiss, at 10). Under the FWA, an "electronic communication" does

not include "any communication from a tracking device." 18 U.S.C. § 2510(12)(C). A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). The Defendants argue that, because the Plaintiffs have expressly acknowledged that the telematics control unit ("TCU") within the OnStar system is a tracking device, all signals sent from the TCU are excepted from the definition of an "electronic communication" under the FWA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 16; Br. in Supp. of Verisk's Mot. to Dismiss; *See* Am. Compl. ¶ 1183). The argument is unpersuasive.

The GM Defendants cite *In re App. for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005), as support for its proposition that "no communication from a tracking device can be an electronic communication." (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 16 (quoting *id.* at 759)). However, the case cited by the GM Defendants cuts against the narrow view taken by them. The court, in addressing whether cell site data is tracking information under 18 U.S.C. § 3117(b), stated that although cell site data is tracking information, cell phones are not regarded solely as tracking devices for all purposes, due to their multifunctional use. *In re App. for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 756. The court further stated that a cell phone would not be a "tracking device" when the information sought involves non-tracking information. *Id.*

Similarly, each GM vehicle used by the Plaintiffs tracks location data, but it also tracks a variety of other information from each Plaintiff's driving behavior. (*See* Am. Compl. ¶ 848). Although the Plaintiffs do state that the TCU is a "tracking device" within one paragraph of a 627-page complaint, the Plaintiffs' other allegations show that the TCU does more than track their locations. (*Id.* ¶¶ 848, 1183). The Plaintiffs also allege that the TCU transmits driving data from the vehicle to the GM Defendants. (*Id.* ¶ 848). While the Defendants may avail themselves of the "tracking device" exception with respect to all allegations pertaining to location tracking, every other data point that is not related to location tracking will still be considered "electronic communications."

**c. Contents**

The FWA defines "intercept" as "the aural or other acquisition of *the contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). The Defendants argue that, even if the Plaintiff's data was "electronic communications," it would not qualify as "contents" under the aforementioned statute because the information generated by the vehicle is a record rather than an intended communication to another party. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 17-19; Br. in Supp. of Verisk's Mot. to Dismiss, at 8-9).

"[C]ontents, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Because "substance", "purport", or "meaning" is not defined within the FWA, the Court looks to the ordinary meaning of the statutory language as it was understood at the time the law was enacted. *See United States v. Dawson*, 64 F.4th 1227, 1236 (11th Cir. 2023). This may be done by looking at dictionaries in existence around the time of enactment. *Id.* The FWA was enacted in 1968. 18 U.S.C. § 2510(8) was subsequently amended under the Electronic Communications Privacy Act of 1986 ("ECPA") to include provisions addressing "electronic communications" and removing from the definition of "contents" information pertaining to the identity of the parties as well as the existence of the communication. *See* 18 U.S.C. § 2510(8) (1968). Using a prominent dictionary in existence at the time of enactment, "substance" is defined as "the characteristic and essential part." *Webster's Third New International Dictionary* 2279 (1961). "Purport" is defined as the "meaning conveyed, professed, or implied." *Id.* at 1847. Finally, "meaning" is defined as "the thing that is conveyed or specified [especially] by language." *Id.* at 1399. In effect, "contents" is defined to include any information that deals with the essential elements or meaning conveyed by the communication. *See* 18 U.S.C. § 2510(8).

Here, the data at issue involves granular details of the vehicle's operation. The question then is whether such vehicular data is part of the

essential elements or meaning conveyed of the electronic communication. Because this question is a matter of first impression within the Eleventh Circuit, the Defendants and the Plaintiffs urge the Court to look outside of the Circuit to support their asserted positions.

On one hand, the Defendants ask the Court to treat vehicle operation data like cell phone call or geolocation data because it is not an essential part of the communication made by the Plaintiffs. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 17-18; Br. in Supp of Verisk's Mot. to Dismiss, at 9). Courts generally do not view phone call data, including the phone numbers, the time a call was made, and the length of the phone call, as "contents" under the Wiretap Act because such data is generated automatically and does not arise from the intended communication itself. *See United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009); *see also United States v. Booker*, 2013 WL 2903562, at *6 (N.D. Ga. Jun. 13, 2013) (holding that historical cellular site location does not constitute "contents" under the Stored Communications Act ("SCA"), which directly references the definition found in the FWA). Courts treat geolocation data as outside of the meaning of "contents" within the FWA for similar reasons. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012); *Gonzales v. Uber Technologies, Inc.*, 305 F. Supp. 3d 1078, 1085 (N.D. Cal. 2018).

As tangential support for their position that vehicle data does not constitute "content," the GM Defendants ask the Court to look to the fact that

"every federal appeals or district court . . . has concluded that silent video surveillance is not covered by the [FWA]." (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 18 (quoting *Allen v. Brown*, 320 F. Supp. 3d 16, 38 (D.D.C. 2018)). The GM Defendants utilize this proposition to argue that, if a videotape of the vehicle is not "contents" under the FWA, the vehicle data would not be either.

On the other hand, the Plaintiffs ask the Court to treat the vehicle operation data like the personal information provided in *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003). (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 10). In *In re Pharmatrak*, the defendant created a web tool for pharmaceutical companies that provided website analytics for their respective websites. *In re Pharmatrak*, 329 F.3d at 13. The tool recorded a number of data points related to each user's experience on the website, creating a "user profile" for each visitor. *Id.* at 13-15. However, the defendant also obtained personal information entered into some of the websites because it incorporated form responses by users into subsequent URLs, which the defendant's tool tracked. *Id.* at 16. Information such as the user's name, date of birth and medical conditions were obtained by the defendant in this manner. *Id.* at 18. In considering whether such information constituted "contents" under the FWA, the First Circuit determined that it did because the defendant relied on devices to capture the personal information provided to a third party. *Id.* at 18-19.

Both approaches have glaring errors when applied to the facts of the instant case. First, if the Court accepts the Defendants' treatment of the data,

it is far too reductive to assume that the data conveyed by the Plaintiffs is not essential in any capacity. The information at issue here includes (1) the number of times the consumer used the car, (2) the date each trip was made, (3) each time the consumer exceeded 80 miles per hour within the vehicle, (4) every time the consumer braked hard, (5) each time the consumer rapidly accelerated, (6) how long the consumer drove in the day and at night, and (7) vehicle mileage. (Am. Compl. ¶ 922). The true extent of the data taken in real time will only be uncovered during discovery. However, at the maximum, the intimate nature of the consumers' driving behavior, especially when such data may lead to injury for the consumers, is more central to the notion of it being material or central to the information conveyed through the electronic communication. This is especially true when the communication with the car was intended for the purposes of generating driving information for use by the consumer. Meanwhile, information arising from geolocation and phone call data are more tangential to the purpose of the electronic communication.

The Defendants' video surveillance argument is also misplaced because it misconstrues the "electronic communication" at issue here. A recorded conversation between individuals without audio does show the conduct of the parties, but it does not give insight into the substance of the oral communication between the parties. However, the Plaintiffs here are transmitting "electronic communications," not oral communications. Through operation of their vehicles, the Plaintiffs are actively communicating their

vehicle data with their onboard systems in order to obtain analytics on their driving from their vehicles. The video surveillance analogue is thus unconvincing to the Court.

On the other hand, the Plaintiffs' assertion that *In re Pharmatrak* directly applies is also misplaced. In this action, the Plaintiffs argue that the FWA applies because their "electronic communications" were with themselves through the GM vehicle and not with the GM Defendants. However, the parties involved in the "electronic communication" in *In re Pharmatrak* do involve multiple parties instead of a single party here. The plaintiffs there voluntarily disclosed personal information to another party, which was captured by the defendant through the website URL. *See In re Pharmatrak*, 329 F.3d at 16, 18. The substance of the communication (the form responses) sent to another party was the information that was intercepted by the defendant, which fits squarely into the definition of "contents" within the FWA no matter how the information was captured.

Instead, the Court finds *In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014), instructive in determining the applicable law, but not for the proposition that the Defendants have briefed the Court. In that case, the Ninth Circuit clarified what information constitutes "contents" with regard to "electronic communications," holding that "record information" is excluded from the definition of contents under the FWA. *In re Zynga Privacy Litig.*, 750 F.3d at 1106. "Record information" includes data "regarding the characteristics

of the message that is generated in the course of the communication." *Id.* Meanwhile, "'contents' refers to the intended message conveyed by the communication, and [it] does not include record information." *Id.*

The Court has already explained why the vehicle information here is not analogous to geolocation or phone site data, which fits the definition of "record information" discussed in *In re Zynga Privacy Litig.* Instead, each driver of a GM vehicle is actively communicating his or her driving behavior to the GM vehicle onboard system in order to obtain data regarding his or her driving behavior while driving to a specific destination. While automatically generated during the course of the driver's actions, the driver intends to send a message to the onboard system utilizing the sensors present throughout the car. Therefore, such information is not "record information" and satisfies the definition of "contents" under the FWA.

**d. Interception**

The GM Defendants also argue that the Plaintiffs have failed to identify an "interception" under the FWA within their Amended Complaint. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 19). Specifically, the GM Defendants contend that the Plaintiffs fail to identify where, among the vehicle's computer systems, the GM Defendants intercepted the Plaintiffs' communications and that any interception by the GM Defendants was not done during the contemporaneous transmission of the electronic communications. (*See id.* at 19, 21).

Addressing the GM Defendant's first argument, the Plaintiffs have sufficiently plead where the GM Defendants intercepted their electronic communications. The Plaintiffs clearly specify that it is the TCU of the computer system within the vehicle where the interception occurs and explains the manner in which the interception occurs. (*See* Am. Compl. ¶¶ 851-56). The Plaintiff's explanation of how the data moves through the computer system does not confound an understanding that the ultimate transmission from the TCU to the GM Defendants is the interception at issue. (*See* Am. Compl. ¶¶ 847-50).

The GM Defendants' second argument fails for similar reasons when reading the Amended Complaint. Here, the Defendants properly point the Court to *Steiger* as the applicable precedent in this instant case. There, the Eleventh Circuit adopted a narrow definition of what constitutes an "interception," holding that an interception of an electronic communication must be contemporaneous, or during "flight," in order to implicate the FWA. *See Steiger*, 318 F.2d at 1048-49. The court in *Steiger* further clarified that contemporaneous interception may include all parts of a transmission, including through automatic routing software. *Id.* at 1050. Under the applicable precedent, the Defendants' assertions appear erroneous when examining the Amended Complaint. Specifically, the Amended Complaint states that "[u]pon information and belief, GM, through the TCU, transmits certain Driving Data to itself in real time—for example, data regarding vehicle

location and speed." (Am. Compl. ¶ 854; *see also* Am. Compl. ¶¶ 986-87).[3] Therefore, the Plaintiffs have adequately identified contemporaneous transmissions at the Motion to Dismiss stage.

**e. Party Exception**

The Defendants argue that they are not liable under the FWA because GM was a party to the electronic communication under the "party exception." (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 23; Br. in Supp. of Verisk's Mot. to Dismiss, at 11). In response, the Plaintiffs argue that GM was not a party to the electronic communication and that they were communicating with themselves through the onboard computer systems within their vehicles. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 15; Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 11-12 [Doc. 152]). Ultimately, the crux of the dispute centers on whether it is possible for the Plaintiffs to communicate with themselves to avoid application of the "party exception" under the FWA.

The "party exception" is an exception, not the rule. Although the Plaintiffs generally bear the burden of establishing a violation of the FWA, the Defendants bear the burden of establishing that the "party exception" applies.

[3] Even if the Plaintiffs' allegations within the Amended Complaint are false, that is not an argument the Court will entertain at the Motion to Dismiss stage, because the Court accepts all facts alleged within the Amended Complaint as true when evaluating the Defendants' motion. *See Wilding*, 941 F.3d at 1122. If the interception of driving data was not contemporaneous and more akin to keylogging cases, as the Defendants argue, then the Defendants may present evidence of this fact at a later stage of the litigation for consideration by the Court.

*In re Pharmatrak*, 329 F.3d at 19; *see also United States v. Burke*, 2025 WL 1456757, at *1 (M.D. Fla. May 21, 2025) (reiterating a prior holding within the criminal case that the "party exception" was a defense to a violation of the FWA instead of an element of the offense, shifting the burden on the defense).

In an effort to fulfill their burden, the Defendants urge the Court to adopt the Third Circuit's reasoning in *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125 (3d Cir. 2015). Similar to *In re Pharmatrak*, *In re Google Cookie* involved tracking "cookies" that captured user behavior on certain websites that contracted with Google. *Id.* at 130-31. Visitors to the websites had the choice to enable the "cookies" upon entry, but the defendants abused an exploit that allowed them to still collect user information without their consent. *Id.* at 131-32. The plaintiffs brought suit, in part, under the FWA. *Id.* at 133. On the defendants' Motion to Dismiss, the court confronted the issue of whether the "party exception" applied to Google. *Id.* at 140. Looking to the allegations within the complaint, the court noted that when a user sends a request to the server hosting the publisher's webpage, the server instructs the user's web browser to send a request to Google. *Id.* Thereafter, the users' browsers directly communicate with the defendants. *Id.* Accordingly, the court concluded that Google was a party to the electronic communication because "direct transmissions between the plaintiffs and the defendants" showed that Google was the "intended recipient," whether or not such a request was induced by deceit. *Id.* at 141-42, 143.

In response, the Plaintiffs urge the Court to adopt the Ninth Circuit's reasoning in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020). The Ninth Circuit confronted similar facts to *In re Google Cookie* and determined that the "party exception" does not apply. *Id.* at 608. Acknowledging the Third Circuit's decision, the Ninth Circuit looked to First and Seventh Circuit decisions to conclude that the "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception" and that such defendants were not the "intended recipients" under the "party exception." *Id.*

The Court need not decide which case is more persuasive because the technology incorporated by GM vehicles is entirely different in operation and scheme. While the Court acknowledges that a circuit split does exist with regard to whether the "party exception" applies where a defendant uses GET commands or cookies, the facts underlying the Amended Complaint leave factual questions that must be resolved before deciding whether the "party exception" applies here. The Court thus turns to a review of the underlying technology.

As alleged within the Amended Complaint, GM incorporates an electronic system into each of the vehicles at issue that is capable of processing data information and transmitting any information received. (Am. Compl. ¶ 845). The vehicle itself uses several sensors and other components that detect and record substantial amounts of data concerning vehicle operation and

driver behavior, such as vehicle speed, vehicle acceleration and deceleration, collision detection, seatbelt usage, road conditions, and information from vehicle cameras. (*Id.* ¶ 844, 846). Over 200 sensors within the vehicle are connected to internal processing units, which operate as mini-computers and are referred to as "electronic control units" ("ECUs"). (*Id.* ¶ 847).

ECUs are connected to a central processing unit or central gateway within the vehicle. (*Id.*) Information sent to a gateway from an ECU is then processed and sent to another ECU or TCU. (*Id.* ¶ 848). Information sent between ECUs is used for internal cross-system interactions. (*Id.*). Information sent to the TCU is then sent to GM during routine vehicle operation and upon the completion of vehicle trips. (*Id.* ¶ 851). This outward communication is conducted using cellular networks in the area for internet connectivity to send the data both in real-time and periodically. (*Id.* ¶ 853-55).

Even if the Court assumes, *arguendo*, that *In re Google Cookie* is more persuasive than *In re Facebook*, there are not enough facts available to determine this matter on a Motion to Dismiss. Congressional intent behind the ECPA's amendments to the FWA was to "prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.'" *In re Facebook*, 956 F.3d at 608 (citing and quoting S. Rep. No. 90-1097, *reprinted in* 1986 U.S.C.C.A.N. 2112, 2154, 2182). While the Amended Complaint sheds some light on how the internal computer system works to

send the driving data to GM, it lacks many of the facts available to the court in *In re Google Cookie*.

From the technology perspective, it is unclear whether the TCU sends all information available to the vehicle to GM automatically or whether it selectively parses through the data and sends only certain information. *See In re Google Cookie*, 806 F.3d at 140-41 ("If users' browsers directly communicate with the defendants about the webpages they are visiting . . . then there is no need for the defendants to acquire that information from transmissions to which they are not a party. After all, the defendants would have the information at issue anyway."). Additionally, it is unclear whether any translation of information that occurred along the path from data taken by the sensors to the eventual transmission from the TCU would constitute a "direct transmission" like it expressly does in the case of the technology behind "cookies." *Id.* at 142 ("In short, our understanding of the plaintiffs' allegations is that the defendants acquired the plaintiffs' internet history information when . . . the plaintiffs' browsers sent that information directly to the defendants' servers.").

Furthermore, apart from the technology, the Court lacks information regarding whether the Plaintiffs were able to give effective consent. The Plaintiffs and the Defendants argue over whether consent under the meaning of the FWA can occur in the presence of potential fraud in the inducement of the consent. However, without a clearer picture of the factual scenario

surrounding the consent given by each Plaintiff in this action, it would be improper to dismiss the FWA claims under the "party exception." Therefore, because of the need for discovery to resolve outstanding factual questions, the Court declines to hold that the "party exception" applies at this stage of the litigation.

**f. Use and Disclosure Violations**

As part of their FWA allegations against the Defendants, the Plaintiffs assert violations of 18 U.S.C. §§ 2511(1)(c) and (d). (Am. Compl. ¶¶ 992-93, 1001-02). Under the FWA, it is a violation if a defendant "intentionally *discloses*, or endeavors to *disclose*, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(c) (emphasis added). Additionally, it is a violation of the FWA if a defendant "intentionally *uses*, or endeavors to *use*, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(d) (emphasis added).

The GM Defendants argue that the Plaintiffs fail to adequately allege the intent element of both statutes. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 25). Specifically, the Defendants argue that the Amended Complaint "simply

parrot[s] the language in §§ 2511(1)(c)-(d), which is not enough to state a claim" (*Id.* at 26). The Court disagrees with the GM Defendants' interpretation of the Amended Complaint.

"To be liable under § 2511(1)(c) or § 2511(d), a defendant must know or have reason to know sufficient facts concerning the circumstances of the interception such that the defendant could, with presumed knowledge of the law, determine that the interception was prohibited." *McCann v. Iroquois Mem'l Hosp.*, 622 F.3d 745, 753 (7th Cir. 2010) (quotation marks and citations omitted); *see O'Neill v. Khuzami*, 2022 WL 704696, at *2 n.1 (N.D. Ga. 2022). "It is not enough to know that the [communication] was intercepted; the defendant must also be able to tell that none of the statutory exceptions apply." *McCann*, 622 F.3d at 753 (citation omitted).

Part of the reason the Amended Complaint is 627 pages and thousands of paragraphs long is because the Plaintiffs detail specifically all the facts that show that it is "plausible" for the GM Defendants to have known that their conduct was illegal. First, the Plaintiffs detail the centrality of consumer privacy in the automotive industry, which the GM Defendants participate in. (*See* Am. Compl. ¶¶ 667-80). The Amended Complaint also details the GM Defendants' efforts to create a marketplace of driving data and outlines their financial motivations for doing so. (*Id.* ¶¶ 682-94, 786-91). The Amended Complaint then turns to discuss the Defendants' efforts to conceal their access and use of the driving data. (*Id.* ¶¶ 792-822). Additional facts interspersed

throughout the Amended Complaint also show that GM was aware of the complications that arise from siphoning consumer data and engaged in the conduct anyways. On these facts alone, the Plaintiffs have met their burden within the Amended Complaint to survive this argument of the GM Defendants' Motion to Dismiss.

**2. State Claims (Counts 14, 23, 25, 30, 35, 38, 41, 43, 55)**

The Plaintiffs have also brought claims under analogous state wiretapping statutes arising out of California, Delaware, Florida, Illinois, Maryland, Massachusetts, Nebraska, New Hampshire, and Pennsylvania. The Defendants move for dismissal of these claims from the Amended Complaint. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 26-28; Br. in Supp. of Verisk's Mot. to Dismiss, at 12-17). First, the Defendants contend that the communications alleged by the Plaintiffs are not proper communications under the respective state law wiretapping statutes. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 27-28; Br. in Supp. of Verisk's Mot. to Dismiss, at 14-17). Second, the CRA Defendants argue that the intercepted communications are not "contents" under state law, relying on their arguments under the FWA. (Br. in Supp. of Verisk's Mot. to Dismiss, at 12). Third, the Defendants argue that the "party exception" of the state law wiretapping statutes bar the claims by the Plaintiffs for the same reasons as in their arguments under the FWA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 28; Br. in Supp. of Verisk's Mot. to Dismiss, at 13). Finally, the Defendants argue that the "tracking device

exception" applies to bar the Plaintiffs' claims for relief, as they argued under the FWA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 28; Br. in Supp. of Verisk's Mot. to Dismiss, at 12-13).

The Court has already explained why the Defendants' arguments under the FWA will not succeed on their Motion to Dismiss, and those same conclusions apply to every argument made under the analogous state statutes. The only argument the Defendants make apart from their FWA arguments hinges on the meaning of "communication" under certain state statutes.

The Defendants argue that the driving data recorded by the Plaintiffs' vehicles are not protected communications under the wiretapping statutes of California, Illinois, Maryland, Massachusetts, or New Hampshire. (Br. in Supp. of Verisk's Mot. to Dismiss, at 14; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 27-28 (arguing the same only for New Hampshire and Massachusetts)).[4] The interpretation of every state wiretap statute except for Massachusetts and New Hampshire rely on the existing interpretation of the FWA, inclusive of oral, wire, and electronic communications.[5] Only the state

[4] The GM Defendants also extend their FWA arguments against the driving data being communications under the state statutes within the Amended Complaint where the wiretapping statutes are analogous. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 27); Because the Court has already ruled that the driving data is an "electronic communication" under the FWA, the GM Defendants' arguments fail here as well.

[5] *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act"); *State v. Brinkley*, 132 A.3d 839, 843 (Del. Super. Ct. 2016) ("the federal wiretap statute and Delaware's wiretap statute [are] in all material respects virtually identical") (quotation marks and citation omitted); *People v.*

wiretap statutes for Massachusetts and New Hampshire differ in the fact that they do not contain a mirror provision that prohibits the interception of "electronic communications."[6] Despite this fact and for the sake of completeness, the Court will look to each state's wiretap statute and evaluate whether the driving data is a "communication."

**a. California (Count 14)**

The Plaintiffs who form part of the California subclass (the "California Plaintiffs") bring Count 14 under the California Invasion of Privacy Act ("CIPA") against the Defendants. (*See* Am. Compl. ¶¶ 1151-79). The California Penal Code prohibits:

> [a]ny person . . . who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or *communication* while the same is in transit or passing over any wire, line, or cable, or is being sent

---

*Ledesma*, 206 Ill.2d 571, 579 (2003), *overruled on other grounds by People v. Pitman*, 211 Ill.2d 502, 512-513 (2004) (looking to the FWA to interpret the Illinois wiretap statute); *Ramos v. Delphi Behav. Health Grp., LLC*, 2022 WL 1415856, at *1 (11th Cir. May 4, 2022) ("The Florida Wiretap Act closely follows the Federal Wiretap Act and similarly proscribes intentionally intercepting any wire, oral, or electronic communication and excludes the use of such interceptions and evidence derived from those interceptions in court"); *Sanders v. State*, 57 Md. App. 156, 164 (1984) ("Maryland's present Wiretapping and Electronic Surveillance Act . . . is modeled after its federal counterpart and extensively tracks its provisions") (citation omitted); *Williams v. Raynor Rensch & Pfieffer*, 2015 WL 2127095, at *13 (D. Neb. May 6, 2015) ("The Nebraska Wiretap Act is patterned after its federal counterpart, and so the Court looks to federal law in interpreting its provisions"); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125-26 (3d Cir. 2022) ("[Pennsylvania's Wiretapping and Electronic Surveillance Control Act] also operates in conjunction with and as a supplement to the Federal Wiretap Act").

[6] *See* Mass. Gen. Laws ch.272, § 99(C); N.H. Rev. Stat. §§ 570-A:1(I), 570-A:2(I).

> from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

Cal. Penal Code § 631 (emphasis added).

The CRA Defendants argue that "communication" under CIPA is limited to "a singular conversation or exchange between two or more participants." (Br. in Supp. of Verisk's Mot. to Dismiss, at 14 (citing *Libman v. Apple, Inc.*, 2024 WL 4314791, at *13 (N.D. Cal. Sep. 26, 2024))). Yet, the facts and analysis underlying *Libman* are entirely distinguishable and arguably cut against the position that the CRA Defendants take. In *Libman*, the plaintiffs alleged that the defendant intercepted information from their mobile devices. 2024 WL 4314791, at *13. The court focused on certain information like "what kind of device was used, the device's screen resolution, and the device's keyboard language" *Id.* (quotations omitted). The Court ultimately held that the information was not a "communication" under CIPA because the electronic communication lacked substance compared to scenarios where full-length URLs were disclosed that contained personal information. *See id.* at *13-*14 (distinguishing *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778 (N.D. Cal. 2022, then distinguishing *Brown v. Google LLC*, 685 F. Supp. 3d 909 (N.D. Cal. 2023)).

In holding such, the court understood that CIPA was meant to be a state law analogue to the FWA which was made in response to "advances in science

and technology that have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications." *Id.* at *13 (citation modified) (citing Cal. Penal Code § 630). Keeping this understanding in mind, the Court is unpersuaded that the analysis on whether driving data constitutes an "electronic communication" under the FWA does not apply to CIPA. Therefore, the driving data obtained by GM from the California Plaintiffs contains enough substance to constitute "communication" under CIPA.

**b. Illinois (Count 30)**

The Plaintiffs who form part of the Illinois subclass (the "Illinois Plaintiffs") bring Count 30 under the Illinois Eavesdropping Law against the Defendants. (*See* Am. Compl. ¶¶ 1398-1416). Illinois law states that "[a] person commits eavesdropping when he or she knowingly and intentionally . . . intercepts, records, or transcribes, in a surreptitious manner, any private electronic communication to which he or she is not a party." 720 Ill. Comp. Stat. 5/14-2(a)(3). Illinois defines "private electronic communication" to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 Ill. Comp. Stat.

5/14-1(e). A reasonable expectation is defined by statute to extend to Constitutional limits. *Id.*

The CRA Defendants focus on the latter part of the definition of "private electronic communication" to argue that, because the driving data arises out of publicly observable vehicle operation, the Illinois Plaintiffs do not have a reasonable expectation of privacy under the federal Constitution. (Br. in Supp. of Verisk's Mot. to Dismiss, at 17). In evaluating the CRA Defendants' argument, "[the Court's] lodestar is *Katz*'s reasonable-expectation-of-privacy test." *United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015), *abrogated on other grounds by Carpenter v. United States*, 585 U.S. 296 (2018). *Katz v. United States*, 389 U.S. 347 (1967), asks that two requirements be met for there to be a reasonable expectation of privacy; first, a person must have "exhibited an actual (subjective) expectation of privacy" and second, society is prepared to recognize that expectation as reasonable. 389 U.S. at 361 (Harlan, J., concurring). Both the subjective and objective requirements must be satisfied before a court recognizes that an expectation of privacy is reasonable. *United States v. Robinson*, 62 F.3d 1325, 1328 (11th Cir. 1995).

When applying the *Katz* test to automobiles, it is well-established that information obtained that could be discerned from visual observation of the vehicle on public roads does not constitute an invasion of a reasonable expectation of privacy. *United States v. Jones*, 565 U.S. 400, 412 (2012). However, in this same vein, the Supreme Court has also determined that this

holding is not absolute and there are certain instances where publicly available information may still constitute a search. *See id.* at 404-13. Ultimately, this requires the Court to conduct a fact-specific inquiry that is improper at the Motion to Dismiss stage to determine whether the driving data obtained crosses over into a violation of the reasonable expectation of privacy. The Court does not foreclose the possibility that the CRA Defendants may be correct in that the information collected in real-time does not constitute an invasion of a reasonable expectation of privacy. However, the Court will not, without further discovery, dismiss the Illinois' Plaintiffs claims at this stage of litigation.

**c. Maryland (Count 35)**

The Plaintiffs who form part of the Maryland subclass (the "Maryland Plaintiffs") bring Count 34 under the Maryland Wiretapping and Electronic Surveillance Act ("MWESA") against the Defendants. (*See* Am. Compl. ¶¶ 1491-1521). Maryland law prohibits any person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(1). The state also prohibits the willful disclosure and willful use of any wire, oral, or electronic communication, if the party has reason to know that the information was obtained through a violation of Section 10-402(a)(1). Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(2), (3). MWESA provides a private right of action for any violation of its provisions. Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

The CRA Defendants argue that no substantive message exists within the driving data for MWESA to apply under existing Maryland case law. (Br. in Supp. of Verisk's Mot. to Dismiss, at 15 (citing *Sun Kin Chan v. State*, 78 Md. App. 287, 307 (1989))). However, the argument fails for much of the same reasons as it did under the FWA. Not only is driving data more substantive, but the extent of the driving data alleged by the Maryland Plaintiffs within their Amended Complaint is more intrusive as well. Therefore, the Maryland Plaintiffs' MWESA claim withstands the Motion to Dismiss.

**d. Massachusetts (Count 38)**

The Plaintiffs who form part of the Massachusetts subclass (the "Massachusetts Plaintiffs") bring Count 38 under the Massachusetts Wiretap Act ("MWA") against the Defendants. (*See* Am. Compl. ¶¶ 1550-80). Under the MWA, it is unlawful for any person to "willfully commit[ ] an interception, attempt[ ] to commit an interception, or procure[ ] any other person to commit an interception or to commit an interception of any wire or oral communication." Mass. Gen. Laws ch. 272, § 99(C)(1). A "wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." Mass. Gen. Laws ch. 272, § 99(B)(1).

Because there exists no prohibition against the interception of "electronic communication" in the MWA, the Massachusetts Plaintiffs attempt

to recast their communications as "wire communications." (*See* Am. Compl. ¶ 1558). However, such a characterization runs against Massachusetts case law. In *Vita v. New England Baptist Hospital*, 494 Mass. 824 (2024), the Massachusetts Supreme Court considered whether browsing or similar website interactions fall into the definition of "wire communications" under the Massachusetts wiretap statute. *Vita*, 494 Mass. at 834. The court turned to the legislative history and Massachusetts case law to find that the communications the wiretap act were meant to protect were those involving person-to-person communication. *Id.* at 841, 844-45. Although Vita pointed the court to FWA cases, the court rejected the cases because the amendment that added "electronic communications" to the FWA "was drafted almost twenty years after [Massachusetts'] wiretap act. *Id.* at 846. Ultimately, the court held that the website communications could not be wire communications under Massachusetts law. *Id.* at 848; *cf. Konop*, 302 F.3d at 876 (holding such communications were "electronic communications").

While the Massachusetts Plaintiffs' communications are "electronic communications" under federal law, they are not "wire communications" under the MWA. The communications of the Massachusetts Plaintiffs, in the Plaintiffs' own words, are communications without a second party and not person-to-person, and are thus not protected under Massachusetts law under *Vita*. *See Vita*, 494 Mass. at 848. As the Massachusetts Plaintiffs allege, all communications are directed towards a vehicle and the onboard computer that

resides within the vehicle. Therefore, the Massachusetts Plaintiffs cannot state a claim under the Massachusetts wiretap act.

**e. New Hampshire (Count 43)**

The Plaintiffs who form part of the New Hampshire subclass (the "New Hampshire Plaintiffs") bring Count 43 under the New Hampshire Wiretapping and Eavesdropping Act ("NHWEA") against the Defendants. (*See* Am. Compl. ¶¶ 1660-93). The NHWEA makes it unlawful for an individual to "[w]illfully intercept[ ], endeavor[ ] to intercept, or procure[ ] any other person to intercept or endeavor to intercept, any telecommunication or oral communication." N.H. Rev. Stat. § 570-A:2(I)(a). The NHWEA also considers the knowing disclosure and use of such information to be a violation of the statute. N.H. Rev. Stat. §§ 570-A:2(I)(b)-(d). A "telecommunication" is defined as "the transfer of any form of information in whole or in part through the facilities of a communications common carrier." N.H. Rev. Stat. § 570-A:1(I). A "communications common carrier" is defined as "a person engaged in providing communications services to the general public through transmission of any form of information between subscribers by means of wire, cable, radio, or electromagnetic transmission, optical or fiber-optic transmission, or other means which transfers information without physical transfer of medium, whether by switched or dedicated facilities." N.H. Rev. Stat. § 570-A:1(IX). A "communications common carrier" also includes "any wireless technology that

uses a wireless entry or access point to transmit or receive any form of information." *Id.*

The New Hampshire Plaintiffs attempt to recast their "electronic communications" under the FWA as "telecommunications." (Am. Compl. ¶ 1668). However, unlike the Massachusetts Plaintiffs, the New Hampshire Plaintiffs properly do so. The Defendants, without providing any authority, ask the Court to interpret the definition of "telecommunication" to require a person-to-person interaction. (Br. in Supp. of Verisk's Mot. to Dismiss, at 16; *see* Br. in Supp of GM Defs.' Mot. to Dismiss, at 27-28). However, New Hampshire courts have already held that the NHWEA is broader in protection than the FWA. *See State v. Locke*, 144 N.H. 348, 356. Considering that New Hampshire courts look to federal cases to interpret the NHWEA, *State v. Telles*, 139 N.H. 344, 346 (1995), it follows that the Court must hold that the communications alleged by the New Hampshire Plaintiffs fall under the NHWEA under the analysis provided by the FWA. Therefore, the New Hampshire Plaintiffs' wiretap claim remains.

### C. SCA Claims

The GM Defendants argue that the Stored Communications Act ("SCA") claim (Count 3) and state-level SCA analogous claims (Counts 36, 42, and 56) should be dismissed. The Court will first address the SCA claim, then turn to the state SCA analog claims.

### 1. Stored Communications Act (Count 3)

Under the SCA, it is a violation under the statute for a person to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided" and thereby "obtain[ ], alter[ ], or prevent[ ] authorized access to a wire or electronic communication while it is in electronic storage in such system. 18 U.S.C. § 2701(a). The SCA also provides for a private right of action for any violation of the statute. *See* 18 U.S.C. § 2707.

The GM Defendants make three arguments in support of their Motion to Dismiss the SCA claim. First, the GM Defendants argue that TCUs and ECUs within their vehicles are not "facilities" under the SCA. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 29-31). Second, the GM Defendants argue that the driving data is not in "electronic storage" within the meaning of the SCA. (*Id.* at 31-33). Third, the GM Defendants argue that the SCA's exceptions apply to GM's conduct. (*Id.* at 33-35). The Court will address each argument in turn.

#### a. Facilities

The Plaintiffs state that the ECUs and TCUs of their vehicles are "facilities" under the SCA. (*See* Am. Compl. ¶ 1021; Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 21-23). To violate the SCA, an individual must access a "facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1). An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or

electronic communications." 18 U.S.C. § 2510(15). "Facility" is not defined by the SCA. To fill this gap, the Eleventh Circuit adopts the plain meaning definition that a "facility" includes "the physical means or equipment for doing something." *Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1177 n.4 (11th Cir. 2017) (citing *facility*, Oxford English Dictionary Online, http://www.oed.com/viewdictionaryentry/Entry/67465 (last visited Apr. 16, 2026)). Combining these definitions, the Court understands that the SCA requires there be a physical means or equipment to provide for the sending or receiving of wire or electronic communications for there to be a violation under the statute.

In their Motion to Dismiss, the GM Defendants argue that the ECUs and TCUs cannot be "facilities" because the SCA does not apply to the personal devices of users. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 30 (quoting *Steiger*, 318 F.3d at 1049)). The Fifth Circuit's decision in *Garcia v. City of Laredo, Tex.*, 702 F.3d 788 (5th Cir. 2012), provides important guidance on this issue to the Court.[7]

In *Garcia*, the Fifth Circuit considered whether an individual's computer, laptop, or mobile device fits the statutory definition of "facility." *Garcia*, 702 F.3d at 792. The court, like the GM Defendants, looked to Eleventh Circuit precedent in *Steiger* and determined that the SCA clearly applies to

[7] *See Brown Jordan Int'l*, 846 F.3d at 1177 n.4 (citing *Garcia* in a footnote when addressing the appellee's argument that he did not access a "facility" within the meaning of the SCA).

information stored with a phone company, Internet Service Provider ("ISP"), or electronic bulletin board system but that it does not apply to the hard drive of an individual's personal computer. *Id.*; *see Steiger*, 318 F.3d at 1049. The court went further and reviewed district court decisions across the United States to come to the conclusion that "the relevant 'facilities' that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage." *Garcia*, 702 F.3d at 792 (quoting *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, 2012 WL 3862209, at *9 (S.D. Ohio Sep. 5, 2012) (quotations omitted)).

The Fifth Circuit then turned to the text of the SCA, finding that the statute "envision[ed] a provider (the ISP or other network service provider) and a user (the individual with an account with the provider), with the user's communications in the possession of the provider." *Id.* at 793 (quoting Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215 n. 47 (2004) (quotations omitted)). Finally, the court turned to legislative history to find that legislators were only concerned with "facilities" operated by electronic communications services and made no mention of individual users' computers. *Id.* (quoting *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y 2001)); *see* S. Rep. No. 99-541, at 36, *reprinted in* 1986 U.S.C.C.A.N.

3555, 3590. Ultimately, the Fifth Circuit concluded that an individual's computer, laptop, or mobile device were not "facilities" under the SCA. *See Garcia*, 702 F.3d at 793.

*Garcia* makes it clear that a key inquiry into whether the physical equipment is a "facility" is a matter of control, whether it be by a user or by an ISP or network provider. *Id.* The Third Circuit, using *Garcia* in its decision, and the Ninth Circuit ultimately came to this same conclusion when reviewing the text of the SCA. *See In re Google Cookie*, 806 F.3d at 146-47 ("There is then the language of 18 U.S.C.§ 2701(c)(1), which provides that [the SCA] 'does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communication service.' This makes sense when talking about third-party access to network service providers' own facilities."); *In re Zynga*, 750 F.3d at 1104 ("Title II of ECPA . . . covers access to electronic information stored in third party computers").

Here, as previously mentioned, the Amended Complaint alleges that the ECUs and TCUs within the vehicle are "facilities" under the meaning of the SCA. (Am. Compl. ¶ 1021). The Plaintiffs allege that they are "facilities" because the technology created by GM provides the electronic communication services by which the Plaintiffs can send and receive the electronic communications. (*Id.*). The Amended Complaint also alleges that, while the driving data was within the ECUs and TCUs, GM accessed the devices without

authorization and transferred the information to GM's servers via cellular network. (*Id.* ¶ 1024).

While the Court agrees with the GM Defendants that the Amended Complaint alleges similar facts to the operation of a non-facility personal computer, the Court will not dismiss the federal claim. The question of whether the ECUs and TCUs are "facilities" under the SCA is a question that requires discovery before the Court can make its determination. (*See* Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 22-23). The GM Defendants are correct in noting that courts have routinely dismissed SCA claims for failing to allege a "facility." (Reply Br. in Supp of GM Defs.' Mot. to Dismiss, at 15 [Doc. 165]). However, each of the cases the GM Defendants cite for this proposition are cases where the "user control" inquiry from *Garcia* is easily applicable.[8]

Based on the Amended Complaint, the Plaintiffs, as users, do not exert the same amount of control over the ECUs and TCUs as an individual does

[8] The GM Defendants direct the Court to the cases of *In re Google Cookie*, *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797 (N.D. Cal 2020), *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836 (N.D. Cal. 2017), *aff'd* 956 F.3d 589 (9th Cir. 2020), and *In re iPhone Application Litig.* for the proposition that courts regularly dismiss SCA claims that fail to state a proper "facility." However, two cases involve website browser tracking arising out of the use of a personal computer. *See In re Google Cookie*, 806 F.3d at 130-31; *In re Facebook*, 263 F. Supp. 3d at 840-41. The other two cases involve personal devices. *See In re Google Assistant*, 457 F. Supp. 3d at 809-10; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1049-51. As stated in *Garcia*, there is little dispute that a personal computer is not a "facility" under the SCA because the user is understood to have complete control over the device. *Garcia*, 702 F.3d at 793. The same reasoning applies to other personal devices because the user has control over each system. *See id.* (with respect to cell phones).

over a personal computer or a cell phone. Both devices are found inside the vehicle and are not easily accessible by the Plaintiffs. GM, instead of the Plaintiffs, appears to have control over the functionality of the ECU and TCU based on its ability to activate and deactivate OnStar. (*See* Am. Compl. ¶ 900). Therefore, the Court will not dismiss the SCA claim because the Plaintiffs allege sufficient facts for the ECUs and TCUs to plausibly be "facilities." The necessary facts to make the final determination are likely to be revealed through discovery.

**b. Electronic Storage**

The GM Defendants next argue that the Plaintiffs' driving data is not in "electronic storage" under the meaning of the SCA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 31-33). The pertinent part of the SCA states that an individual who accesses a facility through which an electronic communication service is provided either without authorization or exceeding their authorization and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in *electronic storage* in such system" is in violation of the statute. 18 U.S.C. § 2701(a) (emphasis added). "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Congress has clarified that "temporary,

intermediate storage" within the SCA referred to the storage of a message in transit to an addressee. *See In re DoubleClick*, 154 F. Supp. 2d at 512 (discussing H. Rpt. No. 106-932 (2000), S. Rep. No. 99-541 (1986), and proposed amendments to the ECPA).

The GM Defendants make three arguments for why the Plaintiffs' driving data is not in "electronic storage" under the SCA. First, they argue that the data is not a "communication" under the SCA because there is no intended counterparty. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 32). Second, they argue that the manner by which the driving data is alleged to be stored within the vehicle does not constitute "electronic storage." (*Id.*). Third, the GM Defendants argue that the communications are not stored during "transmission" to an addressee and are therefore not in "temporary, intermediate storage." (*Id.*). None of the arguments are persuasive.

First, the Plaintiffs' driving data is a "communication" under the SCA because it is an "electronic communication" under the FWA. Congress amended the FWA and created the SCA in 1986 through the ECPA to address the interception of electronic communications. *Steiger*, 318 F.3d 1046-47 (citing S. Rep. No. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557). In doing so, Congress also incorporated by reference the definitions that govern the FWA within the SCA, as amended by the ECPA. *See* 18 U.S.C. § 2711(1) ("the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section"). Because the Court has already

held that the Plaintiffs' driving data is an "electronic communication" under the meaning of 18 U.S.C. § 2510(12), the same applies to defeat the GM Defendants' argument here.

Second, the question of whether the Plaintiffs' driving data is found in "electronic storage" is a fact-specific inquiry and cannot be resolved on a Motion to Dismiss. Courts generally agree that data that is temporarily stored on the hard drive of an individual's personal device is not in "electronic storage" under the SCA.[9] While the Plaintiffs' allegations within their SCA claim show an operation that is more similar to the use of personal devices, the inquiry does not end automatically even if the Court decides to treat the vehicles as personal devices. *See In re Toys R Us,* 2001 WL 34517252, at *3 (discussing the possibility that the presence of data in a personal device's RAM may constitute "electronic storage" under the SCA). Here, it is unclear how the ECUs and

[9] *See In re DoubleClick Inc. Privacy Litig.*, 153 F. Supp. 2d at 511 ("the DoubleClick cookies's residence on plaintiffs' hard drives is certainly not an 'intermediate' step in their transmission to another addressee"); *Garcia*, 702 F.3d at 793 ("[b]ut information that an individual stores to his hard drive or cell phone is not in electronic storage under the statute"); *accord Owens v. Propes*, 601 F. Supp. 3d 1360, 1369 (M.D. Ga. 2022); *see In re Google Cookie*, 806 F.3d at 125, 146 ("[t]emporary storage incidental to transmission and storage for purposes of backup protection are not how personal computing devices keep communications, but how third party network service providers do—or at least did, in 1986"); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d at 1059 (discussing the holding of *In re Toys R Us, Inc., Priv. Litig.*, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001), where the court distinguished data existing on the "random access memory" ("RAM") of a personal device, which may fall under the definition of "electronic storage," from data existing on the hard drive of the personal device, which falls outside the definition of "electronic storage" under the SCA).

TCUs store the information within the vehicle. (*See* Am. Compl. ¶¶ 855-56, 1020-21). Unlike a personal device where a user can easily access such information, the computing systems within a vehicle through GM and OnStar are less easily accessible and such information was not available to the Plaintiffs in drafting their Amended Complaint. Therefore, discovery is necessary in order to resolve the question of whether the driving data is in "electronic storage."

Third, the Plaintiffs have properly pled that its messages are in "temporary, intermediate storage." The GM Defendants are correct in asserting that the term requires there to be a transmission to an intended recipient and that the message must be in transit. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 32-33 (citing *Mastel v. Miniclip* SA, 549 F. Supp. 3d 1129 (E.D. Cal. 2021), then citing *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000 (N.D. Cal. 2018))). However, the GM Defendants argue this point from the perspective that they are the intended recipients of the electronic communication. (*Id.*). The Plaintiffs never make this allegation, instead alleging that their communications were with themselves. (*See* Am. Compl. ¶ 1020). Under the Amended Complaint, the Plaintiffs do so in order to facilitate their driving experience. (*Id.*). In driving the vehicle, a Plaintiff initiates the electronic communication, which is then routed through the electronic components of the vehicle, including the ECUs and TCUs. (*See* Am. Compl. ¶¶ 846-48). The electronic communication itself is processed through

ECUs, which process the communication and send it to gateways for translation between protocols within the vehicle. (*See* Am. Compl. ¶¶ 847-48). The information received is eventually processed and temporarily stored within the TCU either for the vehicle's use to communicate back to the driver or directly to GM. (*See* Am. Compl. ¶¶ 848-55, 1020-21). Because the Plaintiffs allege within the Amended Complaint that the message was in transit to the intended recipient and the storage within the vehicle was temporary for the purpose of conveying the message, the Plaintiffs have properly alleged that the electronic communication was in "electronic storage."

**c. SCA Authorization Exceptions**

Under the SCA, an individual will not be liable for accessing stored communications in violation of 18 U.S.C. § 2701(a) if the conduct is authorized (1) "by the person or entity providing a wire or electronic communications service," (2) "by a user of that service with respect to a communication of or intended for that user," or (3) in 18 U.S.C. §§ 2703 (Required disclosure of customer communications or records), 2704 (Backup preservation), or 2518 (Procedure for interception of wire, oral, or electronic communications). 18 U.S.C. § 2701(c). A "user" under the SCA is any person or entity who "uses an electronic communication service" and "is duly authorized by the provider of such service to engage in such use." 18 U.S.C.§ 2510(13).

"Courts have consistently held that the exception of Section 2701(c) is not an affirmative defense, but rather is an element of the offense." *CreditMax*

*Holdings, LLC v. Kass*, 2013 WL 12080227, at *2 (S.D. Fla. Jan. 25, 2013) (citation modified); *see In re DoubleClick*, 154 F. Supp. 2d at 508 (holding that Section 2701(c) exceptions are not affirmative defenses, but rather statutory exceptions). If a defendant's conduct falls into one of the Section 2701(c) exceptions on the face of the complaint, it is proper for a court to dismiss the claim on a motion to dismiss. *See In re DoubleClick*, 154 F. Supp. 2d at 508.

The GM Defendants argue that, even if the Plaintiffs properly allege a claim under Section 2701(a), the allegations found within the Amended Complaint support a finding that the Section 2701(c) exceptions apply. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 33-35). In doing so, the GM Defendants argue that (1) the Amended Complaint alleges that OnStar provided the electronic communications service and (2) the GM Defendants were the intended recipients of the communications by the Plaintiffs. (*Id.*). Within this Motion to Dismiss, the Court has explained why the GM Defendants are not the intended recipients of the communications by the Plaintiffs and will not belabor that conclusion here. Therefore, the Court now addresses whether 18 U.S.C. § 2701(c)(1) applies.

Courts generally dismiss SCA claims against defendants who are also the providers of the electronic communication services under the allegations of the complaint.[10] Looking to the Amended Complaint, it is plausible that

[10] *See Mohamad v. Central Fla. Tax and Acct., Inc.*, 2025 WL 2695116, at *7 (M.D. Fla. Sep. 22, 2025) ("[a]ccording to Plaintiff . . . Sigma is the provider of the electronic communications service. Because the Sigma

OnStar is the provider of an electronic communications service. The Amended Complaint does make allegations that could support a finding that OnStar is providing the electronic communication service. The Plaintiffs allege that OnStar provides communications, diagnostics, and information services to GM vehicles worldwide through the use of cellular technologies with onboard electronics. (*See* Am. Compl. ¶¶ 656, 661). Additionally, the Plaintiffs allege that the ECUs and TCUs are the facilities through which the electronic communication services are provided and provides imaging depicting OnStar having some level of control over the TCU. (*Id.* ¶¶ 850, 1021).

However, because the technology in this matter is not similar to any previous SCA precedent, there are other confounding allegations within the Amended Complaint which obfuscate whether Section 2701(c)(1) applies. The Plaintiffs never explicitly name OnStar as the provider of the electronic communication services. Furthermore, the Amended Complaint states that OnStar leverages cellular networks for connectivity and that GM partners with multiple wireless carriers to assist OnStar. (Am. Compl. ¶ 853). The allegation cuts against the claim that OnStar is the provider of the electronic communication service because those cellular networks could be the true

---

Defendants presumably authorized their own conduct, count three is dismissed with prejudice under section 2701(c)(1)" (citations omitted)); *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 686 (N.D. Cal. 2021) ("Apple is the service provider here and presumably authorized its own conduct"); *see also Sargeant v. Maroil Trading Inc.*, 2018 WL 3031841, at *14 (S.D. Fla. May 30, 2018) (dismissing SCA claim because the plaintiff failed to plead that the defendants did not have authorization under 18 U.S.C. § 2701(c)(1)).

electronic communication service providers depending on how OnStar leverages them in the system. Finally, the Court sees the need for further information regarding the customer relationship between the GM Defendants and the Plaintiffs. The Plaintiffs allege total ownership over the GM vehicle within the Amended Complaint, but it is unclear to what degree the Plaintiffs own the electronic communications service. (*See* Am. Compl. ¶1020-24; Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 25-26); *see also Expert Janitorial, LLC v. Williams*, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (denying dismissal of an SCA claim because, based on the allegations by the plaintiff, the plaintiff provided the electronic communications service, and the defendant accessed it without authorization). Because discovery will resolve the GM Defendants' liability, and the Plaintiffs' SCA claim under 18 U.S.C. § 2701(a) is adequately pled, the Court will not dismiss Count 3 of the Amended Complaint. *See Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 335-336 (D.D.C. 2011) (permitting SCA claim to proceed when the defendants' argument narrowly construed the complaint and where discovery would resolve a liability dispute).

**2. State Claims (Counts 36, 42, 56)**

The GM Defendants also argue for the dismissal of certain analogous state law claims. Specifically, the GM Defendants ask the Court to dismiss Counts 36 (Maryland Stored Wire and Electronic Communications and Transactional Records Access Act), 42 (Nebraska Stored Communications

Law), and 56 (Pennsylvania Unlawful Access to Stored Communications Act) for the reasons presented against the SCA claim (Count 4). (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 35-36). This is because the substantive portions of the state statutes are almost identical to the SCA. *See* Md. Code Ann., Cts. & Jud. Proc. §§ 10-4A-02(a), (c); Neb. Rev. Stat. §§ 86-2, 104(1), (3); 18 Pa. Cons. Stat. §§ 5741(a), (c). Accordingly, the Court will not dismiss the state analogous claims for the same reasons that apply to the federal claim.[11]

### D. CFAA Claims

The GM Defendants argue that the Computer Fraud and Abuse Act ("CFAA") claim (Count 4) and the California Computer Data Access and Fraud Act ("CDAFA") claim (Count 16) should be dismissed as a state analog to the CFAA. The Court will first address the CFAA claim, then turn to the CDAFA claim.

#### 1. Computer Fraud and Abuse Act (Count 4)

Under the CFAA, an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" is in violation of the statute. 18

[11] The GM Defendants, within their reply briefing, ask the Court to treat the Plaintiffs' nonresponse to their state law dismissal as abandonment. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 19). The decision on whether to treat an argument as abandoned is discretionary. *See Resol. Tr. Corp. v. Dunmar Corp.*, 43 F.3d 587, 599 (11th Cir. 1995) (discussing the consequences of not responding to a claim during briefing of a motion). Here, the Court declines to exercise this discretion because the GM Defendants incorporate their arguments against the federal claim in arguing for dismissal of the state law claims and the Plaintiffs thoroughly responded to the federal claim.

U.S.C. § 1030(a)(2)(C). The prohibition applies "to all information from all computers that connect to the Internet." *Van Buren v. United States*, 593 U.S. 374, 379 (2021). The CFAA also provides a private right of action for "any person who suffers damage or loss by reason of a violation of [18 U.S.C. § 1030]," subject to certain conditions. 18 U.S.C. § 1030(g). Relevant to the Motion to Dismiss, a civil action may be brought under Section 1030 if the conduct involves "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), (g).

The GM Defendants first argue that the Plaintiffs cannot maintain a claim under 18 U.S.C. § 1030(a)(2) because the GM Defendants did not violate the authorization clause of the CFAA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 36-40). The GM Defendants then argue that, even if they were in violation of the CFAA, the Plaintiffs fail to plead a qualifying loss that permits them to pursue a private right of action. (*Id.* at 41-44). The Court takes each argument in turn.

**a. Authorization**

The Plaintiffs allege that GM intentionally accessed the Plaintiffs' driving data without their authorization or in a manner that exceeded authorization. (Am. Compl. ¶ 1045). The GM Defendants argue three points addressing the issue of authorization. First, the GM Defendants argue that they did not act "without authorization" because GM was already authorized to access the driving data. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 36-38).

Second, the GM Defendants argue that GM did not exceed its authorized access to the driving data because it already had full access. Third, the GM Defendants argue that, even if GM acted improperly, there was no intent to do so. (*Id.* at 40).

### i. "Without Authorization" Plaintiffs

The GM Defendants, both in briefing and in oral argument, rely on *Van Buren* for the proposition that whether access is authorized under the CFAA is a "gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 37 (quoting *Van Buren*, 593 U.S. at 390); *see* Sep. 5, 2025 Hearing Tr. at 25:18-26:1, 26:12-26:14 [Doc. 178]). Ultimately, the GM Defendants use *Van Buren* to argue that the term "without authorization" requires a defendant to "circumvent some sort of technological limitation in order to access the data." (Sep. 5, 2025 Hearing Tr. at 25:23-26:1; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 37-38). The Plaintiffs, in response, argue that *Van Buren* is inapplicable to their Amended Complaint because the case does not focus on the provision-at-issue. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 28; *see* Sep. 5, 2025 Hearing Tr. at 90:5-90:15, 91:13-91:24).

If the GM Defendants are correct and *Van Buren* is applicable, then the Court must adhere to the Supreme Court's holding because it has direct application to this case. *See King v. Cessna Aircraft Co.*, 505 F.3d 1160, 1169

(11th Cir. 2007). *Van Buren* is instructive but is not dispositive. In *Van Buren*, a criminal case, the Supreme Court discussed whether an individual was in violation of the "exceeds authorized access" clause of the CFAA. *Van Buren*, 593 U.S. at 380; *see* 18 U.S.C. § 1030(a)(2) ("intentionally accesses a computer without authorization or *exceeds authorized access*, and thereby obtains . . ." (emphasis added)). The defendant, a police sergeant, was paid by a third party to search the state law enforcement computer database to assist the third party in evading a potential undercover officer. *Van Buren*, 593 U.S. at 380. Both parties agreed that the defendant's access was with authorization via his use of his patrol-car computer and valid credentials to log into the law enforcement database. *Id.* at 382. However, the Government argued that the defendant exceeded his authorization under the CFAA by misusing his access to the computer database under the department's policy. *Id.* at 380-81.

The Supreme Court rejected the Government's position that access policies should govern the inquiry on whether there was a violation of the "exceeds authorized access" clause of the CFAA. *Id.* at 390-91. In rejecting the Government's position, the Supreme Court looked to "the interplay between the 'without authorization' and 'exceeds authorized access' clauses of [18 U.S.C. § 1030(a)(2)]." *Id.* at 389. The court determined that, if the "without authorization" clause operates in a gates-up-or-down manner such that one either can or cannot access a computer system, so should the "exceeds authorized access" provision. *Id.* at 390. Ultimately, the Supreme Court held

that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer . . . that are off limits to him." *Id.* at 396.

Here, the GM Defendants correctly assert that the question of whether an individual accesses a computer "without authorization" in violation of the CFAA is a "gates-up-or-down inquiry." Accordingly, a plaintiff pleading a claim under the CFAA must argue that the defendant had no authorization *at all* to access information present on the computer. However, the GM Defendants err in extending *Van Buren* any further. *Van Buren*'s holding explicitly applies only when interpreting the "exceeds authorized access" clause of the CFAA and not when interpreting the "without authorization" clause. *See Van Buren*, 593 U.S. at 396. The discussion of the "without authorization" clause of the CFAA is limited to an explanation of what arguments a court may consider when deciding on whether an individual exceeded his authorization. *Id.* at 389-90. The GM Defendants further err in asserting that *Van Buren* requires a technological limitation to be circumvented. The ultimate holding makes no mention of any limitation in place, such as passwords or otherwise, and simply states that an individual exceeds his authorized access when he accesses information located in particular areas of a computer that are off limits. *Id.* at 396.

A court within this District reached a similar result in dealing with vehicular computer systems. In *Bowen v. Porsche Cars, N.A., Inc.*, 561 F. Supp.

3d 1362 (N.D. Ga. 2021), the plaintiffs, consumers of Porsche vehicles, brought a CFAA claim against Porsche for damages arising out of Porsche's access to Porsche Communication Management ("PCM") devices within each vehicle sold by Porsche. *Bowen*, 561 F. Supp. 3d at 1366-67. The PCM operated as a central control unit for much of the "infotainment" data processing and communication features of Porsche vehicles, including GPS navigation services. *Id.* at 1366. Porsche used the satellite radio functionality of PCMs to send a software or firmware update that caused PCMs to malfunction. *Id.*

The plaintiffs alleged that Porsche acted "without authorization" for their CFAA claim. *Id.* at 1368. On a motion to dismiss the claim, the court determined that the plaintiffs adequately pled their CFAA claim by alleging that Porsche acted "without authorization," holding that any dispute over consent was an issue for discovery. *Id.* at 1370-71. In doing so, the court distinguished *Van Buren* as inapplicable because *Van Buren* did not concern itself with the phrase "without authorization." *Id.* at 1370. The court also did not concern itself with any technological limitation that operated as a barrier for Porsche's entry "without authorization." *Id.* at 137-71.

Ultimately, the inherent flaw within the GM Defendants' approach is that while a technological limitation may more clearly delineate when the gate opens and shuts, it is not a requirement to plead a claim under the CFAA. The key concern of a CFAA claim is whether a defendant has unauthorized access to private information, not whether a username or password is required. *See*

*hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1201 (9th Cir. 2022) (holding that accessing publicly available data would not violate the CFAA, shortly after mentioning that it would violate the CFAA if a person circumvents access permissions).

Here, the relevant Plaintiffs have pled all that is necessary to show that GM acted "without authorization" to sustain their CFAA claim. The Plaintiffs demonstrate, on multiple occasions, that the data taken by GM is private data. (*See e.g.* Am. Compl. ¶¶ 840, 858). The Plaintiffs allege that GM "expressly represented that it would not collect Driving Data at all unless consumers enrolled separately in Smart Driver." (*Id.* ¶ 866). The Plaintiffs also allege that they were never given the choice to activate OnStar and did not knowingly enroll in OnStar because the dealerships enrolled the Plaintiffs without their knowledge. (*See id.* ¶¶ 877-915). Therefore, because the Plaintiffs adequately plead that the GM Defendants acted "without authorization," the GM Defendants' arguments fail.

**ii. "Exceeds Authorized Access" Plaintiffs**

As highlighted by the GM Defendants, at least ten named Plaintiffs allege that they affirmatively enrolled in OnStar, granting GM limited access to the driving data within the Plaintiffs' vehicles. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 24; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 3, at 1-4 [Doc. 142-4]). Therefore, to the extent any authorization was properly given by the Plaintiffs, there are at least some Plaintiffs who must plead that

GM exceeded their authorization. Although the scope of consent is a matter for determination post-discovery, *Bowen*, 561 F. Supp. 3d at 1371, the Court will address the GM Defendants' contention arising out of the facts present in the Plaintiffs' Amended Complaint.

The CFAA explicitly defines the clause "exceeds authorized access" to mean "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The *Van Buren* court considered this definition and held that a defendant "exceeds authorized access" when "he accesses a computer with authorization but then obtains information located in particular areas of the computer . . . that are off limits to him."[12] *Van Buren*, 593 U.S. at 396.

When considering the Plaintiffs to whom the "exceeds authorized access" clause applies to within their CFAA claim, the GM Defendants urge the Court to consider the holding in *Fish v. Tesla, Inc.*, 2022 WL 1552137 (C.D. Cal. May 12, 2022) in evaluating their Motion to Dismiss. In *Fish*, the plaintiffs

[12] Oddly, the GM Defendants argue that the quoted portion of *Van Buren* is the incorrect holding and that the true holding of *Van Buren* is that the CFAA "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them." (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 24-25 (quoting *Van Buren*, 593 U.S. at 378)). Ignoring that the quoted portion is sourced verbatim from the conclusion section of the opinion, it is the Court's view that both quoted portions espouse the same holding. It is irrelevant what the motive of the defendant is in accessing the information. The key issue in an "exceeding authorized access" inquiry is whether the defendant had access to the information prior to the incidents at issue.

brought a claim under the CFAA alleging that Tesla exceeded its authorized access to each vehicle's media control unit ("MCU") to reduce performance, range, battery capacity, and charging speed. *Id.* at *9. The plaintiffs alleged this exceeded authorized access because they did not know of or consent to the updates. *Id.* On Tesla's motion to dismiss, the court held that, on these alleged facts, the plaintiffs "have not plausibly alleged that Defendant did not have unfettered access to their MCUs and battery." *Id.*

The GM Defendants argue *Fish* applies to the Plaintiffs' Amended Complaint because the facts show that the GM Defendants have "unfettered access" to the driving data through control over the ECUs and TCUs. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 25). However, the GM Defendants err in their analysis of *Fish*. The GM Defendants analogize Tesla's access to the MCUs to GM's access to the TCUs and ECUs, but the scenarios are operationally different. The underlying complaint in *Fish* demonstrates that Tesla continually sends updates to Tesla's vehicles which Tesla owners, like the plaintiffs, must accept, and that the plaintiffs would be unable to operate their vehicles without Tesla's software. *See* 1st Am. Class Action Compl. ¶¶ 76-79, *Fish*, 2022 WL 1552137. The *Fish* plaintiffs only brought their CFAA claim against certain updates that were harmful to the plaintiffs. *See Fish*, 2022 WL 1552137, at *9 ("They assert that this was in excess of Defendant's authorized access because they did not know of or consent to these 'damaging updates'" (citation modified)). Because Tesla already had full access to the

MCUs to send such periodic updates to Tesla owners, it is irrelevant to the CFAA claim whether Tesla had a malicious purpose in doing so. *See Van Buren*, 593 U.S. at 396 ("The only question is whether [the defendant] could use the system to retrieve license-plate information. Both sides agree that he could. [The defendant] accordingly did not 'excee[d] authorized access' to the database . . . even though he obtained information from the database for an improper purpose").

The Plaintiffs' allegations within the Amended Complaint portray an entirely different picture. The GM Defendants' access to ECUs and TCUs is constrained to diagnostic tools designed for personal use. (*See* Am. Compl. ¶ 663). Furthermore, GM expressly represented that it was not authorized to collect driving data unless a Plaintiff enrolled in Smart Driver. (*Id.* ¶ 866). Even if a Plaintiff enrolled in Smart Driver, GM represented that it would use technical, administrative, and physical safeguards to protect the data. (*Id.* ¶ 867). Any information OnStar acquired was represented to be anonymized to protect consumer privacy. (*Id.* ¶ 840). Furthermore, the interplay of ECUs and TCUs within GM vehicles shows that access to some devices does not automatically equate to access to all devices and sensors. (*Id.* ¶¶ 846-50). Finally, the Plaintiffs allege that GM continued to access data from the ECUs and TCUs after the subscription period ended. (*See id.* ¶¶ 30, 60, 179, 207, 208, 220, 231, 233, 303, 330, 348, 350, 403, 434, 436, 447-48, 479-80, 525, 551, 880).

The GM Defendants instead point to allegations that GM installed the ECUs and TCUs as support for their claim that the GM Defendants had "unfettered access." (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 25 (citing Am. Compl. ¶¶ 1, 663, 833, 843, 846-50)). However, this fact alone does not show, without discovery, that GM had total access to the devices. Indeed, taking the GM Defendants' position as true would be troublesome from a practical standpoint. Take a personal computer that has pre-installed software and hardware prior to sale, for example. Under the GM Defendants' argument, the provider of the pre-installed software and hardware would have full authorization to access a consumer's personal information under the CFAA solely because it installed the equipment. Such an approach is irreconcilable with the holdings in *Bowen* and *Fish*, because Porsche and Tesla would necessarily be entitled to access the devices it installed within the vehicle.

Ultimately, there is at least an open question as to what level of access GM had to the ECUs and TCUs for driving data. Construing the facts of the Amended Complaint in the light most favorable to the plaintiff, *see Quality Foods de Centro America, S.A.*, 711 F.2d at 994-95, it is at least plausible for the Plaintiffs to establish that GM "exceed[ed] authorized access."

**iii. Intent**

"The intent element under the CFAA requires merely that access to a computer system not be a careless or inadvertent mistake." *Bowen*, 561 F. Supp. 3d at 1369 (citation omitted). "Intent only requires proof that the

defendant intentionally accessed information from a protected computer; the section does not require proof of intent to defraud nor proof that the defendant knew the value of the information obtained." *Health First, Inc. v. Hynes*, 2014 WL 12648552, at *10 (M.D. Fla. Sep. 17, 2014), *aff'd* 628 F. App'x 723 (11th Cir. 2016).

The GM Defendants argue that the Plaintiffs failed to allege adequate facts to satisfy the intent element of their CFAA claim. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 40). The GM Defendants point out that 10 of the 47 Plaintiffs affirmatively enrolled in OnStar and most of the remaining Plaintiffs allege that an independent car dealer activated OnStar without effective consent and without the involvement of GM. (*Id.*). The GM Defendants also state that the dealerships' intent cannot be imputed onto GM under a theory of vicarious liability. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 26). The Court disagrees.

First, addressing the dealerships, the Plaintiffs comprehensively detail how GM incentivized dealership enrollments in OnStar (through reward and punishment systems), how GM dealers responded by enrolling consumers into OnStar without their effective consent, and how GM was aware of the conduct from the moment GM began incentivizing enrollments. (*See* Am. Compl. ¶¶ 884-904). The fact that GM issued a press release stating that they have "reminded dealers of the important role they play in helping to ensure customers are *aware* of the privacy statement, the user terms, and the choices

they can make about vehicle connectivity and communication preferences" shows that GM knew, to a plausible degree, that improper dealer conduct was not limited to isolated incidents and that it was aware of where improper conduct was taking place. (*Id.* ¶ 890 (emphasis added)). At the Motion to Dismiss stage, the facts alleged within the Amended Complaint demonstrate that the Plaintiffs who had OnStar activated by dealerships can plausibly make out a claim that the GM Defendants knew that effective consent was not given and nonetheless accessed the TCUs and ECUs intentionally.[13]

Turning to the Plaintiffs who affirmatively enrolled themselves into OnStar without the involvement of dealerships, the Plaintiff still alleges facts that show that GM intentionally exceeded its authorization. Specifically, the relevant Plaintiffs allege that GM continued to access data after their subscription period to OnStar ended. (*See id.* ¶¶ 30, 60, 179, 207, 208, 220, 231, 233, 303, 330, 348, 350, 403, 434, 436, 447-48, 479-80, 525, 551, 880). The GM Defendants, in a footnote, respond to these factual allegations by disputing that the facts do not show that the Plaintiffs ever revoked their consent after the end of the "free trial" and offering factual inconsistencies. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 26 n. 21). However, as reiterated before,

[13] The Court's holding makes the inquiry into vicarious liability irrelevant. However, to clarify the proper legal standard for the sake of completeness, the CFAA does not prohibit the imposition of vicarious liability on a principal for the agent's offenses. *Abu v. Dickson*, 107 F.4th 508, 514, 520 (6th Cir. 2024); *see Bowen*, 561 F. Supp. 3d at 1369 ("[C]ourts in this circuit have held that even indirect access through a third party may establish intent under the CFAA.").

the determination of whether a defendant exceeds its authorization by acting outside the scope of the plaintiff's consent is often a question that requires further discovery and is not suited for consideration at the Motion to Dismiss stage. *See Bowen*, 561 F. Supp. 3d at 1371 ("After discovery, Porsche may be able to provide evidence that Bowen did authorize the Update."). But at this stage, viewing the Amended Complaint in the light most favorable to the plaintiffs, the Plaintiffs' allegations survive the GM Defendants' challenges to authorization in their Motion to Dismiss.

**b. Loss**

The GM Defendants also argue that the Plaintiffs' CFAA claim should be dismissed because they fail to plead "loss" within the meaning of the CFAA. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 41). As earlier discussed, the CFAA's private right of action is available only if the conduct involves a "loss" amount of at least $5,000 in value. 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), (g). "Loss" is defined under the CFAA to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service." 18 U.S.C. § 1030(e)(11).

The Eleventh Circuit interpreted "loss" as defined by the CFAA in *Brown Jordan Int'l* as an issue of first impression. *See Brown Jordan Int'l*, 846

F.3d at 1173. After reviewing authority from the Fourth and Sixth Circuits, the Eleventh Circuit agreed that, because the definition is written in the disjunctive, there are two separate types of loss that qualify under the CFAA: (1) "reasonable costs incurred in connection with such activities as responding to a violation, assessing the damage done, and restoring the affected data, program system, or information to its condition prior to the offense;" and (2) "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at 1174; *see Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC,* 774 F.3d 1065, 1073 (6th Cir. 2014); *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009).

Here, the Plaintiffs allege that their losses exceed $5,000 in a one-year period arising out of "loss of their privacy interest in and control over their Driving Data," (Am. Compl. ¶ 1047), along with increased insurance premiums for certain Plaintiffs, time spent investigating the accuracy of consumer reports and the increase to their insurance premiums, and seeking out alternative insurance. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 37-38; *see* Am. Compl. ¶¶ 17, 34, 35, 51, 61, 63, 64, 66, 82, 133, 156, 157, 186, 211, 240, 254, 293, 304, 319, 331, 337, 368, 378, 384, 420, 466, 499, 517, 552, 553, 559, 601, 621). At a minimum, the facts contained within the Amended Complaint do not support a finding that the losses complained of arise out of the second category of qualifying loss. While these alleged losses may be related to the cost incurred by the Plaintiffs or their consequential damages,

the Plaintiffs do not allege that GM's CFAA offense caused any interruption of service within the ECUs, TCUs, or the computer systems within the vehicle. Because no damages can arise within the second category without an interruption of service, the losses alleged by the Plaintiffs must arise out of a qualifying loss from the first category.

In evaluating whether a loss alleged under the CFAA fits into the first category, the Court turns to the Eleventh Circuit's decision in *Brown Jordan Int'l* once more. In *Brown Jordan Int'l*, in a bench trial, the defendant was found to violate the CFAA after gaining unauthorized access into email accounts and taking screenshots of numerous emails over the course of half a year. *See Brown Jordan Int'l*, 846 F.3d at 1170-72. On appeal, the defendant argued that costs expended by the plaintiff to investigate how the defendant accessed the emails and expended costs not arising out of damage to a computer or network do not fit the definition of "loss" under the CFAA. *Id.* at 1172, 1175 n. 2. The Eleventh Circuit disagreed, holding that qualifying losses need not arise out of any damage to a computer or network and can arise out of an investigation into the unauthorized access of a protected computer. *Id.* at 1174-75, 1175 n. 2.

Courts within this Circuit have refused to expand the scope of what constitutes a qualifying loss under the CFAA to encompass losses arising out of information misappropriated by a defendant that does not relate to a

computer or a network.[14] Similarly, the Third and Ninth Circuits have found losses arising out of the nonconsensual collection of personal data not to be qualifying losses under the CFAA. *See Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262-63 (holding, in response to the plaintiff's arguments, that "the CFAA is an anti-hacking statute, not an expansive misappropriation statute" (citation modified)); *In re Google Cookie*, 806 F.3d at 148-49 (holding that damages arising out of the acquisition of personal information is not a qualifying loss under the CFAA).

Despite overwhelming authority against their position, the Plaintiffs advance an incredibly broad standard for what a qualifying loss is under the CFAA without any citation to authority directly supporting their position. The Plaintiffs assert "all that is required is that the loss be reasonable and causally linked to GM's conduct." (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 37). A case the Plaintiffs present as tangential support to their claim, *Healthcare Advocates, Inc. v. Harding, Earley, Folmer & Frailey*, 497 F. Supp.

---

[14] *See Gemstone Foods, LLC v. AAA Foods Enters., Inc.*, 2022 WL 1420853, at *45 (N.D. Ala. Apr. 27, 2022), *vacated in part on other grounds*, 2022 WL 1443778 (N.D. Ala. May 6, 2022) (holding that damages arising out of a CFAA violation are not qualifying losses because they relate to the defendants' use of information against the plaintiff and not the computer system itself); *My Energy Monster, Inc. v. Gawrych*, 2021 WL 6125579, at *1, *4 (M.D. Fla. Sep. 29, 2021) (holding that damages arising out of a CFAA violation are not qualifying losses because such damages relate to the defendant's use of the confidential information and there is no "interruption of service"); *Fla. Beauty Flora Inc. v. Pro Intermodal L.L.C.*, 2020 WL 4003494, at *7 (S.D. Fla. Jul. 15, 2020); *HCC Ins. Holdings, Inc. v. Flowers*, 237 F. Supp. 3d 1341, 1357-58 (N.D. Ga. 2017) (same); *IPC Sys., Inc. v. Garrigan*, 2012 WL 12872028, at *7 (N.D. Ga. May 21, 2012) (same).

2d 627 (E.D. Pa. 2007), illustrates the legal deficiency in their position. (*See id.*). The Plaintiffs assert that *Healthcare Advocates* stands for the proposition that "sufficient alleged losses [under the CFAA] can include lost time." (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 37 (citing *Healthcare Advocs.*, 497 F. Supp. 2d at 647)). However, while correct in a technical sense, it removes all context and subsequent language from what the lost time pertains to. The court determined lost time was compensable for investigative work performed because it was time spent investigating how the CFAA violation occurred. *Healthcare Advocs.*, 497 F. Supp. 2d at 647. This is further emphasized one paragraph below, where the court hesitated to consider litigation costs as a qualifying loss under the CFAA because "they do not appear to be involved in assessing the integrity of Healthcare Advocates' computer systems." *Id.*; *see also WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 683 ("[The plaintiffs] have alleged that they incurred costs responding to the unauthorized access to users' phones *by upgrading the WhatsApp system* in response to defendants' intrusion . . . these allegations are sufficient to state a claim for loss." (emphasis added)).

Applying this definition of qualifying loss to the Plaintiff's Amended Complaint, the Court considers the Plaintiffs' alleged losses once more under the first category. The Plaintiffs' loss of privacy interest and control over Driving Data are not "reasonable costs incurred in connection with such activities as responding to a violation, assessing the damage done, and

restoring the affected data, program system, or information to its condition prior to the violation" because such losses are not remedial in any capacity and have been explicitly rejected as qualifying losses. *See Brown Jordan Int'l*, 846 F.3d at 1174; *Andrews*, 932 F.3d at 1262-63; *In re Google Cookie*, 806 F.3d at 148-49. Additionally, the Plaintiffs' alleged losses from increased insurance premiums, any time spent investigating the Plaintiffs' consumer reports and increased premiums, and any time spent finding alternative insurance do not qualify because they relate to GM's alleged misappropriation of the information after committing a CFAA violation and not the CFAA violation itself. *See e.g. Gemstone Foods*, 2022 WL 1420853, at *45; Discussion III.D(1)(b), *supra*, at 78-79 n. 15. Accordingly, because the Plaintiffs fail to allege even a single category of qualified losses under the CFAA, the Court dismisses Count 4 of the Amended Complaint.

**2. California Computer Data Access and Fraud Act (Count 16)**

The CDAFA is a state law analog to the CFAA. *See* Cal. Pen. Code § 502; *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1260 (stating that CDAFA claims generally "rise or fall with" CFAA claims). Accordingly, neither the Plaintiffs nor the GM Defendants present new arguments separate from the CFAA claim. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 44; Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 38).

However, the CDAFA's private right of action statute is slightly different from the CFAA. The CDAFA provides a private right of action for a

violation of the statute that states that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of [the CDAFA] may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief." Cal. Pen. Code § 502(e)(1). The CDAFA does not define "damage or loss," but it does define "compensatory damages" to include "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id.* Additionally, the CDAFA fails to impose any $5,000 loss minimum like the CFAA for bringing a civil action. *See id; Meta Platforms*, 605 F. Supp. 3d at 1259; *Mintz v. Mark Bartelstein and Assocs. Inc.*, 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012).

However, in order for the California Plaintiffs to recover under the CDAFA, they must plead a "damage or loss" as required by the statute. *See* Cal. Penal Code. § 502(e)(1) ("the owner or lessee of the computer, computer system, [etc.] who suffers *damage or loss* by reason of a violation of [the CDAFA] . . . . " (emphasis added)). Here, the California Plaintiffs bring forth their CDAFA claim alleging damage or loss that includes "(a) damage to and diminution of the value of their personal information; (b) violation of their privacy rights; (c) the likelihood of future misuse of their private information; and (d) overpaying for their vehicles as a result of [GM's] failure to inform."

(Am. Compl. ¶ 1207). The California Plaintiffs' pleadings fail to show this damage or loss. [15]

California courts have held that pleading losses based off the diminution of value of their data and the violation of their rights to control and protect their own data does not qualify as "damage or loss" under the CDAFA. *See Cottle v. Plaid Inc.*, 536 F. Supp. 3d at 461, 487-88 (N.D. Cal. 2021); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 2d 1064, 1082 (N.D. Cal. 2023) ("[The plaintiffs'] diminished value of information claim is foreclosed by the reasoning in *Cottle*); *see also Nowak*, 2020 WL 6822888, at *4-5 (dismissing CDAFA claim because a loss of the value of cryptocurrency is not "damage or loss" under the CDAFA). Here, the first three losses alleged by the California Plaintiffs fall directly outside of the scope of "damage or loss" under the meaning of the CDAFA. The fourth loss alleged also falls outside of the scope of the CDAFA because it is derived from the Plaintiff's right to information. Furthermore, the California Plaintiffs have not offered any other source of

[15] Within their CDAFA claim, the Plaintiffs allege, in part, a violation of Cal. Pen. Code. § 502(c)(1), which makes it unlawful to "knowingly access[ ] and without permission . . . use[ ] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to *defraud, deceive, or extort*, or (B) wrongfully control or obtain money, property, or data." (Am. Compl. ¶ 1193(a) (emphasis added)). Courts have held that, for CDAFA claims arising out of fraud, the heightened pleading standard of Rule 9(b) applies. *See e.g. In re Apple Inc. Device Performance Litig.*, 386 F. Supp. 3d 1155, 1181 (N.D Cal. 2019); *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020). The Court need not address whether this standard applies here because the Court's holding is unaffected by a determination of this issue.

damage or loss within their pleadings, briefings, or at oral argument. Because no damage or loss has been alleged within the meaning of the CDAFA, the California Plaintiffs fail to state a claim upon which relief can be granted and Count 16 is dismissed.

**E. FCRA Claim (Count 10)**

The Plaintiffs allege that the CRA Defendants violated the Fair Credit Reporting Act (the "FCRA") when preparing consumer reports. (*See* Am. Compl. ¶¶ 1096-1110). Under the FCRA, "[w]henever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." 15 U.S.C. § 1681e(b). The FCRA also permits a private right of action against any individual or entity found in willful or negligent noncompliance with the FCRA. *See generally* 15 U.S.C. §§ 1681n, 1681o. To state a claim under § 1681e(b), a plaintiff must allege, in his complaint, that (1) the credit reporting agency's consumer report contained factually inaccurate information, (2) the procedures it took in preparing and distributing the report were not reasonable, and (3) damages followed as a result. *Losch v. Nationstar Mortg. LLC*, 995 F.3d 937, 944 (11th Cir. 2021).[16]

[16] The Plaintiffs claim to invoke 15 U.S.C. §§ 1681b, 1681e(a) of FCRA within their FCRA claim by pleading that the CRA Defendants furnished reports for "an impermissible purpose and use of data under the FCRA." (Am. Compl. ¶ 1103). However, they fail to invoke either section within their FCRA claim in the Amended Complaint. They further bolster the facts and law necessary to support claims within their briefing to the Court. (*See* Pls. Br. in Opp'n to LNRS' Mot. to Dismiss, at 36-37). Because "a plaintiff cannot amend

The CRA Defendants challenge the Plaintiffs' CRA claim on each element, then address the issue of civil liability. First, the CRA Defendants claim that most of the named Plaintiffs fail to plausibly allege particularized inaccuracies. (*See* Br. in Supp. of LNRS Mot. to Dismiss, at 19-23 [Doc. 140-1]). Second, they argue that the Plaintiffs failed to plausibly allege that the CRA Defendants did not follow reasonable procedures as required by 15 U.S.C. § 1681e(b). (*Id.* at 23-25). Third, they argue that the Plaintiffs failed to plausibly allege that they suffered any injury as a result of the CRA Defendants reporting the driving data. (*Id.* at 25-27). Fourth, they argue that the Plaintiffs failed to plausibly allege that the CRA Defendants "willfully" violated the FCRA. (*Id.* at 27-30). The Court takes each argument in turn.

**1. Inaccuracy**

The first element of the Plaintiffs' FCRA claim requires the Plaintiffs to plead facts alleging that the CRA Defendants' consumer reports contained inaccuracies. *See Losch*, 995 F.3d at 944. To allege that a credit report is inaccurate under the FCRA, a plaintiff must allege that the credit report-at-issue is misleading or fails to be "technically accurate." *See Erickson v. First Advantage Background Servs. Corp.*, 981 F.3d 1246, 1251-52 (11th Cir.

---

the complaint by arguments of counsel made in opposition to a motion to dismiss," *In re The Home Depot, Inc. Shareholder Derivative Litigation*, 223 F. Supp. 3d 1317, 1329 (N.D. Ga. 2016) (citation modified), their claims under these two sections will not be considered by the Court.

2020). Whether a credit report is inaccurate is an objective determination. *Id.* at 1251.

The CRA Defendants allege that the vast majority of the named Plaintiffs fail to meet this standard. Specifically, the CRA Defendants point to the fact that "42 of the 47 Plaintiffs fail to point to any specific item of information appearing in his or her driving data that was inaccurate." (Br. in Supp. of LNRS' Mot. to Dismiss, at 20). The Plaintiffs obviously disagree, arguing that the information provided by the CRA Defendants is false and misleading, as alleged within the Amended Complaint. (*See* Pls.' Br. in Opp'n to LNRS' Mot. to Dismiss, at 26-29 [Doc. 151]).

Courts in this district routinely dismiss FCRA claims when a plaintiff's claim fails to plead any specific inaccuracy outside of vague, conclusory statements.[17] However, contrary to the CRA Defendants' assertions, the allegations made by at least some of the named Plaintiffs are not conclusory because they are enhanced factually through descriptions of what they found inaccurate about their reports. *Cf. Saho*, 2019 WL 11499337, at *5 (dismissing FCRA claim because "none of Saho's assertions are enhanced factually with specific dates of occurrence or *descriptions of what he found inaccurate about*

[17] *See Williams v. Trans Union LLC*, 2024 WL 4649363, at *3 (N.D. Ga. Oct. 2, 2024), *report and recommendation adopted*, 2024 WL 5104505 (N.D. Ga. Oct. 31, 2024); *Barreto v. Equifax Info. Servs. LLC*, 2023 WL 4047693, at *3-4 (May 25, 2023), *report and recommendation adopted*, 2023 WL 4996555 (Jul 19, 2023); *Saho v. Equifax, Inc.*, 2019 WL 11499337, at *5 (Oct. 31, 2019), *report and recommendation adopted*, 2020 WL 7388449 (N.D. Ga. Mar. 23, 2020).

*his report*" (citation modified) (emphasis added)). Nine named Plaintiffs make some assertion of erroneous information within the reports.[18]

The Plaintiffs also argue that they have alleged that the Verisk Report and LNRS Report are not issued at "maximum possible accuracy" for all named Plaintiffs because the driving data is "*so* decontextualized that safe driving habits (like suddenly braking to avoid a collision), are inaccurately characterized as unsafe." (Pls.' Br. in Opp'n to LNRS' Mot. to Dismiss, at 27). The Plaintiffs have applied these allegations for every named Plaintiff within

[18] Plaintiff Chad Weaver asserts that, after reviewing his Verisk Driving Behavior History Report ("Verisk Report"), he discovered errors pertaining to the time he spent driving his GM vehicle. (Am. Compl. ¶ 17). Plaintiff Dan Carnine asserts that, after reviewing his LexisNexis Consumer Disclosure Report ("LNRS Report"), he discovered errors pertaining to the time at which he drove his GM vehicle. (*Id.* ¶ 61). Plaintiff Joseph McDaniels III asserts that, after reviewing his LNRS Report, he discovered errors pertaining to certain acceleration and hard braking events as he drove the vehicle. (*Id.* ¶ 304). Plaintiff Kenneth Brockington asserts that, after reviewing his LNRS Report, he discovered errors within the report pertaining to certain acceleration, hard braking, and high-speed events as he drove the vehicle. (*Id.* ¶ 304). Plaintiffs Melvin Drews and Karen Drews assert that, after reviewing their LNRS Report, they discovered errors as to misattributed addresses and emails, along with a nonexistent lien. (*Id.* ¶ 331). Plaintiff Grace Gilmore asserts that, after reviewing her LNRS Report, she discovered errors pertaining to her date of birth, address, email addresses, and driver's license information, including previous addresses where she never resided. (*Id.* ¶ 364). Plaintiff Jennifer Melberg asserts that, after reviewing her LNRS Report, she discovered errors pertaining to inconsistent driving behavior, where the report contained many short trips for about or less than a mile, but had Plaintiff Melberg engaging in multiple instances of hard braking and acceleration events despite such trips taking less than five minutes. (*Id.* ¶ 378). Finally, Plaintiff Michael Montgomery asserts that, after reviewing his LNRS Report, he discovered errors pertaining to names and a social security number that were not associated with him. (*Id.* ¶ 553).

the Amended Complaint.[19] In addition, twenty-eight named Plaintiffs allege that their information was inaccurate and misleading because the reports improperly attributed the driving behaviors of other permitted drivers within their GM vehicles as the driving behavior of the named Plaintiffs.[20] Finally, the Plaintiffs' Amended Complaint dedicates an entire factual section to explaining how the CRA Defendants' consumer reports are "inaccurate, flawed, and materially misleading" because the reports are decontextualized. (*See id.* ¶¶ 916-31).

The CRA Defendants make two arguments against this assertion by the Plaintiffs. First, they argue that the FCRA does not require credit reporting agencies to provide context in their reports. (Br. in Supp. of LNRS' Mot. to Dismiss, at 22). Second, the CRA Defendants address the multiple-driver allegations by arguing that insurers do not care who is driving since insurers assess risk by the vehicle, not the individual.

---

[19] (Am. Compl. ¶¶ 18, 32, 48, 62, 78, 93, 104, 116, 129, 143, 154, 166, 180, 197, 209, 221, 234, 251, 278, 291, 305, 320, 333, 351, 366, 377, 393, 404, 415, 437, 449, 461, 481, 495, 513, 529, 542, 554, 572, 585, 595, 615, 633, 646).

[20] These allegations arise from Plaintiffs Weaver, (Am. Compl. ¶ 19), Brian Johnson, (*Id.* ¶ 33), Carnine, (*Id.* ¶ 63), Donald Smith, Jr., (*Id.* ¶ 79), Romeo Chicco, (*Id.* ¶ 130), Tory Skyers, (*Id.* ¶ 155), Stephen Griner, (*Id.* ¶ 181), Pavel Gazhenko, (*Id.* ¶ 192), Peter Gray, (*Id.* ¶ 222), Jeffrey Horvath, (*Id.* ¶ 235), David Lima, (*Id.* ¶ 252), Manuel Martinez, Jr., (*Id.* ¶ 266), Kathleen Martinez, (*Id.* ¶ 279), McDaniels, (*Id.* ¶ 307), Melvin Drews, (*Id.* ¶ 334), Brian LaFalce (*Id.* ¶ 352), Morris D. Gordin, (*Id.* ¶ 394), John Matthew, (*Id.* ¶ 405), Zachary Smith, (*Id.* ¶ 416), Joseph Davids, (*Id.* ¶ 438), Rickie Donovan Baker (*Id.* ¶ 462), Thomas Fuhrer, (*Id.* ¶ 482), Peter Christie, (*Id.* ¶ 496), Julianne Kovein, (*Id.* ¶ 514), Gregory Brakefield, (*Id.* ¶ 543), Wallace Bruce Mason, (*Id.* ¶ 596), Steven Angerhofer, (*Id.* ¶ 616), and Jace Parkhurst, (*Id.* ¶ 634).

Turning to the first argument, the CRA Defendants offer *Peterson v. Equifax Information Services, LLC*, 2018 WL 7348859 (N.D. Ga. Dec. 27, 2018), to illustrate their point. In *Peterson*, a plaintiff brought FRCA claims, including one under 15 U.S.C. § 1681e(b), against a credit reporting agency for reporting her delinquency on certain credit lines at the same time she was engaged in a legal dispute. *Id.* at * 3. The plaintiff did not dispute that she was delinquent on the accounts but argued that the information on the credit report was misleading because the defendant's investigations should have looked into the facts underlying her legal dispute and included it within the report. *Id.* at *3, *9. The court rejected this argument, holding that "if [the plaintiff's] definition of accuracy were adopted, every tradeline that did not contain an explanation for why an account became delinquent . . . would be deemed inaccurate under the FCRA." *Id.* at *9-*10.

The Court is hesitant to apply this illustration to the facts presented because it would be comparing apples to oranges. The reporting of delinquency is much different than the reporting of "bad driving behavior." Generally, in the former case, either an individual pays the amount that is overdue, or he falls into delinquency. It is a binary report. Context is irrelevant in this scenario because the number of times an individual falls into delinquency is directly related to their credit risk. In the latter case, reports on driving behavior issued by the CRA Defendants are not standardized at all and can be subjective. (*See* Am. Compl. ¶¶ 922-926). For example, the Plaintiffs could be

penalized for "high speed driving" even if they were to drive within the speed limit. (*Id.* ¶ 918). Inconsistencies as to what qualifies as "bad driving behavior" across credit reporting agencies, while outwardly portraying the information without any additional context, are objectively misleading. This is not to say that credit reporting agencies are required to solicit context from the plaintiffs, but rather to say that credit reporting agencies must take certain steps to ensure that the beneficiaries or recipients of the reports are aware of what the information within the reports mean.

The CRA Defendants' second argument also fails for similar reasons. While insurers may assess risk on a household level, the facts alleged within the Amended Complaint do not suggest that the consumer reports were presented to insurers under such context. Reports were prepared by the CRA Defendants naming the Plaintiffs with their addresses and email addresses. The information provided by the CRA Defendants, then, would follow the Plaintiffs no matter any change in circumstance, such as changes in their households or in the people permitted to drive their vehicles. Unlike what the CRA Defendants argue, the Plaintiffs are not required to track all driving data driven by permitted drivers to explain what specific information within the report is inaccurate when the presence of other drivers in the vehicle is enough to show inaccuracy within the reports. The CRA Defendants may demonstrate to the court that the consumer reports contain adequate information that allows insurers to make informed decisions. However, at this stage of the

litigation, the Court cannot dismiss the FCRA claim for failure to demonstrate an inaccuracy. [21]

**2. Reasonable Procedures**

The second element of the Plaintiffs' FCRA claim requires the Plaintiffs to plead facts alleging that the CRA Defendants failed to follow reasonable procedures in preparing their consumer reports. *See Losch*, 995 F.3d at 944. The CRA Defendants argue that the Plaintiffs fail to allege facts that show that the CRA Defendants did not follow reasonable procedures. (*See* Br. in Supp. of LNRS' Mot. to Dismiss, at 24-25). Whether a credit reporting agency followed reasonable procedures is a jury question in the overwhelming majority of cases. *Cahlin v. General Motors Acceptance Corp.*, 936 F.2d 1151, 1156 (11th Cir. 1991), *superseded by statute on other grounds*, *Santos v. Healthcare Revenue Recovery Grp., LLC*, 90 F.4th 1144, 1156 (11th Cir. 2024). The Eleventh Circuit laid out two corollary principles in *Losch* to consider when evaluating Section 1681e(b) claims. "First, a reporting agency's procedures will not be deemed unreasonable unless the agency has a reason to believe that the information supplied to it by a data furnisher is unreliable."

[21] The CRA Defendants also cite *Dickens v. Trans Union Corp.*, 18 F. App'x 315 (6th Cir. 2001), in support of their argument that a plaintiff's speculation that a defendant's notation is misleading is not enough to state a claim that the defendant's notation was inaccurate. *Id.* at 318. However, *Dickens* was also directly overruled on this point in *Twumasi-Ankrah v. Chekr, Inc.*, 954 F.3d 938 (6th Cir. 2020), where the court held that *Dickens* applied a far too restrictive standard for "inaccuracy" and reiterated that the case is not precedential. *Id.* at 944. If the Sixth Circuit does not deem *Dickens* precedential, neither will the Court.

*Losch*, 995 F.3d at 945. Second, "when a credit reporting agency has been notified of potentially inaccurate information in a consumer's credit report, it is in a very different position than one who has no such notice." *Id.* (citation modified).

At this stage, the Plaintiffs have properly alleged that the CRA Defendants failed to follow reasonable procedures because the Plaintiffs have alleged facts showing that the CRA Defendants have "a reason to believe that the information supplied to it by a data furnisher is unreliable." *See Losch*, 995 F.3d at 945. First, the Plaintiffs allege that the CRA Defendants knew the dangers inherent in using customer driving data, from issues of inaccuracy to customer consent. (*See e.g.* Am. Compl. ¶¶ 813-14). Concerns over reliability of the driving data are further heightened by the existence of LNRS Report data that shows a "negative" number of events occurring. (*Id.* ¶ 917). Additionally, variances across credit reporting agencies in classifying certain driving behaviors and ongoing criticism aimed at credit reporting agencies for data gathering and classification practices puts the CRA Defendants on notice, as industry participants, that the release of driving data in consumer reports must be heavily scrutinized to ensure accuracy. (*See e.g. id.* ¶ 922 n. 316, 928 n. 320, 924-31).

There is also evidence that LNRS has been notified of the existence of potentially inaccurate information in a consumer's credit report. *See Losch*, 995 F.3d at 945. Within their pleading, the Plaintiffs show at least one named

Plaintiff, Montgomery, disputed the errors within his report. (*See* Am. Compl. ¶ 533). While not pertaining to the driving data itself, the disputed errors pertaining to a misassigned social security number and a name he had never used demonstrate that the dataset that LNRS was working off of had fundamental errors. Accordingly, LNRS should have been on notice of the inaccuracies within its dataset if reasonable procedures had been followed.

The CRA Defendants' reliance on three unreported cases[22] is misplaced. Each case confronts the issue of formulaic recitation of the law within the complaint with no additional factual pleadings that support that claim.[23] Here, the CRA Defendants' argument that the Amended Complaint is factually devoid of allegations satisfying this element of their FCRA claim is divorced from reality. Accordingly, the Amended Complaint contains sufficient factual support for the allegations that the CRA Defendants failed to follow reasonable procedures.

---

[22] *Saint-Cyr v. Equifax Info. Servs., LLC*, 2025 WL 432832 (N.D. Ga. Jan. 8, 2025); *Hill v. Equifax Info. Servs., LLC*, 2021 WL 7708391 (N.D. Ga. Dec. 22, 2021); *Lazarre v. JPMorgan Chase Bank, N.A.*, 780 F. Supp. 2d 1320 (S.D. Fla. 2011).

[23] *Saint-Cyr*, 2025 WL 432832 at *5 ("Saint-Cyr sets forth no facts to support this element of his Section 1681e(b) claim. He simply states that Equifax 'failed to maintain and/or follow reasonable procedures to assure maximum possible accuracy of the information it reported'"); *Hill*, 2021 WL 7708391 at *3 ("Ms. Hill alleges that Equifax 'failed to maintain and/or follow reasonable procedures to assure maximum possible accuracy of the information that it reported to one or more third parties pertaining to Plaintiff.' Likewise, Ms. Hill alleges that, after receiving her dispute, Equifax 'failed to conduct a reasonable reinvestigation.' (citation modified)); *Lazarre*, 780 F. Supp. 2d at 1328-29 ("Lazarre fails to allege any facts, beyond the mere 'formulaic recitation of the elements of a cause of action'" (citation omitted)).

### 3. Damages

The third element of the Plaintiffs' FCRA claim requires the Plaintiffs to plead facts alleging that damages followed as a result of inaccuracies present within the consumer reports. *See Losch*, 995 F.3d at 944. For a plaintiff to show this element of their FCRA claim, he must allege sufficient facts where it is plausible that "a reasonable trier of fact could infer that the inaccurate entry was a 'substantial factor'" in bringing about the damages. *Enwonwu v. Trans Union, LLC*, 364 F. Supp. 2d 1361, 1365-66 (N.D. Ga. 2005), *aff'd*, 164 F. App'x 914 (11th Cir. 2006) (citing Restatement (Second) of Torts § 431(a)).

Here, most of the named Plaintiffs allege an increase in insurance premiums after automotive insurance companies accessed the LNRS Report and/or the Verisk Report. (*See e.g.* Am. Compl. ¶¶ 20-22). However, the CRA Defendants argue that that the Plaintiffs do not allege that the increases were *specifically caused* by the alleged reporting of the driving data. (*See* Br. in Supp. of LNRS' Mot. to Dismiss, at 25-26). They also argue that the Plaintiffs fail to allege any facts showing that the alleged increases in insurance premiums were not caused by some other factor. (*Id.* at 26). The CRA Defendants point to the fact that the cost of insurance premiums is calculated based on a variety of factors, such as age, gender, driving experience, driving records of all members in a household, and nationwide trends. (*Id.* at 27). However, this argument distorts both the applicable case law as well as pleading requirements under the Federal Rules of Civil Procedure.

*Enonwu* is instructive. In *Enonwu*, a pro se plaintiff brought a Section 1681e(b) claim against the defendant for inaccurate information on his credit report that led to a failure to obtain satisfactory financing for two real estate transactions. *Enonwu*, 364 F. Supp. 2d at 1363-64. After discovery, the defendant moved for summary judgment on the issues of causation and harm, not disputing the inaccurate information. *Id.* at 1365. In reviewing the applicable standard, the court held that in showing that inaccurate information was a "substantial factor" in bringing about a denial of credit, a plaintiff need not eliminate the possibility that other factors contributed to the harm suffered by the plaintiff. *Id.* at 1366 (citing *Cahlin*, 936 F.2d at 1161). This is because, the court explained, decisions to deny credit will frequently have more than one cause. *Id.* Ultimately, the court held that the pro se plaintiff failed to present enough evidence to withstand summary judgment because the plaintiff "presented neither direct nor circumstantial evidence indicating that the credit granting agencies actually utilized the inaccurate report." *Id.*; *see Enwonwu*, 164 F. App'x at 918.

Here, like the decisions to deny credit in *Enwonwu*, the decision to increase insurance premiums is one that depends on a variety of factors, as the CRA Defendants admit. (*See* Br. in Supp. of LNRS' Mot. to Dismiss, at 27). Adjusting the standard then to one more relevant for the motion to dismiss stage of litigation, the Plaintiffs are not required to eliminate every other factor for why insurance premiums could go up within their Amended Complaint so

long as the Plaintiffs allege facts that make it *plausible* that the alleged inaccurate information present within the LNRS and Verisk Reports was a "substantial factor" causing insurance premium increases for the named Plaintiffs through their respective insurers.

Here, the Plaintiffs have alleged sufficient direct and circumstantial evidence to make it plausible that insurers utilized the inaccurate LNRS and Verisk Reports. *See Enwonwu*, 364 F. Supp. 2d at 1366. Plaintiff Weaver, for example, alleges that he maintained insurance coverage for his 2023 Chevrolet Corvette through the insurer USAA. (Am. Compl ¶ 20). He alleged that USAA accessed his LNRS Report on or about December 7, 2023. (*Id.*). The same month, USAA informed Plaintiff Weaver that the insurance premium for the vehicle would increase by approximately $50 per month without any explanation for the rate increase. (*Id.*) Plaintiff Weaver further alleges that he had not filed an insurance claim, been in an automobile accident, received a speeding ticket, or experienced any other incident that could account for the increase in insurance premium prices. (*Id.* ¶ 21). Most of the other named Plaintiffs allege similar facts. Where most of the named Plaintiffs allege premium increases after their insurance provider accessed their LNRS Report or Verisk Report, it is difficult for the Court to conclude that it is not plausible, after discovery, that the Plaintiffs will be able to state their claim based on the facts alleged within the Amended Complaint.

However, the CRA Defendants urge the Court to consider *Purdy v. Experian Information Solutions, Inc.*, 2005 WL 8157972 (N.D. Ala. Nov. 3, 2005), citing the case throughout their argument. In *Purdy*, the plaintiff brought a Section 1681e(b) claim against a defendant after alleged inaccurate information regarding a judgment that was not paid off was present on a credit report and resulted in a higher interest rate when the plaintiff sought a loan. *Id.* at *5, *8. The court ultimately held that the plaintiff failed to meet his evidentiary burden on summary judgment because there were a myriad of factors involved in setting an interest rate. *Id.* at *8.

*Purdy* is distinguishable for several reasons apart from the fact that the opinion is a Report and Recommendation and that it is unreported. First, the evidence before the court demonstrated that the inaccuracy of the information on the credit report had little effect on the credit officer's evaluation of the plaintiff's interest rate since past history of a judgment against the plaintiff is a negative factor regardless. *Id.* at *8 n.17. Second, there was ample evidence of other negative factors within the plaintiff's credit report such that the plaintiff could not show that the inaccuracy was a "substantial factor." *Id.* at *9. Third, at a deposition, the plaintiff admitted that he did not know how the inaccuracy affected his interest rate. *Id.* None of these factors are present within the Plaintiffs' allegations here, making *Purdy* wholly distinguishable

As a final note, while the Court will not dismiss the affirmative FCRA claim as it pertains to the vast majority of the named Plaintiffs, certain named

Plaintiffs do not pass muster in bringing an FCRA claim. The CRA Defendants accurately highlight, and the Plaintiffs do not dispute, that nine of the named Plaintiffs fail to allege that their insurance premiums increased at all and do not allege any adverse action arising from the inaccurate reporting by the CRA Defendants. (Br. in Supp. of LNRS' Mot. to Dismiss, at 26 n. 10). Accordingly, the Court will dismiss from Count 10 the claims of Plaintiffs Brunet, Gray, Brockington, Gordin, Matthews, Brakefield, Davids, Guc, and Parkhurst for failure to allege any injury caused by the acts of the CRA Defendants under FCRA.

**4. Civil Liability for a Willful Violation of the FCRA**

The Plaintiffs request relief against the CRA Defendants for the CRA Defendants' willful and negligent noncompliance with Section 1681e(b). (*See* Am. Compl. ¶¶ 1109-10). The CRA Defendants argue that their conduct, as alleged in the Amended Complaint, is not plausibly a willful violation of the FCRA. (*See* Br. in Supp. of LNRS' Mot. to Dismiss, at 27). A willful violation of the FCRA requires that the violation be either knowing or reckless. *See Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 57-58 (2007); *Pedro v. Equifax, Inc.*, 868 F.3d 1275, 1280 (11th Cir. 2017).

For there to be a reckless violation of FCRA, there must be an action that "is not only a violation under a reasonable reading of the statute's terms but shows that the company ran a risk of violating the law substantially greater than the risk associated with a reading that was merely careless."

*Safeco*, 515 U.S. at 69. A consumer reporting agency that adopts a reading of the FCRA that is "not objectively unreasonable" based on the text of the statute, judicial precedent, or guidance from administrative agencies will not be held in willful violation of the statute. *Pedro*, 868 F.3d at 1280 (citing *Safeco*, 515 U.S. at 70). Subjective intent by the consumer reporting agencies is irrelevant to the inquiry of whether a violation was willful. *Id.* Finally, the resolution of "willfulness" on a motion to dismiss is proper when the interpretation of the relevant statute by the consumer reporting agency "[is] not objectively unreasonable." *Id.* at 1282 (collecting district court cases where courts dismissed claims contingent on the finding of a willful violation).

With the Eleventh Circuit's guidance in mind, the Court finds the CRA Defendants' arguments persuasive as it pertains to their use of decontextualized data. While the Court held that the use of decontextualized data could constitute an "inaccuracy" under the FCRA, the Court acknowledges that driving data-based FCRA claims are novel because much of the existing jurisprudence on Section 1681e(b) relates to credit reporting. Based on existing case law relating to Section 1681e(b), courts have generally held that the inclusion of context is not required for negative events as it relates to credit reporting. *See e.g. Peterson*, 2018 WL 7348859 at *9. Furthermore, neither existing administrative guidance nor the text of the FCRA implies that context is clearly necessary when a consumer reporting

agency provides reports.[24] Accordingly, the Court holds that all named Plaintiffs whose claims arise out of injury from purely decontextualized data cannot plead a willful violation of the FCRA.

However, the Court will not dismiss claims arising out of other grounds of inaccuracy, such as the Plaintiffs who allege "multiple-driver" distortions of data or actual errors within the LNRS Report or Verisk Report because such claims allege the reports contained the misattribution of certain data as well as actual false information. Neither the text of Section 1681e(b) nor existing case law permit a consumer reporting agency to rely on potentially unreliable data in creating its consumer reports, as discussed earlier. Although the CRA Defendants argue that insurers underwrite the vehicle instead of the individual, reliance on the industry practice when turning to consumer reports that focus on driving behaviors attributed to the individual does not find its support in administrative decisions, the text of the statute, or existing precedent. *See Pedro*, 868 F.3d at 1280 (citing *Safeco*, 515 U.S. at 70).

Furthermore, the allegations put forth by the Plaintiffs are not conclusory in any nature as the CRA Defendants argue. The Plaintiff put forth

[24] Indeed, if such jurisprudence or administrative decision existed, one would expect the Plaintiffs to provide it within their extensive briefing on the issue. However, the Plaintiffs fail to show any such source material to demonstrate that the CRA Defendants' conduct was objectively unreasonable, both in their briefing for this section, along with their briefing when discussing whether an "inaccuracy" existed under the FCRA, opting to instead show why *Peterson* is inapplicable here. (*See* Pls.' Br. in Opp'n to LNRS' Mot. to Dismiss, at 27-28).

some evidentiary allegations that make it plausible that the CRA Defendants undertook the conduct causing the FCRA violation in a willful manner. First, the Plaintiffs have pled extensively through the Amended Complaint that the CRA Defendants knew the dangers of using driving data and still used the data with inaccurate entries. (*See e.g.* Am. Compl. ¶¶ 813-14). The Plaintiffs have also pled that, despite being put on notice of the inaccuracy of the data, the CRA Defendants continued to use the driving data in their consumer reports. (*See e.g. id.* ¶ 1106(b)). Those pleadings, along with speculative and formulaic pleadings, are enough to make it plausible that a willful violation of the CFRA has occurred.

In sum, the Court will not dismiss the FCRA claim for the vast majority of named Plaintiffs. However, the Court will dismiss from Count 10 the claims of Plaintiffs Brunet, Gray, Brockington, Gordin, Matthews, Brakefield, Davids, Guc, and Parkhurst for failure to allege any injury caused by the acts of the CRA Defendants under FCRA. Furthermore, out of the named Plaintiffs that remain, all Plaintiffs who allege *only* damages arising out of the lack of context provided within their consumer reports may not pursue their FCRA claim under 15 U.S.C. § 1861n due to their failure to sufficiently plead that a willful violation occurred.

### F. State and Common Law Claims

The Plaintiffs allege 32 state law statutory claims and five common law claims against some or all of the Defendants. Before addressing the claims on

the merits, the Defendants put forth three preliminary arguments. First, the CRA Defendants argue that the common law claims must be dismissed from the Amended Complaint because they fail to state a source of law. (*See* Br. in Supp. of Verisk's Mot. to Dismiss, at 17-19). Second, the Defendants argue that the FCRA preempts the great majority of these claims. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 44-51; Br. in Supp. of LNRS' Mot. to Dismiss, at 5-18). Third, the GM Defendants argue that the Plaintiffs fail to allege facts supporting Article III standing. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 51-57). Accordingly, before adjudicating the claims on the merits, the Court will first address the Defendants' preliminary arguments.

**1. Choice of Law for Nationwide Common Law Claims (Counts 5-9)**

The Plaintiffs assert five common law claims against the GM Defendants on behalf of a purported nationwide class, or alternatively, on behalf of the statewide subclasses. Counts 5 and 6 assert an invasion of privacy claim and an accompanying conspiracy claim arising out of the invasion of privacy, (*See* Am. Compl. ¶¶ 1048-77), Count 7 asserts an unjust enrichment claim, (*See id.* ¶¶ 1078-82), Count 8 asserts a breach of contract claim, (*See id.* ¶¶ 1083-88), and Count 9 asserts a trespass to chattels claim, (*See id.* ¶¶ 1089-95).

The CRA Defendants argue that pleading the common law claims in such a manner, without identifying which state's law applies, is impermissible. (Br. in Supp. of Verisk's Mot. to Dismiss, at 18). In response, the Plaintiffs

argue that under Georgia's choice-of-law doctrine, Georgia law applies to each of the common law claims in the Amended Complaint and that a detailed choice-of-law analysis is unnecessary at the motion to dismiss stage. (Br. in Opp'n to Verisk's Mot. to Dismiss, at 18).

First, the Court addresses Plaintiffs' request to punt the choice-of-law determination to the forthcoming motions on class certification. The Plaintiffs, in support of their argument, urge the Court to look at this Court's prior ruling in *In re ConAgra Peanut Butter Prods. Liab. Litig.*, 2008 WL 2132233 (N.D. Ga. May 21, 2008). In *In re ConAgra*, this Court confronted a motion to dismiss where the plaintiffs argued that choice-of-law issues should only be considered at class certification and not at the motion to dismiss stage, similar to the Plaintiffs here. *Id.* at *1. This Court agreed to a certain extent, finding that "it is premature to conduct a rigorous choice of law analysis at [the motion to dismiss] stage." *Id.* Nonetheless, this Court still acknowledged that "some consideration of the applicable rules [regarding choice-of-law] will be necessary for resolution of the motion to dismiss." *Id.* Relying on this Court's previous decision in *ConAgra*, the Court will engage in the choice-of-law analysis necessary here to resolve the Motion to Dismiss and engage in a more rigorous choice-of-law analysis when considering motions on class certification.[25]

[25] As will be discussed further when addressing the Defendants' preemption arguments, understanding what source of law each common law claim arises out of is crucial to a determination of whether the Plaintiffs' claims are preempted. Accordingly, the Court finds it necessary to evaluate whether

Turning to the choice-of-law analysis, the Court's jurisdiction to preside over this putative class arises out of federal question jurisdiction for the federal claims, while the state and common law claims arise out of supplemental jurisdiction. "When a federal court decides a state law claim, whether acting pursuant to . . . supplemental jurisdiction, it applies the choice-of-law rules of the jurisdiction in which it[ ] sits." *Carter v. Porsche Cars N. A., Inc.*, 2021 WL 6805718, at *4 (N.D. Ga. Jun. 25, 2021) (citing *Boardman Petroleum, Inc. v. Federated Mut. Ins. Co.*, 135 F.3d 750, 752 (11th Cir. 1998)). However, in multidistrict litigation actions under 28 U.S.C. § 1407, the transferee court typically applies the state law that the transferor court would have applied. *See Murphy v. F.D.I.C.*, 208 F.3d 959, 965 (11th Cir. 2000) ("Our [federalist] system contemplates differences between different states' laws; thus a multidistrict judge asked to apply divergent state positions on a point of law would face a coherent, if sometimes difficult, task.").

An exception to this rule is relevant here. Multidistrict litigation proceedings may adopt the choice-of-law rules of the transferee court if both parties "consent to filing a 'master complaint' that supersedes the previously filed individual pleadings and merges the transferred actions until pretrial proceedings have concluded." *In re January 2021 Short Squeeze Trading Litig.*, 584 F. Supp. 3d 1161, 1179 (S.D. Fla. 2022) (citing *Gelboim v. Bank of Am.*

---

Georgia law or the law of other states applies to the Plaintiffs' common law claims and whether dismissal of these claims is warranted.

*Corp.*, 574 U.S. 405, 413 n. 3 (2015)); *see In re Bridgestone/Firestone, inc. Tires Prods. Liab. Litig.*, 155 F. Supp. 2d 1069, 1078 (S.D. Ind. 2001) ("However, the parties agree that this Court should be treated as the forum court because Plaintiffs filed their Master Complaint in this Court. Indiana's choice of law rules therefore are applicable.").

Similarly, both parties have consented to a superseding master complaint. (*See* Joint Preliminary Report and Discovery Plan, at 20 [Doc. 84]; Case Management Order No. 2 [Doc. 91]; Am. Compl. ¶ 9). However, the Defendants reserved their right to object to venue and personal jurisdiction upon providing their consent. (*See* Joint Preliminary Report and Discovery Plan, at 20). While the Defendants may argue that the transferor choice-of-law rules apply under 28 U.S.C. § 1407 due to this reservation, the Defendants have provided no authority arguing otherwise, failing to meet their burden on this Motion to Dismiss. (*See* Am. Compl. ¶ 9).

Even if the Defendants are correct in that the Amended Complaint is not intended to be superseding, the facts within the Amended Complaint show that the Plaintiffs intend to seek class certification within this forum. Within their statement of jurisdiction and venue, the Plaintiffs assert that personal jurisdiction exists over all Defendants within this forum. (Am. Compl. ¶ 8). Furthermore, the Plaintiffs provide detailed class action allegations seeking certification of a nationwide class, an FCRA subclass, and state subclasses. (*See id.* ¶¶ 963-73). If class certification were granted, Georgia common law

would apply to the class's common law claims because the Court has supplemental jurisdiction over the claims. Therefore, at the motion to dismiss stage, Georgia's choice-of law rules apply to the common law claims.[26]

Accordingly, the Court now turns to the application of Georgia's choice-of-law rules to determine whether the common law claims should be dismissed for a failure to plead a source of law. When addressing choice-of-law, Georgia courts regularly apply the rules of *lex loci contractus* and *lex loci delecti*. *Sowa v. Mercedes-Benz Group AG*, 764 F. Supp. 3d 1233, 1256 (N.D. Ga. 2024) (citation omitted). "Under these rules, respectively, contract disputes are governed by the 'substantive law of the state where the contract was made' and tort disputes are 'governed by the substantive law of the state where the tort was committed.'" *Monopoli v. Mercedes-Benz USA, LLC*, 2022 WL 409484, at *4 (N.D. Ga. Feb. 10, 2022) (quoting *Rayle Tech, Inc. v. DEKALB Swine Breeders, Inc.*, 133 F.3d 1405, 1409 (11th Cir. 1998)).

However, an exception arises when the complaint is silent as to the source of law of the common law claim. Although subject to much controversy,

---

[26] The CRA Defendants argue, in their reply brief, that the Court cannot apply Georgia's choice-of-law rules to Verisk because the Court has no personal jurisdiction over Verisk. "Arguments not properly presented in a party's initial brief or raised for the first time in the reply brief are deemed waived." *In re Egidi*, 571 F.3d 1156, 1163 (11th Cir. 2009). Additionally, personal jurisdiction is waivable. *See Day v. Persels & Assocs., LLC*, 729 F.3d 1309, 1326 (11th Cir. 2013) ("Our law is clear that 'objections to personal jurisdiction . . . are waivable.'" (citation omitted)). Here, Verisk was aware that Plaintiffs intend to seek class certification within the Court and should have raised their personal jurisdiction argument within the initial briefing. Because Verisk failed to do so, the Court will consider the argument waived.

when a common law claim is silent on whether domestic or foreign law is being pled, Georgia courts stand alone in applying the common law as developed in Georgia rather than applying foreign case law. *See Coon v. The Med. Ctr., Inc.*, 300 Ga. 722, 729 (2017) ("In the absence of a statute, however, at least with respect to a state where the common law is in force, a Georgia court will apply the common law as expounded by the courts of Georgia"); *see also Monopoli*, 2022 WL 409484 at *4 ("Georgia courts stand alone in following this century-old, controversial practice, but the Georgia Supreme Court, nonetheless, has upheld this aspect of Georgia's choice-of-law rules"). Here, because Georgia's choice-of-law rules apply to the Amended Complaint, the Court applies the Georgia rule and holds that the Plaintiffs have adequately pled a source of law for their common law claims.

**2. FCRA Preemption**

The preemption doctrine contains a deceivingly simple premise: "where a federal law and a state law conflict, federal law trumps state law." *Marrache v. Bacardi U.S.A., Inc.*, 17 F.4th 1084, 1094 (11th Cir. 2021) (citation modified). In reality, the Constitutional doctrine borne out of the principles of federalism is anything but simple. The preemption doctrine can be applied either explicitly or implicitly. *See id.* "Express preemption occurs when Congress manifests its intent to displace a state law using the text of a federal statute." *Id.* (citation omitted). In either manner of application, an analysis of preemption is guided by two guideposts. First, the purpose of Congress,

discerned from the language of the preemption statute and the surrounding statutory language, is "the ultimate touchstone in every [preemption] case. *Id.* (citing *Wyeth v. Levine*, 555 U.S. 555, 565 (2009)). Second, courts assume that Congress did not intend to override the powers of the states unless that was "the clear and manifest purpose of Congress." *Id.* Ultimately, "[w]hen the text of an express pre-emption clause is susceptible of more than one plausible reading, courts ordinarily accept the reading that disfavors pre-emption." *Altria Group, Inc. v. Good*, 555 U.S. 70, 77 (2008) (citation omitted).

The fundamental general preemption provision providing support for the Defendants' arguments states that:

> Except as provided in subsections (b) and (c), [the FCRA] 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 [the FCRA], and then only to the extent of the inconsistency.*

15 U.S.C. § 1681t(a) (emphasis added).

Using this provision and other provisions throughout Section 1681, the Defendants argue that the Plaintiffs' claims are preempted. Here, the GM Defendants and the CRA Defendants focus on these provisions when making their preemption arguments. The GM Defendants' preemption argument focuses on 15 U.S.C. § 1681t(b)(1)(F) while the CRA Defendants' argument focuses on 15 U.S.C. § 1681t(a) and 15 U.S.C. § 1681h(e). (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 46-49; Br. in Supp. of LNRS' Mot. to Dismiss, at

18-20). The Defendants also advance arguments related to conflict and implied preemption. The Court will address the preemption arguments separately.

**a. Section 1681t(b)(1)(F)**

Section 1681t(b)(1)(F) states that "[n]o requirement or prohibition may be imposed under the laws of any State . . . with respect to any subject matter regulated under . . . section 1681s-2." 15 U.S.C. § 1681t(b)(1)(F). Section 1681s-2 regulates the responsibilities of furnishers of information to consumer reporting agencies. *See generally* 15 U.S.C. § 1681s-2. The term "furnishers of information" has been interpreted by courts to include entities that provide information to credit reporting agencies. *See Bueno v. Univ. of Miami*, 2023 WL 3093614, at *4 (S.D. Fla. Apr. 26, 2023); *Porter v. Experian Info. Servs., Inc.*, 2021 WL 5068262, at *7 n.12 (N.D. Ga. Oct. 30, 2021), *report and recommendation adopted sub nom.*, *Porter v. Experian Info Servs., LLC*, 2022 WL 887288 (N.D. Ga. Jan. 27, 2022).

The GM Defendants argue that, as a furnisher of information, Section 1681s-2 regulates their disclosures and therefore the FCRA preempts all state and common law claims against them.[27] (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 46). The Plaintiffs do not contest the characterization of the GM Defendants as furnishers. However, they do argue that Section 1681t(b)(1)(F)

[27] The CRA Defendants also adopt the arguments of the GM Defendants within this section in their briefing. (Br. in Supp. of LNRS' Mot. to Dismiss, at 15 n. 4).

does not preempt their state and common law claims because it gives consumers more protection than the FCRA.

The Court reviews the text once more. The United States Supreme Court has held that the phrase "no requirement or prohibition" may preempt both common law and state law claims. *Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 505 (1992); *see Spencer v. National City Mortg.*, 831 F. Supp. 2d 1353, 1363 (N.D. Ga. 2011). However, the inquiry does not end here. *See Spencer*, 831 F. Supp. 2d at 1363. Courts in this district have settled on two elements that must be met for a claim to be preempted under this section: (1) "the 'requirement or prohibition' —i.e., the legal duty giving rise to the claim—must be 'imposed under the laws of any State'" and (2) "the state-law claim must relate to a 'subject matter regulated under . . . section 1681s-2.'" *See e.g. id*; *Bruce v. Homeward Residential, Inc.*, 2015 WL 5797846, at *12 (N.D. Ga. Aug. 31, 2015). The Court will now turn to apply this test to the common law and state law claims asserted against the GM Defendants.

### i. Common Law Claims

"Although § 1681t(b)(1)(F)'s preemption reaches common-law causes of action, it does not preempt *all* claims of whatever nature or origin against furnishers of information to CRAs." *Spencer*, 831 F. Supp. 2d at 1263. Within the Amended Complaint, the Plaintiffs assert four claims arising under Georgia common law: (1) invasion of privacy (conspiracy included), (2) breach

of contract, (3) unjust enrichment, and (4) trespass to chattels. The Court reviews each claim in turn.

### 1. Invasion of Privacy

The Plaintiffs assert a claim under the common law tort of invasion of privacy against all the Defendants. Here, there is little question that the "requirement or prohibition" arises out of the laws of Georgia with respect the Plaintiffs' claim. Georgia courts originally recognized the common law tort of invasion of privacy in *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190 (1905), when the Supreme Court of Georgia created the cause of action. *See Bullard v. MRA Holding, LLC*, 890 F. Supp. 2d 1323, 1332 (N.D. Ga. 2012) (reviewing the history of the common law tort of invasion of privacy in Georgia). In *Pavesich*, the Supreme Court of Georgia held that the common law right of privacy arose out of Georgia law. *Pavesich,* 122 Ga. at 197 ("The right of privacy within certain limits is a right derived from natural law, recognized by the principles of municipal law, and guarantied to persons in this state both by the Constitutions of the United States and of the state of Georgia, in those provisions which declare that no person shall be deprived of liberty except by due process of law."). It is this right of privacy that the Plaintiffs now bring their claim under.

The question then, is whether the Plaintiffs' claims relate to subject matter regulated under Section 1681s-2. At least one court within the district has held that invasion of privacy common law claims are preempted to the

extent they relate to a furnisher's reporting of information. *See Taylor v. Midland Funding, LLC*, 2015 WL 4670314, at *13 (N.D. Ga. Aug. 6, 2015) ("Therefore, § 1681t(b)(1)(F) preempts the plaintiff's invasion of privacy claim to the extent that claim is based on the defendants' reporting of the debt in question."); *see also Frazier v. Synovus Fin. Corp.*, 2023 WL 6323084, at *6 (E.D. Pa. Sep. 28, 2023).

Here, the Plaintiffs allege in the Amended Complaint that they have a privacy interest in their driving data and the underlying activities giving rise to the driving data. (*See* Am. Compl. ¶¶ 1049-50). The Plaintiffs further allege that the Defendants' actions are intentionally intrusive, imposing constant, nonconsensual surveillance on the Plaintiffs through the collection and distribution of their driving data, without regard for its accuracy. (*See id.* ¶¶ 1052-65). The Defendants infringed upon the Plaintiffs' privacy, they allege, by (1) "allowing the dissemination and/or misuse of their Driving Data," (2) "preventing Plaintiffs and Class Members from maintaining control over the type of information that GM track[s] and/or record[s]," and (3) "preventing Plaintiffs and Class Members from making personal decisions and/or conducting personal activities without observation, intrusion, or interference" through the public availability of the data. (*Id.* ¶ 1060).

As far as the GM Defendants are concerned within this count, some of these intrusions into the Plaintiffs' private lives concern the GM Defendants' furnishing of their information. 15 U.S.C. § 1681s-2 contains a few provisions

that cover the "subject matter" of the violation alleged here. As it pertains to inaccuracies in the reported information, 15 U.S.C. §§ 1681s-2(a)(1)-(2) discusses the duty of furnishers to provide accurate information. Neither party disputes its relevance to the instant matter.

The parties do dispute whether 15 U.S.C. § 1681s-2(a)(7) should be considered as part of the "subject matter" of 15 U.S.C. § 1681s-2 with respect to the invasion of privacy claim. The provision discusses the specific furnishers required to provide notice to consumers when negative information is being reported. *See* 15 U.S.C. § 1681s-2(a)(7). The Plaintiffs argue that, in determining whether their claims intersect with Section 1681s-2(a)(7), the GM Defendants are not the furnishers who are regulated under the statute. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 42 n. 33). In response, the GM Defendants argue that, because Congress has regulated certain furnishers with respect to the furnishing of negative information, the subject matter of Section 1681s-2 still covers the Plaintiffs' invasion of privacy claim because the Plaintiffs' claims hinge on notice and consent. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 28).

After reviewing authority within the Circuit, along with the Amended Complaint, the Court holds that Section 1681s-2(a)(7) is inapplicable here when considering the "subject matter" of Section 1681s-2. When an invasion of privacy claim is based on false or inaccurate reporting by a furnisher, that is "conduct that falls squarely within the subject matter of § 1681t(b)(1)(F)."

*Taylor*, 2015 WL 4670314 at *13. However, FCRA preemption has generally only been extended to the extent the common-law claim concerns the inaccurate reporting.[28] Thus, the GM Defendants' position about the applicability of Section 1681s-2(a)(7) would extend FCRA preemption past what courts have already accepted.

The Court declines to extend FCRA preemption further than already recognized within the Circuit. Because courts must disfavor preemption in interpreting the statutory text, the Court finds no reason to cut against this axiom. *See Altria Group, Inc.*, 555 U.S. at 77. Here, the Plaintiffs' theory relies on characterizing the collection of driving data as a surveillance-like activity. Not only do the GM Defendants not qualify as the institutions required to give notice, but Section 1681s-2(a)(7) is part of a broader subsection that discusses the furnisher's duty to provide accurate information. *See* 15 U.S.C. § 1681s-2(a). A single provision discussing notice preempting the entire invasion of privacy claim would broadly expand preemption as understood within the Circuit. Therefore, the Plaintiffs' invasion of privacy claim is

[28] *See id.*; *Streicher v. U.S. Bank Nat'l Assoc.*, 2014 WL 12496565, at *6 (S.D. Fla. Nov. 20, 2014) (holding that the FCRA preempts the plaintiffs' breach of contract claim to the extent it alleges an impairment to their credit in violation of the implied duty of good faith and fair dealing); *Polk v. Wells Fargo Bank, N.A. (Inc.)*, 2020 WL 9599951, at *4-5 (N.D. Ga. Feb. 11, 2020), *report and recommendation adopted in part, rejected in part on other grounds*, 2020 WL 9599753 (N.D. Ga. Mar. 19, 2020) (holding common law claims were not preempted because they were not based on the inaccurate reporting of information to a CRA or failure to correct inaccuracies).

preempted only to the extent it is predicated on the inaccurate reporting of information.

**2. Breach of Contract**

Count 8 of the Plaintiffs' Amended Complaint brings a common law breach of contract claim against GM. While the crux of the GM Defendants' preemption argument focuses on whether the common law claims interfere with the subject matter of Section 1681s-2, they fail to address the preliminary issue of whether Plaintiffs' breach of contract claim arises out of Georgia law. The Court finds that it does not arise out of Georgia law.

Judge Batten's decision in *Spencer* is instructive. In *Spencer*, the plaintiff brought an FCRA claim and three common law claims against the defendant. 831 F. Supp. 2d at 1355-56. Similar to the GM Defendants here, the defendant argued that Section 1681t(b)(1)(F) preempted all state-law claims against furnishers. *Id.* at 1356. After establishing the requirements for a state-law claim to be preempted under Section 1681t(b)(1)(F), the district court turned to analyze whether the Plaintiffs' breach of contract claim was preempted.

Key to its decision, the court considered the Supreme Court's plurality opinion in *Cipollone v. Liggett Group, Inc.*, 505 U.S. 504 (1992), as adopted by the Eleventh Circuit in *Spain v. Brown & Williamson Tobacco Corp.*, 363 F.3d 1183, 1192 (11th Cir. 2004). *See id.* at 1363-64. The district court noted that, for a suit brought under a common law breach of an express warranty claim,

the Eleventh Circuit determined that the "requirement" arose from the express terms of the warranty, not from the laws of any state. *Id.* at 1363-64 (quoting *Spain*, 363 F.3d at 1198). While the district court acknowledged that *Spain* concerned itself with a different federal statute, the court nonetheless found the opinion persuasive due to the analogous reasoning necessary to resolve the issue of preemption. *Id.* at 1364. Despite a circuit split on whether breach of contract claims are preempted by the FCRA, the district court ultimately concluded that the Eleventh Circuit's decision in *Spain* is analogous and would reflect the appellate court's reasoning to exclude breach of contract claims from preemption under Section 1681 if the issue were before it. *Id.*

The Court agrees with Judge Batten. The preemption statute in *Spain* arises out of the Federal Cigarette Labeling and Advertising Act of 1965, as amended by the Public Health Cigarette Smoking Act of 1969. *See Spain*, 363 F.3d at 1191. The statute states, in part, that "[n]o requirement or prohibition based on smoking and health shall be imposed under State law with respect to the advertising or promotion of any cigarettes the packages of which are [lawfully] labeled." *Id.* (quoting 15 U.S.C. § 1334(b)). The requirement that a common-law claim be "imposed under State law" directly mirrors the elements to preempt a state or common law claim under the FCRA. The Eleventh Circuit ultimately extended the holding in *Cipollone* to deny preemption to claims arising out of a breach of both implied and express warranties because they are imposed contractually and not by the State, so there is little reason to

assume that breach of contract claims are any different, given such claims are based on the terms of a purported contract. *See id.* at 1999. Outside of *Spencer*, courts within this Circuit have held similarly.[29] Therefore, the Plaintiffs' breach of contract claim is not preempted by the FCRA.

### 3. Unjust Enrichment

The Plaintiffs bring Count 7 under a theory of unjust enrichment under Georgia law. This claim is brought in the alternative to the Plaintiffs' breach of contract claim. (Am. Compl. ¶ 1084). The Plaintiffs allege that, by driving GM vehicles, the Plaintiffs "unknowingly conferred the benefit of their Driving Data on" the Defendants without consent. (*Id.* ¶¶ 1079, 1081). The Plaintiffs also allege that the Defendants "knew and appreciated that benefit" and demand restitution for the value conferred. (*Id.* ¶¶ 1080, 1082).

Unlike the Plaintiffs' breach of contract claim, unjust enrichment is not derived from any express terms between two parties, likely because it is a common-law claim brought in the absence of a contract. *See Collins v. Athens*

---

[29] *See e.g. Carruthers v. Am. Honda. Fin. Corp.*, 717 F. Supp. 2d 1251, 1254-55 (N.D. Fla. 2010) (holding express warranties are not preempted under Section 1681t(b)(1)(F), while implied warranties in a breach of contract claim are preempted); *Bruce*, 2015 WL 5797846, at *15 n. 6 (in a magistrate judge's report and recommendation, holding that if the district judge finds that the breach of contract claim centers around the false reporting to the credit agencies, then *Spencer* is persuasive and it does not preempt the claim under the FCRA); *Streicher*, 2014 WL 12496565 at *6 (discussing *Spencer*, *Carruthers*, and *Spain* to hold that breach of an express agreement would not be preempted under the FCRA); *Polk*, 2020 WL 9599951 at *4 (agreeing with *Spencer* and holding that breach of contract claims are not preempted by the FCRA).

*Orthopedic Clinic*, 356 Ga. App. 776, 778 (2020) (citation modified). Accordingly, there is little dispute that unjust enrichment is imposed by the laws of Georgia. But the crux of the unjust enrichment claim fails to relate to the "subject matter" of Section 1681s-2 in any discernible way. The Plaintiffs do not allege, in any way, that the purported unjust enrichment occurred because of false reporting by the GM Defendants. The claims by the Plaintiff are direct and are based on the acquisition of the information that the GM Defendants furnished. Therefore, the Plaintiffs' unjust enrichment claim is not preempted by the FCRA.

**4. Trespass to Chattels**

The Plaintiffs also bring Count 9 against all Defendants under a common-law theory of trespass to chattels. The Plaintiffs' Amended Complaint alleges that the Defendants intentionally interfered with their private property by imbedding software and hardware to gather data, causing harm to the Plaintiffs' personal property. (*See* Am. Compl. ¶¶ 1090-93).

Turning to whether Section 1681t(b)(1)(F) preempts the claim, the Court finds no preemption occurs. As to the first element, Georgia law extensively supplies a plaintiff with the common law right to have their personal property undisturbed. Not only is this right codified in the Georgia code, but Georgia state court decisions over the last century have also recognized this right. *See Bowen*, 561 F. Supp. 3d at 1375 (reviewing trespass to chattels under Georgia

law). No authority otherwise suggests that a claim for trespass to chattels does not arise out of Georgia law.

Regarding the second element, and similar to the Plaintiffs' claim for unjust enrichment, the Court sees little, if any, relation between the claim and the "subject matter" of Section 1681s-2. The trespass claim concerns itself with the Plaintiffs' possessory right over their driving data and their vehicles. (*See* Am. Compl. ¶¶ 1090-93). From the face of the Amended Complaint, there is no concern over whether the information furnished by the GM Defendants is accurate. Therefore, the Plaintiffs' trespass to chattels claim will not be preempted.

**ii. State Statutory Claims**

The Plaintiffs also bring various state law statutory claims under state subclasses. The state statutory claims easily satisfy the first element of preemption because these claims are "imposed under the laws of any State." *See Spencer*, 831 F. Supp. 2d at 1363 ("There is no dispute that, at a minimum, § 1681(b)(1)(F) preempts causes of action based on state statutes.").

The question then turns to which of these state-law claims relate to the "subject matter" of Section 1681s-2. As framed by the GM Defendants, some consumer claims are preempted because the Plaintiffs argue that the GM Defendants took action without notice or consent. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 48). In response, the Plaintiffs argue that none of the state law claims relate to issues of informational inaccuracy or credit dispute

resolution and should therefore not be preempted. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 43).

Although discussed at length when considering whether the Plaintiffs' invasion of privacy claim was preempted, the Court undertakes another brief case illustration as it pertains to when state-law claims are preempted. In *Knudson v. Wachovia Bank*, the Plaintiff brought an FCRA claim under Section 1681s-2 and state law, common law, and statutory claims arising out of allegations of inaccuracy. 513 F. Supp. 2d 1255, 1257 (M.D. Ala. 2007). In considering whether the state-law claims were preempted under Section 1681t(b)(1)(F), the court looked to whether the violations of state law concerned conduct which is regulated under Section 1681s-2. *Id.* at 1260. In doing so, the court implicitly defined when state-law claims would be preempted by the FCRA. Specifically, the court found that state-law claims based on facts which are also alleged to be a violation of Section 1681s-2 are preempted. *Id.*

Applying this definition to the case before this Court, the Plaintiffs' theory of preemption appears to prevail. Only the state law claims that allege that the GM Defendants furnished inaccurate information or failed to follow proper dispute resolution procedures are preempted by the FCRA. All other state-law claims, such as those that concern notice and consent, are not preempted under the FCRA. While the GM Defendants may point to Section 1681s-2(a)(7) as evidence that the provision regulates when notice may be given to consumers, the provision is inapplicable to them. Section 1681s-2(a)(7)

concerns *financial institutions* who furnish information to credit reporting agencies, not companies like the GM Defendants. *See* 15 U.S.C. § 1681s-2(a)(7). If the GM Defendants failed to provide notice under Section 1681s-2, they would not be in violation of the statute; therefore, no preemption applies.

The GM Defendants also raise *Synovus* in support of their proposition that state-law privacy claims based on a defendant's responsibilities as a furnisher of information under Section 1681s-2 should be dismissed. 2023 WL 6323084 at *6. However, this out-of-circuit case lacks real reasoning. After citing a number of cases across the nation that support the idea that state and common law claims are preempted, the *Synovus* court did not engage with the key provision that requires the claims to intersect with the subject matter of Section 1681s-2. *See id.* Even if the reasoning were convincing, the Eleventh Circuit's prior decisions on FCRA preemption demonstrate some deviation from the national trend of FCRA preemption as to all state and common law claims, creating a narrow inquiry that must be satisfied before preempting claims under Section 1681t(b)(1)(F). *See Spain*, 363 F.3d at 1191-93, 1198-99; *see also Spencer*, 831 F. Supp. 2d at 1363 (noting that the Eleventh Circuit's approach in *Spain* is not universal among the courts).

In sum, the Court declines to dismiss all state law statutory claims that do not allege inaccuracies in reporting or issues with dispute resolution. However, to the extent that any state law claim does allege either of these

categories regulated under Section 1681s-2, such claims are partially or wholly preempted.[30]

**b. Section 1681h(e)**

The CRA Defendants argue that Section 1681h(e) preempts the Plaintiffs' invasion of privacy-related claims.[31] (Br. in Supp. of LNRS' Mot. to Dismiss, at 15). Section 1681h(e), in relevant part, states:

> Except as provided in sections 1681n and 1681o of [the FCRA], no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user of information, or any person who furnishes information to a consumer reporting agency, based on information disclosed pursuant to section 1681g, 1681h, or 1681m of [the FCRA], or based on information disclosed by a user of a consumer report to or for a consumer against whom the user has taken adverse action, based in whole or in part on the report[,] except as to false information furnished with malice or willful intent to injure such consumer.

15 U.S.C. § 1681h(e).

---

[30] This conclusion also applies to the CRA Defendants' arguments that Section 1681t(a) preempts the Plaintiffs' state law claims through conflict preemption. (*See* Br. in Supp. of LNRS' Mot. to Dismiss, at 7-8, 12-15). Conflict preemption occurs "when it is physically impossible to comply with both the federal and the state laws or when the state law stands as an obstacle to the objective of the federal law." *MSP Recovery Claims, Series LLC v. United Auto. Ins. Co.*, 60 F.4th 1314, 1321 (11th Cir. 2023) (citation modified). Because the state law claims are not predicated on behavior regulated by Section 1681s-2 or other parts of the FCRA, there is no conflict preemption under the terms of Section 1681t(a).

[31] The GM Defendants also adopt the arguments of the CRA Defendants within this section in their briefing. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 51 n. 32).

In determining whether a claim is preempted under Section 1681h(e), courts apply a two-step inquiry, first asking whether the Plaintiffs' claim "falls within the scope of § 1681h(e)" and if so, then asking "whether the 'malice or willful intent to injure' exception to the general bar against state law actions applies." *Hickman v. Pa. Higher Educ. Assistance*, 2017 WL 8186732, at *8 (quoting *Ross v. F.D.I.C.*, 625 F.3d 808, 814 (4th Cir. 2010)).

Turning to the first part of this inquiry, the parties dispute the true scope of Section 1681h(e). The CRA Defendants argue that the provision bars all state law claims for defamation, invasion of privacy, or negligence. (*See* Reply Br. in Supp. of LNRS' Mot. to Dismiss, at 6-7 [Doc. 164]). In response, the Plaintiffs argue that the scope is much narrower, instead only applying to claims arising out of information found in Sections 1681g (concerning disclosures to consumers), 1681h (concerning conditions and form of disclosures to consumers), or 1681m (concerning the requirements on users of consumer reports) and only to tort claims. (*See* Pls.' Br. in Opp'n to LNRS' Mot. to Dismiss, at 18-19).

The CRA Defendants' position is wholly unpersuasive. The CRA Defendants provide two cases in support of their position, but neither case engages in any meaningful analysis on whether the state law claim fits into one of the enumerated sections because it was not necessary for the resolution of their case. For example, in *Jordan v. Equifax Info. Servs., LLC*, the discussion of Section 1681h(e) was part of a four-sentence conclusion where the

court simply stated that "the FCRA preempts defamation and negligent reporting claims brought pursuant to state law unless the plaintiff can prove that the defendant acted with malice or with a willful intent to injure him." 410 F. Supp. 2d 1349, 1355 (N.D. Ga. 2006). The Court does not find the authority persuasive.

Instead, when courts engage with the text of Section 1681h(e), as Judge May did in *In re Equifax Fair Credit Reporting Act Litig.*, 2023 WL 6192732 (N.D. Ga. Sep. 11, 2023), the conclusion is different. In that case, the defendants similarly argued that the scope of Section 1681h(e) preempts all defamation and negligent-reporting claims brought pursuant to state law. *Id.* at *6. In reviewing the plain language of the statute, the court found that it explicitly limited the preempted claims to those arising out of disclosures made pursuant to Sections 1681g, 1681h, or 1681m. *Id.*; *see* 15 U.S.C. § 1681h(e). Finding that the plaintiffs' negligence claim did not arise out of the disclosures made in those sections, the court held that Section 1681h(e) was not applicable to preempt the claim. *Id.*

The Court finds Judge May's reasoning persuasive. The CRA Defendants' position is entirely at odds with the text within the provision. "The plain meaning of legislation should be conclusive, except in the rare cases in which the literal application of a statute will produce a result demonstrably at odds with the intentions of its drafters." *United States v. Crape*, 603 F.3d 1237, 1245 (11th Cir. 2010) (quoting *United States v. Ron Pair Enters.*, 489 U.S. 235,

242 (1989)). The Court is "not at liberty to rewrite the statute to reflect a meaning [the Court] deems more desirable." *Id.* at 1244-45 (quoting *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 228 (2008)).

Therefore, the Court holds that Section 1681h(e) is only applicable when a state law claim sounding in defamation, invasion of privacy, or negligence arises out of disclosures made pursuant to Sections 1681g, 1681h, or 1681m. Because the CRA Defendants do not appear to argue that the Plaintiffs' claims fall under these enumerated sections, Section 1681h(e) does not apply to the Plaintiffs' invasion of privacy claims.

**c. Implied Preemption**

The Defendants argue that, even if the FCRA did not expressly preempt the Plaintiffs' state law claims, the FCRA still impliedly preempts them. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 49-51; Br. in Supp. of LNRS' Mot. to Dismiss, at 9-15). The Defendants argue that Congress enacted the FCRA with the purpose of ensuring fair and accurate credit reporting and that the state law claims frustrate the purpose of the FCRA. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 49-51; Br. in Supp. of LNRS' Mot. to Dismiss, at 9-15). They argue that the Plaintiffs' state law claims, in essence, create an 'opt-out' provision within the FCRA, which courts have rejected. (*Id.*).

In support of their position, the Defendants present persuasive authority within this district and outside of this Circuit to advance their implied preemption argument. However, apart from mere propositions, none

of the cases cited by the Defendants actually show any court finding implied preemption. First, the Defendants cite *Frazier v. TransUnion*, 2023 WL 6323088, at *4 (E.D Pa. Sep. 28, 2023), and *Hayward v. Sw. Credit Sys.*, 2024 WL 169570, at *3 (E.D. Pa. Jan. 16, 2024), for their propositions that the FCRA does not create an opt-out provision. However, both cases state these propositions based on the plaintiffs' claims for relief under the FCRA, not under state law claims. *See id.* Furthermore, in *TransUnion*, the court only found the state law claims to be preempted because of Section 1681t(b)(1)(F) and not because of any implied preemption doctrine. *See TransUnion*, 2023 WL 6323088 at *6.

The Defendants also refer to *Ponder v. Experian Info. Sols.*, 2021 WL 2688648 (N.D. Ga. May 18, 2021), *report and recommendation adopted*, 2021 WL 5033483 (N.D. Ga. Jul. 9, 2021), but Judge Anand ultimately decided the issue of preemption on the basis of Section 1681h(e), not due to principles of implied preemption. *Id.* at *23. Even if the Court were to accept the Defendants' conclusion that the *Ponder* court would have held that the state law claims were impliedly preempted, the Court would still pause to accept *Ponder*'s reasoning because at least one district court within this district discusses a glaring error with the reasoning of the report and recommendation. *See In re Equifax Fair Credit Reporting Act Litig.*, 2023 WL 6192732 at *6 (stating that *Ponder* is unpersuasive because it relied on a single district court case that failed to thoroughly analyze Section 1681h(e) preemption).

Even if the Court were to consider implied preemption as a stand-alone reason to dismiss the Plaintiffs' state law claims, the Court is unpersuaded. The Southern District of New York's decision in *Aghaeepour v. N. Leasing Sys., Inc.*, 378 F. Supp. 3d 254 (S.D.N.Y. 2019), is instructive. The court evaluated whether a notice requirement imposed by New York state law was inconsistent with the FCRA under Section 1681t(a). *See id.* at 261-64. In making that determination, the court carefully reviewed legislative history to conclude that the FCRA was meant to serve as a baseline to protect consumers and that additional protections would not be inconsistent with the ultimate goal of the FCRA. *See id.* at 262-63 (citing S. Rep. No. 517, 91st Cong., 1st Sess. 8 (Nov. 5, 1969)). The court also discussed how neither obligation requires abrogation of the other. *Id.* at 262. Because of this evidence, the Court ultimately held that the state law claim was not preempted. *Id.* at 264.

Here, even if the Court were to accept the Defendants' contention that state law requirements of notice and consent are far greater than what is allowed under the FCRA, these obligations are not inconsistent with each other. The Defendants may follow the requirements of the FCRA along with the requirements of state law because Congress intended the FCRA to protect consumers, not furnishers nor credit reporting agencies. Accordingly, there is

no implied preemption within the FCRA, and the Plaintiffs' state-law claims survive preemption.[32]

### 3. Article III Standing

"In order for a federal court to have jurisdiction under Article III of the Constitution, a plaintiff must have standing to bring the lawsuit." *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1261 (11th Cir. 2021) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 559-60 (1992)). For a plaintiff to have standing, he must "show that the defendant harmed him, and that a court decision can either eliminate the harm or compensate for it." *Id.* (citation modified). To survive a motion to dismiss arising out of an Article III standing challenge, a plaintiff must allege that (1) he "has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical," (2) "the injury is fairly traceable to the challenge action of the defendant," and (3) "it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Fla. Wildlife Fed'n v.*

---

[32] For its consideration of the Defendants' Motions to Dismiss, the GM Defendants provided notice to the Court of recent supplemental authority out of the Consumer Financial Protection Bureau. (*See generally* GM Defs.' Notice of Supplemental Authority in Supp. of Mot. to Dismiss [Doc. 181]). The interpretive rule construes FCRA preemption broadly, reversing a prior interpretive rule relied on by the Plaintiffs from July 2022. *See* Fair Credit Reporting Act; Preemption of State Laws, 90 Fed. Reg. 48710 (Oct. 28, 2025). Generally, agency interpretations of the law may be viewed as persuasive authority by a court. *See Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 402 (2024). In coming to its decision, the Court does not rely on the July 2022 interpretive rule cited to by the Plaintiffs. Accordingly, the Court declines to adopt this interpretation of FCRA preemption and instead will rely on the intra-circuit authority cited within this opinion.

*S. Fla. Water Mgmt. Dist.*, 647 F.3d 1296, 1302 (11th Cir. 2011) (quoting *Friends of the Earth, Inc. v. Laidlaw Envt'l Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)).

The Defendants allege that the Plaintiffs lack standing to bring some or all of their state law claims. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 51). Specifically, the Defendants challenge whether the Plaintiffs have established "injury in fact" and the traceability of the injury. The Court takes each argument in turn.

**a. Injury in Fact**

"An injury in fact consists of 'an invasion of a legally protected interest' that is both 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 996 (11th Cir. 2020) (quoting *Lujan*, 504 U.S. at 560-61). "A 'concrete' injury must be '*de facto*' —that is, it must be 'real, and not abstract.'" *Id.* (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)). "A 'particularized' injury 'must affect the plaintiff in a personal and individual way.'" *Id.*

The Eleventh Circuit has recognized three kinds of harm that satisfy injury in fact: (1) "tangible harms, like 'physical or monetary harms,'" (2) intangible harms, like "injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," and (3) "a 'material risk of future harm' when a plaintiff is seeking injunctive relief." *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023)

(citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 414, 415, 425 (2021)). The GM Defendants argue that several named Plaintiffs fail to show an injury in fact that satisfies any of these categories. The GM Defendants point to the Plaintiffs' state statutory claims within the Amended Complaint which state that the Plaintiffs suffered the injury of the potential misuse of their data. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 52). Further, the GM Defendants point to the Plaintiffs' tort claims and argue that a "diminution of the value of [the Plaintiffs'] personal data" or the lost value of personal information does not confer Article III standing. (*Id.*). The Court discusses each argument separately.

### i. Risk of Future Harm

While the GM Defendants are correct that the "mere risk of future harm" is generally not enough to confer standing on a claim for money damages, courts across the nation have found that an individual's loss of privacy in his data is enough of an injury to confer Article III standing. *See e.g. Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271-74 (9th Cir. 2019) (holding that a breach of biometric data amounts to injury in fact sufficient to confer Article III standing and citing *Pavesich*, 122 Ga. 190 (1905)). The Eleventh Circuit's decision in *Green-Cooper* explains how the loss of control over personal data can satisfy Article III standing. In *Green-Cooper*, the plaintiffs brought suit against the defendant after the defendant faced a cyber-attack causing the plaintiffs' personal information to be stolen from its servers. 73 F.4th at 886-87.

In determining whether an injury in fact was established, the court focused on the plaintiffs' allegation that their personal information was "exposed for theft and sale on the dark web." *Id.* at 889. The Eleventh Circuit found that the potential exposure and misuse of the data established injury in fact because it showed both a present injury and a substantial risk of future injury. *Id.* at 889-90. The exposure established a present injury because the plaintiffs' personal information was floating around on the dark web. *Id.* at 890. And it established a substantial risk of future injury because of the risk of future misuse of personal information associated with the hacking. *Id.*

The harm alleged by the Plaintiffs here is similar to that discussed in *Green-Cooper*. Taking the Plaintiffs' Alabama Deceptive Trade Practices Act (Count 11) as an example, the Plaintiffs allege that they suffered injury by "the loss of privacy, the unauthorized dissemination of their valuable Driving Data, and economic harm stemming from GM's exploitation of their Driving Data." (Am. Compl. ¶ 1123). Both present and future injury can be gleaned from this allegation. There is present injury because the Plaintiffs' driving data has been taken by the GM Defendants, out of the Plaintiffs' control. The present injury here is more severe than in *Green-Cooper* because there are concrete allegations that the GM Defendants sold the data to the CRA Defendants. (*See id.* ¶¶ 24-25, 70-71, 137-38, 258-59, 322-23, 710, 743, 747, 750, 758, 761, 770, 779, 783, 787-90).

There is also a substantial risk of future harm. When discussing the substantial risk of future harm, the GM Defendants point to allegations in the Amended Complaint that show that they sunset the Smart Driver program and ceased sharing data with the CRA Defendants. (*Id.* ¶ 953). However, nowhere in the Amended Complaint is there any allegation that the GM Defendants lost access to the data already collected and would not sell the data to any other company. The loss of privacy and control over the data is concrete enough of an injury for the Plaintiffs to satisfy the injury in fact requirement based on their loss of privacy and substantial future harm.[33]

### ii. Lost Value of Personal Information

The GM Defendants' argument on lost value has far more merit. When considering whether the injury in fact element is satisfied, courts within this Circuit have generally refused to consider the diminished value of personal information as a concrete injury that confers Article III standing by itself without specific pleadings alleging that there exists a market for the information, the plaintiffs intend to sell the information on the market, and that the value of the information has diminished.[34] While the Plaintiffs have

---

[33] The GM Defendants make the argument that there is no "loss of privacy" alleged because the data obtained is not sensitive. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 53). As discussed previously, the Plaintiffs may have a significant privacy interest in their driving data as alleged in the Amended Complaint. Determining the extent of their privacy interest is a fact-intensive inquiry that can only be understood more fully after discovery. Therefore, the Court is unpersuaded by this argument.

[34] *See Bland v. Urology of Greater Atlanta, LLC*, 2024 WL 3313348, at *7-*8 (N.D. Ga. Mar. 14, 2024) (collecting cases); *Everhart v. Colonial Pipeline*

established that a market exists for their driving data within the Amended Complaint, the Plaintiffs have not alleged that they intend to sell their driving data themselves or that the value of their data has diminished in any concrete capacity.

Recognizing this deficiency, the Plaintiffs attempt to distinguish cases from within the Circuit with cases arising out of the Ninth Circuit, arguing that the pleadings do not need such specificity where defendants "unjustly enriched themselves" by exploiting consumer data. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 49). The Court declines to adopt this standard.

"Lost value of personal information" claims are inherently speculative rather than concrete. For there to be actual injury in fact, the Court would have to assume multiple facts, including that: (1) each Plaintiff is able to sell his or her driving data to other companies, (2) each Plaintiff is willing to sell his or her driving data to other companies, and (3) the driving data actually lost value from the dissemination of the data by the Defendants. Only after such facts

---

*Co.*, 2022 WL 3699967, at *2 (N.D. Ga. Jul. 22, 2022) (same); *Provost v. Aptos, Inc.*, 2018 WL 1465766, at *4 (N.D. Ga. Mar. 12, 2018) ("Plaintiff has failed to allege with particularity any facts explaining how her personal identity information is less valuable than it was before the Breach."); *Fraga v. UKG, Inc.*, 2022 WL 19486310, at *11-*12 (S.D. Fla. May 10, 2022) (holding that, despite arguing that a market exists for their personal information, the plaintiffs failed to allege injury because they did not allege participation in the market); *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1257 (M.D. Fla. 2019) ("The Court rejects this theory . . . because Plaintiffs have not alleged that their personal information has an independent monetary value that is now less than it was before the Data Breach.").

are assumed could the Court even consider the claims as concrete. If the Court instead adopted the lax standard advocated by the Plaintiffs, no court would be able to dismiss claims based on "lost value" at the motion to dismiss stage. It is perhaps for this reason that the Plaintiffs fail to cite a single case within the Eleventh Circuit or a binding case within the Ninth Circuit that advocates for their position. Therefore, all of the Plaintiffs who bring claims solely based on the "lost value of their personal information" fail to allege Article III standing for their state-law claims. However, seeing no named Plaintiff presents such a theory alone, the Court does not dismiss any claims at this time.

**b. Traceability**

Traceability requires a causal connection between the plaintiff's injuries and the defendant's injurious conduct. *See Walters v. Fast AC, LLC*, 60 F.4th 642, 650 (11th Cir. 2023) (quoting *Lujan*, 504 U.S. at 560). To establish traceability, "the plaintiff's injuries [must] be 'fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.'" *Id.* (quoting *Lujan*, 504 U.S. at 560).

The Defendants' arguments focus on the named Plaintiffs who allege insurance premium increases. Without explaining what standard of causation is necessary to satisfy standing, the Defendants argue that these Plaintiffs fail to establish standing because the facts underlying the Amended Complaint do not demonstrate that their actions caused the insurance premium increases.

(Br. in Supp. of GM Defs.' Mot. to Dismiss, at 55; *see* Br. in Supp. of Verisk's Mot. to Dismiss, at 44-47). At this stage, the Court holds that the Plaintiffs have satisfied the causation element for the same reasons as explained in Section III.E(3) of this opinion. The Plaintiffs have adequately alleged in the Amended Complaint that it is plausible that the Defendants' actions were a substantial factor in bringing about their increased insurance premiums. Numerous named Plaintiffs have alleged increases after their insurance companies accessed their driving data through reports generated by the CRA Defendants with data acquired by the GM Defendants. Accordingly, the Plaintiffs have adequately alleged causation for Article III standing.

**4. Invasion of Privacy (Counts 5 and 6)**

The Court now turns to the substantive arguments. Under Georgia law, the tort of invasion of privacy encompasses four specific torts: (1) "intrusion upon plaintiff's seclusion or solitude, or into her private affairs," (2) "public disclosure of embarrassing private facts about the plaintiff," (3) "publicity which places the plaintiff in a false light in the public eye," and (4) "appropriation, for the defendant's advantage, of the plaintiff's name or likeness." *Summers v. Bailey*, 55 F.3d 1564, 1566 n. 4 (11th Cir. 1995) (citing *Yarbray v. S. Bell Tel. & Tel. Co.*, 261 Ga. 703, 704-05 (1991), then citing *Cabaniss v. Hipsley*, 114 Ga. App. 367, 370 (1966)). From the Amended Complaint, the Plaintiffs do not explain which theories of invasion of privacy

they proceed under. Accordingly, the Court will briefly review all four sub-torts.

First, there is the tort of intrusion upon seclusion. "The tort of intrusion involves an unreasonable and highly offensive intrusion upon another's seclusion." *Id.* at 1566. "The 'unreasonable intrusion' aspect of the invasion of privacy involves a prying or intrusion, which would be offensive or objectionable to a reasonable person, into a person's private concerns." *Yarbray*, 261 Ga. at 705 (citation modified).

The second tort is the public disclosure of private facts. To recover on a theory of public disclosure of private facts, "a party must prove: (1) the disclosure of the private facts was a public one; (2) the facts disclosed were private, secluded, or secret facts; and (3) the matter made public was offensive and objectionable to a reasonable person of ordinary sensibilities under the circumstances." *Zieve v. Hairston*, 266 Ga. App. 753, 756 (2004). "Pertinent to determining whether a plaintiff may recover for invasion of privacy is the consideration of whether the allegedly tortious behavior is reasonable under the circumstances." *Eason v. Marine Terminals Corp.*, 309 Ga. App. 669, 671-72 (2011).

Third is the tort of false light. To establish a claim of false light, a plaintiff must demonstrate (1) "the existence of false publicity that depicts the plaintiff as something or someone which he is not," and (2) "that the false light in which he was placed would be highly offensive to a reasonable person."

*Williams v. Cobb Cnty. Farm Bureau, Inc.*, 312 Ga. App. 350, 353 (2011) (citation modified). Finally, there is the tort of appropriation of likeness. To establish the elements of this tort, a plaintiff must show (1) the appropriation of their name or likeness, (2) without consent and (3) for the financial gain of the appropriator. *Bullard v. MRA Holding, LLC*, 292 Ga. 748, 752 (2013) (citation omitted).

Under any theory of invasion of privacy, the Defendants argue several reasons for dismissal of Counts 5 (Invasion of Privacy) and 6 (Civil Conspiracy to Commit Invasion of Privacy). The Defendants do not make any independent arguments arguing for the dismissal of Count 6, instead challenging the underlying tort. Because the civil conspiracy claim cannot survive if the underlying tort is dismissed, the Court will address each argument in turn as applied to both counts.

**a. Privacy Interest**

The GM Defendants first argue that the Plaintiffs fail to allege an invasion of a privacy interest, as is required for claims of intrusion upon seclusion and public disclosure of private facts. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 59). The GM Defendants characterize the driving data taken from the Plaintiffs as public conduct because the Plaintiffs were driving on public roads. (*Id.*). In response, the Plaintiffs liken the GM Defendants' intrusion to electronic surveillance and argue that data generated by an

individual's vehicle cannot be private. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 52-53).

The GM Defendants' position relies on the Restatement (Second) of Torts (the "Restatement") and Eleventh Circuit precedent. The Restatement states that there is no liability for intrusion upon seclusion and public disclosure of private facts when the plaintiff's appearance is public and open to the public eye or when the facts disclosed are open to the public eye. *See* Restatement (Second) of Torts §§ 652B, cmt. c, 652D, cmt. b (1977). In line with the Restatement, the Eleventh Circuit in *Summers* stated that "[t]raditionally, watching or observing a person in a public place is not an intrusion upon one's privacy." 55 F.3d at 1566.

Meanwhile, the Plaintiffs' position largely relies on *Carpenter v. United States*, 585 U.S. 296 (2018). There, the Supreme Court confronted the government's acquisition of 12,898 location points of the defendant at an average of 101 data points a day. *Id.* at 302. In determining whether the acquisition of this information constituted a search, the Supreme Court held that pervasive location monitoring that amounts to "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years" implicates a defendant's privacy expectations. *Id.* at 315. This is true even if the individual is traveling publicly. *Id.* at 314-15. However, neither position presented by the parties directly answers the question of whether the driving data at issue here implicates privacy concerns.

The Georgia Supreme Court faced the question of whether an individual has a reasonable expectation of privacy in data contained within his vehicle in *Mobley v. State*, 307 Ga. 59 (2019). There, police officers were called to the scene of a car crash and were directed to retrieve any available data from the airbag control modules ("ACMs") of the vehicles involved. *Id.* at 60. In a subsequent criminal trial, the defendant challenged the use of the data in his ACM, arguing that it was a product of an unreasonable search under the Fourth Amendment and that he had a reasonable expectation of privacy in that data. *See id.* at 62-65. The Georgia Supreme Court declined to rule on whether the defendant had a privacy interest in the data from the ACM, instead holding that a search occurred under an alternate theory of trespass. *See id.* at 66-67.

However, the court still addressed the question in dicta, calling the issue a "close question." *Id.* at 66 n.9. The Georgia Supreme Court opined that, "although an observer independently could ascertain *some* of the information that readily can be gleaned from the data recorded on the ACM, an ordinary observer would not be able to ascertain *all* of that information, much less with anything approaching the precision reflected in the ACM data." *Id.* Additionally, the court also discussed how data derived from devices connected to the ACM through an onboard data port could be sensitive information (such as location data) that individuals have a reasonable expectation of privacy in. *Id.* (citing *Carpenter*, 585 U.S. at 296).

While the GM Defendants do correctly stress upon the Court that *Mobley* is not binding as to whether the Plaintiffs have a privacy interest in their driving data, the Court still finds the Georgia Supreme Court's reasoning instructive. This is because it reconciles both the GM Defendants' position with the Supreme Court's holding in *Carpenter*. It would be improper, without further discovery, for the Court to dismiss the claim on this ground when the parties still dispute the true extent of the driving data collected on each individual Plaintiff. As alleged in the Amended Complaint, the driving data collected by the GM Defendants is extensive and goes far beyond information "an ordinary observer" would be able to glean by observing the vehicles on public roads. *See Mobley*, 307 Ga. at 66 n. 9. Not only does the driving data include location data that may implicate *Carpenter*, but it also includes a variety of discrete driving events compiled over a significant period of time. (*See* Am. Compl. ¶ 922). Therefore, the Court finds that a privacy interest may exist in the driving data of each individual Plaintiff and will not dismiss the claim.

**b. Publication**

To the extent the Plaintiffs allege invasion of privacy under a public disclosure of private facts or a false light theory, the GM Defendants argue that no public disclosure occurred because some of the named Plaintiffs allege only that their data was disclosed to LNRS and Verisk, who shared the information to their insurers. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at

62). The GM Defendants are correct that the tort of public disclosure of private facts requires a disclosure to the public at large. *See Williams*, 312 Ga. App. at 354 (citation omitted). The same requirement exists for an invasion of privacy claim under false light. *See Blakey v. Victory Equip. Sales, Inc.*, 259 Ga. App. 34, 37 (2002) ("Blakey's claim must fail in this case, because he has not shown that the false information about which he complains was distributed to the public at large."). Furthermore, at least one court within this district has held that a plaintiff cannot recover under either theory when credit reports are distributed only to a limited number of people or entities. *See e.g.*, *Peacock v. Retail Credit Co.*, 302 F. Supp. 418, 423, 424 (N.D. Ga. 1969).

Here, several named Plaintiffs allege only that the GM Defendants disclosed their driving data to LNRS and Verisk and that the CRA Defendants disclosed it to certain insurers. There appears to be no allegation that the Defendants' disclosures went further or that the Defendants provided public access to the information provided within the credit reports. Accordingly, to the extent any of the named Plaintiffs allege their invasion of privacy claim under the theories of public disclosure of private facts or false light, their claims are hereby dismissed.

**c. Highly Offensive Conduct**

The remaining two theories under which the Plaintiffs may recover for invasion of privacy are intrusion upon seclusion and the misappropriation of name and likeness. The GM Defendants challenge the first theory, arguing

that the conduct alleged does not amount to "highly offensive" conduct. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 62-64). This tort requires "a plaintiff [to] show a physical intrusion which is analogous to a trespass; however, this 'physical' requirement can be met by showing that the defendant conducted surveillance on the plaintiff or otherwise monitored [plaintiff's] activities." *Sitton v. Print Direction, Inc.*, 312 Ga. App. 365, 369 (2011) (citation modified).

The GM Defendants argue that their conduct was not unreasonable because collecting and sharing ordinary consumer data generally does not meet this standard. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 63). They liken the collection and disclosure of social security numbers, personal data, and geolocation information to the collection of driving data. (*Id.* (citing *Covington v. Gifted Nurses, LLC*, 2023 WL 5167366, at *10 (N.D. Ga. Jul. 19, 2023), then citing *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063, then citing *Ramirez v. LexisNexis Risk Sols.*, 729 F. Supp. 3d 838, 851 (N.D Ill. 2024)).

This argument downplays the amount of data collected and distributed by the Defendants. As already discussed, the extent of the data collected by the GM Defendants, as alleged in the Amended Complaint, is extensive and can be likened to electronic surveillance. Whether such surveillance is reasonable is to be determined on a totality of the circumstances. *See Sitton*, 312 Ga. App. at 369-70. As alleged, the GM Defendants surreptitiously gathered this driving

data by misleading the Plaintiffs about the true extent of Smart Driver and the CRA Defendants distributed the data without regard for the manner in which the data was collected. (*See e.g.* Am. Compl. ¶¶ 665-66, 703, 844-57, 872-76). There is little justification for believing this collection was necessary or permitted for it to be reasonable. *Sitton*, 312 Ga. App. at 370. Accordingly, the Court will not dismiss the Plaintiffs' intrusion upon seclusion theory on this ground.

**d. Misappropriation of Likeness**

The Court now turns to the Plaintiffs' misappropriation of likeness theory under their invasion of privacy claim. Under Georgia law, "the interest protected in an appropriation case is the plaintiff's exclusive use of his or her name and likeness as an inherent aspect of his or her identity." *Bullard*, 292 Ga. at 752 (citation modified). The GM Defendants argue that the Plaintiffs cannot put forth an invasion of privacy claim because the Plaintiffs' driving history is not an element of their personalities. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 64-65). The Plaintiffs fail to meaningfully respond to this argument, abandoning their claim. *See Mora v. Miller*, 2019 WL 1321563, at * 1 (N.D. Ga. Apr. 10, 2019) (collecting cases holding the same within the circuit).

Even if the Court were to address the merits, the Court agrees with the Defendants' position that the driving data taken by the GM Defendants does not qualify as an inherent aspect of the Plaintiffs' identities for the Plaintiffs to bring suit under the theory of misappropriation of likeness. It is hard to

imagine how information on how an individual drives is a key feature of an individual's personality or likeness. Unlike the use of names, photographs, or videos, no court in Georgia has held that data of this sort can be used to maintain a claim for invasion of privacy under a misappropriation of likeness theory. *See e.g. Bullard*, 292 Ga. at 753 (analyzing whether a plaintiff can maintain a misappropriation of likeness claim based off a video of an individual); *Cabaniss*, 114 Ga. App. at 377-80 (same as to photos); *Martin Luther King, Jr. Ctr. for Soc. Change, Inc. v. Am. Heritage Prods., Inc.*, 250 Ga. 135, 143 (1982) (same as to names and sculptures). The Court will not create such precedent here. Therefore, the Court dismisses the Plaintiffs' claims of invasion of privacy to the extent the claim is alleged under the theory of misappropriation of likeness. As a result, the only theory that the Plaintiffs may bring their invasion of privacy and conspiracy claim under is intrusion upon seclusion.

**5. Trespass (Count 9)**

The Plaintiffs bring a claim for trespass against the Defendants. Under Georgia law, "the owner of personalty is entitled to its possession." O.C.G.A. § 51-10-1. "Any unlawful abuse of or damage done to the personal property of another constitutes a trespass for which damages may be recovered." O.C.G.A. § 51-10-3. "The gist of such an action of trespass to personal property is the injury done to the possession of the property." *Caldwell v. Church*, 341 Ga. App. 852, 856 (2017) (citation modified). The GM Defendants make two arguments

in favor of dismissal of the Plaintiffs' trespass claim. First, the GM Defendants argue that the Plaintiffs fail to allege any damage to property required under a trespass claim. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 67-68). Second, the GM Defendants argue that the Plaintiffs fail to allege any actual interference with their property. (*See id.* at 68-70).

The Plaintiffs, in response, implicitly admit that no actual damage was alleged by arguing that interference with an integral component part of a chattel can constitute trespass, relying primarily on *Bowen*. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 60). In the Plaintiffs' view, the element of actual damage is not a requirement because the Georgia law on trespass was developed before widespread electronic systems were common and the common law adopts to technological developments. (*Id.* at 61). The Plaintiffs also argue that their driving data is personal property protected by the trespass doctrine, without supporting authority. (*Id.*). The Court is unpersuaded by the Plaintiffs' arguments.

Addressing the first argument, the Plaintiffs' reliance on *Bowen* is misplaced. First, in *Bowen*, there was actual damage and interference to the vehicles of the plaintiffs. The defendant there allegedly pushed an update to the plaintiffs' vehicles that caused their vehicles to enter "a near-continuous reboot cycle, draining the vehicle's battery, damaging the PCM hard drive, depriving the owner of the ability to enjoy his vehicle, causing an irritating and potentially dangerous 'static' noise, and resulting in numerous other

significant problems." *Bowen*, 561 F. Supp. 3d at 1367. Because the issue of interference and actual damage was not in dispute, the court turned to the issue of consent instead. *See id.* at 1375-76.

The court in *Bowen* still briefly addressed the issue of digital trespass in two sentences, stating that it could sustain a claim for trespass under Georgia law. *See id.* at 1375. The Plaintiffs and the *Bowen* court rely on *AT&T Mobility LLC v. Does 1-4*, 2011 WL 13213864 (N.D. Ga. May 26, 2011), and *Skapinetz v. CoesterVMS.com, Inc.*, 2018 WL 805393 (D. Md. Feb. 9, 2018) in support of this proposition. *Id.*; (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 61). However, in *AT&T Mobility*, the court sustained the digital trespass theory when actual damages still arose out of the interference with personal property. *See AT&T Mobility LLC*, 2011 WL 13213864, at *2 ("Defendants' actions have caused AT&T Mobility to suffer damage to its property and its business because it has deprived AT&T Mobility and its subscribers of legitimate use of the commercial systems and has caused aggravation to AT&T Mobility's customers."). While the District of Maryland held in *Skapinetz* that actual damages or interference to the use of property is not required for a trespass claim under Georgia law, the court relied on reasoning from this district that relied on out-of-circuit case law that failed to analyze Georgia law, so *Skapinetz* is unpersuasive to the Court. *See Skapinetz*, 2018 WL 805393, at *5 (citing *Etzel v. Hooters of Am., LLC*, 223 F. Supp. 3d 1306, 1314 (N.D. Ga.

2016) (citing *Mey v. Got Warranty, Inc.*, 193 F. Supp. 3d 641, 647 (N.D. W. Va. 2016))).

Here, the Plaintiffs allege that their chattel was harmed and diminished in value through the "loss of privacy," the "unauthorized use of Plaintiffs' vehicle systems for Defendants' commercial gain," and "the loss of control over their driving data and its associated economic value." (Am. Compl. ¶ 1093). The Plaintiffs also argue that they suffered economic harm from the unauthorized exploitation of the driving data. (*Id.* ¶ 1094). None of these damages arise out of any interference or harm to the Plaintiffs' chattel—their vehicles. While the Plaintiffs argue that the Defendants exploited their vehicles for their commercial gain, there is no actual harm done to the vehicles nor their internal systems.

Recognizing this, the Plaintiffs also argue that the driving data qualifies as personal property protected by the trespass doctrine. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 61). However, the Plaintiffs' argument lacks merit under Georgia law. The analysis provided by the court in *Dial HD, Inc. v. Clearone Commc'ns, Inc.*, 2010 WL 3732115 (S.D. Ga. Sep. 7, 2010), is instructive. In that case, the defendant was alleged to have obtained confidential payroll and accounting information by burglarizing the plaintiff's residence. *Id.* at *2. The plaintiff brought a trespass claim for this intrusion and theft of information by the defendant. *Id.* at *10. The court, after reviewing Georgia law, held that the trespass doctrine protects only physical property,

not information appropriated from physical property. *Id.* (discussing *J & C Ornamental Iron Co. v. Watkins*, 114 Ga. App. 688 (1966)). Ultimately, the court held that the plaintiff could not maintain a trespass action. *Id.* at *12.

Similarly, while the trespass doctrine allows the Plaintiffs to pursue an action against the Defendants for any interference and damage with their vehicles, there is no remedy under the doctrine as applied to the driving data. Not only does this approach follow Georgia law, but it follows the "weight of authority" nationally. *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012) ("…this court has already rejected a similar argument because the weight of authority holds that a plaintiff's 'personal information' does not constitute property."). Because the Plaintiffs fail to allege damage or interference with their vehicles, and because the plaintiffs' driving data is not a protected interest under the trespass doctrine of Georgia, the Court dismisses Count 9 of the Amended Complaint.

**6. Breach of Contract (Count 8)**

The Plaintiffs' breach of contract claim arises out of the onboarding process where the Plaintiffs were presented with User Terms. (Am. Compl. ¶¶ 891-95). Thirty-seven named Plaintiffs enrolled in OnStar through dealerships, while ten named Plaintiffs enrolled into OnStar themselves. (*See generally* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 3). Before arguing for dismissal, the GM Defendants argue that all named Plaintiffs who enrolled in OnStar are subject to the choice-of-law clause within the User Terms that

requires any claims arising out of the User Terms be governed by Michigan law. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 70-71). The Plaintiffs do not argue otherwise, and the Court agrees. "Although Georgia courts adhere to the rule of *lex loci contractus*, 'parties by contract may stipulate that the laws of another jurisdiction will govern the transaction.'" *Rayle Tech, Inc.*, 133 F.3d at 1409 (citing *Manderson & Assocs., Inc. v. Gore*, 193 Ga. App. 723, 725 (1989)). Here, the User Terms stipulate that the agreement "shall be interpreted in accordance with and governed by the laws of the State of Michigan." (Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 1, at 20 [Doc. 142-2]). Therefore, the Court will apply Michigan law to the GM Defendants' argument for dismissal of the breach of contract claim.

To survive a motion to dismiss, a plaintiff must allege sufficient facts within their complaint that demonstrates that (1) there was a contract, (2) which the defendant breached, (3) thereby resulting in damages to the plaintiff. *Miller-Davis Co. v. Ahrens Const., Inc.*, 495 Mich. 161, 178 (2014). "When the terms of a contract are unambiguous, the meaning of the contract is interpreted from the language alone." *Dignan v. Mich. Pub. Sch. Emp. Ret. Bd.*, 253 Mich. App. 571, 578-79 (2002). Contractual terms are given their ordinary meaning when those terms are not defined in the contract itself. *Barton-Spencer v. Farm Bureau Life Ins. Co. of Mich.*, 500 Mich. 32, 39 (2017).

The GM Defendants argue that the Plaintiffs' breach of contract claim must be dismissed because the User Terms and the Privacy Statement allow

for the collection and sharing of the Plaintiffs' driving data. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 72). The GM Defendants point to the provision within the User Terms that states that "GM collects, uses, and shares information from and about [the Plaintiff] and [the Plaintiff's] Vehicle." (*Id.* at 71; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 1, at 16). The GM Defendants also point to a few provisions within the Privacy Statement that are incorporated into the User Terms that permit the GM Defendants to collect the driving data of the Plaintiffs. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 71-72; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 2, at 3-4 [Doc. 142-3]).

In response, the Plaintiffs argue that GM breached the agreed-upon terms by exceeding the scope of their authorization to collect information as detailed by the User Terms. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 68). The Plaintiffs argue that the terms of the User Terms are ambiguous as to the scope of the data collection allowed and, therefore, a question still remains as to whether the GM Defendants breached the contract between the parties. (*See id.* at 68-69).

Because a court should interpret and construe a contract as a whole, *Smith v. Smith*, 292 Mich. App. 699, 702 (2011), the Court agrees with the Plaintiffs. While provisions exist disclosing the GM Defendants' right to collect and share driving data, such representations can be read to minimize the amount of data collected. For example, within the Privacy Statement, it states that GM may collect . . . [i]nformation about the use of [the plaintiff's] vehicle,

including . . . geolocation, route history, driving schedule, speed, . . . [and] sensor data." (Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 2, at 3-6). Yet, the Plaintiffs allege that far more and detailed information was collected by the GM Defendants, including hard braking events, rapid acceleration events, daytime and nighttime driving minutes, mileage, and other data that falls outside of this list. (*See* Am. Compl. ¶ 922). Of course, the Privacy Statement uses the word "including" to demonstrate that the Privacy Statement is non-exhaustive. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 2, at 3). However, the collection of this data, especially in real-time, could still constitute a breach of contract due to exceeding the scope of authorization allowed, especially when the Plaintiffs have some privacy interest in the data. Therefore, the Court will not dismiss Count 8.

**7. Unjust Enrichment (Count 7)**

To state a claim for unjust enrichment under Michigan law,[35] a plaintiff must allege facts within his complaint sufficient to demonstrate (1) "receipt of a benefit by the defendant from the plaintiff," and (2) "inequity resulting to

[35] The GM Defendants argue that, because the Plaintiffs' unjust enrichment claim is a quasi-contractual claim, Michigan law governs because of the existence of a contractual relationship between the GM Defendants and the Plaintiffs. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 72-73). "A claim for unjust enrichment is not a tort, but an alternative theory of recovery if a contract claim fails." *Am. Mgmt. Servs. E., LLC v. Fort Benning Family Cmtys., LLC*, 333 Ga. App. 664, 692 (2015) (citation modified). Since the Plaintiffs' ancillary unjust enrichment claim arises out of the parties' contractual relationship, Michigan law applies here, too. *See Texas Ed Tech Sols., LLC v. Authentica Sols., LLC*, 2020 WL 5774015, at *3 (N.D. Ga. Sep. 28, 2020).

plaintiff from defendant's retention of the benefit." *Bellevue Ventures, Inc. v. Morang-Kelly Inv., Inc.*, 302 Mich. App. 59, 64 (2013) (citation omitted). Where an express contract governs the relationship between the parties, a claim for unjust enrichment is unavailable. *See Belle Isle Grill Corp. v. City of Detroit*, 256 Mich. App. 463, 478 (2003).

The GM Defendants make four arguments for why the Plaintiffs' unjust enrichment claim fails. First, the GM Defendants argue that unjust enrichment is not available as a remedy because an express contract—the User Terms—governs the relationship with GM. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 73). Second, they argue that the Plaintiffs fail to allege any expectation of payment from the GM Defendants. (*Id.*). Third, the GM Defendants argue that the Plaintiffs have failed to allege any detriment that was caused by the GM Defendants' conduct. (*Id.* at 74). Fourth, they argue that the Plaintiffs have an adequate remedy at law, which precludes the unjust enrichment claim. (*Id.*).

Addressing the first and fourth arguments together, the Plaintiffs are not precluded from asserting an unjust enrichment claim simply because they plead a breach of contract claim on the basis of an express contract or plead other remedies at the motion to dismiss stage. *See Ajuba Int'l, L.L.C. v. Saharia*, 871 F. Supp. 2d 671, 692 (E.D. Mich. 2012); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1330-31 (N.D. Ga.

2019). Because a dispute exists over whether a valid contract exists between the parties, dismissal would be premature. *See id.*

The GM Defendants' second and third arguments are also unconvincing. "Without proof of the expectations of the parties, the presumption of gratuity will overcome the usual contract implied by law to pay for what is accepted." *Roznowski v. Bozyk*, 73 Mich. App. 405, 409 (1977). If the data were not alleged to be stolen without the knowledge of the Plaintiffs, the GM Defendants would prevail in arguing for dismissal. However, because the Plaintiffs do allege so, there is proof that the Plaintiffs did not intend to convey the benefit gratuitously at the time the information was taken. (*See* Am. Compl. ¶ 1079). The detriment suffered by the Plaintiffs arises out of the GM Defendants' retention of profits.[36] (*See id.* ¶ 1081). Because it is plausible that the Plaintiffs did not intend to confer this information gratuitously and that the Plaintiffs suffered a detriment, the GM Defendants' second and third arguments fail. Accordingly, the Court will not dismiss the Plaintiffs' unjust enrichment claim.

**8. State Invasion of Privacy Statutes**

The California Plaintiffs and the Plaintiffs who form part of the New York subclass (the "New York Plaintiffs") bring four state-law statutory invasion of privacy claims against the Defendants arising out of California and

[36] This argument assumes that the GM Defendants are correct that Michigan law requires a detriment be alleged in a claim for unjust enrichment. The GM Defendants fail to provide case law from Michigan supporting such a requirement, nor has the Court found any.

New York law. The CRA Defendants move to dismiss all four claims. (*See* Br. in Supp. of Verisk's Mot. to Dismiss, at 35-41). In response, the New York Plaintiffs consent to withdrawing their New York invasion of privacy claims (Counts 48 and 49) but the California Plaintiffs argue against dismissal of the California claims (Counts 13 and 17). The Court will thus dismiss Counts 48 and 49 and will review each remaining invasion of privacy claim.

**a. California Constitution (Count 13)**

In order to establish an invasion of privacy claim under the California Constitution, a plaintiff must establish that (1) "they possess a legally protected privacy interest, (2) "they maintain a reasonable expectation of privacy," and (3) "the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook*, 956 F.3d at 601 (citing *Hernandez v. Hillsides, Inc.,* 47 Cal. 4th 272, 287 (2009)).

The CRA Defendants and GM Defendants present arguments for dismissal of the invasion of privacy claim. Separately, the CRA Defendants make two arguments. First, they argue that the California Plaintiffs do not have a legally protected privacy interest in their driving data under the first element. (Br. in Supp. of Verisk's Mot. to Dismiss, at 36). Second, they argue that their invasion of privacy, as opposed to the GM Defendants, is not serious enough to constitute an egregious breach of social norms under the third element. (*Id.* at 36-37). No matter the merits of the California Plaintiffs' claim,

both the CRA Defendants and the GM Defendants argue, an invasion of privacy claim under the California Constitution does not confer a private right of action for damages and instead provides only for injunctive relief. (*Id.* at 37; Br. in Supp. of GM Defs.' Mot. to Dismiss, at 75).

Addressing the separate arguments by the CRA Defendants first, the Court need not address their first argument because the California Plaintiffs' invasion of privacy claim fails as the CRA Defendants' conduct does not amount to an egregious breach of social norms. To be clear, the GM Defendants' conduct may amount to such a breach. "Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of 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 whether countervailing interests or social norms render the intrusion inoffensive." *In re Facebook*, 956 F.3d at 606 (citing *Hernandez*, 47 Cal. 4th at 287). "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 as a matter of public policy. *Id.* (citing Hernandez, 47 Cal.4th at 287).

California courts recognize that determining the offensiveness of a breach is a question typically not resolved at the pleading stage. *See Smith v. YETI Coolers, LLC*, 754 F. Supp. 3d 933, 946 (N.D. Cal. 2024). While California courts have been hesitant to extend the tort of invasion of privacy

to "the routine collection of personally identifiable information as part of electronic communications," the collection of such information that is intimate or sensitive could meet this standard. *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (citations omitted). Furthermore, even routine data collection practices may be highly offensive "if a defendant disregards consumers' privacy choices while simultaneously holding itself out as respecting them." *Id.* (citation modified).

Here, assuming that driving data is a protected privacy interest, the California Plaintiffs have alleged sufficient facts supporting their invasion of privacy claim against the GM Defendants. Allegations involving the surreptitious collection of detailed, invasive data has been upheld on a number of occasions at the motion to dismiss stage. *See e.g. In re Facebook,* 956 F.3d at 606; *In re Vizio*, 238 F. Supp. 3d at 1233. Furthermore, the California Plaintiffs have alleged numerous scenarios where the GM Defendants reaffirmed their commitment to consumer privacy, all while allegedly conducting the offending scheme. (*See e.g.* Am. Compl. ¶¶ 665). This information alone supports a finding that it is plausible that the GM Defendants' conduct was egregious and highly offensive.

The California Plaintiffs argue that the CRA Defendants' conduct was also egregious and highly offensive because they conspired with the GM Defendants to surreptitiously collect the California Plaintiffs' data. (Pls. Br. in Opp'n to Verisk's Mot. to Dismiss, at 31). However, just because the GM

Defendants' conduct may satisfy the "highly offensive" standard does not automatically make the CRA Defendants liable for the same conduct. *Smith* is instructive. There, the plaintiff brought suit for invasion of privacy under the California Constitution because, when the plaintiff visited the defendant's website, a third-party the defendant contracted with intercepted and indefinitely stored consumers' personally identifiable information and financial information for the third-party's commercial benefit. *Smith*, 754 F. Supp. 3d at 938-39. Ultimately, the court held that "[w]hether [a defendant's] conduct was highly offensive turns on what specifically [the plaintiff] is alleging [the defendant] knew" and held that the plaintiff did not allege facts sufficiently to meet this standard. *Id.*

Here, like the defendant in *Smith*, the CRA Defendants' conduct appears to arise out of routine commercial activity under the allegations of the Amended Complaint. The CRA Defendants are in the business of gathering data for insurers through their regular commercial activities. (*See* Am. Compl. ¶¶ 695, 738). Accordingly, the CRA Defendants contracted with GM to acquire the driving data GM collected. (*Id.* ¶¶ 698, 742-43).

The inquiry does not end there; there must be some showing that the CRA Defendants knew about the GM Defendants' conduct and the California Plaintiffs argue that they allege as such. (*See* Pls.' Br. in Supp. of GM Defs.' Mot. to Dismiss, at 31 (citing Am. Compl. ¶¶ 1070-74)). However, barring conclusory allegations within the count itself, nowhere in the Amended

Complaint are there sufficient facts supporting their claim of any knowledge or conspiracy. In fact, the manner in which the California Plaintiffs describe how GM entered into these agreements with the CRA Defendants cuts against their "conspiracy" position. GM entered into an agreement with Verisk only after soliciting multiple bids. (*See* Am. Compl. ¶ 697). Verisk's intent for entering into this contract was to secure a foothold in the automotive data marketplace and it publicly announced its involvement with GM. (*See id.* ¶¶ 697-699). Similarly, LexisNexis' interest in entering into an agreement with GM appears to be purely commercial and the Amended Complaint contains no facts that demonstrate its knowledge of GM's activities. (*See id.* ¶¶ 741-44). Therefore, because the California Plaintiffs fail to allege facts sufficient to demonstrate knowledge by the CRA Defendants of the GM Defendants' actions, the CRA Defendants are dismissed from Count 13 of the Amended Complaint.

Because the CRA Defendants are dismissed, the Court now turns to the GM Defendants' remaining argument that the California Constitution does not provide a private action for money damages arising out of an invasion of privacy claim. The Court finds the GM Defendants' argument persuasive. Nearly every federal and state court addressing this issue has recognized that a private action for money damages against a private entity, as opposed to

injunctive relief, cannot be maintained under the California Constitution.[37] Under the test outlined by the California Supreme Court for whether a provision of the California Constitution can give rise to a private action for money damages, there must be "evidence from which we may find or infer, within the constitutional provision at issue, an affirmative intent either to authorize or to withhold a damages action to remedy a violation." *Katzberg v. Regents of Univ. of Cal.*, 29 Cal. 4th 300, 317 (2000).

While the California Plaintiffs highlight isolated instances where federal courts in California have found that a plaintiff may pursue money damages, the courts that do so do not take the additional step to actually evaluate whether the evidence required by *Katzberg* exists. *Cf. Stuart v. Cnty. Of Riverside*, 2024 WL 3086634, at *5 (C.D. Cal. Jun. 14, 2024); *Frasco v. Flo Health, Inc.*, 349 F.R.D. 557, 580-84 (N.D. Cal. 2025). Therefore, the Court will follow the weight of authority and hold that a claim for money damages cannot arise out of the California Constitution's invasion of privacy private right of action. However, the California Plaintiffs may still seek injunctive relief under Count 13.

[37] *See, e.g., Moore v. Rodriguez*, 2021 WL 2222590, at *20 (S.D. Cal. Jun. 2, 2021) (citing *Clausing v. San Francisco Unified Sch. Dist.*, 221 Cal. App. 3d 1224, 1237 (Ct. App. 1990)); *Meyer v. Cnty. of San Diego*, 2025 WL 449747, at *26 (S.D. Cal. Feb. 10, 2025); *Doe v. Regents of Univ. of Cal.*, 672 F. Supp. 3d 813, 819-820 (N.D. Cal. 2023).

### b. California Consumer Privacy Act (Count 17)

The California Consumer Privacy Act ("CCPA") provides a civil cause of action for any plaintiff "whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." Cal. Civ. Code § 1798.150(a)(1). The Defendants make two arguments for dismissal of the California Plaintiffs' CCPA claim.[38] First, they argue that the driving data does not qualify as personal information protected by the CCPA. (Br. in Supp. of Verisk's Mot. to Dismiss, at 38). Second, they argue that the California Plaintiffs' factual allegations within the Amended Complaint supporting their claim are conclusory. The Court finds the first argument persuasive for dismissal of the California Plaintiffs' claim and therefore need not address the second.

The CCPA explicitly defines two types of protected information that qualifies as "personal information" under the statute. *See* Cal. Civ. Code § 1798.81.5(d)(1). The first type requires the breach to involve an individual's unencrypted or unredacted first name or first initial and the individual's last name, in combination with at least one of the following pieces of information: their (1) "[s]ocial security number," (2) driver's license or other unique government identification number used to verify an individual's identity,

[38] The GM Defendants incorporate by reference the CRA Defendants' arguments for dismissal of the CCPA claim. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 85).

(3) "[a]ccount number or credit or debit card number, in combination with any" information that would permit access to an individual's financial account, (4) "[m]edical information," (5) "[h]ealth insurance information," (6) "[u]nique biometric data generated from measurements or technical analysis of human body characteristics," or (7) "[g]enetic data." Cal. Civ. Code § 1798.81.5(d)(1)(A). The second type requires the breach to involve an individual's "username or email address in combination with a password or security question and answer that would permit access to an online account." Cal. Civ. Code § 1798.81.5(d)(1)(B).

It is difficult to fit the California Plaintiffs' driving data in either category. Even if the Court were to assume that the driving data contained the unredacted first and last names of consumers, the California Plaintiffs do not, and cannot, show that the driving data qualifies as one of the seven enumerated categories required to fit under the first category. The driving data fails to satisfy the requirements of the second category because the Amended Complaint contains no allegations that the information contained any details that would permit access to the consumers' online accounts.

The California Plaintiffs attempt to save their CCPA claim by pointing to a singular paragraph within their Amended Complaint that alleges that the information the Defendants "intercepted, collected, and obtained . . . constitutes personal information within the scope of the CCPA." (Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 32 (citing Am. Compl. ¶ 1215)). However,

although courts are required to give deference to "well-pleaded factual allegations," courts are not to give deference to allegations in a complaint that are "merely legal conclusions." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1290 (11th Cir. 2010) (citing *Iqbal*, 556 U.S. at 678). Here, the single paragraph referenced by the California Plaintiffs amounts to nothing more than a legal conclusion and is not entitled to deference by the Court. Accordingly, the California Plaintiffs' CCPA claim is dismissed as to all Defendants.

### 9. State Consumer Statute Claims

The Plaintiffs assert 36 claims arising out of state consumer statutes on behalf of 33 state subclasses. The Defendants assert several arguments for the dismissal of all of these claims.

#### a. Consumer Standing (All Counts)

Focusing solely on the state consumer statutes, the Defendants make two main standing arguments for dismissal of certain claims. First, the GM Defendants argue that the nine Plaintiffs who do not allege an increase in insurance premiums fail to satisfy the heightened standing requirements of certain state consumer statutes. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 54). Second, the Defendants argue that any state law claims that lack a representative plaintiff should be dismissed. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 75-76; Br. in Supp. of Verisk's Mot. to Dismiss, at 54-55). The Court addresses each argument in turn.

### i. Heightened Damages Requirement

The GM Defendants argue that the nine Plaintiffs who fail to allege an increase in insurance premiums should have their claims dismissed under their respective state consumer statutes because they fail to assert "monetary" or "economic damages" that are "ascertainable." (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 54; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex.4, at 1-7, 9-12 [Doc. 142-5]). The specific Plaintiffs have claims arising under Illinois, Connecticut, Michigan, New Jersey, New York, Texas, Pennsylvania, and Oklahoma law. However, the claims arising out of Michigan, New York, and Oklahoma law contain no requirement for either monetary or economic damages. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 4, at 6, 7, 8). Accordingly, the Court will not dismiss the claims of Plaintiffs Brockington, Davids, or Brakefield. Turning to the remaining claims, the Plaintiffs argue that the named Plaintiffs who do not allege increased insurance premiums still assert economic harm in the form of loss of control over personal data. (*See* Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 47-48). The Court will address this contention under each pertinent state's law.

#### 1. Illinois (Count 29)

Plaintiff Gray brings a claim under the Illinois Consumer Fraud and Deceptive Business Practices Act (the "ICFA") but does not allege an increase in insurance premiums. Under the ICFA, a plaintiff must allege actual damages to bring a claim under the statute. *See Cooney v. Chicago Pub. Schs.*,

407 Ill. App. 3d 358, 365 (2010) (citing 815 Ill. Comp. Stat. 505/10a(a)). "[A]ctual damages must arise from purely economic injuries." *Id.* (citation modified). The "actual damage" must be "real and measurable." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 830 (7th Cir. 2018).

Understanding that damages must be measurable, the Plaintiffs quantify the market value of their driving data based on GM's revenue from their sale of the data to insurers, marketers, and data brokers. (*See* Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 48). However, the Plaintiffs misunderstand the requirement of "actual damages" under Illinois law. "[D]amages under the ICFA are determined by looking at the loss to the plaintiff, not the gain to the defendant." *Ramirez v. LexisNexis Risk Sols.*, 729 F. Supp. 3d 838, 850 (N.D. Ill. 2024). Indeed, in *Ramirez*, the plaintiffs alleged that the defendant violated the ICFA and that the damages arose from the economic value of their personal data because the defendant would have had to seek their consent to sell their data or ceased the sale of their data. *Id.* The plaintiffs also argued that they satisfied the requirement for actual damages under the ICFA by alleging injury from anxiety, mental anguish, loss of privacy, and threats to public safety. *Id.* The court found that none of the injuries alleged amounted to actual damages as required by the ICFA because there were no monetary costs to the plaintiff. *Id.*

Here, Plaintiff Gray's theory of economic harm does not comport with the interpretation of "actual damages" within the ICFA as discussed in

*Ramirez* because the loss alleged is based on the gain by the GM Defendants, not any actual money lost by Plaintiff Gray. Because Plaintiff Gray does not advance any theory of damages that fits the ICFA's definition, Plaintiff Gray's claim under the ICFA is hereby dismissed.

**2. Connecticut (Count 21)**

Plaintiff Brunet brings a claim under the Connecticut Unfair Trade Practices Act (the "CUTPA"). Under the CUTPA, "[a]ny person who suffers any *ascertainable loss of money or property,* real or personal, as a result of" a violation of the CUTPA may recover under the consumer statute. Conn. Gen. Stat. § 42-110g(a) (emphasis added). "An ascertainable loss is a loss that is capable of being discovered, observed or established." *Artie's Auto Body, Inc. v. Hartford Fire Ins. Co.*, 287 Conn. 208, 218 (2008) (citation modified). "A loss is ascertainable if it is measurable even though the precise amount of the loss is not known." *Id.* (citation modified). "When plaintiffs seek money damages, the language 'as a result of' in § 42-110g(a) requires a showing that the prohibited act was the proximate cause of a harm to the plaintiff." *Id.* (citation modified).

Unlike Plaintiff Gray's ICFA claim, Plaintiff Brunet has alleged sufficient facts to support her claim under the CUTPA because the Plaintiff's loss of control in her driving data is measurable. There is no requirement underlying the CUTPA that ascertainable losses be a concrete monetary loss for the Plaintiff. All that a plaintiff must demonstrate is that she can obtain

actual damages under her CUTPA claim at the conclusion of trial, as opposed to purely punitive or nominal damages. *See Criscuolo v. Shaheen*, 46 Conn. Supp. 53, 61-62 (1999) (holding that the plaintiff's inability to recover actual damages was fatal to her CUTPA claim). As discussed earlier in the Court's discussion on Article III standing, the Plaintiffs, including Plaintiff Brunet, have alleged sufficient facts to demonstrate that they will recover actual damages from their state consumer statute claims, along with showing that the GM Defendants' conduct was a substantial factor in the Plaintiffs' loss. Therefore, the Court will not dismiss Plaintiff Brunet's CUTPA claim.

### 3. New Jersey (Count 45)

Plaintiffs Gordin and Matthews bring claims under the New Jersey Consumer Fraud Act (the "NJCFA"). Under the statute, "[a]ny person who suffers *any ascertainable loss of moneys or property,* real or personal, as a result of" a violation of the NJCFA may recover by private action against the violator. N.J. Stat. Ann. § 56:8-19 (emphasis added). "An ascertainable loss is a loss that is quantifiable or measurable; it is not hypothetical or illusory." *Lee v. Carter-Reed Co., L.L.C.*, 203 N.J. 496, 522 (2010) (citation modified). "However, the precise amount of damages need not be known as long as the damages are measurable." *Kleinman v. Merck & Co., Inc.*, 417 N.J. Super. 166, 182 (N.J. Super. Ct. Law Div. 2009). Similar to the CUTPA, an ascertainable loss within the NJCFA is one that produces actual damages, whether it be through out-of-pocket losses or the loss-in-value of property. *See Thiedemann*

*v. Mercedes-Benz USA, LLC*, 183 N.J. 234, 248-249 (2005). At least one New Jersey federal court has held that ascertainable loss under the NJCFA encompasses both tangible and intangible harms. *See In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *9 (D.N.J. Mar. 29, 2023).

Here, Plaintiffs Gordin and Matthews allege intangible losses associated with the loss of control over their driving data. (*See* Am. Compl. ¶ 1062). The value of such losses may be ascertained and measurable through the revenue obtained by GM for the sale of consumer data. (*See id.* ¶ 691). Therefore, the Court will not dismiss the claims of Plaintiffs Gordin and Matthews under the NJCFA.

**4. Texas (Count 60)**

Plaintiff Parkhurst brings a claim under the Texas Deceptive Trade Practices Consumer Protection Act (the "TDTPA"). Under the TDTPA, "[a] consumer may maintain an action where any of [an enumerated list of conduct] constitute a producing cause of *economic damages or damages for mental anguish*." Tex. Bus. & Com. Code § 17.50(a) (emphasis added). "Texas law requires [p]laintiffs to demonstrate 'actual injury' to pursue a claim." *Martin v. Home Depot U.S.A., Inc.*, 369 F. Supp. 2d 887, 890 (W.D. Tex. 2005) (citing *Polaris Indus., Inc. v. McDonald*, 119 S.W.3d 331, 338-42 (Tex. App. 2003), then citing *Hines v. Evergreen Cemetery Ass'n*, 865 S.W.2d 266, 268 (Tex. App. 1993), then citing *Munoz v. Gulf Oil Co.*, 732 S.W.2d 62, 65 (Tex. App. 1987), and then citing *Gideon v. Johns-Manville Sales Corp.*, 761 F.2d 1129, 1136 (5th

Cir. 1985)). Thus, Texas law does not permit no injury product liability claims. *Id.* (citing *Rivera v. Wyeth-Ayerst Labs*, 283 F.3d 315 (5th Cir. 2002)). Damages that are conjectural, uncertain, or remote are not actionable under the TDTPA. *Higbie Roth Const. Co. v. Houston Shell & Concrete*, 1 S.W.3d 808, 814 (Tex. App. 1999).

Here, Plaintiff Parkhurst, like the other named Plaintiffs who do not allege an increase in insurance premiums, asserts damages associated with the loss of control over his driving data. (*See* Am. Compl. ¶ 1062). There is no indication under Texas law that the damages required by the TDTPA must arise out of tangible losses. Furthermore, the damages alleged do not arise out of any theory of product liability but instead arise out of a theory of invasion of privacy. (*See id.* ¶ 1048-67). Because the Court has already determined that such an injury is sufficient to survive the injury-in-fact requirement of Article III standing, the Court finds no reason to conclude that Plaintiff Parkhurst's demonstration is insufficient to survive at this stage. Therefore, the Court will not dismiss Plaintiff Parkhurst's TDTPA claim.

**5. Pennsylvania (Count 54)**

Plaintiff Guc brings a claim under the Pennsylvania Unfair Trade Practices and Consumer Protection Law (the "PUTPCPL"). Under the PUTPCPL, "[a]ny person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers *any ascertainable loss of money or property*, real or personal, as a result" of a

violation of the consumer statute. 73 Pa. Cons. Stat. § 201-9.2(a) (emphasis added). "To allege an ascertainable loss, the plaintiff must be able to point to money or property that he would have had but for the defendant's fraudulent actions." *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 541 (M.D. Pa. 2021) (citation modified). "These damages must be identifiable and cannot be speculative." *Id.* (citation modified). Pennsylvania law has "sanctioned the application of several damage assessment schemes under the [P]UTPCPL." *Dibish v. Ameriprise Fin., Inc.*, 134 A.3d 1079, 1087 (Pa. Super. Ct. 2016) (citation modified). Furthermore, it stresses that "an ascertainable loss must be established by the facts of the case." *Id.* at 1088 (citation omitted).

Here, Plaintiff Guc, like every other applicable named Plaintiff, alleges damages arising out of the loss of control associated with his driving data. While no court analyzing the PUTPCPL has addressed whether such losses are ascertainable under Pennsylvania law, courts have analyzed the PUTPCPL in the context of data breaches. Here, the Court finds two courts that can provide guidance. The court in *In re Rutter's Inc. Data Security Breach Litigation* held that allegations of loss arising solely out of lost time to remedy a violation of the PUTPCPL do not qualify as an ascertainable loss. 511 F. Supp. 3d at 541. However, the court in *In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, 613 F. Supp. 3d 1284 (S.D. Cal. 2020), found that losses arising out of the diminution in value of personal information, as well as

those arising out of the benefit of the bargain, can independently satisfy the ascertainable loss requirement of the PUTPCPL. *Id.* at 1308.

The Court has already held that all Plaintiffs bringing claims arising only out of the lost value of personal information cannot satisfy Article III standing. Here however, Plaintiff Guc alleges more. Because Pennsylvania courts apply the definition of "ascertainable loss" broadly, the Court will not dismiss Plaintiff Guc's claim. *See Dibish*, 134 A.3d at 1087-88. Pennsylvania courts stress the importance of jury involvement in determining the question of whether an ascertainable loss exists, and Plaintiff Guc has alleged sufficient facts to survive the Defendants' motion. *See id.* at 1088. Therefore, the Court will not dismiss Plaintiff Guc's PUTPCPL claim.

**ii. Lack of Representative Plaintiff**

The Defendants argue that the Plaintiffs lack standing to assert claims under certain state statutes because there is no named Plaintiff to assert the claim. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 75-76; Br. in Supp. of Verisk's Mot. to Dismiss, at 54-55). Specifically, the Defendants focus their argument on the claims asserted by the Massachusetts Plaintiffs (Counts 37-38), the Plaintiffs who form part of the Nebraska subclass (the "Nebraska Plaintiffs") (Counts 41-42), the New Hampshire Plaintiffs (Count 43), the Plaintiffs who form part of the Rhode Island subclass (the "Rhode Island Plaintiffs") (Count 57), the Plaintiffs who form part of the Utah subclass (the "Utah Plaintiffs") (Count 61), the Plaintiffs who form part of the Vermont

subclass (the "Vermont Plaintiffs") (Count 62), the Plaintiffs who form part of the Virginia subclass (the "Virginia Plaintiffs") (Count 63), and the Plaintiffs who form part of the West Virginia subclass (the "West Virginia Plaintiffs") (Count 65).

It is true that "prior to the certification of a class, and technically speaking before undertaking any formal typicality or commonality review, [a] district court must determine that at least one named class representative has Article III standing to raise each class subclaim." *Prado-Steiman ex rel. Prado v. Bush*, 221 F.3d 1266, 1279 (11th Cir. 2000). Further, district courts within this Circuit have applied this doctrine to dismiss claims at the motion to dismiss stage prior to any class certification. *See Sowa*, 764 F. Supp. 3d at 1247 (dismissing Florida state law claims for lack of a named plaintiff); *In re Takata Airbag Prods. Liab. Litig.*, 462 F. Supp. 3d 1304, 1315 (S.D. Fla. 2020) (dismissing South Carolina and Kentucky state law claims for lack of a named plaintiff).

However, the Defendants go too far in asserting that the Eleventh Circuit requires a district court to dismiss such claims at the motion to dismiss stage. (*See* Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 45 (citing *Mills v. Foremost Ins. Co.*, 511 F.3d 1300 (11th Cir. 2008), then citing *Fox v. Ritz-Carlton Hotel Co.*, 977 F.3d 1039 (11th Cir. 2020))). In *Mills*, the Eleventh Circuit's analysis of whether named plaintiffs had standing as putative class representatives on a motion to dismiss was followed by subsequent analysis on

class certification. 511 F.3d at 1307. Because the plaintiffs brought the issue of class certification, the Eleventh Circuit had to decide the issue of Article III standing with regard to the missing named plaintiffs prior to deciding the second issue. In *Fox*, the Eleventh Circuit determined the issue of Article III standing on the pleadings but was not confronted with the issue of missing representative plaintiffs for all claims. 977 F.3d at 1046-47.

The only direct requirement under Eleventh Circuit precedent is that Article III standing be determined prior to any determination on class certification. *Prado-Steiman ex rel. Prado v. Bush*, 221 F.3d 1266, 1279 (11th Cir. 2000). Accordingly, as this Court has held before, all that is required is that the Plaintiffs allege that individuals nationwide have suffered from the Defendants' conduct. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.* 362 F. Supp. 3d at 1344. Here, the Plaintiffs have done so, detailing a nationwide scheme by the Defendants that is not constrained to one or a few states. Therefore, the Plaintiffs have alleged sufficient facts to maintain their claims without a named Plaintiff at this stage in the litigation. Should the Plaintiffs file a motion for class certification, the Defendants may renew their arguments regarding standing if the Plaintiffs have not found a named Plaintiff to represent the Massachusetts, Nebraska, New Hampshire, Rhode Island, Utah, Vermont, Virginia, and West Virginia subclasses. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.* 362 F. Supp. 3d at 1344; *In re*

*Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014).[39]

**b. Pre-Suit Notice (Counts 11, 19, 31, 37, 40, 60, 61, 65)**

The Defendants turn to eight state consumer statutes and argue for dismissal of these claims because the Plaintiffs failed to comply with pre-suit notice requirements. Specifically, the Defendants argue for dismissal because (1) the Plaintiffs failed to provide written notice of the alleged violation within the proscribed time period of five consumer state statutes, (2) the Plaintiffs' pre-suit notice itself was deficient, and (3) the Plaintiffs failed to resolve their claim through an informal dispute settlement program, as required under Mississippi law. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 76-77; Br. in Supp. of Verisk's Mot. to Dismiss, at 51-53).

Before addressing the merits, the Plaintiffs argue that issues of sufficiency and timeliness of the notice are issues of fact that cannot be decided on the pleadings. (*See* Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 70-71 (citing *Sunshine Children's Learning Ctr., LLC v. Waste Connections of Fla., Inc.*, 2022 WL 218896 (S.D. Fla. Jan. 25, 2022), then citing *Leach v. Honeywell*

[39] Although the Plaintiffs thoroughly respond to the GM Defendants' argument for dismissal, the Plaintiffs fail to respond to the CRA Defendants' similar argument. Understandably, the CRA Defendants argue that the pertinent claims should be dismissed for failure to respond. (Reply Br. in Supp. of Verisk's Mot. to Dismiss, at 1 n. 1 [Doc. 166]). However, a failure to respond does not automatically warrant ruling in a movant's favor. Because Eleventh Circuit precedent supports the Court's holding, as opposed to the CRA Defendants' position, the Court will not dismiss the claims on this basis.

*Int'l Inc.*, 2014 WL 12585799 (D. Mass. Nov. 17, 2014)); Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 44 (citing *Sunshine*)). However, the cases the Plaintiffs rely on to assert this claim are clearly distinguishable. While the court in *Sunshine Children's Learning Ctr.* held that the adequacy of notice was a factual issue that could not be determined on a motion to dismiss, it held so when considering whether a breach in notice obligations was material in an action for breach of contract. 2022 WL 218896, at *4. Furthermore, the facts surrounding notice were actually disputed. *Id.*

Here, the timing of the notice is not in dispute. The Defendants show that the Plaintiffs issued pre-suit notice on November 22, 2024, and the Plaintiffs do not dispute this fact. (*See generally* Br. in Supp. of GM Defs.' Mot. to Dismiss, Ex. 8 [Doc. 142-9] ("GM Defs.' Pre-Suit Notice"); Br. in Supp. of Verisk's Mot. to Dismiss, Ex. 1 [Doc. 141-2] ("CRA Defs.' Pre-Suit Notice")). Further, the Amended Complaint was filed with the Court on December 13, 2024, twenty-one days after the Plaintiffs' transmittal of the notice. (*See generally* Am. Compl.). The parties also do not dispute the contents of the pre-suit notice. Therefore, unlike the court in *Sunshine Children's Learning Ctr.*, a determination of whether the notice is adequate is critical to determining the motion to dismiss.

*Leach* is distinguishable as well. In a breach of warranty action, the *Leach* court only held that the issue of notice was not appropriate for resolution on a motion to dismiss because, under Massachusetts law, whether notice is

timely depends on the reasonableness of the buyer's behavior under the circumstances. 2014 WL 12585799, at *5. Here, as will later be discussed, the issue of timeliness is constrained to concrete deadlines and does not require an evaluation of reasonableness. In any case, there is ample authority where courts have dismissed claims because the plaintiffs have failed to comply with the pre-suit notice requirements under various state statutes.[40] As such, the Court will address each of the Defendants' arguments on the merits.

[40] The Plaintiffs cite to a district court case within the Seventh Circuit for the proposition that a failure to follow state procedural law does not preclude the Plaintiffs from pursuing their class action claims in federal court under Federal Rule of Civil Procedure 23. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 71-72 (citing *In re Hair Relaxer Mktg. Sales Pracs. & Prods. Liab. Litig.*, 2024 WL 4333246 (N.D. Ill. Sep. 27, 2024)). In that case, the court was bound by Seventh Circuit precedent that followed the plurality opinion of Justice Scalia in *Shady Grove Orthopedic Associates., P.A. v. Allstate Insurance Co.*, 559 U.S. 393 (2010), and concluded that pre-suit notice requirements conflicted with the requirements for class actions under federal law. *See In re Hair Relaxer Mktg. Sales Pracs. & Prods. Liab. Litig.*, 2024 WL 4333246, at *13. This is not the case within the Eleventh Circuit. Courts within this Circuit have found that no conflict exists between Rule 23 and pre-suit notice requirements in statutes. *See, e.g.,, In re Takata Airbag Prods. Liab. Litig.*, 193 F. Supp. 3d 1324, 1345 (S.D. Fla. 2016); *Deerman v. Fed. Home Loan Mortg. Corp.*, 955 F. Supp. 1393, 1399-1400 (N.D. Ala. 1997) (applying a pre-suit notice requirement and dismissing claim); *see also Helpling v. Rheem Mfg. Co.*, 2016 WL 1222264, at *14 (N.D. Ga. Mar. 23, 2016) (holding that Justice Stevens's narrower concurring opinion controls the interpretation of *Shady Grove* as opposed to Justice Scalia's plurality); *Brown v. Electrolux Home Prods., Inc.*, 817 F.3d 1225, 1237-38 (11th Cir. 2016) (remanding case where the district court failed to consider pre-suit notice requirements when conducting its predominance inquiry for class certification). Accordingly, the argument fails.

### i. Timeliness of Notice

The Defendants argue that the Pre-Suit Notice was not timely under California, Massachusetts, Texas, West Virginia, and Indiana law. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 77; *See* Br. in Supp. of Verisk's Mot. to Dismiss, at 51-52 (as to Massachusetts and Indiana)).

Under the California Consumers Legal Remedies Act (the "CCLRA") and the Massachusetts Consumer Protection Act (the "MCPA"), a plaintiff asserting a violation of these statutes must provide notice of the claim to the defendant at least thirty days prior to the filing of any such action. Cal. Civ. Code § 1782(a); Mass. Gen. Laws ch.93A, § 9(3). The West Virginia Consumer Credit and Protection Act (the "WVCCPA") and TDTPA contain more onerous provisions, requiring a plaintiff to provide notice at least forty-five and sixty days, respectively, prior to the filing of an action. W. Va. Code. § 46A-5-108(a); Tex. Bus. & Com. Code § 17.505(a). Under the Indiana Deceptive Consumer Sales Act (the "IDCSA"), a plaintiff must generally provide notice to the defendant within the sooner of (1) "six [ ] months after the initial discovery of the deceptive act," (2) "one [ ] year following such consumer transaction," or (3) "any time limitation, not less than thirty [ ] days, of any period of warranty applicable to the transaction." Ind. Code § 24-5-0.5-5(a).

However, some exceptions to these requirements exist. Under the MCPA, notice is not required when the defendant does not maintain a place of business or keep assets within Massachusetts. *See* Mass. Gen. Laws ch. 93A,

§ 9(3). Additionally, under the IDCSA, notice is not required when the deceptive act is "incurable." Ind. Code § 24-5-0.5-5(a). However, no exception exists for the pre-suit notice statutes under the CCLRA, WVCCPA, and the TDTPA. Therefore, because the Plaintiffs filed their Amended Complaint sooner than what is statutorily proscribed by the three state statutes, Counts 19, 60, and 65 are hereby dismissed.

Turning to the MCPA, the CRA Defendants ask the Court to take judicial notice of the fact that they have places of business in Massachusetts and supply their company websites.[41] (*See* Reply Br. in Supp of Verisk's Mot. to Dismiss, at 32-33). "Under Rule 201 of the Federal Rules of Evidence, a court '*may* take judicial notice on its own' or '*must* take judicial notice if a party requests it and the court is supplied with the necessary information.'" *Lodge v. Kondaur Cap. Corp.*, 750 F.3d 1263, 1273 (11th Cir. 2014) (citing Fed. R. Evid. 201(c)). "The taking of judicial notice of facts is a highly limited process." *Id.* (citation modified). "The reason for this caution is that the taking of judicial notice bypasses the safeguards which are involved with the usual process of proving facts by competent evidence in district court." *Id.* (quotation marks and citation omitted). Under these principles, the Eleventh Circuit has upheld a district court's decision to decline to judicially notice content from a defendants'

[41] The GM Defendants make no argument in their Reply Brief explaining why Mass. Gen. Laws ch. 93A, § 9(3) is inapplicable to them.

website when the defendants did not provide either screenshots or their addresses. *Id.*

While the CRA Defendants provide website addresses to their own websites that show that they have places of business within Massachusetts, the Court declines to judicially notice these facts because such information is within the control of the CRA Defendants. The Court may only take judicial notice of facts that are not "subject to reasonable dispute because it . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b)(2). Taking judicial notice of information sourced directly from the CRA Defendants strains the requirements of this Rule. Additionally, the CRA Defendants have not provided any additional information outside of their website addresses that demonstrates the reliability of the information contained on their websites. Therefore, the Plaintiffs' MCPA claim survives the Motion to Dismiss on pre-suit notice grounds.

The Court now turns to the IDCSA. The Plaintiffs argue that the pre-suit notice period is inapplicable to them because the Defendants caused incurable harm to the applicable named Plaintiffs. (Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 45). However, the Plaintiffs cite no law that backs this assertion. Instead, the Plaintiffs argue that the applicable Plaintiff suffered incurable harm because the Defendants collected and distributed his

data without his consent, which increased his insurance premiums. (*Id.* (citing Am. Compl. ¶¶ 249-253)).

"Incurable deceptive act" is defined by statute as "a deceptive act done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead." Ind. Code § 24-5-0.5-2(8). None of the facts put forth by the Plaintiffs in response to the Motion to Dismiss fit this statutory definition. In fact, the Plaintiffs explicitly argue that their IDCSA claim does not sound in fraud in an earlier part of their Response Brief. (*See* Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 41-43). When the Plaintiffs argue as such, the Court cannot conclude that the Defendants have caused incurable harm. Therefore, because the Plaintiffs have failed to allege sufficient facts to properly allege incurable harm, Count 31 is hereby dismissed.

### ii. Content Deficiency

The remaining pertinent causes of action arise out of the Alabama Deceptive Trade Practices Act (the "ADTPA") (Count 11), the MCPA (Count 37), the Mississippi Consumer Protection Act (the "Miss. CPA") (Count 40), and the Utah Truth in Advertising Act (the "UTAA") (Count 61). The Defendants argue that the remaining counts within the Amended Complaint should be dismissed because the Plaintiffs' notice was deficient under each of the state statutes. (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 77; *see* Br. in Supp. of Verisk's Mot. to Dismiss, at 51 (as to the ADTPA and MCPA)).

Under the ADTPA and the MCPA, a plaintiff's pre-suit notice must "identify[ ] the claimant and reasonably describe[e] the unfair or deceptive act or practice relied upon and the injury suffered." Ala. Code § 8-19-10(e); Mass. Gen. Laws ch. 93A, § 9(3). The UTAA requires that "the complaining person first give[ ] notice of the alleged violation to the prospective defendant and provide[ ] the prospective defendant an opportunity to promulgate a correction notice by the same media as the allegedly violating advertisement." Utah Code § 13-11a-4(4)(a).[42]

However, for the notice provisions to be effective under the ADTPA and, as previously discussed, the MCPA, a defendant must have a place of business or assets within the state. *See* Ala. Code § 8-19-10(e); Mass. Gen. Laws ch. 93A, § 9(3). The Plaintiffs have not alleged within their Amended Complaint that the Defendants have a place of business or assets within Alabama or Massachusetts, and the Defendants fail to make an effective argument for the inapplicability of this provision. Therefore, the Plaintiffs' claims under the ADTPA and the MCPA survive.

The UTAA has no exception to notice like the ADTPA and the MCPA. Under the consumer statute, a pre-suit notice must allege a violation of the UTAA and must notify the defendant that it must post a correction notice in order to avoid an injunctive relief action. *See Nunes v. Rushton*, 299 F. Supp.

[42] The Miss. CPA does not appear to have any notice requirement. *See* Miss. Code § 75-24-15. Accordingly, the Court will not dismiss the Miss. CPA claim for insufficiency of notice.

3d 1216, 1241 (D. Utah 2018); *Lynch v. Leatherheads Sports Grill, LLC*, 2024 WL 3675927, at *3 (D. Utah Aug. 6, 2024). Here, within their pre-suit notice, the Plaintiffs notified GM of the conduct they allege to be a violation of the UTAA. (*See* GM Defs.' Pre-Suit Notice, at 1-2). The Plaintiffs then mentioned that the conduct is a violation of the UTAA, among other state statutes. (*See* GM Defs.' Pre-Suit Notice, at 2). Finally, the Plaintiffs demanded that GM undertake specific corrective action. (*See* GM Defs.' Pre-Suit Notice, at 4).

However, nowhere in its notice did the Plaintiffs demand that GM post a correction notice as required by the UTAA to avoid an action for injunctive relief. While the notice does demand that GM notify all individuals whose driving data was collected so that they may seek compensation, that is not the correction notice required by the UTAA. (*See* GM Defs.' Pre-Suit Notice, at 4). Because the UTAA claim arises out of false advertising, the remedy sought by the Plaintiffs is injunctive relief to retract alleged false claims. In that same vein, under the UTAA, the notice must provide the prospective defendant the opportunity to issue a correction notice "by the same media as the allegedly violating advertisement." Utah Code § 13-11a-4(4)(a). Thus, because the Plaintiffs failed to comply with the notice requirements of the UTAA, the Plaintiffs' UTAA claim (Count 61) is hereby dismissed.

### iii. Dispute Settlement Program

Finally, the Defendants argue for dismissal of the Miss. CPA claim (Count 40) because the Plaintiffs failed to engage in the alternative dispute

resolution program as required by the consumer statute. (Br. in Supp. of Verisk's Mot. to Dismiss, at 53; *see* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 76-77, 77 n. 55). Under the Miss. CPA, before filing suit under the statute, "the plaintiff must have first made a reasonable attempt to resolve any claim through an informal dispute settlement program approved by the Attorney General." Miss. Code § 75-24-15(2). The Plaintiffs make no effective argument in response, and the Amended Complaint does not allege any effort to comply with this provision. Accordingly, the Court will dismiss the Miss. CPA claim.

To summarize, the Plaintiffs' claims arising out of the CCLRA (Count 19), WVCCPA (Count 65), TDTPA (Count 60), IDCSA (Count 31), UTAA (Count 61) and Miss. CPA (Count 40) are dismissed. However, the Plaintiffs' MCPA (Count 37) and ADTPA (Count 11) claims survive.

**c. Pleading Fraud with Particularity (All Counts)**

The Defendants next argue for the dismissal of all state consumer statute claims for failing to plead with particularity under Federal Rule of Civil Procedure 9(b). (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 77-82; Br. in Supp. of Verisk's Mot. to Dismiss, at 48-51 (as to fourteen of the state consumer statutes)). Generally, 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." *Ashcroft*, 556 U.S. at 678 (quotation marks and citation omitted). However, under Rule 9(b), if a party alleges fraud or mistake, "a party

must state with *particularity* the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b) (emphasis added). As another court explained:

> A complaint satisfies Rule 9(b) if it sets forth precisely what statements or omissions were made in what documents or oral representations, who made the statements, the time and place of the statements, the content of the statements and manner in which they misled the plaintiff, and what benefit the defendant gained as a consequence of the fraud.

*In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1348 (N.D. Ga. 2000) (citing *Brooks v. Blue Cross and Blue Shield of Fla., Inc.*, 116 F. 3d 1364, 1371 (11th Cir. 1997)).

The Defendants argue that the state consumer statutes all "sound in fraud" and therefore must comply with Rule 9(b). (Br. in Supp. of GM Defs.' Mot. to Dismiss, at 77-78; *see* Br. in Supp. of Verisk's Mot. to Dismiss, at 49-51). Indeed, claims are subject to Rule 9(b)'s heightened pleading standards if they "sound in fraud." *See In re AFC Enters., Inc. Sec. Litig.*, 348 F. Supp. 2d 1363, 1376 (N.D. Ga. 2004). "A claim 'sounds in fraud' when a plaintiff alleges 'a unified course of fraudulent conduct and relies entirely on that course of conduct as the basis of that claim.'" *Burgess v. Religious Tech. Ctr., Inc.*, 2014 WL 11281382, at *6 (N.D. Ga. Feb. 19, 2014) (citation modified). For a state law claim to "sound in fraud," the elements of the claim must be similar to that of common law fraud, requiring—among other things—proof of scienter, reliance, and injury. *Fed. Trade Comm'n v. Hornbeam Special Situations, LLC*, 308 F. Supp. 3d 1280, 1287 (N.D. Ga. 2018).

Under this standard, the Court concludes that the Defendants fail to make a showing that Rule 9(b) applies to any of the consumer claims. Simply arguing that the state statutes require deceptive conduct is not enough to prove that the statutes contain elements that are similar to that of common law fraud. *See Fed Trade Comm'n*, 308 F. Supp. 3d at 1287 n. 6 (rejecting premise that "deception claims" or "misrepresentations" automatically trigger Rule 9(b)). Additionally, the Defendants have failed to show that the Plaintiffs' theory of recovery rests on any unified course of fraudulent conduct. *See In re Equifax, Inc. Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d at 1336.

The Defendants direct the Court to consider *Young v. Grand Canyon University, Inc.*, 57 F.4th 861 (11th Cir. 2023), where the Eleventh Circuit distinguished this Court's analogous decision in *In re Equifax, Inc. Customer Data Security Breach Litigation*. (Reply Br. in Supp. of GM Defs.' Mot. to Dismiss, at 48 n. 42 (citing *Young*, 57 F.4th at 875)). In *Young*, the Eleventh Circuit held that the plaintiff's claim under the Arizona Consumer Fraud Act was subject to the heightened pleading requirements of Rule 9(b). 57 F.4th at 875. There, the plaintiff alleged that the defendant intentionally misrepresented the amount of time it takes to complete a doctoral program at the institution. *Id.* The court distinguished *Equifax* by stating that "it involved claims related to a consumer data breach" and held that it was inapplicable to the factual situation in *Young*. *Id.* Yet, *Young*'s reasoning is inapplicable to the Court's determination in this case that Rule 9(b) does not apply. The

Defendants here have failed to show *how* the misrepresentations "sound in fraud" within their Motion to Dismiss. Plainly, arguing that the Plaintiffs allege misrepresentations does not automatically make a pleading "sound in fraud." Additionally, unlike the representations by the defendant in *Young*, the scope and impact of the misrepresentations do not amount to fraud-like behavior. The Court views the facts alleged in the pleadings as conduct somewhere between the facts in *Equifax* and *Young*, with *Young* being conduct that squarely "sounds in fraud." Therefore, because the facts here do not reach the level of conduct in *Young*, the Court concludes that the heightened pleading standard of Rule 9(b) does not apply to any of the state consumer statutes.

**d. Omissions-Based Claims**

The GM Defendants argue that, to the extent any of the state consumer claims are entirely based on omissions, such claims should be dismissed. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 82-84). First, the GM Defendants contend that they did not omit material facts about collecting and using the Plaintiffs' data because such information was present within the User Terms and Privacy Statement. (*See id.* at 82-83).

This argument is not persuasive to the Court for a few reasons. It is true that "the presence of true information or a disclaimer can rebut a claim of deception" in a Motion to Dismiss. *Kurimski v. Shell Oil Co.*, 2022 WL 2913742, at *7 (S. D. Fla. Jun. 30, 2022) (citing *Freeman v. Time, Inc.*, 68 F.3d 285 (9th Cir. 1995), then citing *Zlotnick v. Premier Sales Grp., Inc.*, 480 F. 3d 1281 (11th

Cir. 2007)). However, the facts alleged in the Amended Complaint do not suggest that the User Terms or Privacy Statement were presented or disclosed to the Plaintiffs upon purchasing a GM vehicle. *Cf. id.* at *7-*8 (dismissing a claim under Florida's consumer protection statute because the plaintiff alleged facts that showed that the defendant fully disclosed pricing information at the gas pump prior to use and payment). As alleged, the GM Defendants knew to some degree that there were at least some Plaintiffs who were enrolled into OnStar but were not adequately being shown the User Terms and Privacy Statement prior to enrollment. (*See* Am. Compl. ¶ 890). Without clear disclosure, there is no true information or disclaimer to dismiss the claim on a motion to dismiss.

As to the Plaintiffs who had full disclosure of the User Terms and the Privacy Statement, the GM Defendants' argument still fails. As more fully discussed in the Court's discussion on Count 8, the allegations within the Amended Complaint demonstrate potential issues related to the Plaintiffs' scope of consent and whether the GM Defendants exceeded the consent.

Turning to the GM Defendants' second argument, they argue that the Plaintiffs' omission-based claims are not actionable absent a freestanding duty to disclose, which numerous states do not impose. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 83-84). Further, the GM Defendants argue that even in the states that do impose a duty to disclose, the duty exists only where a defendant had knowledge of the latent defect and the plaintiff was unable to

discover it through reasonable diligence. (*See id.* at 84). The Plaintiffs do not dispute this fact but instead argue that the GM Defendants' public statements and partial disclosures give rise to a duty to correct false impressions. (Pls.' Br. in Opp'n to GM Defs.' Mot. to Dismiss, at 75-76).

"In the absence of a confidential relationship, no duty to disclose exists when parties are engaged in arm's length business negotiations." *Infrasource, Inc. v. Hahn Yalena Corp.*, 272 Ga. App. 703, 705 (2005). However, "if a manufacturer made a representation, then it had a duty to disclose new information if it became aware that the new information made the earlier representation misleading or untrue." *Counts v. General Motors, LLC*, 606 F. Supp. 3d 678, 716 (E.D. Mich. 2022) (citation modified).

Here, GM and the Plaintiffs are engaged in an arm's length transaction through the purchase of a GM vehicle. As alleged in the Amended Complaint, GM made numerous public representations to both the general public and their consumers about their data collection practices which were vague and misleading, at best. (*See* Am. Compl. ¶¶ 800-803, 805, 807, 817-22, 828-43, 859-67, 871-912). This is further bookended by allegations of GM's concealment of its practices. (*See id.* ¶¶ 792-802, 805, 807, 817-22). Under these alleged facts, GM could be found to have a duty to disclose under numerous state consumer statutes. Therefore, the Court will not dismiss any omissions-based claims.

**e. Scienter (Counts 11, 12, 29, 32, 34, 44, 45, 51, 59)**

Next, the GM Defendants focus on certain state statutes that require a plaintiff bringing suit to plead that GM acted with scienter.[43] The Defendants argue that the Plaintiffs fail to allege this element of their state consumer claims. (*See* Br. in Supp. of GM Defs.' Mot. to Dismiss, at 84-85). The Court disagrees.

To be sure, the Defendants are correct to assert that intent is alleged within each Count in a conclusory manner by simply stating that "GM acted intentionally, knowingly, and maliciously." (Am. Compl. ¶¶ 1118, 1131, 1387, 1443, 1484, 1700, 1716, 1777, 1904). However, the Plaintiffs' Amended Complaint goes further than those barebone provisions. The Plaintiffs, in their general factual allegations, detail a comprehensive scheme where scienter can be gleaned. *See* Discussion III.D(1)(a)(iii), *supra*, at p. 74-76. Therefore, the Court will not dismiss these claims for lack of scienter.

---

[43] *See* Ala. Code § 8-19-13 (requiring knowledge to allege a violation of the ADTPA); Ariz. Rev. Stat. § 44-1522(A) (requiring scienter to allege a violation); 815 Ill. Comp. Stat. 505/2 (same); Kan. Stat. Ann. § 50-626(b) (similar); Nev. Rev. Stat. § 598.0923(1) (same); N.J. Stat. Ann. § 56:8-2 (requiring scienter for omissions claims); Ohio Rev. Code Ann. § 1345.03(B) (requiring scienter for unconscionable acts); S.D. Codified Laws § 37-24-6(1) (requiring scienter for misrepresentations or omissions). The Maryland Consumer Protection Act does not appear to require scienter, but a plaintiff can allege a violation under the statute by doing so. *See* Md. Code Ann. Com. Law § 13-301. The GM Defendants also addressed the IDCSA and the UTAA within their argument, but these claims have already been dismissed.

**f. Consumer Relationship (Counts 11, 12, 18, 21, 24, 28, 29, 32, 33, 37, 44, 46, 52, 54, 57, 58)**

The CRA Defendants focus on almost every remaining Count arising out of a consumer protection statute lodged against them in the Amended Complaint. They argue that these state consumer protection statutes require the Plaintiffs to allege a "direct, transactional relationship between a plaintiff and a defendant," which the Plaintiffs fail to plead. (Br. in Supp. of Verisk's Mot. to Dismiss, at 42; *see generally* Br. in Supp. of Verisk's Mot. to Dismiss, Ex. B ("CRA Defendants' Consumer Statute Table") [Doc. 141-4]). The Plaintiffs only respond with case law discussing Counts 18, 29, 46, and 54.[44] (*See id.*). Because the Plaintiffs fail to provide case law addressing their other counts, the Court will dismiss the CRA Defendants from Counts 11, 12, 21, 24, 28, 32, 33, 37, 44, 52, 57, and 58. *See Fawcett v. Carnival Corp.*, 682 F. Supp. 3d 1106, 1112 (S.D. Fla. 2023) ("The failure to respond to arguments regarding claims addressed in a motion to dismiss is [a] sufficient basis to dismiss such claims as abandoned or by default."); *Hooper v. City of Montgomery*, 482 F. Supp. 2d 1330, 1334 (M.D. Ala. 2007) (citing *See Resol. Tr. Corp. v. Dunmar Corp.*, 43 F.3d 587, 599 (11th Cir. 1995). The Court will now address the remaining Counts.

[44] The Plaintiffs also respond to Counts 31 (IDCSA) and 60 (TDTPA). (*See* Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 33-35). However, Count 31 has already been dismissed and Count 60 is not relevant to the CRA Defendants' argument.

### i. California (Count 18)

The California Plaintiffs bring a claim under the California Unfair Competition Law (the "CUCL"). The CUCL prohibits "any unlawful, unfair[,] or fraudulent business act or practice and unfair, deceptive, untrue[,] or misleading advertising." Cal. Bus. & Prof. Code § 17200. "Its purpose is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services." *Kwikset Corp. v. Super. Ct. of Orange Cnty.*, 51 Cal. 4th 310, 320 (2011) (citation modified). "Private standing is limited to 'any person who has suffered injury in fact and has lost money or property' as a result of unfair competition." *Id.* at 320-21 (citing Cal. Bus. & Prof. Code § 17204). Ultimately, to satisfy standing under the CUCL, a party must (1) "establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., *economic injury*," and (2) "show that the economic injury was the result of, i.e., *caused by*, the unfair business practice or false advertising that is the gravamen of the claim." *Id.* at 322. It does not require any allegation of a consumer relationship with the defendant.

The crux of the CRA Defendants' argument relies on a footnote within *Kwikset Corp.* that discusses voter intent behind Proposition 64, which amended Section 17204 in 2004. (*See* CRA Defendants' Consumer Statute Table, at 1-2 (citing *Kwikset Corp.*, 51 Cal. 4th at 335 n. 21)). However, the reliance is misplaced when reading the court's opinion as a whole. In *Kwikset Corp.*, the California Supreme Court noted that while the intent of the voters

was to constrain standing to only those who have used the defendant's products or services, the language of Proposition 64 and the new Section 17204 was broader, conferring standing to more plaintiffs than intended. *See Kwikset Corp.*, 51 Cal. 4th at 321. Therefore, while the California Supreme Court acknowledged the intent of the voters within the footnote, it did not hold that only plaintiffs who engage in a commercial relationship with the defendant may file suit against the defendant. *See Clayworth v. Pfizer, Inc.*, 49 Cal.4th 758, 788-89 (2010) (holding the same). Accordingly, the Court will not dismiss the California Plaintiffs' CUCL claim for failure to allege a consumer relationship.

**ii. Illinois (Count 29)**

The Plaintiffs who form part of the Illinois subclass (the "Illinois Plaintiffs") bring a claim under the ICFA. "To have standing to bring a claim under the ICFA, a plaintiff must either be a consumer *or* satisfy the consumer nexus test." *Ramirez*, 729 F. Supp. 3d at 846 (citation omitted) (emphasis added). Under the ICFA, a "consumer" is defined as "any person who purchases or contracts for the purchase of merchandise not for resale in the ordinary course of his trade or business but for his use or that of a member of his household." 815 Ill. Comp. Stat. 505/1(e).

The consumer nexus test is less clear. Two versions of the consumer nexus test are potentially applicable because the Illinois Supreme Court has yet to weigh in on which test is proper. *See Ramirez*, 729 F. Supp. 3d at 846.

The first test requires a plaintiff to plead that the defendant engaged in violative trade practices directed towards the market generally or violative conduct that otherwise implicates consumer protection concerns. *Id.*; *see Frazier v. U.S. Bank Nat. Ass'n*, 2013 WL 1385612, at *4 (N.D. Ill. Apr. 4, 2013). The second test requires the Court to engage in a four-element test that requires a plaintiff to show (1) "that their actions were akin to a consumer's actions to establish a link between them and consumers," (2) "how defendant's representations concerned consumers other than [the] plaintiff," (3) "how [the] defendant's particular activity involved consumer protection concerns," and (4) "how the requested relief would serve the interests of consumers." *Roppo v. Travelers Companies*, 100 F. Supp. 3d 636, 651 (N.D. Ill. 2015).

Here, the Illinois Plaintiffs are not consumers, and they do not argue as such. Therefore, for the Illinois Plaintiffs to state a claim under the ICFA, they must satisfy the consumer nexus test. Although the Illinois Supreme Court has not spoken on which test is operative, the Court need not decide because the Illinois Plaintiffs fail to plead sufficient facts under a common principle underlying both tests. Specifically, both tests are satisfied when the plaintiff alleges that the defendant targets the market at large and that the plaintiff suffered some injury as a result.

*Ramirez* is entirely instructive. There, the plaintiffs brought suit against the defendant because of its ongoing collection of consumer data which they sold to 400,000 entities, including private corporations, government

agencies, and law enforcement agencies. *Ramirez*, 729 F. Supp. 3d at 845. In holding that the plaintiffs failed to satisfy the consumer nexus test, the court noted that the plaintiffs were individuals, while the defendant's actions were targeted towards its consumers, who were entities rather than individuals. *Id.* at 847. Although the plaintiffs felt repercussions from the defendant's conduct, the defendant only targeted a subset of the Illinois market. *Id.*; *see Beatty v. Accident Fund Gen. Ins. Co.*, 2018 WL 3219936, at *10 (S.D. Ill. Jul. 2, 2018) (holding that the plaintiff failed to satisfy the consumer nexus test when the defendant failed to pay *medical providers*, which impacted Illinois consumers at large); *Tile Unlimited, Inc. v. Blanke Corp.*, 788 F. Supp. 2d 734, 739-40 (N.D. Ill. 2011) (holding that the plaintiff failed to satisfy the consumer nexus test when the defendant's conduct as alleged was targeted only towards tile installers and only tile installers suffered injury).

Here, like *Ramirez*, while the Illinois Plaintiffs and other potential Illinois consumers are affected by the repercussions of the CRA Defendants' conduct, the CRA Defendants only sold consumer reports to insurance companies, not the Illinois consumers individually. (*See* Am. Compl. ¶¶ 705, 749). Therefore, the Illinois Plaintiffs fail to satisfy this version of the consumer nexus test. The Illinois Plaintiffs fail the second version of the consumer nexus test for similar reasons. Under the first element, the Illinois Plaintiffs' actions are not akin to the actions of the consumers because the Illinois public is not the targeted market. Because the Illinois Plaintiffs cannot demonstrate this

first element, they cannot satisfy the consumer nexus test. Therefore, the Illinois Plaintiffs' ICFA claim fails and the CRA Defendants are hereby dismissed from Count 29.

### iii. New York (Count 46)

The Plaintiffs who form part of the New York subclass (the "New York Plaintiffs") bring a claim under New York General Business Law ("NYGBL") § 349. To assert a claim under NYGBL § 349, a plaintiff must allege (1) "the challenged act or practice was consumer-oriented," (2) "the act or practice was misleading in a material way," and (3) "the plaintiff suffered injury as a result of the deceptive act." *In re Blackbaud, Inc., Customer Data Breach Litig.*, 2021 WL 3568394, at *12 (D.S.C. Aug. 12, 2021) (quoting *Stutman v. Chem. Bank*, 95 N.Y.2d 24, 29 (2000) (citation modified)). "An act or practice is 'consumer-oriented' if it has 'a broader impact on consumers at large.'" *Id.* (quoting *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 25 (1995)). Unlike the requirements within the ICFA, NYGBL § 349 "does not impose a requirement that consumer-oriented conduct be directed to all members of the public." *Id.* (quoting *Plavin v. Grp. Health Inc.*, 35 N.Y.3d 1, 11 (2020) (citation modified)). "The consumer-oriented act or practice requirement has been construed liberally." *Id.* (quoting *New York v. Feldman*, 210 F. Supp. 3d 294, 301 (S.D.N.Y. 2002) (citation modified)). "Indeed, there is no requirement of privity, and victims of indirect injuries are permitted to sue under the Act." *Id.* at *13 (quoting *In re Methyl Tertiary Butyl*

*Ether Prods. Liab. Litig.*, 175 F. Supp. 2d 593, 630-31 (S.D.N.Y. 2001) (citation modified)). "The critical question, then, is whether the matter affects the public interest in New York, not whether the suit is brought by a consumer or a competitor." *Id.* (quoting *Securitron Magnalock Corp. v. Schnabolk*, 65 F.3d 256, 264 (2d Cir. 1995) (citation modified)).

The CRA Defendants' argument is less than compelling. The CRA Defendants argue that a consumer relationship is required under NYGBL § 349 by citing to *In re USAA Data Security Litigation*, 621 F. Supp. 3d 454 (S.D.N.Y. 2022). However, that case fails to consider whether a consumer relationship is required at all, instead focusing all of the court's analysis on causation. *See id.* at 472 ("Plaintiffs thus fail plausibly to allege their injuries were 'caused' by any deceptive conduct on the part of USAA."). Thus, the CRA Defendants cite no compelling authority for their position that NYGBL § 349 requires a consumer relationship.

Even the CRA Defendants' attempt to distinguish *Blackbaud* fails. They argue that, while there was no privity between the plaintiff and the defendant, there was some commercial relationship with the plaintiff due to the consumer-oriented transactions. (Br. in Supp. of Verisk's Mot. to Dismiss, at 25). The Court sees no reason why such a relationship does not exist here. The CRA Defendants' offending conduct involves the dissemination of the New York Plaintiffs' information to insurance companies. (*See* Am. Compl. ¶ 1724). Each insurance company has a consumer relationship with the New York

Plaintiffs through their insurance. Therefore, through the CRA Defendants' offending conduct, the New York Plaintiffs have alleged indirect harm through a chain of consumer-oriented transactions. Therefore, the Court will not dismiss the New York Plaintiffs' NYGBL § 349 claim.

### iv. Pennsylvania (Count 54)

The Plaintiffs who form part of the Pennsylvania subclass (the "Pennsylvania Plaintiffs") bring a claim under the PUTPCPL. The PUTPCPL clearly states that "[a]ny person *who purchases or leases goods or services* . . . and thereby suffers any ascertainable loss . . . may bring a private action to recover actual damages." 73 Pa. Cons. Stat. § 201-9.2(a). "[T]he statute unambiguously permits only persons who have purchased or leased goods or services to sue." *Katz v. Aetna Cas. & Sur. Co.*, 972 F.2d 53, 55 (3d Cir. 1992) (citing *id.*). "Had the Pennsylvania legislature wanted to create a cause of action for those not involved in a sale or lease, it would have done so." *Id.* While the PUTPCPL does not require strict privity, it does require some amount of commercial dealing between the parties for a private cause of action to lie. *See id.* at 57. Additionally, the statute requires that a plaintiff not receive the benefit free of charge. *See Dobson v. Milton Hershey Sch.*, 356 F. Supp. 3d 428, 435 (M.D. Pa. 2018).

Despite the clear words of the statute, the Pennsylvania Plaintiffs argue that the PUTPCPL does not require a consumer relationship. (*See* Pls.' Br. in Opp'n to Verisk's Mot. to Dismiss, at 34 n. 17). In doing so, they cite to

*Weinberg v. Sun Co.*, 565 Pa. 612 (2001) and *Hunt v. U.S. Tobacco Co.*, 538 F.3d 217, 223 (3d Cir. 2008) for the proposition that all the PUTPCPL requires is a showing that they suffered an ascertainable loss as a result of the CRA Defendant's actions. (*Id.*). Both cases are inapplicable here because, in those cases, there was no dispute over whether the plaintiffs purchased goods or services. *See Weinberg*, 565 Pa. at 614 ("Appellees . . . were purchasers of Sunoco Ultra® gasoline"); *Hunt*, 538 F.3d at 219, 221-28 (discussing the plaintiffs, as class members, bringing a claim for increased prices for smokeless tobacco and discussing only justifiable reliance as the sole issue on appeal).

Here, the Pennsylvania Plaintiffs cannot allege a sale or lease of goods or services because the only thing some Pennsylvania Plaintiffs received from the CRA Defendants was a free-of-charge annual disclosure. (*See* Am. Compl. ¶¶ 571, 583). Without an allegation of such a relationship, the Pennsylvania Plaintiffs cannot maintain their PUTPCPL claim. Therefore, the Court dismisses the CRA Defendants from Count 54 of the Amended Complaint.

In sum, the CRA Defendants are dismissed from Counts 11, 12, 21, 24, 28, 29, 32, 33, 37, 44, 52, 54, 57, and 58. However, the CRA Defendants are not dismissed from Counts 18 and 46.

**g. Vague and Conclusory (Counts 18, 46, 50)**

The CRA Defendants argue for dismissal from all remaining state consumer statute counts where they are named as a party for two reasons. First, they argue that the Plaintiffs fail to allege facts that demonstrate that

they are liable under each element of the consumer statutes. (*See* Br. in Supp. of Verisk's Mot. to Dismiss, at 47). Second, they argue that the Plaintiffs fail to identify which section of the statutes the they violated within each of these counts. (*See id.* at 47-48). The Court is not persuaded.

While the Plaintiffs make conclusory allegations within each count, the Plaintiffs detail a comprehensive scheme that the CRA Defendants took part in in the general factual section of the Amended Complaint. Such detailed factual allegations satisfy the causation requirement of standing as to the CRA Defendants. *See* Discussion III.F(3)(b), *supra*, at p. 134-35. The same argument applies to the CRA Defendants' point that the Plaintiffs fail to identify the specific statutes that the CRA Defendants are accused of violating. Because the Plaintiffs allege that the GM Defendants and CRA Defendants operated together to engage in deceptive conduct, the allegations against the GM Defendants put the CRA Defendants on notice of where their involvement lies as to their liability. Therefore, the Court will not dismiss the remaining counts against the CRA Defendants.

### G. Declaratory and Injunctive Relief

Finally, the Defendants argue for the dismissal of the Plaintiffs' requests for injunctive and declaratory relief for two reasons. First, the CRA Defendants argue that declaratory and injunctive relief is improper when the Plaintiffs already possess an adequate remedy at law. (*See* Br. in Supp. of Verisk's Mot. to Dismiss, at 53). Second, the Defendants argue that the

Plaintiffs are not at risk of future harm. (*See id.* at 54; Br. in Supp. of GM Defs.' Mot. to Dismiss, at 52 n. 33). The Court takes each argument in turn.

**1. Adequate Remedy at Law**

"To obtain injunctive relief, it is well-settled that a plaintiff must demonstrate that her remedies at law are inadequate." *Clark v. Aaron's, Inc.*, 914 F. Supp. 2d 1301, 1307 (N.D. Ga. 2012) (citation omitted). However, the Federal Rules of Civil Procedure authorize parties to plead for "alternative or different types of relief." Fed. R. Civ. P. 8(a)(3); *see Rozier v. Harford Ins. Co. of the Midwest*, 2014 WL 6751639, at *4 (S.D. Fla. Dec. 1, 2014). While courts in this Circuit have dismissed claims for equitable relief at the motion to dismiss stage, the Court declines to do so here. The Court sees no reason to preemptively strip the Plaintiffs of the opportunity to develop the evidentiary record prior to weighing the equitable factors. *See Amin v. Mercedes-Benz USA, LLC*, 301 F. Supp. 3d 1277, 1297 (N.D. Ga. 2018). Therefore, the Court will allow the Plaintiffs to plead alternative remedies at this time.

**2. Risk of Future Harm**

"A prayer for injunctive and declaratory relief requires an assessment, at this stage in the proceeding, of whether the plaintiff has sufficiently shown a real and immediate threat of future harm." *Elend v. Basham*, 471 F.3d 1199, 1207 (11th Cir. 2006) (citing *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983)). "[F]or an injury to suffice for prospective relief, it must be imminent." *Id.* (citation omitted). "[P]ast 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." *Id.* at 1207-08 (quoting *Lyons*, 461 U.S. at 102). In the context of a data breach, this Court has held that pleading that the defendant continues to follow inadequate security measures in protecting customer data is sufficient to show that the plaintiffs will suffer substantial harm in order to maintain an action for injunctive and declaratory relief. *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016).

Here, the factual allegations within the Amended Complaint support a finding that, without injunctive and declaratory relief, the Plaintiffs suffer "a real and immediate threat of future harm." *See Elend*, 471 F.3d at 1207 (citing *Lyons*, 461 U.S. at 105). While GM sunset the Smart Driver program and ceased sharing data with the CRA Defendants, (Am. Compl. ¶ 953), GM continues to share data with other companies. (*See* Am. Compl. ¶¶ 769-85, 1056, 1066). There is no indication within the Amended Complaint that GM has ceased such practices.

Furthermore, while the CRA Defendants no longer collect consumer data from the GM Defendants, previously collected data is still maintained by the CRA Defendants with or without any security measures. The allegedly improper receipt and continued possession of the driving data means the data can still be transferred to insurers who request reports through LNRS and

potentially, Verisk. (*See* Am. Compl. ¶¶ 957-58, 960). Therefore, the Court will not dismiss the Plaintiffs' request for injunctive or declaratory relief.

## IV. Conclusion

For the foregoing reasons, Defendant LNRS' Motion to Dismiss [Doc. 140] is GRANTED in part and DENIED in part, Defendant Verisk's Motion to Dismiss [Doc. 141] is GRANTED in part and DENIED in part, and the GM Defendants' Motion to Dismiss is GRANTED in part and DENIED in part [Doc. 142]. The Court presents a table below identifying which Counts have been dismissed, exclusive of issues surrounding FCRA preemption and Article III standing.

| Count | GM | CRA Defendants |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | Dismissed | |
| 5 | Dismissed in Part | Dismissed in Part |
| 6 | Dismissed in Part | Dismissed in Part |
| 7 | | |
| 8 | | |
| 9 | Dismissed | Dismissed |
| 10 | | Dismissed in Part |
| 11 | | Dismissed |

| | | |
|---|---|---|
| 12 | | Dismissed |
| 13 | Dismissed in Part | Dismissed |
| 14 | | |
| 15 | | [redacted] |
| 16 | Dismissed | |
| 17 | Dismissed | Dismissed |
| 18 | | |
| 19 | Dismissed | [redacted] |
| 20 | | |
| 21 | | Dismissed |
| 22 | | [redacted] |
| 23 | | |
| 24 | | Dismissed |
| 25 | | |
| 26 | | [redacted] |
| 27 | | |
| 28 | | Dismissed |
| 29 | Dismissed in Part | Dismissed |
| 30 | | |
| 31 | Dismissed | Dismissed |
| 32 | | Dismissed |
| 33 | | Dismissed |

| | | |
|---|---|---|
| 34 | | [redacted] |
| 35 | | |
| 36 | | [redacted] |
| 37 | | Dismissed |
| 38 | Dismissed | Dismissed |
| 39 | | [redacted] |
| 40 | Dismissed | Dismissed |
| 41 | | |
| 42 | | [redacted] |
| 43 | | |
| 44 | | Dismissed |
| 45 | | [redacted] |
| 46 | | |
| 47 | | [redacted] |
| 48 | | |
| 49 | | |
| 50 | | |
| 51 | | [redacted] |
| 52 | | Dismissed |
| 53 | | [redacted] |
| 54 | | Dismissed |
| 55 | | |

| | | |
|---|---|---|
| 56 | | [redacted] |
| 57 | | Dismissed |
| 58 | | Dismissed |
| 59 | | [redacted] |
| 60 | Dismissed | |
| 61 | Dismissed | |
| 62 | | |
| 63 | | |
| 64 | | |
| 65 | Dismissed | |

SO ORDERED, this 22nd day of April, 2026.

THOMAS W. THRASH, JR.
United States District Judge