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

DELIA ARELLANO, MATTHEW BAUMGARTNER, DARREN BRISSETT, DANNY CARROL, BRIANNA CLAY, TOYETTE FLOWERS, CHRISTOPHER FREEL, JADE GAMBLE, KIMBERLY KELLEY, DANIEL KILGO, SOFIA MALVAR, JAMES MCNEILL, DAVID MURRY, AMANDA QUAM, ANNETTE RASTRELLI, NICOLE REHFUSS, BILLY ROBINSON, DORIAN ROCHESTER, ROBERT SANGINITO, KAYLA SMITH, ROBERT SMITH, AUSTIN TOPCHI, TRACY TUPPER, JAMES WILLIAMS AND EBONI WRIGHT, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

THE ALLSTATE CORPORATION, ALLSTATE INSURANCE COMPANY, ALLSTATE VEHICLE AND PROPERTY INSURANCE COMPANY, ARITY LLC, ARITY 875 LLC, and ARITY SERVICES LLC

Defendants.

Case No.: 1:25-cv-01256

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Delia Arellano, Matthew Baumgartner, Darren Brissett, Danny Carroll, Brianna Clay, Toyette Flowers, Christopher Freel, Jade Gable, Kimberly Kelley, Daniel Kilgo, Sofia Malvar, James McNeill, David Murry, Amanda Quam, Annette Rastrelli, Nicole Rehfuss, Billy Robinson, Dorian Rochester, Robert Sanginito, Kayla Smith, Robert Smith, Austin Topchi, Tracy Tupper, James Williams, and Eboni Wright (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, and against Defendants The Allstate Corporation, Allstate Insurance

Company, Allstate Vehicle and Property Insurance Company, Arity LLC, Arity 875 LLC, and Arity Services LLC (collectively, "Defendants'), allege the following upon their own knowledge, or where they lack personal knowledge, upon information and belief, including the investigation of counsel.

I. INTRODUCTION

1. Defendants conspired to covertly collect and sell "trillions of miles" of consumers' driving data and personal data from mobile devices, in-car devices, and vehicles. This data included geolocation data, accelerometer data, magnetometer data, gyroscopic data, altitude, longitude, latitude, bearing, GPS time, speed, and accuracy. Defendants used this "driving behavior" data to create individualized driver profiles based on driving habits and movement.

2. Defendants illegally collected this information without informing or seeking consent from the millions of Americans, including Plaintiffs and Class Members, that their data was continuously being extracted and sold.

3. Defendants were so effective that they created the "world's largest driving behavior database," consisting of trillions of miles driven by over 45 million Americans. Defendants profited from this illicit behavior by selling data, including driving data, to third parties, including other insurance carriers ("Insurers"), and by supporting Defendants' own insurance business.

4. Defendants accomplished this scheme by creating a software development kit ("SDK"), for third party mobile applications. SDKs provide application developers with the tools necessary to build their applications including APIs and other automated functions that operate in the background. As such, third party developers may not have known the full scope of how Defendants' SDK (the "Arity SDK") operated in the background of their applications.

5. Defendants encouraged the adoption of their SDK by paying these app developers millions of dollars to integrate Defendants' software into their apps and by providing developers bonus incentives based on the size of their dataset.

6. Defendants' Arity SDK ensured that when a user downloaded the relevant third-party application, the user would unwittingly download Defendants' software. This allowed Defendants to siphon off these trillions of miles of Plaintiffs and Class Members' data. Defendants' own website admits that they are able to capture data "every 15 seconds or less" from "40 [million] active mobile connections."[1]

7. Defendants profited from this ill-gotten database by selling access to other Insurers and to inform their own underwriting. In either instance, when providing a quote to an insured or when renewing coverage, Insurers would use Defendants' data as a basis for denying coverage, increasing auto-insurance premiums, or dropping the insureds from coverage.

8. Defendants' database is not only illegal, but also likely faulty because it relies on user phones without verification that Plaintiffs were driving. As such, much of the information upon which Insurers are increasing premiums may not have been generated while the user was in-fact driving. Much of this ill-gotten data may have been generated while the user was riding mass transit or riding in a taxi. Presumably in response to this inherent inaccuracy, Defendants also purchased vehicle data from manufacturers including Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram.

9. Plaintiffs and Class Members did not consent to the collection and sale of their personal, sensitive, and valuable data. Plaintiffs and Class Members were not even clearly or plainly advised that this information was being collected and sold. Pursuant to their agreements

[1] https://arity.com/solutions/real-time-insights/

with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented and obtained from consumers. Defendants made no effort to directly obtain consumer consent themselves, knowing full-well that consumers would roundly decline to use an app if they knew it would track their every movement and ascribe it as driving behavior that would then be sold to Insurers to increase consumers' insurance rates.

10. Defendants never informed Plaintiffs or Class Members about their data collection practices and Defendants never received consent to compile this data. Defendants similarly never informed Plaintiffs or Class Members of the many ways their data would be manipulated, analyzed, packaged, and sold.

11. As described throughout this Complaint, Defendants violated several federal and state laws and invaded the privacy of Plaintiffs and Class Members.

12. Plaintiffs bring this action against Defendants on behalf of themselves and all those similarly situated for damages, injunctive relief, and restitution.

II. JURISDICTION & VENUE

13. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from Capital One, there are more than 100 Class members nationwide, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a). This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and ancillary jurisdiction pursuant to 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendants because Defendants maintain their principal headquarters in this District, do business in this District, directly or through agents, and have sufficient minimum contacts with this District such that they have

intentionally availed themselves of the laws of the United States and Illinois.

15. Venue is proper under 28 U.S.C. § 1391(a) through (d) because Defendants' headquarters and principal place of business are located in this District, Defendant resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel.

III. PARTIES

Plaintiffs

16. Plaintiff Delia Arellano is a citizen and resident of the State of Utah, currently residing in Millcreek. Plaintiff Arellano used the mobile application Life 360 which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

17. Plaintiff Matthew Baumgartner is a citizen and resident of the State of South Carolina, currently residing in Woodruff. Plaintiff Baumgartner used the mobile applications Life 360, GasBuddy, and Fuel Rewards which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

18. Plaintiff Darren Brissett is a citizen and resident of the State of Illinois, currently residing in Chicago Heights. Plaintiff Brissett used the mobile application Life 360, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was

tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

19. Plaintiff Amanda Quam is a citizen and resident of the State of Illinois, currently residing in Dwight. Plaintiff Quam used the mobile applications Routely, Life 360, GasBuddy, and Fuel Rewards, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

20. Plaintiff Danny Carroll is a citizen and resident of the State of Mississippi, currently residing in Arnold. Plaintiff Carroll used the mobile applications GasBuddy and Fuel Rewards which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

21. Plaintiff Brianna Clay is a citizen and resident of the State of North Carolina, currently residing in Charlotte. Plaintiff Clay used the mobile application Life 360 which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

22. Plaintiff Christopher Freel is a citizen and resident of the State of Texas, currently residing in Cypress. Plaintiff Freel used the mobile application Life 360, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

23. Plaintiff Annette Rastrelli is a citizen and resident of the State of Texas, currently residing in Dallas. Plaintiff Rastrelli used the mobile applications GasBuddy and Fuel Rewards, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

24. Plaintiff Toyette Flowers is a citizen and resident of the State of Wisconsin, currently residing in Milwaukee. Plaintiff Flowers used the mobile application Routely which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

25. Plaintiff Jade Gable is a citizen and resident of the State of Arizona, currently residing in Surprise. Plaintiff Gable used the mobile application Life 360 which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

26. Plaintiff Eboni Wright is a citizen and resident of the State of Florida, currently residing in Thonotosassa. Plaintiff Hunter used the mobile application Life 360, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

27. Plaintiff Kimberly Kelley is a citizen and resident of the State of Georgia, currently residing in Dunwoody. Plaintiff Kelley used the mobile applications Life 360, GasBuddy, and Fuel Rewards, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's

mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

28. Plaintiff Billy Robinson is a citizen and resident of the State of Georgia, currently residing in Trion. Plaintiff Robinson used the mobile application Life360 which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

29. Plaintiff Daniel Kilgo is a citizen and resident of the State of Alabama, currently residing in Arab. Plaintiff Kilgo used the mobile applications Life 360 and Fuel Rewards, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

30. Plaintiff Sofia Malvar is a citizen and resident of the State of California, currently residing in Vallejo. Plaintiff Malvar used the mobile application Fuel Rewards which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

31. Plaintiff Austin Topchi is a citizen and resident of the State of California, currently residing in Menifee. Plaintiff Topchi used the mobile applications Life360, GasBuddy, and Fuel Rewards which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data

database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

32. Plaintiff James McNeill is a citizen and resident of the State of Louisiana, currently residing in Sulphur. Plaintiff McNeill used the mobile application Life 360, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

33. Plaintiff David Murry is a citizen and resident of the State of Missouri, currently residing in Foxworth. Plaintiff Murry used the mobile application Life 360, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

34. Plaintiff Nicole Rehfuss is a citizen and resident of the State of Kentucky, currently residing in Augusta. Plaintiff Rehfuss used the mobile application Fuel Rewards which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

35. Plaintiff Dorian Rochester is a citizen and resident of the State of Pennsylvania, currently residing in Allenwood. Plaintiff Rochester used the mobile applications Life360, GasBuddy, and Fuel Rewards, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

36. Plaintiff Robert Sanginito is a citizen and resident of the State of New Jersey, currently residing in Hackensack. Plaintiff Sanginito used the mobile applications Life360 and GasBuddy, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

37. Plaintiff Kayla Smith is a citizen and resident of the State of Indiana, currently residing in Crown Point. Plaintiff Smith used the mobile application GasBuddy, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

38. Plaintiff Robert Smith is a citizen and resident of the State of Ohio, currently residing in the City of Delaware. Plaintiff Smith used the mobile applications Fuel Rewards and GasBuddy, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

39. Plaintiff Tracy Tupper is a citizen and resident of the State of New York, currently residing in Cadyville. Plaintiff Tupper used the mobile application Routely, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

40. Plaintiff James Williams is a citizen and resident of the State of Washington, currently residing in Seattle. Plaintiff Williams used the mobile applications Life360 and GasBuddy, which incorporated Defendants' covert SDK. On information and belief, Plaintiff's mobility data was tracked through Defendants' SDK and transmitted to Defendants' mobility data database and used by Defendants and/or sold by Defendants without Plaintiff's knowledge or consent.

Defendants

41. Defendant The Allstate Corporation is a public corporation headquartered in Chicago, Illinois and incorporated under the laws of Illinois. Together with its subsidiaries, Defendant The Allstate Corporation provides insurance products, including car insurance, throughout the United States, including in Illinois.

42. Defendant Allstate Insurance Company is a wholly owned subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Insurance Company provides insurance products, including car insurance, throughout the United States, including in Illinois.

43. Defendant Allstate Vehicle and Property Insurance Company is a subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Vehicle and Property Insurance Company provides insurance products, including car insurance, throughout the United States, including in Illinois.

44. Defendant Arity, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Illinois. Defendant Arity, LLC, is a mobility data and analytics company that, together with the other subsidiaries of The Allstate Corporation, collects

and analyzes data obtained throughout the United States, including the State of Illinois, and uses predictive analytics to build solutions to sell to third parties.

45. Defendant Arity 875, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Illinois. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of The Allstate Corporation, collects and analyzes data obtained throughout the United States, including the State of Illinois, and uses predictive analytics to build solutions to sell to third parties.

46. Defendant Arity Services, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Illinois. Defendant Arity Services, LLC, is a mobility data and analytics company that, together with the other subsidiaries of The Allstate Corporation, collects and analyzes data obtained throughout the United States, including the State of Illinois, and uses predictive analytics to build solutions to sell to third parties.

IV. FACTS

47. Defendants have collected the data of at least forty-five million Americans to create highly detailed driver behavior profiles of these Americans, including Plaintiffs.

48. Defendants amassed this data without consumers' knowledge by surreptitiously integrating software into consumer mobile applications allowing Defendants to extract this data directly from consumers' phones. Defendants have monetized this data by informing their own underwriting and by building and selling access to the "world's largest driving behavior database" including the personal data of these forty-five million Americans. Defendants never provided

Plaintiff and Class Members notice of their data collection and sale methods. Defendants never received consent from consumers to collect and sell their driving behavior data.

49. On information and belief, through their affiliate Arity, Defendants developed an SDK to be integrated into mobile phone applications in 2015. This SDK was meant to collect the location and movement data from a person's phone. Generally, SDKs provide application developers with the tools necessary to build their applications including APIs and other automated functions that operate in the background. However, the primary purpose of Defendants' SDK was to extract large volumes of highly granular and valuable consumer data from the sensors within consumers' smartphones, under the false pretext of providing necessary functionality.

A. Defendants' Created Software to Covertly Exfiltrate Consumers' Data

50. Once Plaintiffs and Class Members installed an applicable mobile app, Defendants' Arity SDK harvested consumer data including, but not limited to:

a. The mobile phone's geolocation, accelerometer, magnetometer, and gyroscopic data;

b. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end locations, start and end time, speed, rate of change, and signal strength;

c. "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;

d. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone; and

e. Metadata, such as ad ID, country code, IOS vs Android, User ID, device type, app version, and OS version.

51. Defendants' SDK extracts and exfiltrates extensive consumer data that is de-anonymized as this data is collected in coordination with sensitive identifiable information such as unique device ID. Defendants can integrate this sensitive driver information with personally identifiable information ("PII") connected with a device ID to create individualized and detailed consumer profiles.

52. Mobile Advertising IDs ("MAID") are unique phone identifiers that are used by advertisers to aid in personalized advertising to consumers. AdID is the MAID for all Android devices, a 32-digit individualized string, and IDFA functions similarly for every IOS device. As such, MAIDs act as a unique marker or signature for consumers across their mobile activities.

53. Within applications from an individual developer, Identifiers for Vendors ("IDFV") similarly function to track user activity within IOS applications, which allows for cross-promotion among their various apps. These and other identifiers allow developers, marketers, and data brokers with more accurate attribution for user actions.

54. Using these and other unique identifiers, application developers can track consumers' locations, habits, and characteristics. These developers can further share or sell this information with third parties, as Defendants have done here.

55. Defendants' SDK covertly operated in the background, so absent notification by Defendants or the relevant mobile application, users would be reasonably ignorant of the SDK's existence.

56. App users would similarly be unaware that Defendants were directly collecting data from their phones through this covert SDK and these unique personal identifiers. Defendants never

informed or notified app users that they were collecting their sensitive data through the SDK and the mobile applications. And they never informed or notified app users that they would sell and otherwise use the data they collected to enrich themselves.

B. Defendants Paid Developers to Integrate the Arity SDK Into Their Apps

57. Since 2017, Defendants have promoted the use of their SDK through paying mobile developers millions of dollars to integrate the Arity SDK into their applications. Applications that integrated Defendants' SDK include Routely, GasBuddy, Life360 and Fuel Rewards.

58. These applications request and receive user permission to use their location, which enabled in-app features before integrating the Defendants' SDK. Once Defendants' SDK was integrated into these applications, then that same user unwittingly allowed the SDK to collect this and other sensitive data far beyond what was needed by the applicable app to function as intended.

59. Defendants made agreements with these mobile developers granting a license to integrate with the SDK and granting Defendants permission to collect the SDK data from consumers. These agreements further ensured that Defendants owned the SDK data and allowed Defendants to use this information for their own independent purposes. Plaintiffs and Class Members, however, were not privy to these agreements, did not assent to them, did not give permission for their data to be used other than as needed by the app in question and had no way to know that their data was being exfiltrated to Defendants and collected and monetized by Defendants.

60. On information and belief, Defendants' SDK data could not reliably be connected to a specific individual without also obtaining user information from the app that was running Defendants' SDK. In response, app publishers licensed the personal information collected from their users to Defendants including first and last name, phone number, address, and zip code.

Combining this licensed PII with the Arity SDK data allowed Defendants to more precisely identify the consumer and create unique driver behavior profiles.

61. But even with the PII licensed from the app developers the database is inherently and woefully inaccurate and unreliable because Defendants have no way to determine whether the mobile device providing the tracking information is owned by the driver of a vehicle on a specific trip, is owned by a passenger, if the owner is riding public transit, or in an Uber, on a roller coaster, or even on a closed race track during a driving instruction course.

C. Defendants Monetized Consumer Data to the Detriment of Consumers

62. A primary function of the SDK is the transmission of precise consumer location data to Defendants.

63. Defendants used their SDK data and Personal data to develop, advertise, and sell different products and services to third parties, including Insurers, and for their own underwriting business. Defendants' products and services included:

a. Drivesight. In 2015, Defendants created Drivesight, a system designed to calculate a driving score by analyzing data using their proprietary scoring model, which assesses and assigns a value to an individual's driving risk.

b. Arity Audiences. Defendants permitted companies and Insurers to "[t]arget drivers based on risk, mileage, commuting habits" and "[m]ore effectively reach [their] ideal audiences with the best offers to eliminate wasted spend, increase retention, and achieve optimal customer LTV."[2] As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.

[2] Arity, "Arity Audiences," https://www.arity.com/solutions/arity-audiences/ (last visited Jan. 22, 2025).

c. Arity IQ. Defendants permitted companies and Insurers to access "actual driving behavior insights on tens of millions of drivers."[3]

d. Real Time Insights. Defendants marketed that their service provides "granular driver probe data for real-time applications."[4] Defendants provide that their "mobility data helps validate minute-by-minute speed and density information to better understand and manage traffic."[5] Defendants advertise that "[b]y collecting data from tens of millions of mobile phones, Arity has a continuous data flow representing diverse regions and road types, car makes and model year. Our unmatched feed of live mobile phone connections fill gaps in speed and density other sources leave behind."[6]

e. Routley. Defendants offer Routely to consumers, which purports to be a "free" application that provides "helpful insights" into consumers' driver data. By contrast, Defendants market Routely to Insurers as a "telematics mobile app [that] can help you identify and manage risk in your book of business."[7] Defendants state that Routely is "Telematics in a box."[8]

64. Defendants marketed their highly sensitive and individualized data as "driving behavior" data. However, on information and belief, Defendants had no way to reliably determine whether a consumer was actually driving a car when they were collecting this "driving behavior" data. The consumer could have been a passenger, they could have been riding a bus, or they could

[3] Arity, "Arity IQ," https://arity.com/solutions/arity-iq/ (last visited Jan. 22, 2025).
[4] Arity, "Arity Real Times Insights," https://arity.com/solutions/real-time-insights/ (last visited Jan. 22, 2025).
[5] *Id*.
[6] *Id*.
[7] Arity, "Routely," https://arity.com/solutions/routely/ (last visited Jan. 22, 2025).
[8] *Id*.

have taken a taxi. They could even have been in a race car driving school on a closed track. Regardless, Defendants' SDK data would attribute this "driving behavior" to the unwitting consumer. This fundamental failure of data integrity did not stop Defendants from using or capitalizing on this information.

65. Defendants subsequently used this information to determine a consumers' allegedly bad driving habits, and insurability, in their own underwriting and risk analysis. Defendants further sold this information to other insurers who likely did the same, even though Defendants did not disclose this fundamental flaw in their data.

66. Defendants attempted to account for their lack of data integrity by purchasing driver data from car manufacturers, such as Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram.

67. On information and belief, consumers were not aware and did not consent to the sale of their data.

68. Since Defendants' SDK records location and other data regardless of whether the device is active or idle, and this information is transmitted to Defendants every few seconds, Defendants are able to collect highly sensitive information about consumers. Defendants could determine where someone lived, where they worked, where their children go to school, where they go for medical treatment, where they worship, whether and which rallies, demonstrations or protests they attend, and any and all information that can be determined by tracking a person's location and movement. Defendants collected all of this highly sensitive information along with identifiers such as MAID, AdID, IDFA, and IDFV and integrated this with other unique PII and demographic data.

69. Despite the depth and scope of Defendants data collection, Defendants did not disclose this practice to consumers and they did not seek consent for this practice from consumers. Defendants failed to obtain informed consent.

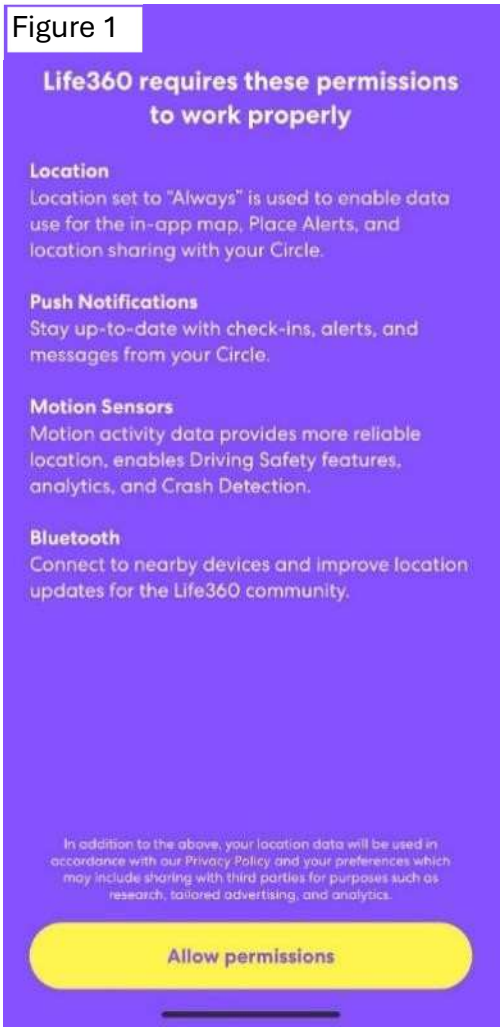
D. Defendants' Lack of Privacy Disclosures

70. Defendants had varying levels of control over privacy disclosures and consent language that application developers presented to consumers.

71. Neither Defendants nor the mobile applications informed consumers that Defendants were collecting the SDK data. Defendants and mobile applications similarly did not inform consumers of how they would aggregate, manipulate, exfiltrate and monetize this data.

72. Defendants did not provide consumers with any sort of notice of their data and privacy practices, nor did the mobile apps notify consumers about Defendants' practices on Defendants' behalf. *See* Figure 1. Similarly, neither Defendants nor the mobile apps notified consumers of the ways in which their SDK data would be used, nor did consumers agree to have their data used for Defendants' own products or services. *See id*.

Figure 1



73. Even if a consumer investigated Defendants outside of their app, navigated to their website, and read their privacy disclosures, a consumer would still not be aware of the extent of their data that was being collected, exfiltrated and monitored and/or what Defendants did with their sensitive data once it had been collected and in real time. Defendants' privacy disclosures include a series of untrue and contradictory statements that do not accurately reflect Defendants' actual practices.

74. Defendants state that they "do not sell personal information for monetary value."[9] This statement is untrue. Defendants sold several products and services linked to a specific app user and their "driving behavior" derived from the personal information Defendants collected. Further, Defendants do not provide consumers with the ability to request that Defendants stop selling their data.

75. Defendants similarly obscure how they use consumers' sensitive information. Defendants' privacy statement provides that they use "personal data for analytics and profiling," but their description of this profiling is not an accurate reflection of their conduct.[10] Defendants describe their profiling and use of personal data as follows:

> We use your personal data to assist in our development of predictive driving models. We may profile your personal data only for the purposes of creating a driving score ("Driving Score"), which is used for our analytics purposes to develop and validate our predictive driving models. To develop our predictive driving models we gather information about your driving behaviors, such as speed, change in speed, and other aspects of how much, where and when you drive to predict driving risk. These driving behaviors may be combined with other demographic or geographic information about driving risk for certain locations, which incorporate relative risks.

76. Defendants' description is in stark contrast with the reality that their analytics has substantial data integrity problems, they combine SDK data with PII to create profiles for forty-five million Americans, and they sell this information to companies and Insurers. Regardless of whether a consumer took the extraordinary step of tracking down Defendants' privacy statement, finding the subparagraph describing profiling, parsing through the convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a

[9] Arity, "Privacy," https://arity.com/privacy/ (last visited Jan. 22, 2025).
[10] *Id.*

"Driving Score" about them, consumers still could do nothing to stop Defendants from collecting their data and creating a Driving Score. Defendants did not describe, nor provide, a method for a consumer to request that their data not be used to profile them.

77. Similarly, if a consumer concluded they did not want Defendants to use their data for targeted advertising, Defendants instructed them that they could "[l]earn how to opt out of targeted advertising" by visiting another link. But if a consumer followed that link, they would be taken to a page that—instead of offering them a way to submit a request to opt out of targeted advertising—only provided them with links to several third-party websites, such as the Apple Support Center.

78. These third-party websites merely contained explanations regarding how a consumer could turn off certain types of targeted advertising and did not contain a way for a consumer to submit an actual request to Defendants specifically.

E. Defendants' Covert Practices Cause Substantial Injury to Consumers

79. Defendants' SDK data is used to identify individual consumers and their visits to sensitive locations ranging from their doctor's office to their child's school. The collection and sale of this data poses an unwarranted and unauthorized intrusion into the most private areas of someone's life and caused, or is likely to cause, substantial injury to consumers and their privacy interests.

80. Defendants' practice of obtaining and integrating additional consumer information with their SDK data, all without users' knowledge or consent, is likely to result in substantial consumer injury.

81. The precise geolocation data associated with each phone's MAID, including data surreptitiously collected and sold by Defendants can be used to track consumers' highly sensitive locations.

F. Plaintiffs' Injuries

82. As described more fully above, the data that Defendants extracted, manipulated, and monetized may be used to identify a consumers' sensitive location and infer "driving behavior, which may in fact having nothing to do with a consumer's actual driving behavior. The collection and sale of this data is an unwarranted and unauthorized intrusion into the most private areas of a consumer's life and has caused, or is likely to cause, substantial injury to the consumers and their privacy interests.

83. Each Plaintiff's cell phone contains one or more mobile applications that have embedded Defendants' Arity SDK.

84. On information and belief, the SDK harvested several types of data from each Plaintiff's phone without their knowledge or consent, and exfiltrated this data to Defendants, including but not limited to his:

a. Mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;

b. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end locations, start and end time, speed, rate of change, and signal strength;

c. "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;

d. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone; and

e. Metadata, such as ad ID, country code, IOS vs Android, User ID, device type, app version, and OS version.

85. Each Plaintiff was entirely unaware that Defendants' SDK was covertly installed on his or her phone. Each Plaintiff was similarly unaware that this SDK was secretly collecting her or his highly granular location, driving, and other data and exfiltrating it to Defendants.

86. None of the Plaintiff consented to Defendants' conduct and they do not have any relationship with the Defendants concerning the collection of private information from their mobile devices.

87. Several Plaintiffs have had insurers drop them from coverage, Plaintiffs were denied coverage, or they have experienced a substantial increase in insurance premiums over these last years compared to the steady and regular increase as they would otherwise expect. These Plaintiffs have not had any accidents, speeding tickets, or other moving violations that could reasonably be attributed to their loss of coverage or these otherwise unreasonable rate increases.

88. Upon information and belief, Plaintiffs' higher premiums, inflated quotes, and dropped coverage are caused by insurers purchasing "driving behavior" and other data from Defendants that has substantial integrity issues, that is misleading, and that was extracted from Plaintiffs without knowledge or consent.

89. Plaintiffs' data has tangible value. Defendants' conduct has caused Plaintiffs and Class Members to lose control over the data that Defendants have secretly taken from them and sold for profits. This data is now in the possession of third parties, including insurers, that have used it to their own financial advantage, and will continue to use it to their advantage.

90. Plaintiffs and Class Members have a reasonable expectation of privacy in their vehicles, in taxis, on public transit, while going about their daily lives, and at their doctors' offices. Plaintiffs and Class Members reasonably expect that their location, driving behavior, routes, and schedule would not be collected, transmitted to third parties or sold without express consent or authorization. By covertly harvesting, exfiltrating, manipulating, and selling their personal information Defendants have invaded Plaintiffs and Class Members' privacy rights.

V. TOLLING

91. All applicable statutes of limitations have been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein. The causes of action alleged did not accrue until Plaintiffs and Class Members discovered that Defendants were secretly collecting, exfiltrating, selling, and sharing their driving and other data to third party companies and insurers. Plaintiffs and Class Members could not have reasonably discovered Defendants' practices as their actions were covert.

92. Plaintiffs and Class Members had no realistic ability to discern that Defendants were collecting, exfiltrating and selling their driver data until—at the earliest— January 13, 2025, when it was reported in The New York Times that the Texas Attorney General sued Defendants for their collection and sale of consumer driver data.

93. Defendants remain under a continuing duty to disclose to Plaintiffs and Class Members their data harvesting practices, their sale of this data to third parties, and the use of this data in informing insurance underwriting. As such, all applicable statutes of limitations have been tolled.

VI. CLASS ALLEGATIONS

94. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), Plaintiffs bring this action on behalf of a proposed Class (the "Nationwide Class") and "State Subclasses" defined as follows:

The Nationwide Class

All persons in the United States whose data was collected by Defendants through the Arity SDK (the "Class").

The Alabama Subclass

All members of the Class who are residents of the State of Alabama.

The Arizona Subclass

All members of the Class who are residents of the State of Arizona.

The California Subclass

All members of the Class who are residents of the State of California.

The Florida Subclass

All members of the Class who are residents of the State of Florida.

The Georgia Subclass

All members of the Class who are residents of the State of Georgia.

The Illinois Subclass

All members of the Class who are residents of the State of Illinois.

The Indiana Subclass

All members of the Class who are residents of the State of Indiana.

The Kentucky Subclass

All members of the Class who are residents of the State of Kentucky.

The Louisianna Subclass

All members of the Class who are residents of the State of Louisianna.

The Montana Subclass

All members of the Class who are residents of the State of Montana.

The Mississippi Subclass

All members of the Class who are residents of the State of Mississippi.

The Missouri Subclass

All members of the Class who are residents of the State of Missouri.

The North Carolina Subclass

All members of the Class who are residents of the State of North Carolina.

The New York Subclass

All members of the Class who are residents of the State of New York.

The Ohio Subclass

All members of the Class who are residents of the State of Ohio.

The Pennsylvania Subclass

All members of the Class who are residents of the State of Pennsylvania.

The South Carolina Subclass

All members of the Class who are residents of the State of South Carolina.

The Texas Subclass

All members of the Class who are residents of the State of Texas.

The Utah Subclass

All members of the Class who are residents of the State of Utah.

The Washington Subclass

All members of the Class who are residents of the State of Washington.

The Wisconsin Subclass

All members of the Class who are residents of the State of Wisconsin.

95. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, all persons who make a timely election to be excluded from the Class, and any judge who adjudicates this case, including their staff and immediate family.

96. Plaintiffs reserve the right to amend the class definition and/or subclass definitions.

97. Certification of Plaintiffs' claims for classwide treatment is appropriate because Plaintiffs can prove the elements of their claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims

98. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that individual joinder of all Class members is impracticable. There are, at a minimum, millions of members of the proposed Class and, at minimum, thousands of members of each State Subclass.

99. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendants collected Plaintiffs' and Class Members' driving and other data;

b. Whether Plaintiffs and Class Members were made aware or consented to the collection of this data;

c. Whether Plaintiffs and Class Members were made aware or consented to their data being shared with third parties;

d. Whether Defendants were unjustly enriched to the detriment of Plaintiffs and Class Members;

e. Whether Defendants' conduct constitutes violations of the Federal Wiretap Act and/or Stored Communications Act;

f. Whether Defendants' conduct constitutes violations of state consumer protection and privacy statutes;

g. Whether and to what extent Plaintiffs and Class Members have been damaged by Defendants' conduct and the amount of such damages; and

h. Whether Plaintiffs and Class Members are entitled to restitution, disgorgement, or other equitable or injunctive relief.

100. These common questions of law and fact predominate over questions that affect only individual Class Members.

101. **Typicality—Federal Rule of Civil Procedure 23(a)(3):** Plaintiffs' claims are typical of Class Members' claims because they are based on the same underlying facts, events, and circumstances relating to Defendants' conduct.

102. **Adequacy—Federal Rule of Civil Procedure 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the Class, have no interests incompatible with the interests of the Class, and have retained counsel competent and experienced in class action litigation.

103. **Superiority—Federal Rule of Civil Procedure 23(b)(3):** Class treatment is superior to other options for resolution of the controversy because the relief sought for each Class Member is small, such that, absent representative litigation, it would be infeasible for Class Members to redress the wrongs done to them.

104. Defendants have acted on grounds applicable to the Class, thereby making appropriate final injunctive and declaratory relief concerning the Class as a whole.

VII. CAUSES OF ACTION

COUNT ONE
VIOLATIONS OF COMMON LAW RIGHT TO PRIVACY
(On behalf of each Plaintiff for the state they reside in and the members of the respective State Subclass)

105. Plaintiffs incorporate by reference paragraphs 1-104 as if fully set forth herein.

106. Common law prohibits Defendants from intentional intrusion into the personal matters of Plaintiffs and Class Members, including their PII, driver behavior information, and location.

107. Plaintiffs and Class Members hold, and at all relevant times held, a legally protected privacy interest in their PII and other personal data and are entitled to the protection of private property, matters, and information therein from intentional intrusions and unauthorized access.

108. As Plaintiffs and Class Members used and carried their phones, visiting family and going about their days, they have unknowingly created troves of highly sensitive data mapping of their respective personal lives which is then collected, captured, transmitted, accessed, compiled, stored, analyzed, and sold—all without their knowledge or informed consent.

109. The private Information of Plaintiffs and Class Members consists of PII and other personal data that were never intended to be shared to third parties.

110. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy regarding their PII and other personal data and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

111. Defendants intentionally invaded Plaintiffs' and Class members' privacy interests by deliberately designing devices and programs that surreptitiously obtain, improperly gain knowledge of, review, retain, package, and sell their PII and other data.

112. Defendants' unauthorized acquisition and collection of Plaintiffs' and Class Members' PII and other personal data, is highly offensive to a reasonable person. The continued nonconsensual surveillance of an individual in their private capacity, as Defendants have done and continue to do, represents a fundamental violation of personal privacy, freedom, and autonomy. It is not simply an intentional intrusion but a profound and egregious infringement upon the most personal and sacred aspects of one's life. Plaintiffs have unknowingly been subjected to constant observation while they go about their days, which destabilizes the very essence of personal liberty.

113. Defendants' conduct exploited Plaintiffs' phone in order to record and transmit Plaintiffs' highly sensitive and personally identifiable data and behavior.

114. Defendants' willful and intentional use of Plaintiffs' and Class Members' PII and other personal data constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns of a kind that would be highly offensive to a reasonable person.

115. Defendants intentionally and willfully acquired Plaintiffs' data, Defendants had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

116. Defendants' conduct constitutes and, at all relevant times, constituted serious and highly offensive invasions of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would record, collect, capture, sell, take and make use of—and allow third-party companies to take and make use of Plaintiffs' and Class Members' PII and other personal data.

117. Defendants profited from Plaintiffs' and Class members' data without compensating them, and often inaccurately reporting on Plaintiffs' and Class members' driving abilities and history to third parties. Plaintiffs and Class members did not receive any compensation in return for the improper use of their personal data. Defendants deprived Plaintiffs and Class members of the right to control how their personal information is collected, used, or disseminated and by whom.

118. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, loss of time, money, and opportunity costs, plus prejudgment interest, and costs.

119. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendants.

120. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their PII and other personal data. A judgment for monetary damages will not undo Defendants' disclosure of the information to third parties, who on information and belief, continue to possess and utilize that information.

121. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiffs' and Class members' PII and other data and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT TWO
VIOLATION OF THE FEDERAL WIRETAP ACT,
18 U.S.C. §§ 2510, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

122. Plaintiffs incorporate by reference paragraphs 1-104 as if fully set forth herein.

123. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

124. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the "contents of any wire, oral, or electronic communication, knowing or having reason to know that" the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

125. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a). 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).

126. The FWA defines "electronic communication" as "any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

127. The FWA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

128. The FWA defines "contents," with respect to any covered communication, to include "any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8).

129. The FWA defines "person" to include "any individual, partnership, association, joint stock company, trust, or corporation[.]" 18 U.S.C. § 2510(6).

130. Defendants, corporations, are each a person as defined by 18 U.S.C. § 2510(6).

131. As alleged herein, the Defendants have intercepted, in real time and as they were transmitted, the contents of electronic communications.

132. The data and transmissions within, to, and from Plaintiff's and Class Members' phones constitute "electronic communications," as defined by 18 U.S.C. § 2510(12), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photo optical systems that affect interstate commerce.

133. Defendants intercepted these transmissions via the SDK.

134. As detailed herein, the electronic communications are tied to individuals and are not anonymized because, on information and belief, Defendants' SDK collects app users' mobile device identifiers and other information that app developers provide to Defendants.

135. Plaintiffs and Class Members have a reasonable expectation of privacy within their phones. Further, there is a reasonable expectation that the activities a person conducts with their phones, *i.e.*, app usage and data related thereto, are private.

136. Common understanding of how smartphones work creates a reasonable expectation that Defendants would not intercept and divert the electronic communications described above.

137. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that

the information was obtained through interception in violation of 18 U.S.C. §2511(1)(a). 18 U.S.C. §2511(1)(d).

138. Specifically, Defendants have used the contents of the communications described above to: (1) sell the information collected to third parties; and (2) increase driving insurance premiums for members of the Class for their own financial and commercial benefit, obtaining substantial profit.

139. As a result, Plaintiffs and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and Personal Information.

140. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

141. Plaintiffs and Class Members seek compensatory, injunctive, and equitable relief in an amount to be determined at trial, including an award of reasonable attorneys' fees and costs and punitive or exemplary damages for Defendants' willful violations.

COUNT THREE
VIOLATION OF THE STORED COMMUNICATIONS ACT
18 U.S.C. §§ 2701, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

142. Plaintiffs incorporate by reference paragraphs 1-104 as if fully set forth herein.

143. The Federal Stored Communications Act ("SCA"), enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA"), creates a civil remedy for those whose stored electronic communications have been obtained by one who "intentionally accesses without authorization" or "intentionally exceeds an authorization to access" a facility through which an electronic communication service ("ECS") is provided. 18 U.S.C. §§ 2701, 2707.

144. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of communications in electronic storage.

145. "Electronic communication" is defined as "any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

146. "Electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)).

147. "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication ...." 18 U.S.C. §§ 2510(17) (incorporated by reference in 18 U.S.C. § 2711(1)).

148. Plaintiffs and Defendants, as corporations or legal entities, are "persons" within the meaning of 18 U.S.C. § 2510(6), and for purposes of 18 U.S.C. § 2707.

149. The data and transmissions within, to, and from Plaintiffs and Class Members' phones constitute "electronic communications," as defined by 18 U.S.C. § 2510(12).

150. Plaintiffs and Class Members' data was intercepted by Defendants' SDK, and stored on their own servers, unbeknownst to Plaintiffs and Class Members.

151. The electronic communications Defendants intercepted are tied to individuals and are not anonymized.

152. There is a reasonable expectation of privacy within a person's electronic communications, and Plaintiffs and Class Members reasonably expected privacy while using their phones.

153. Plaintiffs and Class Members did not authorize Defendants to access their phones or the communications stored within them.

154. Defendants intentionally accessed these communications without authorization.

155. Defendants intentionally exceeded their authority to access these communications without authorization.

156. Defendants violated the SCA, 18 U.S.C. § 2701 by accessing Plaintiffs' and Class Member's phones and private data without authorization and by obtaining access to the electronic communications stored on their devices.

157. Defendants' conduct was willful and intentional, and it invaded Plaintiffs and Class Members' expectations of privacy.

158. Defendants have profited from their violation of the SCA, by, among other things, using improperly accessed communications and highly sensitive Arity SDK Data for Defendants' commercial gain and benefit.

159. The communications unlawfully accessed by Defendants have significant value, evidenced by the expenditures made by Defendants in order to deploy the Arity SDK's across applications and to collect information directly from vehicles.

160. Because of Defendants conduct, Plaintiffs and Class Members have forever lost the value of their data, their privacy interest in the data, and their control over its use.

161. Because Plaintiffs and Class Members have been aggrieved by Defendants' intentional acts in violation of the SCA, they are entitled to bring this civil action to recover relief and damages. 18 U.S.C. § 2707.

162. As a result of Defendants' conduct, Plaintiffs and Class Members are entitled to all damages set forth in 18 U.S.C. § 2707 including declaratory and equitable relief, compensatory damages measured by actual damages and Defendants' profits, reasonable attorneys' fees and costs, all available statutory relief, and punitive damages as determined by the Court.

COUNT FOUR
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

163. Plaintiffs incorporate by reference paragraphs 1-104 as if fully set forth herein.

164. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

165. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of information within their computers.

166. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[]…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

167. The CFAA also specifically provides that it is unlawful to "knowingly and with intent to defraud, access[] a protected computer without authorization or exceed[ing] authorized

access" and thereby "further[] the intended fraud and obtain[] anything of value…." 18 U.S.C. § 1030(a)(4).

168. Plaintiffs and Defendants, as corporations or legal entities, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

169. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

170. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

171. A "protected computer" is defined as "a computer . . . which is used in or affecting interstate or foreign commerce or communication…, [or that] has moved in or otherwise affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B).

172. Plaintiffs' and Class Members' phones constitute a "computer" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

173. The phones of Plaintiffs and Class Members are used in and affect interstate and foreign commerce and constitute "protected computers" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

174. Defendants intentionally accessed the protected computers in Plaintiffs and Class Members' possession via the Arity SDK and other software without Plaintiffs' or Class Members' authorization, or in a manner that exceeded Plaintiffs' and Class Members' authorization, and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

175. As alleged herein, Defendants' conduct constituted a knowing intent to defraud Plaintiffs and Class Members of their valuable personal data and profit thereby. 18 U.S.C. §1030(a)(4).

176. Defendants' use of MAIDs, IDFAs, IDFVs and its SDK constitutes access to Plaintiffs' and Class Members' smartphones.

177. The value of the information Defendants obtained from the protected computers in Plaintiffs' and Class Members' possession exceeded $5,000 in a one-year period, as evidenced by Defendants' significant profits from the disclosures of this information. 18 U.S.C. § 1030(a)(4).

178. Plaintiffs and Class Members have suffered harm and injury due to Defendants' unauthorized access to their smartphones.

179. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." Because the loss to Plaintiffs and Class Members during any one-year period within the relevant timeframe, including the loss of their privacy interest in and control over their personal data, exceeded $5,000 in the aggregate, Plaintiffs and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g)

COUNT FIVE
ALABAMA DECEPTIVE TRADE PRACTICES ACT
Ala. Code §§ 8-19-1, *et seq*.
(On behalf of The Alabama Subclass)

180. The Alabama Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

181. Plaintiff and the Alabama Subclass Members are each a "consumer" as defined in Ala. Code § 8-19-3.

182. Defendants are each a "person" as defined by Ala. Code § 8-19-3.

183. Plaintiff sent pre-suit notice pursuant to Ala. Code 7 8-19-10(e).

184. Defendants are each engaged in "trade or commerce" affecting the people of Alabama by advertising, offering for sale, selling, or distributing goods and services in the State of Alabama. *See* Ala. Code § 8-19-3.

185. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Ala. Code § 8-19-3.

186. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Ala. Code § 8-19-5, including:

a. Intercepting, collecting, using, and selling Plaintiff's and Alabama Subclass Members' data, including driving data, without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Alabama Subclass Members' data, including driving data, to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that other third parties collected, manipulated, used, and sold Plaintiff's and Alabama Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and the associated mobile applications with respect to the privacy of consumers;

e. Misrepresenting the purpose of the SDK and that it would protect the privacy of Plaintiff's and the Alabama Subclass Members' data, including that it would not intercept, collect, use or sell such data; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Alabama Subclass Members' data, including driving data.

187. These statements, misrepresentations, omissions, and concealments constitute violations of Ala. Code § 8-19-5 (5), (7), (9) and (27).

188. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Alabama Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Subclass Members' data without obtaining their consent.

189. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Alabama Subclass Members'datawas material to Plaintiff and Alabama Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

190. Plaintiff and Alabama Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of the SDK and associated applications, the security and privacy of their data, and their privacy, to their detriment.

191. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging the conduct alleged herein, including by harvesting, selling, and disseminating Plaintiff and Alabama Subclass Members'datawithout Plaintiff's and Subclass Members' consent.

192. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Alabama Subclass Members have suffered and will continue to suffer injury, including, but not limited to, the loss of privacy, the unauthorized dissemination of their valuable data, and economic harm stemming from Defendants' exploitation of their data.

193. Defendants' unconscionable and unfair acts and practices caused substantial injury to Plaintiff and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

194. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

COUNT SIX
ARIZONA CONSUMER FRAUD ACT
Ariz. Rev. Stat. §§ 44-1521, *et seq*.
(On behalf of The Arizona Subclass)

195. The Arizona Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Arizona Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

196. Plaintiff and members of the Arizona Subclass are each a "person" as defined by Ariz. Rev. Stat. § 44-1521.

197. Defendants are each a "person" as defined by Ariz. Rev. Stat. § 44-1521.

198. Defendants are each engaged in trade directly or indirectly affecting the people of Arizona by advertising, offering for sale, selling or distributing goods and services in the State of Arizona. See Ariz. Rev. Stat. § 44-1521.

199. Defendants are engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Arizona Revised Statute § 44-1522(A), including:

a. Intercepting, collecting, using, and selling Plaintiff's and Arizona Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Arizona Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants collected, manipulated, used, and sold Plaintiff's and Arizona Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of the SDK and associate applications with respect to the privacy of consumers;

e. Misrepresenting the purpose of their SDK and associated applications, and that it would protect the privacy of Plaintiff's and the Arizona Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Subclass Members' data.

200. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Arizona Subclass Members' rights, because Defendants

intentionally intercepted, collected, used, and sold Plaintiff's and Arizona Subclass Members' Driving data without obtaining their consent.

201. The fact the Defendants intercepted, collected, used and sold Plaintiff's and Arizona Subclass Members' data was material to Plaintiffs and Arizona Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase , download or use an application.

202. Plaintiff and Arizona Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of their SDK and associated mobile applications, the security and privacy of their data, and their privacy while going about their day, to their detriment.

203. Plaintiff's and the Arizona Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and Arizona Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

204. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Arizona Subclass Members have suffered and will continue to suffer injury, including, but not limited to, the loss of privacy, the unauthorized dissemination of their valuable data, and economic harm stemming from Defendants' exploitation of their data.

205. Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT SEVEN
CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY
California Constitution, Article I, Section 1
(On behalf of The California Subclass)

206. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

207. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

208. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

209. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27.

210. Plaintiffs and California Subclass Members have legally protected privacy interests, as recognized by the California Constitution.

211. Plaintiffs and California Subclass Members have an interest in precluding Defendants' interception, collection, dissemination and use of their data.

212. Plaintiffs and California Subclass Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendants would violate state and federal privacy laws and collect, disseminate and use their data. Plaintiffs and California Subclass Members were not aware and could not have reasonably expected that Defendants would use applications attached to their phones that would track and transmit their data to third parties without authorization.

213. Defendants' conduct in secretly intercepting, collecting, disseminating, and using Plaintiffs' and California Subclass Members' data is an egregious breach of societal norms and is highly offensive to a reasonable person.

214. Defendants' conduct was intentional and intruded on Plaintiffs' and California Subclass Members' seclusion and use of their personal property.

215. Plaintiffs and California Subclass Members had no knowledge and did not consent or otherwise authorize Defendants to track, collect, obtain, disseminate, or otherwise use their data.

216. Defendants were unjustly enriched as a result of their invasion of Plaintiffs' and California Subclass Members' privacy.

217. As a direct and proximate result of Defendants' invasion of their privacy, Plaintiffs and California Subclass Members were injured and suffered damages, including, but not limited to, the loss of privacy, the unauthorized dissemination of their valuable data, and economic harm stemming from Defendants' exploitation of their data.

218. Plaintiffs and California Subclass Members are entitled to equitable relief and just compensation in an amount to be determined at trial. Plaintiffs and California Subclass Members

seek all relief available for the invasion of privacy under the California Constitution, including nominal damages and general privacy damages.

COUNT EIGHT
CALIFORNIA INVASION OF PRIVACY ACT — WIRETAPPING LAW
Cal. Pen. Code §§ 631
(On behalf of The California Subclass)

219. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

220. California Penal Code Section 630 recognizes that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

221. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

222. The California Wiretapping Act prohibits:

> any 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 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[.]

223. Defendants are each a "person" within the scope of the California Wiretapping Act.

224. The data and transmissions within, to, and from Plaintiffs' and California Subclass Members' phones constitute messages, reports, and/or communications, within the scope of Cal. Penal Code § 631(a), as they are transfers of signals, data, and intelligence transmitted by a wire, line, or cable system.

225. As alleged herein, Defendants intercepted, in real time and as they were transmitted, the contents of communications, and have diverted those communications to itself without consent.

226. Defendants intercepted these data transmissions by diverting them to its own servers, unbeknownst to Plaintiffs and California Subclass Members

227. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individual persons, are easily re-identified through use of MAIDs and other identifiers, and are for Defendants' purposes, not anonymous.

228. Defendants' SDK and associated mobile applications constitute a machine, instrument, or contrivance that taps or makes unauthorized connection to Plaintiffs' and California Subclass Members' mobile phone communication system.

229. Plaintiffs and California Subclass Members have a reasonable expectation of privacy within their vehicles and while going about their day, and Plaintiffs and California Subclass Members reasonably expected privacy while driving their vehicles and walking about their daily lives. Further, there is a reasonable expectation that their location and other data are private.

230. In further violation of the California Wiretapping Act, Defendants intentionally disclosed or endeavored to disclose to third parties the contents of the communications described above while knowing or having reason to know that the information was obtained through the interception of the communications.

231. In further violation of the California Wiretapping Act, Defendants have intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that the information was obtained through unlawful interception.

232. Specifically, Defendants have disclosed and used the contents of the communications described above by selling Plaintiffs' and Class Members' personal data, including driving data, to third parties for their own financial and commercial benefit, obtaining substantial profit.

233. Specifically, Defendants have used the information derived from the communications described above to create products they market, license, and sell, including driving scores, risk ratings, and access to databases containing Plaintiffs' and California Subclass Members' data.

234. Further, Defendants have used the information derived from the communications described above for their own financial and commercial benefit, obtaining substantial profit.

235. Specifically, Defendants knew or should have known that the detailed information they used and sold was captured in secret in violation of the Act for the following reasons, among others that will become known through discovery:

a. The opaque disclosures in Defendants' various terms and polices, which did not operate as a reasonable basis for inferring consumer consent to share the information with third parties;

b. The lack of public knowledge about Defendants' collection and sharing practices until at least January 2025;

c. The fact that Defendants continue to collect after it was publicized that collection was secret/happening without consent or knowledge; and

d. The nature of the data as such that it had to be obtained via a wiretap.

236. Upon information and belief, Defendants disclose and unlawfully obtain data for their own financial gain to this day.

237. Defendants, collectively, agreed, employed and conspired with one another to intercept, collect, disseminate and use data concerning Plaintiffs' and California Subclass Members.

238. At all relevant times, Plaintiffs and California Subclass Members were not aware that Defendants were intercepting and recording their data, and therefore could not provide consent to have any part of their communications intercepted and recorded, transmitted or used.

239. Neither Defendants nor any other person informed Plaintiffs and California Subclass Members that Defendants were intercepting and transmitting their data. Plaintiffs and California Subclass Members did not know Defendants were intercepting and recording their data, as such they could not and did not consent for their data to be intercepted and/or used by Defendants.

240. As a direct and proximate result of Defendants' violations of the Wiretapping Act, Plaintiffs and California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

241. Defendants were unjustly enriched by their violations of the Wiretapping Act.

242. Pursuant to California Penal Code Section 637.2, Plaintiffs and California Subclass Members have been injured by Defendants' violations of the Wiretapping Act, and seek damages

for the greater of $5,000 or three times the amount of actual damages, and injunctive relief, plus reasonable attorneys' fees and costs.

COUNT NINE
CALIFORNIA INVASION OF PRIVACY ACT — ELECTRONIC TRACKING DEVICE
Cal. Pen. Code §§ 637.7
(On behalf of The California Subclass)

243. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

244. California Penal Code Section 637.7 prohibits any person from using an electronic tracking device to determine the location or movements of any person.

245. Defendants are each a "person" within the scope of CIPA.

246. Defendants SDK covertly integrated within associated mobile applications and downloaded onto Plaintiffs' and California Subclass Members' phones is an "electronic tracking device" as defined by CIPA as it is a device that is integrated into the user's phone and reveals the user's location, movement, and other data by the transmission of electronic signals through the intercept, collection, and dissemination of Plaintiffs' and California Subclass Members' location information.

247. Defendants violated Cal. Penal Code § 637.7 by attaching Defendants'' SDK to Plaintiffs' and California Subclass Members' phones and thereby intercepting, collecting, taking, storing, using, and disseminating Plaintiffs' and California Subclass Members' data.

248. Neither Defendants nor any other person informed Plaintiffs and California Subclass Members or meaningfully disclosed that Defendants integrated their SDK, an electronic tracking device, into Plaintiffs' and California Subclass Members' phones.

249. The collection of Plaintiffs' and California Subclass Members' data without full and informed consent violated and continues to violate Cal. Penal Code § 637.7.

250. As a direct and proximate result of Defendants' violations, Plaintiffs and California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

251. Pursuant to Calif. Penal Code Section 637.2, Plaintiffs and California Subclass Members have been injured by Defendants' violations of the CIPA and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief, plus reasonable attorneys' fees and costs

COUNT TEN
CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT
Cal. Pen. Code §§ 502, *et seq*.
(On behalf of The California Subclass)

252. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

253. The California legislature enacted the Computer Data Access and Fraud Act ("CDAFA") to "expand the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The enactment of CDAFA was motivated by the finding that

"the proliferation of computer technology has resulted in a concomitant proliferation of . . . unauthorized access to computers, computer systems, and computer data." *Id.*

254. The CDAFA provides a private right of action to 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 any of the provisions of subsection (c)." Cal. Penal Code § 502(e).

255. Defendants' SDK and associated mobile applications on Plaintiffs' and California Subclass Members' phones constitute "computers" within the scope of the CDAFA. Plaintiffs and California Subclass Members are owners and/or lessees of the computers or computer systems, their phones.

256. Defendants violated the following sections of the CDAFA:

a. Section 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;"

b. Section 502(c)(2), which makes it unlawful to "knowingly access[] and without permission take[], cop[y], or make[] use of any data from a computer, computer system, or computer network, or take[] or cop[y] any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

c. Section 502(c)(6), which makes it unlawful to "knowingly and without permission provide[] or assist[] in providing a means of accessing a computer, computer system, or computer network in violation of this section;"

d. Section 502(c)(7), which makes it unlawful to "knowingly and without permission access[] or cause[] to be accessed any computer, computer system, or computer network."

257. As alleged herein, the electronic communications transmitted within, to, and from Plaintiffs' and California Subclass Members' phones are stored in electronic components of those phones.

258. Mobile phones, are facilities through which electronic communication services are provided because they provide users, such as Plaintiffs and California Subclass Members, the ability to send and receive electronic communications including related to their personal data.

259. As alleged herein, there is a reasonable expectation of privacy within a person's vehicle and while walking through daily life, and Plaintiffs and California Subclass Members reasonably expected privacy while driving their vehicles and going about their day. Further, there is a reasonable expectation that the interactions and communications between user and phone, *i.e.*, personal data, including driving data, are private.

260. Common understanding and experience regarding how mobile phones work create a reasonable expectation that Defendants would not access the electronic communications described above that are stored in Plaintiffs' and California Subclass Members' phones.

261. Defendants knowingly accessed Plaintiffs' and California Subclass Members' computers and/or computer systems without their permission, and thereby intercepted, took, copied and made use of the data concerning Plaintiffs and California Subclass Members.

262. Defendants intercepted, collected, disseminated and used Plaintiffs' and California Subclass Members' data as part of a scheme to deceive and defraud Plaintiffs and California

Subclass Members, and to wrongfully and unjustly enrich itself at the expense of Plaintiffs and California Subclass Members.

263. Defendants knowingly accessed Plaintiffs' computers and/or computer systems without Plaintiffs' and California Subclass Members' informed consent.

264. Defendants accessed these stored electronic communications in addition to and separately from intercepting other electronic communications transmitted in real time.

265. As detailed herein, the data contained in the electronic communications detailed above that Defendants accessed are tied to individual drivers, MAIDS, and are not anonymized.

266. Defendants' conduct was willful and intentional, and invaded Plaintiffs' and California Subclass Members' expectations of privacy.

267. Defendants were unjustly enriched by intercepting, acquiring, taking, or using Plaintiffs' and California Subclass Members' data without their permission, and using it for financial benefit. Defendants have been unjustly enriched in an amount to be determined at trial.

268. The communications accessed by Defendants in violation of Cal. Penal Code § 502 have significant value, evidenced by the profits that Defendants have obtained from, among other things, selling the improperly accessed communications to third parties, and as evidenced by the significant value of the aggregated data for various applications.

269. Because of Defendants' conduct, Plaintiffs and California Subclass Members have forever lost the value of their data, their privacy interest in the data, and their control over its use.

270. As a direct and proximate result of Defendants' violations of the CDAFA, Plaintiffs and California Subclass Members suffered damages. Plaintiffs and California Subclass Members suffered actual injuries, including but not limited to (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) unreasonably increased insurance premiums, denials of insurance coverage, and/or being dropped from their insurance coverage.

271. Pursuant to CDAFA Section 502(e)(1), Plaintiffs and California Subclass Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

272. Pursuant to CDAFA Section 502(e)(2), Plaintiffs and California Subclass Members seek an award of reasonable attorneys' fees and costs.

273. Pursuant to CDAFA Section 502(e)(4), Plaintiffs and California Subclass Members seek punitive or exemplary damages for Defendants' willful violations of the CDAFA.

COUNT ELEVEN
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100, *et seq*.
(On behalf of The California Subclass)

274. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

275. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, *et seq.*, was enacted to protect consumers' personal information from collection and use by businesses without appropriate notice and consent.

276. Defendants are each businesses that control the collection of consumers' personal information within the scope of the CCPA.

277. Plaintiffs and California Subclass Members are consumers within the scope of the CCPA.

278. The data that Defendants intercepted, collected, and obtained from Plaintiffs' and California Subclass Members' constitutes personal information within the scope of the CCPA.

279. Pursuant to Civil code § 1798.150, Defendants owed a duty to implement and maintain reasonable security procedures and practices to maintain the security of the information that it obtained concerning Plaintiffs and California Subclass Members.

280. Defendants violated its duty to implement and maintain reasonable security procedures and practices by disclosing Plaintiffs' and California Subclass Members' data, including driving data, without their authorization or consent.

281. Defendants further violated their duty to implement and maintain reasonable security procedures and practices by accepting, using, and disclosing Plaintiffs' and California Subclass Members' data without their authorization and knowing that it was obtained without their consent.

282. In accordance with Civil Code §1798.150(b), prior to the filing of this complaint, Plaintiffs served Defendants with notice of these CCPA violations.

283. Plaintiffs need not notify Defendants of their violations of Section 1798.110 of the CCCPA because notice would be futile. Notwithstanding, Plaintiffs provided notice to Defendants.

284. On behalf of the California Subclass, Plaintiffs seek injunctive relief in the form of an order enjoining Defendants from continuing to violate the CCPA, as well as actual, punitive, and statutory damages; restitution; attorneys' fees and costs; and any other relief the Court deems proper as a result of Defendants' violations of the CCPA.

COUNT TWELVE
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Civ. Code §§ 17200, *et seq*.
(On behalf of The California Subclass)

285. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

286. The California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, prohibits, *inter alia*, "any unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

287. Defendants are each a "person" as defined by Cal. Bus. & Prof. Code § 17201.

288. Defendants violated the UCL by engaging in business acts and practices which are unlawful, unconscionable, and unfair under the UCL.

289. Defendants' acts and practices are unlawful because Defendants violated and continue to violate California common law, constitutional, and statutory rights to privacy, including but not limited to the California Constitution Article I, Section 1, CIPA, CCPA, CDAFA, CLRA, and FAL.

290. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of the UCL by:

a. Intercepting, collecting, using, and selling Plaintiffs' and California Subclass Members' data, including driving data, without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiffs' and California Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and third parties collected, manipulated, used, and sold Plaintiffs' and California Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associate mobile applications with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated mobile applications that they would protect the privacy of Plaintiffs' and California Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiffs' and California Subclass Members' data.

291. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiffs' and California Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiffs' and Subclass Members' data, including driving data, without obtaining their consent.

292. The fact that Defendants intercepted, collected, used, and sold Plaintiffs' and Subclass Members' data was material to Plaintiffs and California Subclass Members. This is a fact that reasonable consumers would consider important when choosing to download Routely, GasBuddy, Life360, Fuel Rewards, or any other application using Defendants' SDK.

293. Plaintiffs and California Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of their SDK and associated mobile applications, the security and privacy of their data, and their privacy, including Defendants' sale of consumer data.

294. In the course of their business, Defendants repeatedly and regularly engaged in the unlawful, unconscionable, and unfair acts or practices, which caused serious harm to consumers, including Plaintiffs and California Subclass Members.

295. Plaintiffs' and the California Subclass' data, including driving data, has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs' and California Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit

296. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

297. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unlawful, unfair, and unconscionable practices or use of their data; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT THIRTEEN
CALIFORNIA CONSUMERS LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750, *et seq*.
(On behalf of The California Subclass)

298. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

299. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

300. Defendants are each a "person" under Cal Civ. Code §§ 1761(c) and 1770, and has provided "services" as defined by Cal. Civ. Code §§ 1761(b) and 1770.

301. Plaintiffs and California Class Members are "consumers" as defined by Cal. Civ. Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Cal Civ. Code §§ 1761(e) and 1770.

302. Defendants' conduct, as described herein, in misrepresenting the characteristics, qualities, benefits and capabilities of their SDK, and omitting material information concerning their SDK and associated applications, violates the CLRA. Specifically, Defendants violated the CLRA by omitting, suppressing, and concealing the material fact that Plaintiffs' and California Subclass Members' data was being intercepted, collected, used and/or disseminated, which violates the following practices proscribed by Cal. Civ. Code § 1770(a):

a. Representing that the goods or services have approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. Representing that the goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising the goods or services with the intent not to sell them as advertised; and

d. Representing that subject of a transaction has been supplied in accordance with previous representations when they have not.

303. Defendants violated the CLRA by advertising and leasing their SDK that transmitted Plaintiffs' and California Subclass Members' data and by advertising applications that do the same. The fact that Defendants intercepted, collected, and transmitted Plaintiffs' and California Subclass Members' data was material to Plaintiffs and California Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase or download an app.

304. Defendants knew and failed to disclose at the time of their lease of the SDK mobile applications to Plaintiffs and California Subclass Members that its SDK intercepted, collected, and transmitted data. Defendants further knew and failed to disclose at the time of their advertising of applications, including Routley, to Plaintiffs and California Subclass Members that they intercepted, collected, and transmitted data, including driving data.

305. As a direct and proximate result of Defendants' misconduct, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

306. Plaintiffs need not notify Defendants of its violations of Section 1770 of the CLRA because notice would be futile. Notwithstanding, Plaintiffs provided notice to Defendants.

307. Plaintiffs and the California Subclass seek all monetary and non- monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, and reasonable attorneys' fees and costs under the CLRA.

COUNT FOURTEEN
CALIFORNIA FALSE ADVERTISING LAW
Cal. Bus. & Prof. Code §§ 17500, *et seq*.
(On behalf of The California Subclass)

308. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

309. The California False Advertising Law ("FAL"), Cal. Bus. & Prof. Code § 17500, *et seq.*, prohibits making any statement that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services. Cal. Bus. & Prof. Code 17500.

310. Defendants are each a person, firm, corporation, and/or association within the scope of the FAL.

311. Defendants advertising was highly misleading. Defendants failed to disclose or did not meaningfully disclose that its SDK and associated applications, intercepted, collected, used, and disseminated Plaintiffs' and California Subclass Members' data, or that Defendants profited from the dissemination, sale, and use of such data.

312. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the true function and purposes of Defendants' products and services. Reasonable consumers lack the means to verify Defendants' representations and omissions concerning the SDK's, and associated mobile applications', data collection practices, or to understand the fact or significance of Defendants' practices concerning the collection, dissemination and use of Plaintiffs' and California Subclass Members' data.

313. Plaintiffs and California Subclass Members have been harmed and have suffered economic injuries as a result of Defendants' misrepresentations and omissions, including but not

limited to (a) damage to and diminution of the value of their personal information; (b) violation of their privacy rights; and (c) the likelihood of their private information.

314. As a result of its misrepresentations and omissions, Defendants have been able to reap unjust profits and revenues from the sale, dissemination, and use of Plaintiffs' and California Subclass Members' ata.

315. Unless restrained and enjoined, Defendants will continue to misrepresent its data collection and sales practices and will not recall or destroy the data collected concerning Plaintiffs and California Subclass Members. Accordingly, injunctive relief is appropriate.

COUNT FIFTEEN
VIOLATION OF THE FLORIDA

UNFAIR AND DECEPTIVE TRADE PRACTICES ACT,
Fla. Stat. §§ 501.201, *et seq*.
(On behalf of The Florida Subclass)

316. The Florida Plaintiff identified above ("Plaintiff" for purposes of this Count) repeat and reallege Paragraphs 1-104, as if fully alleged herein.

317. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, *et seq.*, prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" Fla. Stat. § 501.204.

318. Plaintiff and the members of the Florida Subclass are each a "consumer" as defined in Fla. Stat. Ann. § 501.203.

319. Defendants are each a "person" as defined in Fla. Stat. Ann. § 504.203.

320. Defendants each engaged in "trade or commerce" affecting the people of Florida by advertising, offering for sale, selling or distributing goods and services in the State of Florida. Fla. Stat. Ann. § 501.203.

321. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of the FDUTPA by:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding;

e. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Florida Subclass Members' data.

322. These deceptive statements, misrepresentations, omissions, concealments and acts constitute violations of Fla. Stat. 7 501.204(1).

323. Defendants acted intentionally, knowingly, and maliciously to violate FDUTPA, and recklessly disregarded Plaintiff's and Florida Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Florida Subclass Members' data without obtaining their consent.

324. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Florida Subclass Members' data was material to Plaintiff and Florida Subclass Members. This is a fact that reasonable consumers would consider important when choosing download, use, or purchase an application.

325. Plaintiff and Florida Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of their SDK, the security and privacy of their data, and their privacy in their own vehicles to their detriment.

326. Plaintiff's and the Florida Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and Florida Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

327. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

328. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT SIXTEEN
FLORIDA SECURITY OF COMMUNICATIONS ACT
Fla. Stat. §§ 934.01, *et seq*.
(On behalf of The Florida Subclass)

329. The Florida Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeat and reallege Paragraphs 1-973, as if fully alleged herein.

330. The Florida Security of Communications Act ("FSCA"), Fla. Stat. § 934.01, *et seq.*, states that any person who "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication" is subject to liability. Fla. Stat. § 934.03(1)(a).

331. Plaintiff, including members of the Florida Subclass, and Defendants each constitute a "person" as defined in Fla. Stat. § 934.02.

332. The data and transmissions within, to, and from Plaintiff's and Class Members' vehicles constitute "electronic communications," as defined by Fla. Stat. § 934.02, as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems that affect intrastate, interstate or foreign commerce.

333. The FSCA prohibits any person from intentionally disclosing, or endeavoring 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 [the FSCA]." Fla. Stat. Ann. § 934.03(c).

334. The FSCA prohibits any person from intentionally using, or endeavoring 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 [the FSCA.]" Fla. Stat. Ann. § 934.03(d).

335. As alleged herein, Defendants intercepted, in real time and as they were transmitted, the contents of electronic communications, and diverted those communications to itself without consent.

336. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individual drivers and vehicles, and are not anonymized.

337. Plaintiff and Florida Subclass Members have a reasonable expectation of privacy within their vehicles, and Plaintiff and Florida Subclass Members reasonably expected privacy while driving their vehicles, in their homes, and in their doctor's office. Further, there is a reasonable expectation that the interactions between a driver and their phone, including their personal data, are private.

338. Defendants intercepted these electronic communications in real time separately from and in addition to accessing data stored in Plaintiff's and Florida Subclass Members' MAIDs.

339. Defendants intercepted these data transmissions by diverting them, during flight, to their own servers, unbeknownst to Plaintiff and Florida Subclass Members.

340. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individuals and vehicles, and are not anonymized.

341. In further violation of the FSCA, Defendants have disclosed or attempted to disclose to third parties the contents of the communications described above while knowing or having reason to know that the information was obtained through interception in violation of the FSCA.

342. In further violation of the FSCA, Defendants have used or attempted to use the contents of the communications described above while knowing or having reason to know that the information was obtained through interception in violation of the FSCA.

343. In further violation of the FSCA, Defendants have used the information derived from the communications described above to create products they market, license, and sell, including so-called driving scores, risk ratings, and access to databases containing Plaintiff's and the Florida Subclass Members' data.

344. Upon information and belief, Defendants continue to disclose and use unlawfully obtained data, including driving data, for their own financial gain.

345. Plaintiff and Florida Subclass Members did not consent or otherwise authorize Defendants to intercept, disclose, or use their communications.

346. As a result, Plaintiff and Florida Subclass Members have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and personal information.

347. Defendants' violations of the FSCA have directly and proximately caused Plaintiff and the Florida Subclass to suffer harm and injury due to the interception, disclosure, and/or use of their private and personal information in an amount to be ascertained at trial.

348. Pursuant to Fla. Stat. § 934.10(1), Plaintiff and Florida Subclass Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the FSCA and are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Florida Subclass or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT SEVENTEEN
VIOLATION OF THE GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Ga. Code Ann. §§ 10-1-370, *et seq*.
(On behalf of The Georgia Subclass)

349. The Georgia Plaintiffs identified above ("Plaintiffs" for purposes of this Count) repeat and reallege Paragraphs 1-104, as if fully alleged herein.

350. Defendants, Plaintiffs, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

351. Defendants engaged in deceptive trade practices in the conduct of its business in violation of Ga. Code § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

352. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of the Georgia UDTPA by:

a. Intercepting, collecting, using, and selling Plaintiffs' and Georgia Subclass Members' data, including driving data, without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiffs' and Georgia Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and third parties collected, manipulated, used, and sold Plaintiffs' and Georgia Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, particularly Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, particularly Routely, and that it would protect the privacy of Plaintiffs' and the Georgia Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiffs' and Georgia Subclass Members' data.

353. Defendants acted intentionally, knowingly, and maliciously to violate the Georgia UDTPA, and recklessly disregarded Plaintiffs' and Georgia Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiffs' and Georgia Subclass Members' data without obtaining their consent.

354. The fact that Defendants intercepted, collected, used, and sold Plaintiffs' and Georgia Subclass Members' data was material to Plaintiffs and Georgia Subclass Members. This is a fact that reasonable consumers would consider important when choosing which applications to download.

355. Plaintiffs and Georgia Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, and the security and privacy of their and data.

356. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants' spent millions of dollars to influence application developers to

integrate their SDK that covertly harvested user data demonstrates that Defendants were aware that consumers would not consent to the collection and disclosure of their Data, thus necessitating Defendants' omissions and misrepresentations regarding their actions.

357. Plaintiffs' and the Georgia Subclass' Data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs' and Georgia Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

358. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiffs and Georgia Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

359. Plaintiffs and Georgia Subclass Members seek all monetary and non- monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs under O.C.G.A. § 10-1-373.

COUNT EIGHTEEN
RECOVERY OF EXPENSES OF LITIGATION,
O.C.G.A §§ 13-6-11, *et seq*.
(On behalf of The Georgia Subclass)

360. The Georgia Plaintiffs identified above, individually and on behalf of the Georgia Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

361. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

362. Defendants, through its actions alleged and described herein, acted in bad faith, was stubbornly litigious, or caused the Georgia Subclass unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

363. The Georgia Subclass therefore requests that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT NINETEEN
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 Ill. Comp. Stat §§ 505, *et seq*.
(On behalf of The Illinois Subclass)

364. The Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

365. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

366. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

367. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

368. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Intercepting, collecting, using, and selling Plaintiffs' and Illinois Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiffs' and Illinois

Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and third parties collected, manipulated, used, and sold Plaintiffs' and Illinois Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and that it would protect the privacy of Plaintiffs' and the Illinois Subclass Members' ata, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiffs' and Illinois Subclass Members' data.

369. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Illinois Subclass Members' data without obtaining their consent.

370. The fact that Defendants intercepted, collected, used, and sold Plaintiffs' and Illinois Subclass Members' data, including data, was material to Plaintiffs and Illinois Subclass Members. This is a fact that reasonable consumers would consider important when downloading and using applications.

371. Plaintiffs and Illinois Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associate application, including Routley, the security and privacy of their data to their detriment. Defendants intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

372. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive.

373. Had Defendants disclosed to Plaintiffs and Illinois Subclass Members that it was collecting and disclosing data, it would have been unable to enroll so many individuals in its programs. Instead, in order to drastically increase the numbers of consumers enrolled in its programs and third-party applications, Defendants did not disclose material terms or obtain actual, written consent for them. Instead, Defendants omitted material facts from consumers and misrepresented the actual purpose of its programs. Accordingly, Plaintiffs and the Illinois Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

374. Defendants are engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by selling and disseminating Plaintiffs' and Illinois Subclass Members' data without their consent.

375. Plaintiffs' and the Illinois Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs' and Illinois Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

376. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

377. Plaintiffs and Illinois Subclass Members seek all monetary and non- monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT TWENTY
ILLINOIS WIRETAPING, ELECTRONIC SURVEILLANCE, AND INTERCEPTION OF COMMUNICATIONS LAW,
720 ILCS 5/14-1, *et seq*.
(On behalf of The Illinois Subclass)

378. The Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

379. The Illinois Eavesdropping law, 720 ILCS 5/14-1, et seq., prohibits, *inter alia*, any person from knowingly or intentionally "intercept[ing], record[ing], or transcrib[ing], in a surreptitious manner, any private electronic communication" without the consent of all parties. 720 ILCS 5/14-2(a)(3).

380. The Illinois Eavesdropping law also prohibits any person from using or disclosing "any information which he or she knows or reasonably should know was obtained" in violation of the Act, unless such use or disclosure is done "with the consent of all of the parties." 720 ILCS 5/14-2(a)(5).

381. Defendants are each a "person" within the scope of the Illinois Eavesdropping law.

382. The data and transmissions within, to, and from Plaintiffs' and Illinois Subclass Members' phones constitute "private electronic communications" as defined by 720 ILCS 5/14-1(e), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems.

383. Plaintiffs and Illinois Subclass Members have a reasonable expectation of privacy within their vehicles, and while going about their day, and Plaintiffs and Illinois Subclass Members reasonably expected privacy while driving their vehicles and while going about their day.

384. As alleged herein, Defendants have intercepted, in real time and as they were transmitted, the contents of private electronic communications, and diverted those communications to itself without consent.

385. Defendants intercepted these data transmissions by diverting them, during flight through Defendants' SDK or similar device, to their own servers, unbeknownst to Plaintiffs and Illinois Subclass Members.

386. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individual drivers and vehicles and are not anonymized.

387. In further violation of the Illinois Eavesdropping law, Defendants intentionally disclosed or endeavored to disclose to third parties the contents of the private electronic communications described above while knowing or having reason to know that the information was obtained through the interception of the private electronic communications.

388. In further violation of the Illinois Eavesdropping law, Defendants intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that the information was obtained through interception in violation of the Act.

389. Defendants disclosed and used contents of the communications described above by selling consumers' personal data to the third parties or its own financial and commercial benefit, obtaining substantial profit.

390. Defendants further used the information derived from Plaintiffs' and Illinois Subclass Members' private electronic communications to create products they market, license, and sell, including so-called driving scores, risk ratings, and access to databases containing Plaintiffs' and Illinois Subclass Members' data. Defendants also used the information derived from the communications described above in aggregate fashion to develop risk models and other products they market and sell.

391. Plaintiffs and Illinois Subclass Members did not consent or otherwise authorize Defendants to intercept, disclose, or use their communications.

392. As a result, Plaintiffs and Illinois Subclass Members have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and personal information.

393. Pursuant to 720 ILCS 14-6, Plaintiffs and Illinois Subclass Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Eavesdropping law and are entitled to: (1) damages, in an amount to be determined at trial; (2) punitive damages; (3) injunctive relief prohibiting Defendants from further eavesdropping; and (4) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT TWENTY-ONE
INDIANA DECEPTIVE CONSUMER SALES ACT,
Ind. Code §§ 24-5-035-1, *et seq*.
(On behalf of The Indiana Subclass)

394. The Indiana Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

395. Defendants are each a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

396. Defendants are each a "supplier" as defined by § 24-5-0.5-2(a)(1), because they regularly engages in or solicits "consumer transactions," within the meaning of Ind. Code § 24-5-0.5-2(a)(3)(A).

397. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions by advertising, offering for sale, selling or distributing goods and services in the State of Indiana. Ind. Code § 24-5-0.5-3(a).

398. Defendants' representations and omissions include both implicit and explicit representations.

399. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade or commerce in violation of Ind. Code § 24-5-0.5- 3 by:

a. Intercepting, collecting, using, and selling Plaintiff's and Indiana Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Indiana Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiff's and Indiana Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated application, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated mobile application, and that it would protect the privacy of Plaintiff's and the Indiana Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Indiana Subclass Members' data.

400. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Indiana Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Indiana Subclass Members' data, including driving data, without obtaining their consent.

401. The fact that Defendant intercepted, collected, used, and sold Plaintiff's and Indiana Subclass Members' data was material to Plaintiff and Indiana Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

402. Plaintiff and Indiana Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the

functionality of Defendants' SDK and associated applications, the security and privacy of their ata, and their privacy in their own vehicles and while going about their day, to their detriment.

403. Defendants intended to mislead the Indiana Plaintiff and Indiana Subclass Members and induce them to rely on their misrepresentations and omissions.

404. In the course of their business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants paid mobile developers millions to integrate their SDK, which covertly harvested user data, demonstrating that consumers would not consent to the collection and disclosure of data, thus necessitating Defendants' omissions and misrepresentations regarding their programs.

405. Had Defendants disclosed to Plaintiff and Indiana Subclass Members that they were collecting and disclosing their data, they would have been unable to enroll so many individuals in their programs or disseminate Defendants' SDK. Instead, in order to drastically increase the numbers of consumers enrolled in its programs, Defendants did not disclose material terms or obtain actual, written consent for them. Instead, Defendants omitted material facts from consumers, and misrepresented the actual purpose of its programs. Accordingly, Plaintiff and the Indiana Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

406. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by selling and disseminating Plaintiff's and Indiana Subclass Members' data with knowledge that such data was obtained without Plaintiff's and Indiana Subclass Members' consent.

407. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Indiana Subclass Members have suffered and will

continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

408. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5. Defendants have not cured their unfair, abusive, and deceptive acts and practices, or their violations of Indiana Deceptive Consumer Sales Act were incurable. Defendants' conduct was incurable because Plaintiff's and Indiana Subclass Members' data has already been used and shared with third parties.

409. Defendants' violations present a continuing risk to Plaintiff and Indiana Subclass Members as well as to the general public if injunctive relief does not prevent them from continuing their deceptive acts and practices in the future.

410. Plaintiff and Indiana Subclass Members seek all monetary and non- monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT TWENTY-TWO
KENTUCKY CONSUMER PROTECTIONS ACT,
Ky. Rev. Stat. §§ 367.110, *et seq*.
(On behalf of The Kentucky Subclass)

411. The Kentucky Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

412. Defendants are each a "person" as defined by Ky. Rev. Stat. § 367.110(1).

413. Defendants advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

414. Defendants engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Intercepting, collecting, using, and selling Plaintiff's and Kentucky Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Kentucky Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiff's and Kentucky Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the Kentucky Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Kentucky Subclass Members' data.

415. Defendants' representations and omissions include both implicit and explicit representations.

416. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Kentucky Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Kentucky Subclass Members' data without obtaining their consent.

417. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Kentucky Subclass Members' data was material to Plaintiff and Kentucky Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

418. Plaintiff and Kentucky Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data to their detriment.

419. In the course of their business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants paid mobile developers millions of dollars to integrate their SDK, which covertly harvested user Data, demonstrating that Defendants knew consumers would not consent to the collection and disclosure of data, thus necessitating Defendants' omissions and misrepresentations regarding their programs.

420. Had Defendants disclosed to Plaintiffs and Kentucky Subclass Members that they were collecting and disclosing data, they would have been unable to enroll so many individuals in their programs. Instead, in order to drastically increase the numbers of consumers enrolled in its programs and third-party applications, Defendants did not disclose material terms or obtain actual,

written consent for them. Instead, Defendants omitted material facts from consumers and misrepresented the actual purpose of its programs. Accordingly, Plaintiffs and the Kentucky Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

421. Defendants are engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by selling and disseminating Plaintiffs' and Kentucky Subclass Members' data without their consent.

422. The above unfair, deceptive, and unconscionable practices and acts by Defendants a were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

423. Defendants acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff's and Kentucky Subclass Members' rights.

424. Plaintiff's and the Kentucky Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and Kentucky Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefits.

425. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Kentucky Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the

likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

426. Plaintiff and Kentucky Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs. Defendants' violations present a continuing risk to Plaintiff and Kentucky Subclass Members as well as to the general public if injunctive relief does not prevent them from continuing their deceptive acts and practices in the future.

COUNT TWENTY-THREE
VIOLATION OF THE MISSISSIPPI CONSUMER PROTECTION ACT,
Miss. Code. §§ 75-24-1, *et seq*.
(On behalf of The Mississippi Subclass)

427. The Mississippi Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

428. Plaintiffs and Defendants are each "persons" as defined by Miss. Code. § 75-24-1(a).

429. Defendants engaged in "trade" and "commerce" as defined by Miss. Code. § 75-24-1(b)

430. Defendants engaged in trade and commerce in Mississippi and/or directly or indirectly affecting the people of Mississippi.

431. Defendants engaged in unfair or deceptive trade practices in or affecting commerce, in violation of Miss. Code. 75-24-5, including by:

a. Intercepting, collecting, using, and selling Plaintiffs' and Kentucky Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiffs' and Kentucky Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiffs' and Kentucky Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the Kentucky Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiffs and Kentucky Subclass Members' data.

432. Defendants intended to mislead Plaintiffs and induce Mississippi Subclass Members to rely on its misrepresentations and omissions.

433. Defendants acted intentionally, knowingly, and maliciously to violate the At, and recklessly disregarded Plaintiffs' and Mississippi Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiffs' and Mississippi Subclass Members' data without obtaining their consent.

434. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Mississippi Subclass Members' data was material to Plaintiffs and Mississippi Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or sue an application.

435. Plaintiffs and Mississippi Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of the SDK, the security and privacy of their data, and their privacy in their own vehicles and while going about their day, to their detriment.

436. Defendants engaged in unfair and deceptive trade practices in or affecting commerce, in violation of Miss. Code. § 75-24-5, by engaging in the conduct alleged herein, including by using, selling and disseminating Plaintiffs' and Mississippi Subclass Members' data without their consent.

437. Defendants acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiffs' and the Mississippi Subclass' rights.

438. Plaintiffs' and the Mississippi Subclass' data, including driving data, has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and Mississippi Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

439. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiffs and Mississippi Subclass Members have suffered and will continue to suffer injury ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to: loss of privacy; unauthorized dissemination of

their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

440. Plaintiffs' and the Mississippi Subclass' data was exploited without informed consent. Accordingly, Plaintiffs and the Mississippi Subclass are entitled to part of Defendants' profits that were generated by their data without informed consent.

441. Plaintiffs and the Mississippi Subclass seek all monetary and non- monetary relief allowed by law, including damages, disgorgement, injunctive relief, attorneys' fees and costs, and any other relief that is just and proper. Miss. Code. § 75-24-15.

COUNT TWENTY-FOUR
NEW JERSEY CONSUMER FRAUD ACT,
N.J. Stat. Ann. §§ 56:8-1, *et seq*.
(On behalf of The New Jersey Subclass)

442. The New Jersey Plaintiff identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

443. Defendants are "person(s)" as defined by N.J. Stat. Ann. § 56:8-1(d).

444. Defendants sell "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) and (e).

445. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1*, et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

446. Defendants unconscionable and deceptive practices include:

a. Intercepting, collecting, using, and selling Plaintiffs' and New Jersey Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and New Jersey Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiff's and New Jersey Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the New Jersey Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and New Jersey Subclass Members' data.

447. Defendants intended to mislead Plaintiff and New Jersey Subclass members and induce reliance on their misrepresentations and omissions.

448. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and New Jersey Subclass Members' rights, because Defendants

intentionally intercepted, collected, used, and sold Plaintiff's and New Jersey Subclass Members' data without obtaining their consent.

449. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and New Jersey Subclass Members' data was material to Plaintiff and New Jersey Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

450. Plaintiff and New Jersey Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

451. Plaintiff's and the New Jersey Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and New Jersey Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

452. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

453. Plaintiff and New Jersey Subclass Members have suffered injuries in fact and ascertainable losses of money or property as a result of Defendants' deceptive acts and practices.

Plaintiff's data has tangible economic value, which was wrongfully appropriated by Defendants for financial gain.

454. Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, treble damages under N.J. Stat. Ann. § 56:8-19, attorneys' fees, filing fees, and costs.

COUNT TWENTY-FIVE
VIOLATION OF NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law §§ 349
(On behalf of The New York Subclass)

455. The New York Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

456. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce, in violation of N.Y. Gen. Bus. Law § 349. Defendants engaged in deceptive acts and practices by:

a. Intercepting, collecting, using, and selling Plaintiff's and New Jersey Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and New Jersey Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiff's and New Jersey Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the New Jersey Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and New Jersey Subclass Members' data.

457. Defendants' omissions and misrepresentations were material because they were likely to deceive reasonable consumers into believing that their data would not be sold or used for financial gain without their knowledge or consent.

458. Defendants acted intentionally, knowingly, and maliciously to violate N.Y. Gen. Bus. Law § 349, or acted with reckless disregard for the rights of Plaintiff and New York Subclass Members.

459. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

460. Plaintiff and New York Subclass Members have suffered injuries in fact and ascertainable losses of money or property as a result of Defendants' deceptive acts and practices.

Plaintiff's and New York Subclass Members' data has tangible economic value, which was wrongfully appropriated by Defendants for financial gain.

461. The public interest and consumers at large were harmed by Defendants' deceptive and unlawful acts, which affected thousands of New York residents.

462. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief available under N.Y. Gen. Bus. Law § 349, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, attorneys' fees, and costs.

COUNT TWENTY SIX
VIOLATION OF NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law §§ 350
(On behalf of The New York Subclass)

463. The New York Plaintiff identified above ("Plaintiff," for purposes of this Count) individually and on behalf of the New York Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

464. Defendants engaged in advertising, including labeling, of goods and services that was misleading in a material respect in violation of New York General Business Law § 350-a(1).

465. Defendants' advertising was misleading in a material respect because it falsely implied that their goods and services included privacy protections for consumers' data and failed to disclose material facts regarding the collection and sale of such data. Specifically, Defendants failed to disclose that it was surreptitiously collecting Plaintiff's and New York Subclass Members' data and subsequently selling that data to third parties for profit.

466. The omission of these material facts rendered Defendants' representations misleading in light of the advertised nature of their goods and services. Plaintiff and New York

Subclass Members reasonably believed, based on Defendants' advertising, that their data would not be collected or sold without their knowledge and consent.

467. Defendant knowingly and intentionally engaged in false advertising with the intent to induce Plaintiff and New York Subclass Members to use their goods and services, and the goods and services of applications using Defendants' SDK, relying on the misleading representations and omissions regarding privacy protections for data.

468. As a direct and proximate result of Defendants' false advertising, Plaintiffand New York Subclass Members were injured in that they purchased or downloaded goods and services under false pretenses and suffered a loss of privacy and control over their data, which has tangible value. Plaintiff and New York Subclass Members would not have purchased or downloaded Defendants' goods and services, or the goods and services of mobile applications utilizing Defendants' SDK, or would have paid less for them, had the true facts been disclosed.

469. Plaintiff seeks all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of five hundred dollars per violation, whichever is greater, treble damages for willful or knowing violations, injunctive relief, reasonable attorneys' fees, costs, pre-judgment interest, and any other relief the Court deems just and proper.

COUNT TWENTY-SEVEN
VIOLATION OF NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law §§ 899-aa; 899-bb (SHIELD ACT)
(On behalf of The New York Subclass)

470. The New York Plaintiff identified above ("Plaintiffs," for purposes of this Count) individually and on behalf of the New York Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

471. Defendants are businesses that own, license, or maintain computerized data that includes private information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Accordingly, Defendants are subject to the requirements of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

472. Plaintiff's and Class Members' data includes private information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b), as it contains sensitive, identifiable information, including records of their driving events.

473. Defendants collected and maintained data from Plaintiff and New York Subclass Members without informing them of the scope of the data collection or obtaining their consent for its subsequent use and sale to third parties.

474. Pursuant to N.Y. Gen. Bus. Law § 899-bb(2), Defendants were required to implement and maintain reasonable administrative, technical, and physical safeguards to protect Plaintiff's and New York Subclass Members' data, including driving data, against unauthorized access, acquisition, or misuse.

475. Defendants failed to implement such reasonable safeguards, as they failed to disclose the sale of Plaintiff's and New York Subclass Members' data and enabled unauthorized access and transfer of this private information.

476. Defendants violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3) by failing to provide timely, accurate, and sufficient notice to Plaintiff and New York Subclass Members of the unauthorized collection, use, and sale of their data.

477. Defendants' failure to adhere to the administrative and security requirements of the SHIELD Act (N.Y. Gen. Bus. Law § 899-bb(2)) further compromised the security and confidentiality of Plaintiff's and New York Subclass Members' private information.

478. As a direct and proximate result of Defendants' violations of N.Y. Gen. Bus. Law §§ 899-aa and 899-bb, Plaintiff and New York Subclass Members suffered damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

479. Plaintiff and New York Subclass Members seek all remedies available under N.Y. Gen. Bus. Law § 899-aa(6)(b) and § 899-bb(2), including actual damages, injunctive relief, and any other relief deemed just and proper by the Court.

COUNT TWENTY-EIGHT
VIOLATION OF NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT,
N.C. Gen. Stat. §§ 75-1.1, *et seq*.
(On Behalf of the North Carolina Subclass)

480. The North Carolina Plaintiff identified above ("Plaintiff," for purposes of this Count) individually and on behalf of the North Carolina Subclass, repeat and reallege Paragraphs 1-104, as if fully alleged herein.

481. Defendants and Plaintiff are "persons" as defined by N.C. Gen. Stat. § 75-1.1(d).

482. Defendants advertised, offered, or sold goods and services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. § 75-1.1(b).

483. Defendants engaged in unfair, unconscionable, and deceptive practices in violation of N.C. Gen. Stat. § 75-1.1(a). These practices include:

a. Intercepting, collecting, using, and selling Plaintiffs' and North Carolina Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and North Carolina Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiffs' and North Carolina Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiffs' and the North Carolina Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiffs' and North Carolina Subclass Members' data.

484. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiffs' and North Carolina Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiffs' and North Carolina Subclass Members' data, including driving data, without obtaining their consent. Defendants intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on the omissions to their detriment.

485. The fact that Defendants intercepted, collected, used, and sold Plaintiffs' and North Carolina Subclass Members' data was material to Plaintiff and North Carolina Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

486. Plaintiff and North Carolina Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their ata, and their privacy to their detriment.

487. Plaintiffs' and the North Carolina Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs' and North Carolina Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

488. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and North Carolina Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable Data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

489. Plaintiff and the North Carolina Subclass seek all monetary and non- monetary relief allowed by law, including actual damages or statutory damages of $500 per violation, whichever is greater, treble damages pursuant to N.C. Gen. Stat. § 75-16, injunctive relief, attorneys' fees under N.C. Gen. Stat. § 75-16.1, pre-judgment interest, costs, and any other relief the Court deems just and proper.

COUNT TWENTY-NINE
VIOLATION OF THE OHIO CONSUMER SALES PRACTICES ACT,
Ohio Rev. Code §§ 1345.01, *et seq*.
(On Behalf of the Ohio Subclass)

490. The Ohio Plaintiff identified above ("Plaintiff," for purposes of this Count) individually and on behalf of the Ohio Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

491. Plaintiff and Ohio Subclass Members are "persons" as defined by Ohio Rev. Code § 1345.01(B).

492. Defendants are a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) and (C), by offering goods and services to consumers in Ohio.

493. Defendants engaged in unfair and deceptive acts and practices in connection with consumer transactions, in violation of Ohio Rev. Code §§ 1345.02 and 1345.03.

494. Defendants violated Ohio Rev. Code § 1345.02(B)(1) by representing that its goods and services had characteristics, uses, and benefits that they did not have, including misleading Plaintiff and Ohio Subclass Members into believing their data would remain private and secure, while surreptitiously collecting and selling such data to third parties.

495. Defendants further violated Ohio Rev. Code § 1345.02(B)(2) by representing that its goods and services were of a particular standard or quality when they were not, misleading Plaintiff and Ohio Subclass Members into believing that their ata, including driving data, would not be misused for Defendants' profit.

496. Defendants engaged in unconscionable acts in connection with consumer transactions, in violation of Ohio Rev. Code § 1345.03, by surreptitiously collecting and monetizing Plaintiff's and Ohio Subclass Members' data without their knowledge or consent and

by exploiting the inability of consumers to reasonably protect their interests in the face of Defendants' concealed practices.

497. Defendants failed to disclose material facts about its data collection and monetization practices, despite a duty to do so, and concealed its sale of data to third parties, in violation of Ohio Rev. Code §§ 1345.02 and 1345.03.

498. Defendants acted knowingly, intentionally, and maliciously to violate the Ohio Consumer Sales Practices Act by surreptitiously monetizing Plaintiff's and Ohio Subclass Members' data without consent and in reckless disregard of Plaintiff's and Ohio Subclass Members' rights.

499. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass Members have suffered ascertainable losses of money or property, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

500. Plaintiff and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or statutory damages, treble damages, injunctive relief, attorneys' fees and costs, and any other relief the Court deems just and proper.

COUNT THIRTY
UNFAIR TRADE PRACTICES ACT,
S.C. Code §§ 39-5-10, *et seq*.
(On Behalf of the South Carolina Subclass)

501. The South Carolina Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

502. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") makes unlawful unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. S.C. Code § 39-5-10(a).

503. Defendants are each a "person" as defined by S.C. Code § 39-5-10(a), which includes corporations, trusts, partnerships, incorporated or unincorporated associations and any other legal entity.

504. Defendants are each engaged in "trade" or "commerce" as defined by S.C. Code § 39-5-10(b), which includes the advertising, offering for sale, sale or distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of South Carolina.

505. The South Carolina UTPA is guided by the interpretations given by the Federal Trade Commission and the Federal Courts to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

506. Pursuant to 15 U.S.C. 45(n), an act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. Sec. 45(n).

507. By surreptitiously collecting Plaintiff's and South Carolina Subclass Members' ata, including driving data, and exploiting that data for their own commercial gain, Defendants have engaged in unfair practices.

508. Plaintiff and South Carolina Subclass Members could not have reasonably avoided Defendants' practices as described herein because Defendants concealed their practices.

509. Plaintiff and South Carolina Subclass Members have derived no benefit from Defendants' surreptitious collection and exploitation of their private information, and there are no countervailing benefits to consumers or to competition in engaging in the unauthorized tracking and sale of consumer data.

510. Plaintiff and South Carolina Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because they have experienced economic loss.

511. As a direct and proximate result of Defendants' unfair practices, Plaintiff and South Carolina Subclass Members have suffered and will continue to suffer injury, losses, and damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

512. In violating Plaintiff's and South Carolina Subclass Members' rights under the South Carolina UTPA as described herein, Defendants acted intentionally, knowingly, and/or with reckless disregard of the rights of Plaintiff and South Carolina Subclass Members.

513. Plaintiff and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages, treble damages, punitive damages, and reasonable attorneys' fees and costs.

COUNT THIRTY-ONE
TEXAS DECEPTIVE TRADE PRACTICES-CONSUMER PROTECTION ACT,
Tex. Bus. & Com. Code §§ 17.41
(On Behalf of the Texas Subclass)

514. The Texas Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

515. The Texas Trade Practices-Consumer Protection Act ("Texas TPCPA") "shall be liberally construed and applied to promote its underlying purposes, which are to protect consumers against false, misleading, and deceptive business practices, unconscionable actions, and breaches of warranty and to provide efficient and economical procedures to secure such protection." Tex. Bus. & Com. Code § 17.44(a).

516. Defendants are each a "person" as defined by 73 Pa. Stat. § 201-2(2), which includes partnership, corporation, association, or other group, however organized.

517. Defendants engage in "trade" or "commerce" as defined by Tex. Bus. & Com. Code § 17.45(6), which includes advertising, offering for sale, sale or distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity, or thing of value wherever situate, and includes any trade or commerce directly or indirectly affecting the people of Texas.

518. Defendants engaged in unfair and deceptive trade practices by representing to Plaintiffs and Texas Subclass Members, as well as third party applications, that their data would be kept secure and that data would not be shared, when in fact Defendants regularly collected detailed consumer data.

519. Defendants further engaged in deceptive and unfair trade practices by failing to disclose to and concealing from Plaintiffs and Texas Subclass Members that their detailed data was being collected and sold to third-parties, who then used the data to make products and profit.

520. These deceptive statements, misrepresentations, and omissions, and concealments constitute violations of Tex. Bus. & Com. Code § 17.46(b).

521. Defendants violated Tex. Bus. & Com. Code § 17.46(b)(5), (9), and (20) and (24) by:

a. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiffs' and Texas Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

b. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiffs' and Texas Subclass Members' data for their own financial and commercial benefit;

c. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles; and

d. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiffs' and the Texas Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent;

522. Plaintiffs and Texas Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the

functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, including driving data, and their privacy in their own vehicles to their detriment.

523. Further, Defendants violated Tex. Bus. & Com. Code § 17.46(b)(2) and (3) by causing likelihood of confusion or misunderstanding as to the source, sponsorship, approval, certification, affiliation, connection, or association with Plaintiffs' and Texas Subclass Members' data, namely that the collection and sale of such data was not authorized or consented-to by them, and therefore unlawfully obtained.

524. In engaging in the above-described practices, Defendants acted intentionally and with flagrant disregard of prudent and fair business practices to the extent that Defendant should be treated as having acted intentionally. Tex. Bus. & Com. Code § 17.45(13).

525. Plaintiffs and Texas Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because substantial numbers of them have experienced economic loss.

526. As a direct and proximate result of Defendants' deceptive practices, Plaintiffs and Texas Subclass Members have suffered and will continue to suffer injury, losses, and damages, including but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

527. Plaintiffs and Texas Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages, punitive damages, and reasonable attorneys' fees and costs.

COUNT THIRTY-TWO
UTAH TRUTH IN ADVERTISING ACT,
Utah Code Ann. §§ 13.11a-1, *et seq*.
(On Behalf of the Utah Subclass)

528. The Utah Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

529. The Utah Truth in Advertising Act prohibits "deceptive, misleading, and false advertising practices and forms in Utah." Utah Code Ann. § 13.11a-1.

530. Defendants are each a "person" as defined by Utah Code Ann. § 13.11a-2(7).

531. Defendants engaged in the complained-of conduct in connection with "sales transaction[s]," as defined by Utah Code Ann. § 13.11a-2(15).

532. Defendants engaged in deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Plaintiff and the Utah Subclass Members in violation of Utah Code Ann. § 13.11a-2(e), (g), and (i), including by:

a. Intercepting, collecting, using, and selling Plaintiff's and Utah Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Utah Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiffs' and Utah Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the Utah Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Utah Subclass Members' data.

533. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Utah Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Utah Subclass Members' data, including driving data, without obtaining their consent.

534. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Utah Subclass Members' data was material to Plaintiff and Utah Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

535. Plaintiff and Utah Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

536. Defendants intended to mislead Plaintiff and Utah Subclass Members and induce them to rely on their misrepresentations and omissions.

537. Defendants benefited from misleading Plaintiff and Utah Subclass Members as it obtained a profit from the collection of data, including driving data.

538. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

539. Defendants deceptive acts directly and proximately caused Plaintiff and Utah Subclass Members to suffer damages including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

540. Plaintiff and Utah Subclass Members seek all monetary and non- monetary relief allowed by law, including actual damages sustained or $2,000, whichever is greater, restitution, injunctive relief, and attorneys' fees and costs.

COUNT THIRTY-THREE
WASHINGTON CONSUMER PROTECTION ACT,
Wash. Rev. Code §§ 19.86.010, *et seq*.
(On Behalf of the Washington Subclass)

541. The Washington Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges Paragraphs 1-104, as if fully alleged herein.

542. The Washington Consumer Protection Act ("Washington CPA") declares that unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful. Wash. Rev. Code § 19.86.020.

543. Defendants are each a "person" as defined by Wash. Rev. Code § 19.86.010(1), which includes corporations, trusts, unincorporated associations and partnerships.

544. Defendants engage in "trade" or "commerce" as defined by Wash. Rev. Code § 19.86.010(2), which includes the sale of assets or services, and any commerce directly or indirectly affecting the people of the state of Washington. Defendants have engaged in unfair practices by:

a. Intercepting, collecting, using, and selling Plaintiff's and Washington Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Washington Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Plaintiff's and Washington Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Plaintiff's and the Washington Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Washington Subclass Members' data.

545. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Washington Subclass Members' rights, because Defendants

intentionally intercepted, collected, used, and sold Plaintiff's and Washington Subclass Members' data, including driving data, without obtaining their consent.

546. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Washington Subclass Members' data was material to Plaintiff and Washington Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

547. Plaintiff and Washington Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

548. Plaintiff and Washington Subclass Members could not have reasonably avoided Defendants' practices as described herein because Defendants concealed their practices.

549. Plaintiff and Washington Subclass Members have derived no benefit from Defendants' surreptitious collection and exploitation of their private information, and there are no countervailing benefits to them or to competition in engaging in the unauthorized tracking and sale of consumer data.

550. Plaintiff and Washington Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because substantial numbers of them have experienced economic loss. As such, Defendants' deceptive and unfair acts and practices affect the public interest as they have had the capacity to injure and have injured other persons.

551. As a direct and proximate result of Defendants' unfair practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, losses, and

damages, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and all others similarly situated, request the Court enter judgment against Defendants as follows:

a. An Order declaring this action to be a proper class action, appointing Plaintiffs as Class Representative, and appointing Plaintiffs' undersigned counsel as Class Counsel;

b. An Order requiring Defendants to bear the cost of Class Notice;

c. A judgment awarding Plaintiffs and other Class Members appropriate monetary relief, including statutory, actual, compensatory, and punitive damages (as permitted by law), in an amount to be determined at trial;

d. A judgment awarding any and all further equitable, injunctive, and declaratory relief as may be appropriate;

e. Pre-judgment and post-judgment interest, as permitted by law;

f. Attorneys' fees and costs; and

g. Any other and further relief that the Court deems necessary, just, and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: February 5, 2025

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger (Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

COTCHETT, PITRE & MCCARTHY, LLP
Thomas E. Loeser (*pro hac vice* forthcoming)
Jacob M Alhadeff (*pro hac vice* forthcoming)
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Telephone: (206)-802-1272
Facsimile: (206)-299-4184

Counsel for Plaintiffs and the Prospective Class

CIVIL COVER SHEET

The ILND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. ***(See instructions on next page of this form.)***

I. (a) PLAINTIFFS

SEE ATTACHMENT A, on behalf of themselves and all others similarly situated

(b) County of Residence of First Listed Plaintiff Salt Lake County, UT
(Except in U.S. plaintiff cases)

(c) Attorneys *(firm name, address, and telephone number)*

Gary M. Klinger, Milberg Coleman Bryson Phillips Grossman, PLLC
227 W. Monroe St., Ste. 2100, Chicago, IL 60606; (866) 252-0878

DEFENDANTS

The Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity LLC, Arity 875 LLC, and Arity Services LLC

County of Residence of First Listed Defendant Cook County, IL
(In U.S. plaintiff cases only)

Note: In land condemnation cases, use the location of the tract of land involved.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Check **one** box, only.)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government not a party.)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate citizenship of parties in Item III.)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(For Diversity Cases Only.)*

*(Check **one** box, only for plaintiff and **one** box for defendant.)*

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business in This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business in Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Check **one** box, only.)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loan (Excludes Veterans)
- ☐ 153 Recovery of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

PROPERTY RIGHTS
- ☐ 820 Copyright
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016 (DTSA)

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Arts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/Accommodations
- ☐ 445 Amer. w/ Disabilities-Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus – Alien Detainee (Prisoner Petition)
- ☐ 465 Other Immigration Actions

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAXES
- ☐ 870 Taxes (U.S. Plaintiff or Defendant
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Check **one** box, only.)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

(Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

28 USC 1332(d)

VII. PREVIOUS BANKRUPTCY MATTERS

(For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

☒ Check if this is a **class action** under Rule 23, F.R.CV.P.

Demand $ 5,000,000

CHECK Yes only if demanded in complaint:

Jury Demand: ☒ Yes ☐ No

IX. RELATED CASE(S) IF ANY *(See instructions):*

Judge Jeremy C. Daniel Case Number 1-25-cv-00407

X. Is this a previously dismissed or remanded case?

☐ Yes ☒ No **If yes, Case #** **Name of Judge**

Date: 2/5/2025

Signature of Attorney of Record /s/ Gary M. Klinger

ATTACHMENT A
LIST OF PLAINTIFFS

DELIA ARELLANO
MATTHEW BAUMGARTNER
DARREN BRISSETT
DANNY CARROL
BRIANNA CLAY
TOYETTE FLOWERS
CHRISTOPHER FREEL
JADE GAMBLE
KIMBERLY KELLEY
DANIEL KILGO
SOFIA MALVAR
JAMES MCNEILL
DAVID MURRY
AMANDA QUAM
ANNETTE RASTRELLI
NICOLE REHFUSS
BILLY ROBINSON
DORIAN ROCHESTER
ROBERT SANGINITO
KAYLA SMITH
ROBERT SMITH
AUSTIN TOPCHI
TRACY TUPPER
JAMES WILLIAMS
EBONI WRIGHT