CAUSE NO. _____

THE STATE OF TEXAS, *Plaintiff,*	)	
v.	)	IN THE DISTRICT COURT OF
THE ALLSTATE CORPORATION, ALLSTATE INSURANCE COMPANY, ALLSTATE VEHICLE AND PROPERTY INSURANCE COMPANY, ARITY, LLC, ARITY 875, LLC, *and* ARITY SERVICES, LLC,	)	MONTGOMERY COUNTY, TEXAS
Defendants.	)	_____ JUDICIAL DISTRICT
	)	**JURY TRIAL DEMANDED**

PLAINTIFF'S ORIGINAL PETITION

Plaintiff, the State of Texas ("Plaintiff" or the "State"), acting by and through the Attorney General of Texas, Ken Paxton ("Attorney General"), brings this action against Defendant The Allstate Corporation, Defendant Allstate Insurance Company, Defendant Allstate Vehicle and Property Insurance Company (collectively, "Allstate Defendants"), Defendant Arity, LLC, Defendant Arity 875, LLC, and Defendant Arity Services, LLC (collectively, "Arity Defendants," and collectively with Allstate Defendants, "Defendants") for violating the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §§ 541.001 *et seq*. ("TDPSA"); Tex. Bus. & Com. Code §§ 509.001 *et seq*. ("Data Broker Law"); and Tex. Ins. Code §§ 541.001 *et seq*. ("Texas Insurance Code").

INTRODUCTION

1. Defendants, a series of companies owned by insurance giant, Defendant The Allstate Corporation, conspired to secretly collect and sell "trillions of miles" of consumers' "driving behavior" data from mobile devices, in-car devices, and vehicles.[1] Defendants used the illicitly obtained data to build the "world's largest driving behavior database," housing the driving behavior of over 45 million Americans.[2] Defendants created the database for two main purposes: (1) to support Allstate Defendants' car insurance business and (2) profit from selling the driving behavior data to third parties, including other car insurance carriers ("Insurers").[3] Millions of Americans, including Texans, were never informed about, nor consented to, Defendants' continuous collection and sale of their data.

2. Defendants covertly collected much of their "trillions of miles" of data by maintaining active connections with consumers' mobile devices and harvesting the data directly from their phone. Defendants developed and integrated software into third-party apps so that when a consumer downloaded the third-party app onto their phone, they also unwittingly downloaded Defendants' software. Once Defendants' software was downloaded onto a consumer's device, Defendants could monitor the consumer's location and movement in real-time.

3. Through the software integrated into the third-party apps, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones. The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

[1] https://arity.com/
[2] https://arity.com/solutions/vehicle-miles-traveled/
[3] https://arity.com/

4. To encourage developers to adopt Defendants' software, Defendants paid app developers millions of dollars to integrate Defendants' software into their apps. Defendants further incentivized developer participation by creating generous bonus incentives for increasing the size of their dataset. According to Defendants, the apps integrated with their software currently allow them to "capture[] [data] every 15 seconds or less" from "40 [million] *active* mobile connections."[4]

5. Once collected, Defendants found several ways to monetize the ill-gotten data, including by selling access to Defendants' driving behavior database to other Insurers and using the data for Allstate Defendants' own insurance underwriting. If a consumer requested a car insurance quote or had to renew their coverage, Insurers would access that consumer's driving behavior in Defendants' database. Insurers then used that consumer's data to justify increasing their car insurance premiums, denying them coverage, or dropping them from coverage.

6. Defendants marketed and sold the data obtained through third-party apps as "driving" data reflecting consumers' driving habits, despite the data being collected from and about the location of a person's phone. More recently, however, Defendants have begun purchasing data about vehicles' operation directly from car manufacturers. Defendants ostensibly did this to better account for their inability to distinguish whether a person was actually driving based on the location and movements of their phone. The manufacturers that Defendants purchased data from included Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram. Allstate Defendants have used this data for their own insurance underwriting purposes.

7. Consumers did not consent to, nor were aware of Defendants' collection and sale of immeasurable amounts of their sensitive data. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that

[4] https://arity.com/solutions/real-time-insights/ (emphasis added).

app developers presented and obtained from consumers. However, Defendants never informed consumers about their extensive data collection, nor did Defendants obtain consumers' consent to engage in such data collection. Finally, Defendants never informed consumers about the myriad of ways Defendants would analyze, use, and monetize their sensitive data.

8. Defendants' conduct violates the TDPSA, the Data Broker Law, and the Texas Insurance Code's prohibition on unfair and deceptive acts and practices in the business of insurance.[5] The State of Texas contends that this proceeding is in the public interest and brings this action to end and penalize the privacy and financial harms caused by Defendants' conduct.

JURISDICTION AND VENUE

9. This action is brought by the Texas Attorney General's Office through its Consumer Protection Division in the name of the State of Texas and in the public interest, pursuant to the authority granted by Section 541.155 of the TDPSA, Section 509.008 of the Data Broker Law, and Sections 541.201 through 541.207 of the Texas Insurance Code.

10. In enforcement actions filed pursuant to Section 541.155 of the TDPSA, the Attorney General may seek civil penalties and injunctive relief. In addition, the Attorney General may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing an action.

11. In enforcement actions filed pursuant to Section 509.008 of the Data Broker Law, the Attorney General may recover civil penalties. In addition, the Attorney General may recover reasonable attorney's fees and court costs incurred in bringing the action.

[5] *See, e.g.*, Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson, *In re Gravy Analytics, Inc. & In re Mobilewalla, Inc.*, Federal Trade Commission, Matter Nos. 2123035 & 2023196 (Dec. 3, 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/gravy_-mobilewalla-ferguson-concurrence.pdf ("Given that the failure to obtain meaningful consent to the collection of precise location data is widespread, data brokers that purchase sensitive information cannot avoid liability by turning a blind eye to the strong possibility that consumers did not consent to its collection and sale. The sale of precise location data collected without the consumer's consent poses a similarly unavoidable and substantial risk of injury to the consumer as does the sale of the non-anonymized data.").

12. In enforcement actions filed pursuant to Sections 541.201 through 541.207 of the Texas Insurance Code, the Attorney General may seek civil penalties, redress for consumers, and injunctive relief. In addition, the Attorney General may pursue reasonable attorney's fees and litigation expenses in connection with the prosecution of the instant action, in accordance with Texas Government Code Section 402.006(c).

13. Jurisdiction is proper for the reasons described throughout this Petition, including because Defendants engaged in unlawful conduct targeting the data of Texans, profited from Texans' data, and harmed millions of Texas consumers through their actions. Venue of this suit lies in Montgomery County, Texas, pursuant to Section 541.202 of the Texas Insurance Code, because Defendants have done business in Montgomery County and because transactions at issue in this suit have occurred in Montgomery County.

DISCOVERY

14. The discovery in this case should be conducted under Level 3 pursuant to Texas Rule of Civil Procedure 190.4. Restrictions concerning expedited discovery under Texas Rule of Civil Procedure 169 do not apply because the State seeks non-monetary injunctive relief as part of its claims.

15. In addition to injunctive relief, the State claims entitlement to monetary relief in an amount greater than $1,000,000.00, including civil penalties, reasonable attorney's fees, litigation expenses, restitution, and costs.

PARTIES

16. The **Office of the Attorney General of Texas by and through its Consumer Protection Division** brings this action pursuant to its authority under Section 541.155 of the TDPSA, Section 509.008 of the Data Broker Law, and Sections 541.201 through 541.207 of the Texas Insurance Code.

17. **Defendant The Allstate Corporation** is a United States public corporation headquartered in Glenview, 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 Montgomery County, Texas. Defendant The Allstate Corporate may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

18. **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 Montgomery County, Texas, and maintains at least one office in Montgomery County, Texas. Defendant Allstate Insurance Company may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

19. **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 Montgomery County, Texas. Allstate Vehicle and Property Insurance Company may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

20. **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 Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity, LLC, is a mobility data and

analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Montgomery County, Texas, and uses predictive analytics to build solutions to sell to third parties. Arity, LLC, may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

21. **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 Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Montgomery County, Texas, and uses predictive analytics to build solutions to sell to third parties. Arity 875, LLC, may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

22. **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 Delaware. Defendant Arity Services, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Montgomery County, Texas, and uses predictive analytics to build solutions to sell to third parties. Arity Services, LLC, may be served through its registered agent, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The State requests service at this time.

PUBLIC INTEREST

23. The State has reason to believe that Defendants are engaging in or have engaged in the unlawful acts or practices set forth below. In addition, the State has reason to believe that Defendants have caused injury, loss, and damage to the State, and have caused adverse effects to the lawful conduct of trade and commerce, thereby directly or indirectly affecting the people of this State. Therefore, the Consumer Protection Division of the Office of the Attorney General initiates this proceeding in the public interest. *See* Tex. Ins. Code § 541.201.

PRE-SUIT NOTICE

24. Section 541.154 of the TDPSA requires the Attorney General to "notify a person in writing, not later than the 30th day before bringing [an] action, identifying the specific provisions of [the TDPSA] the attorney general alleges have been or are being violated." Further, the Attorney General may not bring an action if, within thirty (30) days of receiving notice from the Attorney General, a person "provides the attorney general a written statement that the person: (A) cured the alleged violation; (B) notified the consumer that the consumer's privacy violation was addressed, if the consumer's contact information has been made available to the person; (C) provided supportive documentation to show how the privacy violation was cured; and (D) made changes to internal policies, if necessary, to ensure that no such further violations will occur." Tex. Bus. & Com. Code § 541.154.

25. On November 29, 2024, the Attorney General, by and through the Consumer Protection Division of the Office of the Attorney General, notified Arity Defendants that their collection and sale of consumers' sensitive data appeared to violate Sections 541.102(a)(1), 541.101(b)(4), 541.102(b), 541.103, 541.051(b)(5), and 541.102(a)(3) of the TDPSA. *See* Nov. 29, 2024 Notice of Violation ("Attachment 1").

26. As of December 29, 2024—thirty (30) days after receiving the Notice of Violation—Arity Defendants did not cure the alleged violation(s) in accordance with Section 541.154 of the TDPSA because Arity Defendants did not provide the Attorney General a written statement and supportive documentation showing that Arity Defendants: (1) cured the alleged violation(s), (2) notified affected consumers of the privacy violations, and (3) made changes to internal policies, if necessary.

27. The Consumer Protection Division also provided Arity Defendants notice on April 2, 2024, that Arity Defendants had apparently failed to register with the Texas Secretary of State as required by the Data Broker Law. On information and belief, Arity Defendants have not registered with the Texas Secretary of State as of the filing of this Petition.

FACTS

28. Defendants have amassed the data of at least 45 million Americans, including—on information and belief—millions of Texans.[6] Defendants obtained the data without consumers' knowing by integrating a piece of software into various mobile apps that enabled them to collect data directly from consumers' phones.

29. Defendants have monetized this data in a variety of ways, including by building and selling Insurers access to the "world's largest driving behavior database," which contains the driving behavior data of over 45 million Americans.[7] Defendants never notified consumers nor obtained their consent to collect or sell their data.

I. Defendants Developed Software to Covertly Collect Consumers' Location Data

30. On information and belief, in 2015 Allstate Defendants designed a software development kit ("SDK") that could be integrated into mobile phone applications to collect data

[6] https://arity.com/solutions/vehicle-miles-traveled/
[7] https://arity.com/

about the location and movements of a person's phone. In general, SDKs can provide app developers a helpful tool to build and develop their apps. SDKs usually consist of a set of tools (APIs, software, etc.) with preprogrammed functions that are integrated into an app and operate in the background.

31. But the SDK Defendants developed was little more than a way for Defendants to scrape user data from several third-party apps under the pretext of providing a necessary function. Specifically, Defendants designed the Arity Driving Engine SDK ("Arity SDK") to collect an immense amount of granular data points from or about the location of a person's mobile phone ("Arity SDK Data").

32. Once installed in a mobile app, the Arity SDK harvested several types of data, including but not limited to:

(a) a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;

(b) "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;

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

(d) "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and

(e) Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, device type, app version, and OS version.

33. Because the Arity SDK operated and collected data in the background, absent being notified by Defendants or the app, users would be kept in the dark about the Arity SDK's existence. App users would likewise be unaware that Defendants were directly collecting Arity SDK Data from their phones. Defendants never notified nor otherwise informed consumers that they were collecting their data via the Arity SDK and the apps.

II. Defendants Paid to Integrate the Arity SDK into Mobile Apps

34. Since at least 2017, Defendants have been "licensing" the Arity SDK by paying app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. On information and belief, to avoid alerting consumers of their data collection, Defendants only sought to partner with apps that, prior to contracting with Defendants, already contained features that relied on location information to function properly. The apps that integrated the Arity SDK included Routely,[8] Life360, GasBuddy, and Fuel Rewards.

35. Each of these apps routinely requested and received permission from users to use their location information to enable certain in-app features prior to integrating the Arity SDK. But after an app integrated the Arity SDK, if an app user allowed the app to access their location information for those same in-app features, the user was also unwittingly enabling Defendants to collect the Arity SDK Data via the Arity SDK.

36. Defendants' agreements with app developers generally had similar key provisions. Pursuant to these agreements, Defendants granted an app developer a limited license to integrate the Arity SDK into the developer's mobile app. Once integrated into an app, Defendants were permitted to use the Arity SDK to collect and use the Arity SDK Data from app users' mobile phones.

[8] On information and belief, Defendants now own the Routely app.

37. Pursuant to their agreements with the app developers, Defendants owned any Arity SDK Data they collected from an app user and were permitted to use the Arity SDK Data for their own independent purposes. Defendants further agreed to license or transfer subsets of the Arity SDK Data to the app developers to use to support specific features in their apps, such as displaying a summary of a user's trip and fuel efficiency.

38. On information and belief, the Arity SDK Data in isolation could not (or at least could not reliably) be linked to a specific individual. To allow Defendants to match specific individuals to the Arity SDK Data, the app publishers licensed the personal data that they collected from their users to Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), device ID, and ad-ID (collectively, "Personal Data"). Upon combining the Personal Data with the Arity SDK Data, Defendants could more reliably identify the specific person being monitored by the Arity SDK.

III. Defendants Products and Services Monetized Consumers' Data

39. Defendants used the Arity SDK Data and Personal Data, alone and in conjunction with one another, to develop, advertise, and sell several different products and services to third parties, including Insurers, and used the Arity SDK Data and Personal Data for the Allstate Defendants' own underwriting purposes. Defendants' products and services included:

(a) Drivesight. In 2015, Allstate Defendants developed Drivesight to generate a driving score based on Defendants' own scoring model by analyzing data and generating driving scores that assign a particular value to an individual's driving risk.

(b) ArityIQ. Defendants let companies, including Insurers, "[a]ccess actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver."[9]

(c) Arity Audiences. Defendants let companies, including Insurers, "[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."[10] As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.

(d) Real Time Insights. Defendants advertised that their business customers could "[r]eceive granular driver probe and event data for real-time applications."[11]

(e) Routely. Defendants offer consumers Routely, a "free" application which purports to provide "helpful insights" into the consumers' driver data. By contrast, when marketing to Insurers, Defendants describe Routely as "telematics in a box" that Insurers can use to "more accurately identify drivers with riskier driving profiles based on actual driving data, provide personalized discounts or surcharges at renewal, promote safer driving habits, and improve retention of [their] safer drivers."[12]

40. Notably, Defendants primarily marketed the Arity SDK Data to third parties as "driving behavior" data as opposed to what the Arity SDK Data really was: data about the movements of a person's *mobile phone*. On information and belief, Defendants had no way to

[9] https://arity.com/solutions/arity-iq/
[10] https://arity.com/solutions/arity-audiences/
[11] https://arity.com/solutions/real-time-insights/
[12] https://arity.com/solutions/routely/

reliably determine whether a person was driving at the time Defendants collected the Arity SDK Data.

41. For example, if a person was a passenger in a bus, a taxi, or in a friend's car, and that vehicle's driver sped, hard braked, or made a sharp turn, Defendants would conclude that the passenger, not the actual driver, engaged in "bad" driving behavior based on the Arity SDK Data.[13] Defendants would then subsequently sell and share the data so it could be used to inform decisions about that passenger's insurability based on their "bad" driving behavior. Defendants' public advertising for their products and services do not disclose the limitations of the Arity SDK Data.

42. To potentially account for the Arity SDK Data's limitations, Defendants sought to combine the SDK Data with data collected directly from vehicles. As a result, Defendants began purchasing consumers' driving-related data from car manufacturers, such as Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram. On information and belief, consumers did not consent, nor were otherwise aware that, Defendants purchased their driving-related data from these car manufacturers.

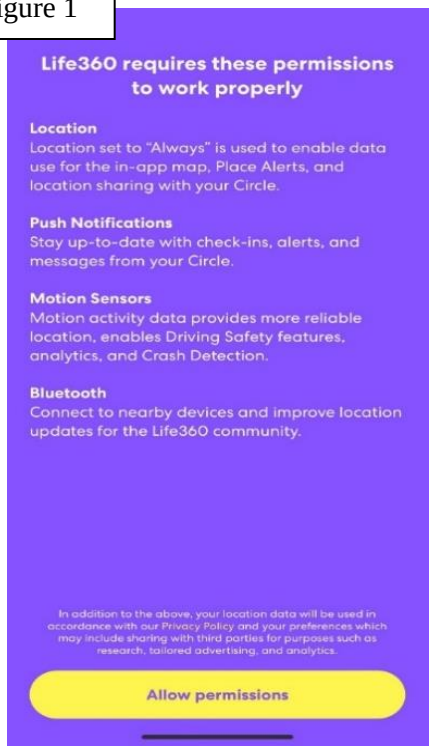
IV. Defendants' Lack of Privacy Disclosures

43. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented to consumers. However, neither Defendants, nor the apps on Defendants' behalf, informed consumers that Defendants were collecting Arity SDK Data. Nor did Defendants, nor the apps on Defendants' behalf, inform consumers of the various ways that Defendants would collect, use, and ultimately monetize the Arity SDK Data.

[13] As a further example, it was publicly reported that a person's driving score was lowered because the "driving" behavior data collected from his phone claimed he was driving when he was actually riding a roller coaster. https://www.cincinnati.com/story/entertainment/2024/10/08/insurance-cuts-driving-score-man-riding-the-beast-kings-island/75554987007/.

44. For example, Life360 merely told app users that it needed location sharing turned on "to enable data use for the in-app map, Place Alerts, and location sharing with [a user's] Circle." Nowhere did Life360 even mention Defendants' existence, let alone any of Defendants' data collection or sales.

Figure 1



45. Because Defendants did not disclose their conduct, consumers were wholly unaware that Defendants were collecting the Arity SDK Data from their phone. Consumers were likewise wholly unaware that Defendants would use the Arity SDK Data to create and sell several different products and services to third parties, including Insurers.

46. 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.*

47. Even if a consumer took the extra step to investigate Defendants outside of their app, navigated to Defendants' website, and located their privacy disclosures, they would still not understand what Defendants did with their data. Consumers reading Defendants' privacy disclosures are met with a series of untrue and contradictory statements that do not reflect Defendants' practices.

48. For example, Defendants state that they "do not sell personal information for monetary value," which is untrue. Defendants sold a number of data-based products and services for monetary value that linked a specific app user to their alleged driving behavior. Further, Defendants do not provide consumers with the ability to request that Defendants stop selling their data. *See* Attach. 1, Ex. A.

49. Defendants likewise obscured how they used consumers' data. In Defendants' privacy disclosures, Defendants state that they "[u]se [consumers'] personal data for analytics and profiling." But in describing how Defendants "profile" consumers, the description does not reflect their actual "profiling" conduct—which consisted of Defendants combining the Arity SDK Data and Personal Data to create a database of driving profiles for more than 45 million Americans and selling access to said database. Rather Defendants describe their profiling activities as follows:

> "We use your personal data to assist in our development of predictive driving models. We may profile [consumers'] 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." *See* Attach. 1, Ex. A.

50. In the event a consumer took the extraordinary steps of tracking down Defendants' privacy statement, finding the subparagraph describing profiling, parsing through Defendants' convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a "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.

51. 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. 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 a request to Defendants specifically.

CAUSES OF ACTION

COUNT I (*Arity Defendants*)

Violations of the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §§ 541.001 *et seq*. ("TDPSA")

52. The State incorporates and adopts by reference each and every factual allegation contained in all preceding paragraphs of this Petition as if fully set forth herein.

53. The TDPSA "regulates the collection, use, processing, and treatment of consumers' personal data by certain business entities."[14] The TDPSA defines "personal data" as "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual," including "pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual." Tex. Bus. & Com. Code § 541.001(19).

[14] Tex. House Committee Report (https://capitol.texas.gov/tlodocs/88R/analysis/pdf/HB00004H.pdf).

54. In addition to protecting consumers' personal data, the TDPSA provides heightened protections for the "processing" or sale of "sensitive data." The TDPSA defines "processing" as an "operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data." *Id*. at 541.001(22).

55. The TDPSA defines "sensitive data" by providing several examples of sensitive "categor[ies] of personal data," such as "precise geolocation data." *Id*. at 541.001(29). The TDPSA defines as "information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet." *Id*. at 541.001(21).

56. Arity Defendants obtained a consumer's sensitive precise geolocation data by using the Arity SDK integrated into mobile apps to collect the data directly from a consumer's mobile phone, including their phone's latitude, longitude, speed, GPS time, bearing, and altitude. Arity Defendants would take the precise geolocation to analyze and sell the data for their own purposes.

57. Based on Arity Defendants' collection, processing, and sale of consumers' sensitive precise geolocation data, the Attorney General notified Arity Defendants that their conduct violated the following sections of the TDPSA:

Violation 1: Section 541.102(a)(1)

58. Section 541.102(a)(1) of the TDPSA requires a "controller [to] provide consumers with a reasonably accessible and clear privacy notice that includes . . . any sensitive data processed by the controller." The TDPSA defines a "controller" as an "individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data." Tex. Bus. & Com. Code § 541.001(8).

59. Arity Defendants acted as a controller in several respects, including by exercising ownership over the data, integrating the Arity SDK into several mobile apps to collect consumers' sensitive data, analyzing the data for certain driving behaviors, combining the data with other data sets, and repurposing the data to sell as part of various products and services.

60. Despite being the controller of the data, consumers were wholly unaware of Arity Defendants' processing of their sensitive data, and Arity Defendants never provided consumers with a privacy notice. By extension, Arity Defendants did not provide consumers with notice about Arity Defendants' processing of consumers' sensitive data. Additionally, the mobile apps did not provide consumers with notice of Arity Defendants' processing of their sensitive data on behalf of Arity Defendants or in a reasonably accessible or clear manner.

61. Arity Defendants did not provide a reasonably clear and accessible privacy notice indicating the sensitive data processed by the controller. As a result, Arity Defendants violated TDPSA Section 541.102(a)(1).

Violation 2: Section 541.101(b)(4)

62. Section 541.101(b)(4) of the TDPSA prohibits a controller from "process[ing] the sensitive data of a consumer without obtaining the consumer's consent." The TDPSA defines "consent" as a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer." Tex. Bus. & Com. Code § 541.001(6).

63. The TDPSA also explicitly excludes the following practices from its definition of consent: "(A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (B) hovering

over, muting, pausing, or closing a given piece of content; or (C) agreement obtained through the use of dark patterns." *Id*.

64. Consumers were wholly unaware of any of Arity Defendants' conduct, including that by downloading and using a mobile app with the Arity SDK integrated, Arity Defendants would own, collect, analyze, and sell their sensitive data. Further, neither Arity Defendants, nor the mobile apps on Arity Defendants' behalf, informed consumers that Arity Defendants were collecting their sensitive data, nor did Arity Defendants or the mobile apps obtain consumers' consent to do so. Rather, consumers were entirely unaware that by allowing one of the mobile apps to access their "location," they were also permitting Arity Defendants to own, collect, analyze, and sell their sensitive data in a variety of ways, including by selling it to Insurers to adjust their car insurance premiums.

65. Arity Defendants processed consumers' sensitive data without obtaining their consent through a clear affirmative act signifying their freely given and informed agreement to permit Arity Defendants to process their sensitive data. In doing so, Arity Defendants violated Section 541.102(b).

Violation 3: Section 541.102(b)

66. Section 541.102(b) of the TDPSA requires a "controller engag[ing] in the sale of personal data that is sensitive data, [to] include the following notice: 'NOTICE: We may sell your sensitive personal data.'" The TDPSA further requires that this notice "be posted in the same location and in the same manner as the privacy notice." *Id*. The TDPSA defines the "sale of personal data" as the "sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party." *Id*. at 541.001(28).

67. Pursuant to the agreements with app developers, Defendants owned the sensitive data collected by the Arity SDK and/or were permitted to use Arity SDK Data for their own purposes. After collecting and analyzing consumers' sensitive data, Arity Defendants then sold the sensitive data to several third parties, including app developers and Insurers.

68. The sensitive data Arity Defendants sold to third parties included but was not limited to GPS points, such as the accuracy, position, speed, GPS time, bearing and altitude of a consumer's phone, start and end location of a trip, start and end time of a trip, distance traveled, duration of travel, hard braking events, and whether a consumer picked up or opened their phone while traveling at certain speeds.

69. Arity Defendants licensed app developers the sensitive data and permitted them to use it for specific purposes, such as displaying trip and fuel efficiency summaries to their respective users. With respect to Insurers, Arity Defendants packaged the sensitive data in various ways to sell Insurers several products, such as ArityIQ, which lets Insurers "[a]ccess actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver."[15]

70. Arity Defendants did not provide the required notice as required under the TDPSA. As a result, Arity Defendants violated Section 541.102(b) of the TDPSA.

Violation 4: Section 541.103

71. Section 541.103 of the TDPSA requires a "controller sell[ing] personal data to third parties or process[ing] personal data for targeted advertising, [to] clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process." Tex. Bus. & Com. Code § 541.103. "Targeted advertising" is defined as "displaying to

[15] https://arity.com/solutions/arity-iq/

a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. *Id*. at 541.001(19).

72. Arity Defendants sold personal data as part of several products and services that let businesses target consumers based on the personal data Arity Defendants collected about them. Arity Defendants, however, did not provide consumers any notice of their activities whatsoever, let alone a clear and conspicuous disclosure about their sales of personal data to third parties, their processing of personal data for targeted advertising, or a mechanism to opt out of either.

73. Because Arity Defendants did not provide any disclosure regarding their sales of personal data, targeted advertising practices, or a method to opt-out of either, Arity Defendants violated Section 541.103 of the TDPSA.

Violation 5: Sections 541.102(a)(3) and 541.051(b)(5)

74. Section 541.102(a)(3) of the TDPSA requires a "controller [to] provide consumers with a reasonably accessible and clear privacy notice that includes . . . how consumers may exercise their consumer rights." The consumer rights contained in Section 541.051(b)(5) of the TDPSA include the right to "opt out of the processing of [their] personal data for the purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer." The TDPSA defines "profiling" as "any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." *Id*. at 541.001(21).

75. Arity Defendants acted as a controller by collecting consumers' personal data using the Arity SDK and using that data in a variety of ways, including by selling it to third parties.

76. Consumers were wholly unaware that Arity Defendants were collecting their personal data, and Arity Defendants never provided consumers with any privacy notice whatsoever. By extension, Arity Defendants did not provide consumers with notice of their right to opt out of processing for the purposes specified in Section 541.051(b)(5) of the TDPSA. Further, the mobile apps did not provide consumers with Arity Defendants' privacy notice in a reasonably accessible or clear manner on behalf of the Arity Defendants.

77. In addition, even if a consumer navigated to Arity Defendants' website and located Arity Defendants' privacy disclosures, Arity Defendants did not provide consumers with a method for consumers to exercise their rights. Arity Defendants had no method for consumers to request that Arity Defendants stop selling their data, nor did Arity Defendants provide consumers a method to request that Arity Defendants stop using their data to create "driving behavior" profiles about them.

78. Similarly, Arity Defendants did not describe or provide consumers with a method to submit either a request to opt out of the sale of their personal data or a request to opt out of targeted advertising. Rather, Arity Defendants merely told consumers that they do not sell personal information but that consumers could "[l]earn how to opt out of targeted advertising" by visiting another link.

79. 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, only provided them with links to several third-party websites, such as the Apple Support Center. These websites 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 a request to Arity Defendants specifically. Arity Defendants did not provide any method to actually submit a request to them.

80. Arity Defendants failed to supply a reasonably accessible privacy notice that included how consumers may exercise their rights under the TDPSA. In doing so, Arity Defendants violated Sections 541.102(a)(3) and 541.051(b)(5) of the TDPSA.

COUNT II (*Arity Defendants*)

The Data Broker Law, Tex. Bus. & Com. Code §§ 509.001 *et seq*.

81. The State incorporates and adopts by reference each and every factual allegation contained in all preceding paragraphs of this Petition as if fully set forth herein.

82. Any company that "derives revenue from processing or transferring the personal data of more than 50,000 individuals that the data broker did not collect directly from the individuals to whom the data pertains" was required to register with the Texas Secretary of State by March 1, 2024. Tex. Bus. & Com. Code §§ 509.003(a)(2), 509.005; Tex. Admin. Code § 106.3(c).

83. As of March 1, 2024, Arity Defendants were conducting business in the State of Texas and deriving revenue by processing and transferring the personal data of more than 50,000 individuals that Arity Defendants did not collect directly from the individuals to whom the data pertains. Specifically, several app developers licensed the Personal Data of over 45 million individual app users to Arity Defendants, which included information about individuals such as an app user's first and last name, phone number, zip code, number of vehicles associated with their account, device ID, and mobile ad-ID.

84. Arity Defendants subsequently used the Personal Data in a number of ways, including by combining it with the Arity SDK Data and selling it to third parties, including Insurers.

85. Arity Defendants failed to register with the Texas Secretary of State's Office by March 1, 2024, and as of the date of this Petition, still have not registered with the Texas Secretary of State's Office. In doing so, Arity Defendants violated Section 509.005 of the Data Broker Law.

COUNT III (*All Defendants*)

Unfair Methods of Competition and Unfair or Deceptive Acts or Practices in the Business of Insurance, Tex. Ins. Code §§ 541.001 *et seq*.

86. The State incorporates and adopts by reference each and every factual allegation contained in all preceding paragraphs of this Petition as if fully set forth herein.

87. The Texas Insurance Code "regulate[s] trade practices in the business of insurance" by broadly prohibiting businesses from engaging in "unfair or deceptive acts or practices" related to insurance. Tex. Ins. Code § 541.001. The Texas Insurance Code is to be "liberally construed" to prohibit a "person [from] engag[ing] in this state in a trade practice that is defined in this chapter as or determined under this chapter to be an unfair method of competition or an unfair or deceptive act or practice in the business of insurance." *Id*. at 541.003; 541.008. The Texas Department of Insurance has promulgated rules determining that "no person may engage in this state in any trade practice which is determined pursuant by law to be an unfair method of competition or an unfair or deceptive act or practice in the business of insurance." 28 Tex. Admin. Code § 21.3(a)–(b).

88. Pursuant to the Texas Insurance Code, the Texas Attorney General may request a civil penalty of not more than $10,000 per violation when a person has engaged in an act or practice determined to be unlawful under any chapter or rule under the Texas Insurance Code. Tex. Ins. Code § 541.204.

89. Defendants engaged in several acts and practices in the business of insurance that, alone and in conjunction with each other, constitute unfair and deceptive acts and practices, including by "failing to verify" consumers' consent before purchasing driving-related data from vehicle manufacturers, "turning a blind eye to the strong possibility that consumers did not consent to [their] collection and sale" of their sensitive and/or non-anonymized data to Insurers,[16] using the unlawfully obtained data for Defendants' own car insurance underwriting processes, and marketing and advertising the data to Insurers as "driving behavior" data.

90. By engaging in these practices, Defendants violated Section 541.003 of the Texas Insurance Code.

PRAYER FOR RELIEF

91. Pursuant to Section 541.155 of the TDPSA, the State of Texas respectfully requests that this Honorable Court impose a civil penalty in an amount of not more than $7,500 per violation.

92. Pursuant to Section 509.008 of the Data Broker Law, the State of Texas respectfully requests that this Honorable Court impose a civil penalty of up to $10,000 and in an amount of: (1) not less than the total of $100 for each day Defendants were in violation of Section 509.004 or 509.005; and (2) the amount of unpaid registration fees for each year the entity failed to register in violation of Section 509.005. Tex. Bus. & Com. Code § 509.008(b)(1).

[16] Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson, *In re Gravy Analytics, Inc. & In re Mobilewalla, Inc.*, Federal Trade Commission, Matter Nos. 2123035 & 2023196 (Dec. 3, 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/gravy_-mobilewalla-ferguson-concurrence.pdf (explaining that it is an unfair practice to sell precise location data without verifying that a consumer consented to such a sale because such a practice poses an "unavoidable and substantial risk of injury to the consumer").

93. Pursuant to Section 541.204 of the Texas Insurance Code, the State of Texas respectfully requests that this Honorable Court impose a civil penalty in an amount of not more than $10,000 per violation.

94. The State of Texas further respectfully requests that this Honorable Court issue an order:

(a) Declaring Defendants' conduct as described herein to be in violation of the TDPSA;

(b) Declaring Defendants' conduct as described herein to be in violation of the Data Broker Law;

(c) Declaring Defendants' conduct as described herein to be an unfair or deceptive act or practice in the business of insurance in violation of the Texas Insurance Code;

(d) Directing Defendants to delete or otherwise destroy all data obtained prior to the entry of any judgment by this Court, including any data in the possession of any third party;

(e) Directing Defendants to make full restitution or restoration to all consumers who suffered a loss as a result of the acts and practices alleged in this Petition and any other acts and practices proved by the State, pursuant to Section 541.205 of the Texas Insurance Code; and

(f) Permanently enjoining Defendants, their agents, employees, and all other persons acting on their behalf, directly or indirectly, from violating the TDPSA, the Data Broker Law, and the Texas Insurance Code.

95. The State of Texas further respectfully requests that this Honorable Court award the Office of the Texas Attorney General attorney's fees and costs of court pursuant to the TDPSA,

the Data Broker Law, and the Texas Insurance Code, under which attorney's fees and costs of court are recoverable by the Office of the Texas Attorney General.

96. Lastly, the State of Texas respectfully requests that this Honorable Court grant any other general, equitable, or further relief this Court deems just and proper.

Dated: January 13, 2025

Respectfully submitted,

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

RALPH MOLINA
Deputy First Assistant Attorney General

JAMES LLOYD
Deputy Attorney General for Civil Litigation

JOHNATHAN STONE
Chief, Consumer Protection Division

Tyler Bridegan

TYLER BRIDEGAN (TX Bar No. 24105530)
RICHARD R. MCCUTCHEON (TX Bar No. 24139547)
ROBERTA H. NORDSTROM (TX Bar No. 24036801)
MADELINE FOGEL (TX Bar No. 24141985)
Assistant Attorneys General
Office of the Attorney General of Texas
Consumer Protection Division
808 Travis Street, Suite 1520
Houston, Texas 77002
Telephone: (713) 225-8922
Fax: (713) 223-5821
Tyler.Bridegan@oag.texas.gov
Richard.McCutcheon@oag.texas.gov
Roberta.Nordstrom@oag.texas.gov
Madeline.Fogel@oag.texas.gov

SUMMER R. LEE (TX Bar No. 24046283)
MONICA WADLEIGH (TX Bar No. 24132098)
ADAM HOLTZ (TX Bar No. 24143021)
Assistant Attorneys General
Office of the Attorney General of Texas
Consumer Protection Division
P.O. Box 12548
Austin, Texas 78711
Telephone: (512) 475-3082
Fax: (512) 473-8301
Summer.Lee@oag.texas.gov
Monica.Wadleigh@oag.texas.gov
Adam.Holtz@oag.texas.gov

GABRIELLA GONZALEZ (TX Bar No. 24080184)
JOHN C. HERNANDEZ (TX Bar No. 24095819)
Assistant Attorneys General
Office of the Attorney General of Texas
Consumer Protection Division
112 E. Pecan Street, Suite 735
San Antonio, Texas 78205
Phone: (210) 225-4191
Fax: (210) 225-1075
Gabriella.Gonzalez@oag.texas.gov
JC.Hernandez@oag.texas.gov

ATTACHMENT 1

KEN PAXTON
ATTORNEY GENERAL OF TEXAS

November 29, 2024

ARITY, LLC

Via Electronic Mail:
krollins@sheppardmullin.com

c/o Kari Rollins
Sheppard Mullin
30 Rockefeller Plaza
New York, NY 10112-0015

Re: Notice of Violation of Tex. Bus. & Com. Code Ann. § 541.001 *et seq*. by Arity, LLC

Dear Ms. Rollins,

Based on a review of the privacy notice(s) and practices of Arity, LLC, and its subsidiaries and affiliates, including Arity 875, LLC (collectively, "Arity"), the Office of the Attorney General of Texas has found that Arity is in violation of, Chapter 541, Subtitle C of the Texas Business and Commerce Code, the Texas Data Privacy and Security Act (hereinafter, the "TDPSA").

The TDPSA, effective as of July 1, 2024, governs a company's collection, use, processing, and treatment of Texans' personal data, including Texans' sensitive information. To that end, the TDPSA imposes several obligations on a company that conducts business in Texas or that produces products or services consumed by Texans. These obligations include, but are not limited to, requirements that a company make certain public disclosures about their privacy and data practices. *See* Tex. Bus. & Com. Code Ann. §§ 541.055, 541.102-.103.

This Office is authorized to bring an enforcement action against a company that violates the TDPSA's requirements. Specifically, this Office may bring an action where, after receiving a notice of violation, a company fails to cure any violation identified in the notice pursuant to Section 541.154 of the TDPSA. The TDPSA also authorizes this Office to seek up to $7,500 per violation and other relief, including injunctive relief, as appropriate. *See* Tex. Bus. & Com. Code Ann. § 541.155.

This Office has reviewed Arity's privacy notice(s), last updated November 1, 2024 (attached as Exhibit A) and practices, and found that they violate the following provisions of the TDPSA:

(1) Section 541.102(a)(1) for failing to provide consumers with a reasonably clear notice of the categories of sensitive data being processed.

(2) Section 541.101(b)(4) for processing consumers' sensitive data without obtaining their consent, defined as a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement."

a. This violation includes Arity's processing of sensitive data through its use of a software development kit ("SDK") to collect sensitive data from various mobile applications, including precise geolocation information and the other information Arity derives from the location of a consumer's mobile phone, including how fast a consumer's mobile phone is moving. This violation also includes Arity's analysis and sale of sensitive data to car insurance companies.

(3) Section 541.102(b) for failing to provide consumers with the required notice.

(4) Section 541.103 for failing to clearly and conspicuously disclose the process by which it sells personal data to third parties.

(5) Sections 541.051(b)(5) and 541.102(a)(3) for failing to describe and provide the methods by which consumers may exercise their right to opt out of the processing of personal data for purposes of targeted advertising, sales of personal data, and profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumers.

We request that Arity immediately address the violations of the TDPSA identified in this Notice and within 30 days of the date of this Notice, provide a written statement and supporting documentation to this Office explaining how Arity cured the violations. Failure to address any violations identified herein may result in this Office taking action against Arity by seeking civil penalties, injunctive relief, attorney's fees, court costs, and any other appropriate relief.

Any responsive material may be sent electronically or by courier or certified mail to the Office of Attorney General, 300 W. 15th St., 9th Floor, Austin, Texas 78701. Please contact the undersigned if you have any questions.

Sincerely,

Tyler Bridegan

TYLER BRIDEGAN
Assistant Attorney General
Office of the Attorney General of Texas
Tyler.Bridegan@oag.texas.gov

ROBERTA NORDSTROM
Assistant Attorney General
Office of the Attorney General of Texas
Roberta.Nordstrom@oag.texas.gov

RICHARD MCCUTCHEON
Assistant Attorney General
Office of the Attorney General of Texas
Richard.McCutcheon@oag.texas.gov

EXHIBIT A

Privacy statement

Arity Privacy Statement

Effective date: November 1, 2024

At Arity, we understand your privacy is a top priority. This Privacy Statement describes the privacy practices of Arity, LLC and Arity 875, LLC ("Arity", "we" or "us"). While this Privacy Statement addresses data privacy requirements from across the globe, some parts of this Privacy Statement apply to certain regions, states, or countries only. We urge all visitors to our site to read this Privacy Statement in its entirety.

Use this Table of Contents to link directly to a specific section of the Privacy Statement.

About Arity

Arity is a technology company focused on making transportation smarter, safer, and more useful for everyone. Arity transforms large amounts of data into actionable insights to help better predict risk and make smarter decisions in real time. Arity provides services directly to consumers and indirectly through companies such as mobile application providers and insurance companies to capture and understand driving

behavior. Arity also provides some products only to business customers, referred to as business clients, for their own purposes. Arity designs its products and services with privacy and data protection in mind.

Arity works with many different business clients such as mobile application providers, website publishers, vehicle manufacturers, and insurance companies. When working with these business clients, Arity may collect information directly from consumers or the business client may collect the information and share it with Arity.

Personal information we collect

Arity collects both personal and non-personal information about you. Personal information (also referred to as personal data in some jurisdictions) is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with you. In contrast, non-personal information does not and cannot reveal an individual's identity such as information that has been deidentified or aggregated.

Please note that the type and amount of personal information collected from or about you will differ based on the products, features, and services you use, your relationship with Arity, and the country in which the products, features and services are provided. In certain circumstances, Arity may collect personal information about you in its role as a service provider on behalf of its business clients. When Arity acts as a service provider, the collection and use of personal information is subject to the privacy policies of the business clients and not this Privacy Statement.

We collect the following categories of personal information:

- **Geolocation data:** Includes geolocation coordinates, including latitude, longitude, and altitude, your direction of travel, Wi-Fi access points, and the time the information was recorded.
- **Personal identifiers:** Includes name, alias, postal address, phone number, fax number, date of birth, partial social security number, vehicle identification number (VIN), unique device or personal identifier, online identifier – such as Mobile Ad ID, internet protocol (IP) address, and email address.
- **Personal characteristics:** Age, marital status, gender, education and occupation, employment status, household income, household size, household children, community type and other demographic information. For transparency, we collect some demographic information for research purposes including race and ethnicity.
- **Commercial and service related information:** Services purchased, obtained, considered, or other purchasing or consuming histories or tendencies. If Arity's services are provided in connection with an insurance product (provided by an insurance company or employer), we may also receive the following information: Insurance policyholder demographic information and policy information, insurance claims data, motor vehicle records and consumer report data, including credit score.
- **Internet or other electronic network activity information (including mobile app information):** Includes browsing history, search history, information regarding your interaction with our website, mobile apps, and advertisements we facilitate, links you use, referral pages or web pages you visit while visiting our websites, browser type, internet service provider (ISP), and cookies. It also includes mobile app and device usage information (e.g., frequency of use, application marketplace from where you downloaded the mobile app, operating system, device model and time zone) and driving behavior (e.g., phone handling, miles, speed, and if a mobile app detects a collision, information about the collision).
- **Multimedia Information:** Audio, electronic, or similar information.
- **Inferences:** Inferences drawn from personal information collected to create a profile reflecting preferences, characteristics, predispositions, and driving habits and behavior. For example, Arity may derive miles traveled, acceleration,

deceleration, braking behavior, cornering, speed, and trip routing from information coming from your mobile device or vehicle, including location data.

- **Sensitive personal information:** Some personal information we collect is defined under the law as sensitive personal information. The sensitive personal information we collect includes precise geolocation information. When engaging in market research surveys, we may also collect race and ethnicity.

Sources of personal information

We collect personal information about you in several ways and from several sources. Personal information is collected from the following sources:

- Directly from consumers via our websites, emails, phone conversations, third-party mobile apps, Arity's mobile app (Routely®) or devices installed in vehicles. For some products, Arity embeds its technology in its business clients' mobile app, allowing Arity to collect geolocation and related driving behavior information directly from consumers.
- From Arity business clients via their mobile app or other device or directly from the business client (not via the mobile app) in connection with services you've requested from the business client such as vehicle manufacturers. For example, a business client may provide Arity with information not collected from an app that would help Arity better develop its models.
- From other parties such as our corporate affiliates, data brokers, service providers, and marketing companies.
- Directly from consumers during or in connection with an interview, survey or similar interaction.
- From third parties when Arity is acting as a service provider. Arity often acts as a service provider to business clients and collects and uses certain additional personal information only in connection with performing services on behalf of those business clients. The use of this information is subject to the privacy practices of those business clients and not this Privacy Statement.

Use of information

Arity's use of your information differs based on your services, features and products and your country of origin. See **Specific Information Related to Users in the EU, UK, EEA and Switzerland** below for details about the collection and use of data from data subjects in the European Union, United Kingdom, European Economic Area or Switzerland. See also **Privacy Practices for Select Arity Products** below for more details about the differences in data usage for certain products.

Personal information may be used for business purposes including to:

- **Create, deliver or improve our services, features and products.** We may use your personal information to create, deliver or improve our services, features or products. We use personal information to perform actuarial studies, model development, and statistical analysis to create and refine our risk, driving behavior, and advertising models and analytics that allows us to create, deliver or improve our products and services, including providing services to our business clients. Our services, features and products, such as telematics features within a mobile app (Routely® or a business client's app, for example), may be provided directly to you in connection with your relationship with one of our business clients or may be provided to you by or through the business client. We also use personal information to improve or repair our services, features and products, including addressing bugs or other issues.
- **Facilitate a business client's services, features and products:** Arity's services, features and products are provided to you, directly or indirectly, in connection with a relationship you have with one of our business clients and facilitate the business

clients' services or products. These services, features and products, that rely on Arity's use of your personal information may include:

  - Creating insights on driving behavior based on geolocation and other driving related data, which is provided to our business clients for purposes of the business client providing you a service or product such as insurance, family or friendship groups or weather and traffic information, which may include providing some of those insights to you;
  - Providing functionality in Routely® or a business client mobile application, such as providing you with navigation services or information on how to improve the safety of your driving;
  - Providing you with towing and repair options or contacting emergency personnel;
  - Providing you offers for products and services that may interest you based on your location and driving habits.

- **Conduct analytics and research.** We also use personal information to conduct research and analysis for purposes of product development, enhancement or improvement to products and services or for other reasons in the public interest. Where possible, we use deidentified information for model development and analytics and have implemented practices to limit the use of personal information for analytics purposes.
- **Targeted advertising.** We use personal information, including device identifiers, to create segments of similar individuals to help advertisers serve you interest-based advertising based on geolocation information, insights derived from driving behavior, and demographic information. We use this data to serve ads through our advertising platform and measure the effectiveness of advertising campaigns. Note that Arity does not collect or use personal information from the Routely® app, insurance provider apps or from individuals in certain jurisdictions to serve targeted ads; however, Arity may collect personal information such as device identifiers, demographic information, or inferences from other non-insurance related business clients or other data providers for this purpose.
- **Improve, develop and analyze our websites.** We use personal information to analyze, improve, develop or deliver our website using algorithms, analytics software and other similar methods and analyze how visitors use our website to improve the website and enhance and personalize your experience. We collect some information used for these purposes using analytics software, cookies and other tracking technologies. For more information about the collection and use of this information, see **Your Privacy Choices**.
- **Communicate with you about your service, feature or product.** We may use your personal information to communicate with you about a service, feature or product, respond to customer service requests, or to investigate, respond to, and resolve issues or complaints or other inquiries. We may also provide you confirmations or other service or product related messages. Communication may be via text, email or other available methods such as push notifications.
- **Provide marketing communications.** We may use your personal information to serve you ads or customized content on the internet, send you promotional communications about products, services, features, and options we believe may be of interest to you. We may send communications via email or other methods.
- **Comply with legal requirements and protect the safety and security of our business, services, and sites.** We may use your personal information to comply with laws, regulations or other legal obligations, to assist in an investigation, to protect and defend our rights and property or the rights of third parties or enforce terms and conditions. We may also use your personal information to prevent suspected fraud, threats to our network or other illegal activities, prevent misuse or for any other reason permitted by law. We may use your personal information to protect our company, our affiliates, our customers, our network and our websites and mobile apps.

Update or correct our records. We may use personal information collected about you from you or other sources, including publicly available databases or third parties from whom we have purchased data to update our records.

Business client's use of information

Arity shares your information with its business clients as part of your purchase, or use, of services from those business clients. Those business clients include, but are not limited to, insurance companies as well as mobile app providers who track the location of members of a defined group or who provide weather related information. If you have purchased an insurance product offered by an Arity business client, then your information may also be used by that business client to calculate insurance rates or rewards provided under the product or service. Our insurance company business clients may also use your information to update their pricing and underwriting models. All such use of your personal information by our business clients is subject to their privacy policies and not this Privacy Statement.

Sharing your information

We may share personal information about you for several reasons and with different parties including with service providers and other third parties. We may also share your personal information with our affiliates for business purposes consistent with the uses described in this Privacy Statement.

For all personal information that can reasonably be aggregated or deidentified, Arity will take steps to do so before sharing with unaffiliated third parties. This means that we will take steps to alter that personal information such that it cannot reasonably be used to identify you or relate the information back to you. For any personal information that cannot be completely aggregated or deidentified, we take steps to modify the information before sharing to remove information such as name, account number, address, or unique vehicle identifiers when possible. Before sharing such deidentified or modified information with unaffiliated third parties, Arity contractually prohibits third parties from taking any steps to reidentify the data or relate any deidentified personal information back to you and also contractually limits the purposes for which they can use the information. In some cases, we may share personal information such as your name, address, and contact information with third parties at your direction for the purposes of obtaining insurance quotes. When we share information, we strive to work with companies that share our commitment to privacy.

We may share your personal information for business purposes or as required or permitted by law with:

- **Business clients:** We share your personal information with our business clients through which you receive Arity's features, products or services. For example, when using our Routely® mobile app or a business client's mobile app that has Arity's technology embedded, information is shared with our business client for purposes of servicing the product or service you have requested from that business client. If you are using our Routely® mobile app as a driver relative to your employer's usage-based commercial insurance policy, information may be shared with your employer. We may also share your contact information provided via one of our websites with our business clients so that they may contact you to offer their products and services.
- **Service providers to Arity:** Personal information may be shared with service providers who perform services on our behalf for a business purpose including service providers that:
    - provide marketing and advertising, email or other communication services;
    - provide services that support our online activities including providing tracking technologies, web hosting and analytics;
    - provide tax and accounting, legal services, delivery, and data enhancement services;

    - provide technology services and enhance security, privacy and fraud protections;
    - provide analytics services or conduct research or actuarial studies; and
    - provide support to our operations.
- **Marketing and advertising partners**: On certain websites, Arity permits third party online and other marketing and advertising partners to collect information from you directly to facilitate online advertising of Arity's services. See the "Cookies and other tracking technologies and settings" section below for more details about these activities.
- **Third parties in connection with a business transaction:** Personal information may be disclosed to third parties in connection with a corporate transaction, such as a merger, sale of any or all of our company assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by an affiliate or third party, or in the event of a bankruptcy or related or similar proceedings.
- **Law enforcement, regulators and other parties for legal reasons:** Personal information may be disclosed to third parties, as required by law or subpoena, or if we reasonably believe such action is necessary to:
    - comply with the law and the reasonable requests of regulators, law enforcement or other public authorities;
    - protect our or others safety, rights or property; and
    - investigate fraud or to protect the security or integrity of our websites and mobile apps or any product or services.

We share the following categories of personal information with the following parties:

- **Geolocation data:** Business clients; Service providers to Arity; Law enforcement or regulators; Third parties in connection with a business transaction.
- **Personal identifiers:** Business clients; Service providers to Arity; Marketing and advertising partners; Law enforcement or regulators; Third parties in connection with a business transaction.
- **Personal characteristics:** Law enforcement or regulators; Third parties in connection with a business transaction.
- **Commercial and service related information:** Business clients; Service providers to Arity; Law enforcement or regulators; Third parties in connection with a business transaction.
- **Internet or other electronic network activity information (including mobile app information):** Business clients; Service providers to Arity; Marketing and advertising partners; Law enforcement or regulators; Third parties in connection with a business transaction.

Inferences: Business clients; Service providers to Arity; Marketing and advertising partners; Law enforcement or regulators; Third parties in connection with a business transaction.

Retention of personal information

We retain personal information in accordance with applicable laws or regulatory requirements and also for as long as necessary to fulfill the purposes for which it was collected and to fulfill the business or commercial purposes that are explained in this Privacy Statement. Refining and developing statistical models relies on information collected over a long period of time, and this information is stored until it is no longer needed to provide products or services to you and to develop and refine our models. Where possible, we keep this information in a pseudonymized format. We retain Mobile Ad IDs and geolocation information used to serve targeted advertising for up to 3 years

from the date of collection. When no longer needed, we delete or deidentify the personal information. We review our data retention policies periodically and comply with local legal requirements.

Privacy practices for select Arity products

Targeted advertising service: Arity collects geolocation and driving behavior data, and we may use that information to link driving behavior information to device identifiers, demographic information or other personal information to help serve targeted advertising and measure advertising effectiveness. Learn how to opt out of targeted advertising including by opting out of the sharing or selling your personal information by visiting **Your Privacy Choices** .

Arity is a member of the Network Advertising Initiative (NAI), and we adhere to the NAI Codes of Conduct. To learn more about the NAI and the Code of Conduct please visit **The NAI Code of Conduct**.

Arity IQ℠ network: Arity Services, LLC, is a consumer reporting agency regulated by the Fair Credit Reporting Act (FCRA) that delivers an Arity driving score or driving behaviors to an insurance company for its use in providing you with insurance quotes, rating, and underwriting. We furnish personal information to Arity Services, LLC, which uses the data to create a consumer report. With your consent and upon your request, Arity Services, LLC will share this consumer report with an insurance company. For information on your rights under FCRA relating to this product including how to submit a consumer request, visit the **Arity Services Data Support Center**.

Cookies and other tracking technologies and settings

Tracking Technologies used online: When you visit certain Arity websites or use our mobile apps, we, our third party marketing and analytics providers operating, may automatically collect information about your use of and access to these websites and mobile apps using a variety of tracking technologies, including cookies, Flash objects, web beacons (also called “clear GIFs” or pixel tags), embedded scripts, location-identifying technologies, analytics, remarketing and similar technology (collectively, “tracking technologies”).

We and our third-party marketing and analytics providers (such as Google Analytics, Adobe Analytics, Meta, Microsoft and DemandBase) use these tracking technologies to help us provide users with an enhanced and more customized web experience. Additionally, we and our marketing and analytics providers use tracking technologies, analytics, and other technologies to monitor visits to our websites. This information may also be combined or linked with personal information we collect directly from you. The information collected in this manner includes:

- The websites which linked you to, or away from, our websites, how frequently you visit the websites, your interaction with emails we send, pages you visit on our websites, and the ads you view, or your location when you access our websites, recordings of mouse clicks, mouse movements, keystrokes, and other communications you make on our sites;
- Information about the computer, tablet, smartphone or other device you use, such as your IP address, browser type, internet service provider, platform type, device type/model/manufacturer, operating system, date and time stamp, unique device identifiers or advertiser ID, and other similar information, and
- Analytics information collected by us or via third-party analytics tools, to help us measure traffic and usage trends for the websites and to understand more about the demographics and behaviors of our users.

For additional details about how we use cookies and other tracking technologies, including how not to accept cookies, see **Your Privacy Choices**.

Use of the information: The information collected through tracking technologies allows us to provide you with an improved, enhanced and personalized customer experience,

to monitor and improve our website and for other internal purposes such as:

- Provide custom, personalized content and information, including targeted content across other mobile applications and websites, communications and advertising,
- Identify and contact you across multiple devices,
- Provide and monitor the effectiveness of our sites,
- Perform analytics and detect usage patterns on our sites,
- Diagnose or fix technology problems,
- Detect or prevent fraud or other harmful activities, and
- Otherwise to plan for and enhance our sites.

Your choices regarding cookies: For our sites containing cookies or pixels that enable targeted advertising, you may update your cookie preferences by accessing the “Cookie Settings” link within that site’s **Your Privacy Choices.** You may also opt-out by enabling a universal tool that automatically communicates your opt-out preferences through browser settings such as the Global Privacy Control (“GPC”). All website visitors, regardless of residency, can opt-out of this sharing. Most browsers will also allow you to manage cookies in your browser settings to disable or block cookies, remove existing cookies, automatically accept cookies or to notify you when you receive a cookie. These settings are browser or device specific, and options available may vary by browser. However, if you disable, modify, or reject cookies, some parts or functionalities of our site may be inaccessible or not function properly. For example, disabling cookies may require you to repeatedly enter information to take advantage of services or promotions. Also, if you clear your cookies on your browser or make selections using a different device or browser, you may need to redo your cookie settings.

Some browsers offer a setting called “Do Not Track.” Although we do our best to honor the privacy preferences of our visitors, we may not be able to respond to all “Do Not Track” signals from your browser.

Collection of information from mobile devices: Geolocation and other driving behavior information is collected via mobile apps only when Location Services is enabled on your device. Other permissions through the operating system of your device may also be required for our services or products to function properly. If enabled, our Routely® mobile app or our business client’s mobile app may collect location data in the background of your device in order to understand your driving behaviors even while you are not engaging with the Routely® app or our client’s mobile application. Disabling the location services functionality on your mobile device may impact your app’s services.

Privacy rights and choices

You have specific rights under certain state privacy laws. These rights differ by state and by the type of products and services you have with Arity. For example, rights under certain state laws do not apply to personal information that is regulated by the Fair Credit Reporting Act.

California, Connecticut, New Hampshire, Texas, Oregon, and Virginia Residents

California residents have rights to access, correct, and delete their personal information as well as other rights described below. Similar rights exist for Connecticut, New Hampshire, Texas, Oregon, and Virginia residents.

Right to know and access your personal information: You have the right to request the specific pieces of personal information we have collected about you and the right to know:

- the categories of personal information collected;
- the categories of sources from which personal information was collected;
- the business purpose for collecting the personal information, and

- the categories of third parties with whom we disclose or share personal information.

Right to deletion of personal information: You have the right to request we delete the personal information collected about you, subject to certain exceptions including that we need the personal information to:

- Complete a transaction or provide a good or service you requested, or take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- Debug products to identify or repair errors that impair functionality;
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law;
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
- Comply with a legal obligation, or
- Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

Right to correct personal information: You have the right to request we correct any inaccurate information we have about you. We may request that you provide documentation to support your request and we will correct your information unless we determine that the personal information is more than likely accurate.

Non-discrimination rights: We don't discriminate against you if your exercise any of the privacy rights described in this privacy statement.

Submitting a request: To submit a request, visit our **online webform** or call us at 1-800-654-1412. Responses to a verified request may take up to 45 calendar days, or longer depending on the nature of the request. If additional time is needed, we will notify you of the additional time. We may only respond to two access requests within a 12-month period.

Connecticut, New Hampshire, Texas, Oregon, and Virginia residents: If we are unable to fulfill your request to access, review, delete or correct your personal information, we will respond to you explaining why. If you would like to appeal for additional review of our inability to fulfill your request, visit our **appeals webform**.

Sharing or sale of personal information: We do not sell personal information for monetary value. For our Targeted Advertising Service, we utilize personal information such as device identifiers to provide you with relevant, targeted advertising, build advertising models and monitor the effectiveness of advertising campaigns. We do not disclose personal information to third parties as a part of this service without your consent. On some Arity websites, we allow third-party pixels and other tracking technology which enables the sharing of personal information about website users with third parties for the purpose of serving you interest-based advertising. This sort of online advertising is called cross-context behavioral advertising under the California Consumer Privacy Act (CCPA) or targeted advertising under other state laws.

CCPA provides California residents the right to opt-out of the "sharing" of your information for cross-context behavioral advertising. Connecticut, New Hampshire, Oregon, Texas, and Virginia residents have the right to opt out of the processing of personal data for the purposes of targeted online advertising. Regardless of where you live, you can learn how to opt out of this "sharing" for targeted advertising by visiting **Your Privacy Choices.**

Use and sharing of sensitive personal information: Arity uses sensitive personal information (precise geolocation data) and shares insights derived from that information for targeted online advertising. California residents have the right to limit this use of your

sensitive personal information. Regardless of where you live, you can learn how to limit this use by visiting **Your Privacy Choices**.

Consumer request metrics: The following lists the number of access, deletion, correction and data sale/share opt out requests Arity received, complied with and denied from residents of California in 2023 and the average number of days it took to complete a request. Please note that these metrics do not include requests made to our Business Clients.

2023 Data Access Requests	
Number of requests received	6
Number of requests complied with in whole or in part	0
Number of requests denied	6
Average days to complete a request	2

2023 Data Deletion Requests	
Number of requests received	30
Number of requests complied with in whole or in part	5
Number of requests denied	25
Average days to complete a request	3

2023 Data Correction Requests	
Number of requests received	0
Number of requests complied with in whole or in part	0
Number of requests denied	0
Average days to complete a request	0

2023 Data Sale/Share Opt Out Requests*	
Number of requests received	20,104
Number of requests complied with in whole or in part	20,104
Number of requests denied	0
Average days to complete a request	7

***Number includes all "CCPA Opt Out Tool" global opt out requests received by the DAA's AppChoices tool.**

Social media, links, and external sites

Links to other companies' websites may be provided on the Arity website as a convenience to you. If you choose to go to these external websites, you will be subject to the privacy practices of those external websites; Arity is not responsible for the privacy practices of those websites. We encourage you to be aware when you leave our website to read the privacy policies or statements of every website you visit, as those privacy policies or statements may differ from ours.

Our website includes Social Media Features, such as the Facebook "Like" button and Widgets, the Share This button or interactive mini-programs that run on our website. These features may collect your IP address, which page you are visiting on our website, and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our website. Your interactions with these features are governed by the privacy policy of the company providing it.

Security

We recognize the importance of keeping your personal secure. We use a combination of reasonable technical, administrative, and physical safeguards to protect your personal information. However, no website, mobile application, database or system is completely secure or "hacker proof". So, we cannot guarantee its absolute security. You are also responsible for taking reasonable steps to protect your personal information against unauthorized disclosure or misuse.

We limit access to your personal information to those who need it to do their jobs. We comply with all applicable federal and state data security laws.

Children's personal information

We do not knowingly gather personal information or market products or services to children under the age of sixteen. If we become aware that we have collected personal information from a child without the required parental consent, we will make reasonable efforts to delete such data from our records.

Specific information for users in the EU, UK, EEA, and Switzerland

This section applies to personal information (referred to in this section as personal data) collected from users in the European Union (EU), the European Economic Area (EEA), United Kingdom (UK) or Switzerland or otherwise subject to the General Data Protection Regulation (GDPR).

Our legal basis for processing: For personal data that we process in connection with any products or services we offer to you or our business clients, we will generally process that personal data (i) based on consent, (ii) in order to take steps at your request, or (iii) for our legitimate interests in providing our services to you or otherwise in supporting the business needs.

Your Access and Choices: You may have the following rights in relation to your personal data:

- Rectify any inaccurate personal data that we hold about you;
- Have your personal data erased under certain circumstances;
- Have the processing of your personal data restricted where you dispute its accuracy, if you think its processing is unlawful, if you otherwise object to its processing, or when we no longer need your personal data and you need it in relation to a legal claim;
- Have access to your personal data, and the right to receive copies of your personal data in a structured, commonly used and machine-readable format and transfer those copies to another data controller, under certain circumstances;
- Complain to your national data protection regulator if you feel that any of your personal information is not being processed in accordance with the GDPR.

To exercise your rights to access, rectify or erase your personal data, you can submit a request to privacy@arity.com.

Use of your personal data for analytics and profiling: 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.

However, we take steps to remove all personal data that is not necessary to the predictive driving models. So, while your Driving Score incorporates your GPS location data, it will not be directly connected to your name, contact information, or vehicle information unless we have obtained your explicit consent to do so in advance.

In addition, we do not do any of the following without obtaining your prior explicit consent to do so:

- Use personal data or Driving Scores to make automated decisions that have significant effects for individuals, because individuals are not identifiable within the

data set;

- Use any insights, model output, or Driving Scores with personal data for any purpose other than internal analytics or our predictive driving models; or
- Use your profile or Driving Score to advertise to you.

After pseudonymizing the Driving Scores, we may share the pseudonymized Driving Scores with business clients. Please refer to the business client's privacy notices for the products and services you have elected to use for details about their privacy practices. Other than sharing pseudonymized Driving Scores with business clients, we do not share Driving Scores with third parties, unless we are required pursuant to lawful legal process.

Your Driving Score will in no way impact the availability or your use of our products or services.

Your right to withdraw consent: If you withdraw your consent, we will stop processing the relevant personal data except to the extent we have other grounds for processing under applicable laws. We will respond to your request within a reasonable timeframe. You may withdraw your consent at any time; however, Arity will not be able to provide or continue to provide products or services to you.

There may be cases where restrictions on the amount of data that can be disclosed to data subjects under applicable law (for example, if that would necessarily involve disclosing data about another person). Arity is permitted to withhold some types of personal data in certain circumstances, subject to applicable local law requirements. If there is a dispute, please contact us using the information in the "Contact Us" section. In addition, data subjects have the right to lodge a complaint with a supervisory authority. The name and contact details of the supervisory authorities in the European Union can be found at **http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm**.

Contact us: For questions about the collection of personal data by Arity, or to exercise the right to access, correct, update, or delete such data or object, for legitimate purposes, to the processing of personal data, as provided under applicable law, please contact us at:

For users in the UK:
Arity
Attn: Data Protection Representative
10 Mays Meadow
Belfast, Country Antrim, BT1 3PH
Northern Ireland

For users in the EU, EEA, and Switzerland:
Email: **eurep@arity.com**

Please note: When sending inquiries to us, we may need additional information such as the business client you have engaged for which we collected data to better assist you.

Personal data transfers: Transfers of personal data outside of the EU, UK or EEA must meet certain legal requirements. Arity relies on Standard Contractual Clauses that have been approved by the European Commission to comply with these requirements. Under the GDPR, Arity acts as data controller with respect to such transfers. Arity also ensures it uses corresponding Standard Contractual Clauses with any vendor that it engages in connection with the processing of any of your personal data that is subject to these transfer requirements.

EU-U.S., Swiss-U.S. Privacy Shield, and UK Extension Data Privacy Framework: Arity complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Arity has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Arity has certified to the

U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit **https://www.dataprivacyframework.gov/**

Accountability for onward transfer: Where Arity transfers personal data as provided above to a third party, we will do so consistent with the notice provided to you and any consent provided (if applicable), and contractually require the third party to process the personal data for limited and specified purposes consistent with the lawful basis for processing, and provide us notice of any concerns with its ability to comply with these promises. We will also contractually require the third party to stop processing personal data or take other reasonable and appropriate steps to in the event it cannot meet its data protection obligations. Arity remains liable under the DPF Principles where any third-party service provider processes personal data subject to its DPF certification in a manner inconsistent with the Principles, except where Arity is otherwise not responsible for the event giving rise to the damage.

Recourse, enforcement and liability: Arity's participation in the DPF Frameworks is subject to investigation and enforcement by the Federal Trade Commission. Arity commits to address inquiries, requests to exercise your rights under applicable law, or resolve complaints about our collection or use of your personal information. In compliance with the DPF Principles, after you have contacted us at the email below, if we are unable to resolve your concerns, Arity has further committed to refer unresolved privacy complaints under the DPF Principles to an independent dispute resolution mechanism. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at **https://feedback-form.truste.com/watchdog/request**. Further, under certain circumstances, data subjects may also be able to involve binding arbitration before the DPF Panel to be created by the U.S. Department of Commerce and the European Commission. Arity may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Contact us

If you should have questions or concerns about our privacy practices, please contact us through the below methods.

Please note: When sending inquiries to us, we may need additional information such as the business client you have engaged for which we collected data to better assist you.

For users in the U.S. and other users (outside of Switzerland, the UK, European Union, and EEA):

Email: **privacy@arity.com**

Mail: Arity
Attn: Data Protection Officer
PO Box 227238
Dallas, TX 75222-7238
United States of America

For users in the United Kingdom:

Arity
Attn: Data Protection Representative
10 Mays Meadow
Belfast, Country Antrim, BT1 3PH
Northern Ireland

For users in the European Union, EEA, and Switzerland:

Email: **eurep@arity.com**

To request that you no longer receive business-related promotional e-mails from Arity, please email us at **info@arity.com.**

If you opt out from receiving marketing emails, we may still send you transactional, non-marketing emails such as emails about your products or services, responses to your requests and inquiries, or notices of updates to terms and conditions or our privacy practices.

Changes to this Privacy Statement

We may periodically update or revise this Privacy Statement. The effective date at the top of the document shows when this Privacy Statement was last revised. We will let you know when we update the Privacy Statement by changing the date or other appropriate means.