202-3088

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of

INMARKET MEDIA, LLC,
a limited liability company.

COMPLAINT

The Federal Trade Commission, having reason to believe that InMarket Media, LLC, a limited liability company ("Respondent"), has violated the provisions of the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent InMarket Media, LLC ("InMarket"), is a Delaware limited liability company with its principal office or place of business at 111 Congress Avenue, Suite 500, Austin, TX 78701.

2. The acts or practices of Respondent alleged in this Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondent's Business Practices

3. Respondent InMarket is a digital marketing platform and data aggregator. It collects consumer location data through its software development kit (the "InMarket SDK") and also purchases consumer information from other sources. InMarket obtains large swaths of personal data on consumers—including information about their movements over time tracked on their mobile devices, as well as their purchasing history, and demographic and socioeconomic backgrounds—and has kept that information for up to five years. Respondent uses the consumer data to facilitate targeted advertising to consumers on their mobile devices for the company's clients, which include brands and advertising agencies. InMarket displays this advertising itself using the InMarket SDK, and also categorizes consumers into groups called "advertising audiences" that enable its clients to target

consumers more precisely on third-party advertising platforms. Respondent fails to notify consumers that their location data will be used for targeted advertising and fails to verify that mobile applications ("apps") incorporating the InMarket SDK have notified consumers of such use.

Respondent collects consumer location data through its SDK.

4. Respondent created the InMarket SDK, which is a collection of development tools that can be incorporated into a mobile application. Respondent incorporates the InMarket SDK into the two apps that it owns and operates: CheckPoints, which offers shopping rewards for completing tasks such as watching videos and taking online quizzes, and ListEase, which helps consumers create shopping lists (the "InMarket Apps"). The InMarket Apps have been downloaded onto over 30 million unique devices since 2017. Respondent also makes the InMarket SDK available to third party app developers, and it has been incorporated into more than 300 such apps which have been downloaded onto over 390 million unique devices since 2017. App developers are incentivized to incorporate the InMarket SDK into their app because they receive a portion of InMarket's advertising revenue from each ad served through their apps.

5. One of the primary functions of the InMarket SDK is to transmit a consumer's precise location back to Respondent. Apps that incorporate the InMarket SDK request access to the location data generated by a mobile device's operating system. If the user allows access, the InMarket SDK receives the device's precise latitude and longitude, along with a timestamp and a unique mobile device identifier, as often as the mobile device's operating system provides it— ranging from almost no collection when the device is idle, to every few seconds when the device is actively moving—and transmits it directly to Respondent's servers. From 2016 to the present, about 100 million unique devices sent Respondent location data *each year*.

6. Through the InMarket SDK, Respondent collects sensitive information from consumers, including where they live, where they work, where they worship, where their children go to school or obtain child care, where they receive medical treatment (potentially revealing the existence of medical conditions), where they go to rallies, demonstrations, or protests (potentially revealing their political affiliations), and any other information that can be gleaned from tracking a person's day-to-day movements. All of the above information is collected along with several identifiers (including a unique mobile device identifier). Respondent has retained this information for up to five years.

Respondent uses location data to engage in targeted advertising through its SDK and to create advertising audiences for use on third-party advertising platforms.

7. Respondent processes the location data it collects so that it can determine how long a particular mobile device (and therefore a particular consumer) stays at a given location. All data collected through the SDK is processed together, meaning that InMarket may use data from multiple apps to determine when a particular consumer arrived at a particular location, how long she stayed there, and when she left.

8. Respondent cross-references consumers' location histories with advertising-related points of interest to identify consumers who have visited those locations. Respondent sorts consumers, based on their visits to points of interest, into audience segments to which it can target advertising. Respondent has created or maintains almost two thousand distinct advertising audience segments. For example, an InMarket brand client can target shoppers who are likely to be low-income millennials; well-off suburban moms; parents of preschoolers, high-school students, or kids who are home-schooled; Christian church goers; convenience-sensitive or price- sensitive; single parents or empty-nesters; affluent savers or blue collar workers; "healthy and wealthy" or "wealthy and not healthy," to name only a selection of the categories InMarket offers or has offered to its brand clients.

9. InMarket classifies audiences based on both past behavior and predictions it makes about consumers based on that behavior. For example, if a consumer's past location data shows that she has visited a car dealership, InMarket can combine that information with the consumer's attributes purchased from other sources (age, income, family structure, education level), and can potentially predict that she may be in the market for a certain type of vehicle.

10. The InMarket SDK displays the ads and determines which ads appear in which apps incorporating the SDK. Respondent additionally offers advertisers a product that sends push notifications based on a consumer's location and "geofencing," the creation of a virtual fence around a particular point of interest. When the InMarket SDK transmits a location that is inside a virtual fence, the app will send a push notification for a particular ad. For example, a consumer who is within 200 meters of a pharmacy might see an ad for toothpaste, cold medicine, or some other product sold at that location.

11. Respondent also makes its advertising audience segments available on real-time bidding platforms. An advertiser using one of these platforms can select an advertising audience, and identify the amount that it is willing to pay (that is, its bid) each time its ad appears on a mobile device that is a part of that audience. The advertiser's ad will appear on a particular device if it has the highest bid for that device. Respondent receives some revenue each time an advertiser uses one of its audiences in this process.

Respondent fails to notify users of its own apps that their location data will be used for targeted advertising.

12. Before an app can access a mobile device's location data, the mobile device user must grant access in a system prompt generated by the device's operating system. Despite collecting vast amounts of consumer location and other data for consumer advertising and targeting purposes, InMarket does not fully disclose such collection and use in the system prompts seeking a user's consent to location collection or in-app screens that precede the prompt. InMarket fails to obtain informed consent in its proprietary apps, CheckPoints and ListEase, and also fails to verify the third-party apps that incorporate InMarket's SDK obtain informed consumer consent.

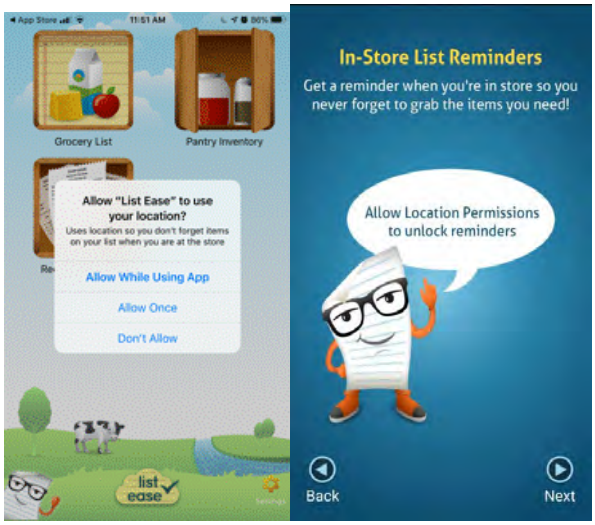
13. Since 2010, InMarket has offered the CheckPoints app on both the iOS and Android platforms. InMarket's CheckPoints app is marketed as a "rewards app," and promises users

"easy money—earn as you shop." It tells consumers to "join the millions earning free gift cards and more every day." Users of the app collect points by performing various tasks (checking into retail locations, watching videos, scanning certain products while in store, taking surveys and quizzes), and then exchange those points for rewards, such as gift cards. The app is free to download and includes in-app advertising.

14. From at least 2017 through 2020, as required by iOS and Android, CheckPoints requested users' permission to collect their precise location information. For iOS users, CheckPoints stated: "Allow CheckPoints to access your location? This allows us to award you extra points for walking into stores." CheckPoints consent screen inquired of Android users: "CheckPoints finds nearby earning opportunities by using your device's location," and then asks users to "Enable Location Services."

15. Since 2012, InMarket has offered the ListEase app on both the iOS and Android platforms. The ListEase app markets itself as an electronic shopping list app. The app is free to download and includes in-app advertising.

16. From at least 2017 through 2020, as required by iOS and Android, ListEase has requested users' permission to collect their precise location information. ListEase's iOS consent screen stated the following: "Allow ListEase to use your location? Uses location so you don't forget items on your list when you are at the store." For Android devices, ListEase stated, "Allow Location Permissions to unlock reminders. Get a reminder when you're in the store so you never forget to grab the items you need!"



17. The consent screens used for both the CheckPoints and ListEase apps tell consumers that their location will be used for the app's functionality (earning points and keeping lists), which are misleading half-truths. At no point during the consent process for either the CheckPoints or ListEase Apps did InMarket also disclose that it was collecting users' precise location, often multiple times per hour, along with data collected from multiple other sources—including through other apps using the InMarket SDK—to build extensive profiles on users to be used to precisely target them with advertising.

18. Although InMarket discloses in its privacy policy that it uses consumer data for targeted advertising, its consent screen does not link to the privacy policy language, and the misleading prompts do not inform consumers of the apps' data collection and use practices.

19. Representations related to use of consumers' location information for advertising and tracking are material to consumers.

Respondent fails to verify that users of third-party apps incorporating InMarket's SDK have been notified that their location data will be used to target advertising.

20. In addition to not disclosing its data collection practices in its proprietary apps, InMarket also does little to verify that third-party apps incorporating its SDK obtain informed consumer consent before granting InMarket access to their sensitive location data. InMarket additionally neither collects nor retains records of the disclosures that third-party apps incorporating the InMarket SDK provide consumers before accessing their location data.

21. In fact, InMarket does not require the third-party apps that incorporate its SDK to obtain informed consumer consent. Aside from general guidelines requiring the app developers to "comply with all applicable laws," and to maintain a "privacy policy in line with legal requirements," InMarket's contract with the developers requires nothing more from them in terms of privacy.

22. Even if these third-party app developers wanted to provide adequate disclosure to their users about InMarket's use of their location data, InMarket does not provide the developers with sufficient information to provide that notice. Specifically, InMarket's contract with third-party app developers merely states that InMarket will serve ads on the developer's apps in return for developers passing user information to InMarket, including precise location and advertising identifiers. InMarket does not disclose that information collected from these third-party users will be supplemented and cross-referenced with purchased data and analyzed to draw inferences about those users for marketing purposes. Nor does it disclose to these app developers that it retained their users' location information for up to five years. Moreover, although InMarket's privacy policy generally describes its use of consumer data for advertising purposes, InMarket does not even reference this privacy policy in its third-party developer agreements.

23. InMarket therefore does not know whether users of hundreds of third-party apps that incorporate the InMarket SDK were informed of their data being collected and used for targeted advertising. In fact, several of these third-party apps seek users' location using incomplete and misleading disclosures that are similar to those that InMarket uses. For example, one photo- editing app that incorporates InMarket's SDK seeks location permission with the prompt: "Your location is used to provide you with rewards and discounts when you visit retail partners." Based on this disclosure, a consumer may believe that her location data will be used for this one purpose and used solely by the photo-editing app itself. The consumer would never know, based on the above disclosure, that her location will be collected multiple times per day (whether or not she was near the app's retail partner) and that her movements will be shared with third parties like InMarket, who will then purchase additional data about her in order to create her detailed consumer profile. The consumer would never know that, by granting location permission to a photo-editing app, she actually set into motion a string of data collections that enabled InMarket, a third-party she likely never heard of, to amass a mountain of sensitive data about her without her knowledge.

24. Because InMarket readily combined the location data of those users into its databases and systems without confirming user consent, InMarket obtained and used that data without informed user consent, resulting in likely consumer injury, as discussed below.

Respondent retains consumer data longer than reasonably necessary for its business purposes leading to likely consumer injury.

25. After collecting sensitive precise location data about consumers' daily movements, InMarket retains that information longer than reasonably necessary to accomplish the purpose for which that information was collected and thereby exposes consumers to significant unnecessary risk. Specifically, InMarket has retained consumer location data for five years prior to deletion.

26. This unreasonably long retention period—far longer than is necessary to accomplish InMarket's stated purpose for collection (to allow a consumer to earn shopping points or make shopping lists)—significantly increases the risk that this sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing sensitive information

about that consumer's life.

27. InMarket's comprehensive collection and long-term retention of location data subjects consumers to a likelihood of substantial injury through the exposure of their re-identified location.

Violations of the FTC Act

28. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

29. Misrepresentations or deceptive failures to disclose a material fact constitute deceptive or unfair practices prohibited by Section 5(a) of the FTC Act.

30. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that are not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45 (n).

Count I
Unfair Collection and Use of Consumer Location Data

31. As described in Paragraphs 4-6, 12-19, Respondent collects consumers' location data through apps that it owns and operates while failing to notify consumers that it uses the data to develop consumer profiles and target them with advertising.

32. Respondent's collection of location data without disclosure of intended uses results in substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers and an increased risk of disclosure of such sensitive information. This injury is not reasonably avoidable by consumers themselves, as they are not aware of the scope of these practices. This injury is also not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's collection of consumers' location data through apps that it owns is an unfair act or practice.

Count II
Unfair Collection and Use of Consumer Location Data from Third Party Apps

33. As described in Paragraphs 4-6, 20-24, Respondent collects consumers' location data through third-party apps that incorporate its SDK without taking reasonable steps to verify that consumers are notified that it uses the data to develop consumer profiles and target them with advertising.

34. Respondent's collection of location data without verification of notification results in substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, and an increased risk of disclosure of such sensitive information. This injury is

not reasonably avoidable by consumers themselves, as they are not aware of the scope of these practices. This injury is also not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's collection of consumers' location data through third- party apps is an unfair act or practice.

Count III
Unfair Retention of Consumer Location Data

35. As described in Paragraphs 25-27, Respondent has retained detailed, sensitive information about consumers' movements for five years, which is longer than reasonably necessary to effectuate its business purpose.

36. Respondent's retention of detailed location data for such an extended period has caused or is likely to cause substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, and an increased risk of disclosure of such sensitive information. This injury is not reasonably avoidable by consumers themselves, as they are not aware of the scope of these practices. This injury is also not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's retention of consumers' detailed location data for longer than is reasonably necessary to effectuate its business purpose is an unfair act or practice.

Count IV
Deceptive Failure to Disclose InMarket's Use of Consumer Location Data

37. As described in Paragraphs 12-18, Respondent represented, directly or indirectly, expressly or by implication, that CheckPoints and ListEase app users' location information would be used for awarding extra points for walking into stores or list reminders.

38. In fact, as set forth in Paragraphs 4-11, since at least 2017, InMarket has been using location data collected from CheckPoints and ListEase users for targeted advertising, has supplemented that information with additional data purchased about those users, has shared that information with third parties for the purpose of advertising, and has used that information to develop predictions about consumer behavior and characteristics. These facts would be material to consumers in deciding whether to use or grant location permissions to InMarket's apps.

39. InMarket's failure to disclose material information described in Paragraph 38, in light of the representations set forth in Paragraph 37, is a deceptive act or practice.

Violations of Section 5

40. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 2023, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL: