IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MAPLEBEAR INC. d/b/a INSTACART, a Delaware corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING AND OPERATING A MALICIOUS APPLICATION KNOWN AS SHOPPER HELPER, Defendants.	Civil Action No: 1:21-cv-00474 (AJT/IDD)

DECLARATION OF LIKE LIU IN SUPPORT OF INSTACART'S MOTION FOR CONTEMPT SANCTIONS, OR IN THE ALTERNATIVE FOR ISSUANCE OF AN ORDER TO SHOW CAUSE RE CONTEMPT AGAINST JOHN DOES 1-2 AND LIMITED EXPEDITED DISCOVERY

I, Like Liu, declare as follows:

1. I work for Maplebear Inc. dba Instacart ("Instacart") as a Staff Software Engineer. I have worked as a software engineer at Instacart since April 2022. I make this declaration in support of Instacart's Motion For Contempt Sanctions, Or In The Alternative For Issuance Of An Order To Show Cause Re Contempt Against John Does 1-2 And Limited Expedited Discovery. I make this declaration of my own personal knowledge or on information and belief where indicated and based on my review of records Instacart maintains in the ordinary course of business.

I. INSTACART'S SERVICES AND APPLICATIONS

A. Instacart's Customer Application and Shopper Application

2. Instacart operates a multi-sided technology and communications platform via the

Instacart website and its smartphone applications ("Instacart Platform") that facilitates fast on-demand grocery and retail delivery services by connecting customers who wish to purchase grocery items from Instacart's local retail partners with personal shoppers ("Shoppers") who will shop for and/or deliver the orders.

3. Customers can order groceries and other retail products through Instacart's website or through the Instacart customer mobile application. Accessing either the website or the app, customers can select a local retailer where shopping and/or delivery is available by a Shopper.

4. Shoppers are independent service providers with whom Instacart enters into written agreements to perform services as independent contractors. To accept and fulfill customer orders, Shoppers use a mobile application, the Instacart Shopper App ("Shopper App") (available on Android or iOS devices), which is distinct from the Instacart customer app.

B. Access to Shopper App Data and Technical Countermeasures to Prevent Unauthorized Access

5. Instacart does not sell ownership rights, copyright, or other intellectual property rights to its Shopper App. Instead, Instacart's Shoppers must obtain a license, which grants Shoppers limited rights to install the Shopper App and to access and use the Shopper App, including accessing and viewing batches of orders, subject to Instacart's technical security measures.

6. Instacart's servers and information contained in the Shopper App (e.g., batches of orders) are not open to the general public. Rather, each call to Instacart's servers requires Instacart to authorize and permit the Shopper seeking to access Instacart's servers to view orders on the Shopper App. This is because Instacart's servers are protected by sophisticated defenses designed to prevent unauthorized access and abuse, and which

evaluate whether to grant each request made to Instacart's servers.

7. Instacart works hard to protect the integrity and security of its network and systems. Among other things, it employs an array of technological safeguards and barriers designed to prevent data scrapers, bots, and other automated systems from accessing and copying its data on a large scale or from accessing its systems without proper authorization.

8. Among other technical measures, Instacart deploys SMS verification and/or a password barrier to verify the user. When a user logs into the Shopper App, they are required to enter their password or request a temporary SMS verification number, which confirm the user's telephone number associated with their shopper profile. The information contained in Instacart's Shopper App (e.g., batches of orders) is behind this password or SMS verification barrier. This is a built-in security system that controls access to Instacart's servers and the orders managed by the Instacart Platform. Because the Shopper App is authentication protected, the general public is not authorized to access any data or information available on the Shopper App beyond the password or SMS verification barrier. This technical security measure controls the integrity and quality of the Shopper App and protects sensitive information from public disclosure in accordance with Instacart's license terms.

9. Another technical countermeasure that application developers can use to combat scraping or any unauthorized access to servers is through the use of security authentication tokens. An authentication token allows users to confirm their identity in order to access an application. Each time a user wishes to use a legitimate version of an application on a mobile device, the application will communicate with a server to verify a token. An authentication token is issued to the user's mobile device upon successful verification of

the user's credentials. If the user's profile cannot be verified as a user of a legitimate application, then the authentication server will not issue a token and the user will be unable to access the application. Once a token has been issued, that user can access the application for which the token has been issued. The user retains access to the application until the user logs out of the application.

10. As part of its technical countermeasures, Instacart deploys a security authentication token in order to prevent unauthorized access to Instacart's servers by unauthorized users or unauthorized applications. Each time a Shopper enters their credentials in the Shopper App, the Shopper's mobile device will connect with an authentication server to verify the Shopper's credentials. Once the Shopper's credentials have been verified, the Shopper can access the legitimate Shopper App and Instacart's associated servers. Each Shopper's access token will be disabled once the Shopper logs out of the application.

11. The Shopper App for mobile devices is available through Google Play or the Apple App Store. In order to serve as a Shopper, members of the public must download the Shopper App and create a Shopper account with an email and a mobile phone number. Shoppers who download the Shopper App and create an account must accept Instacart's Shopper Terms and Conditions ("Shopper App Terms"). This licensing arrangement, along with various technical means, is one of many ways Instacart protects the Instacart Platform from conduct that can threaten the integrity and reputation of Instacart and its users.

II. INSTACART SHOPPERS AND THE SHOPPER APP

A. Instacart's Shoppers

12. Shoppers are integral to the Instacart platform. Their role is at the core of Instacart's business and the services they provide are essential to its success. Without

enough Shoppers, customer confidence in their ability to receive fast and reliable deliveries would be compromised. Maintaining a positive relationship with Shoppers is essential to Instacart's success and it is committed to addressing issues that affect Shoppers' ability to use the platform.

13. Instacart has strived to create a platform and app that Shoppers can use to maximize the value they get from the platform while creating a level playing field for all Shoppers. Additionally, Instacart has worked to create an app that is easy for Shoppers to navigate, offering details about batches to help Shoppers choose whether to accept them. Instacart has safeguards in place to make sure more desirable batches are fairly distributed to Shoppers across the platform.

B. The Shopper App

14. The Shopper App is the primary way that Shoppers interact with Instacart. After accessing the Shopper App, the Shopper can indicate their availability to receive and accept orders at their discretion. The Shopper App provides an automated matching function to offer customer orders to Shoppers, using proprietary software. Orders are offered in "batches" consisting of one or more customer orders to be shopped and delivered together.

15. Instacart has developed complex algorithms to offer batches to available Shoppers, considering numerous factors including fairness to the Shoppers. Once the algorithm processes the batches, a Shopper can then review a list of the batches offered to them and accept or decline those batches based on criteria such as the size of the orders (i.e., number of items to shop), batch payment amount, and the location of the retailer of the goods.

16. The servers that support the functionality of the Shopper App and associated services are located in Northern Virginia. Instacart hosts its software and services that

support the Shopper App with Amazon Web Service's ("AWS") on servers located in the Northern Virginia region. AWS provides, in essence, a network of physical computer servers that store computer data for internet companies.

III. THE LUCKYBOT APP

17. LuckyBot is an unauthorized third-party mobile application that leverages Instacart's Shopper App's user interface and core functionality to enable users to improperly circumvent Instacart's Shopper App—and Instacart's algorithms that are thoughtfully designed to promote efficiency and fairness—and attempt to gain an unfair advantage in selecting order batches.

18. Once installed, LuckyBot runs certain scripts on Instacart's Shopper App that automatically snatch batches prior to other Shoppers.

19. Instacart has engaged Nisos Holdings, Inc., as a technical consultant to investigate the LuckyBot application. I refer the Court to the declaration of Vincas D. Čižiūnas for further information on other aspects of LuckyBot, including identified technical functionalities to circumvent Instacart's anti-circumvention technology and access batch information from Instacart's infrastructure without authorization.

IV. HARM TO INSTACART CAUSED BY THE LUCKYBOT APP

A. LuckyBot Causes Harm by Diminishing Confidence Among Shoppers in the Fairness of Instacart's Services

20. Through its misuse of Instacart's software, LuckyBot disrupts the distribution of batches among Shoppers. LuckyBot seeks to give its users an unfair advantage that harms legitimate Instacart shoppers. By circumventing Instacart's batch algorithm, the LuckyBot app can cause Shoppers using the legitimate Instacart Shopper App to miss out on opportunities for batches that would otherwise be available to them. This causes dissatisfaction with Instacart's Shopper App and services and diminishes Shopper

confidence in the Instacart Platform

B. LcukyBot Causes Harm by Making Unauthorized Changes To Instacart's Shopper App

21. LuckyBot inflicts damage on Instacart whose products and trademarks Defendants systematically misuse as part of LuckyBot's operations. For example, once LuckyBot is installed on a Shopper's mobile device, it compromises the underlying code of Instacart's Shopper App through the creation and operation of a counterfeit, adulterated version of the Shopper App. The compromised Shopper App does not appear any different to party viewing that app on the mobile device. Anyone viewing the LuckyBot app, thus, would think that the compromised Shopper App, in the form of LuckyBot , is developed and distributed by Instacart, despite the fact that it is the operators of LuckyBot that are compromising the Shopper App. This harms Instacart's reputation and goodwill among the public, and particularly among Shoppers who may incorrectly believe that LuckyBot is sanctioned, sponsored, or associated in some manner with Instacart.

22. LuckyBot's fraudulent app also harms Instacart's Shopper App's functionality by interfering with the batch selection process. For example, LuckyBot's users can configure Shopper Helper to crawl Instacart's batch end points and automatically select the batches of the highest dollar value. By automatically selecting batches, LuckyBot is making unauthorized changes to Instacart's Shopper App by systematically disrupting Instacart's algorithms for the batching process, rendering batches unavailable to genuine users.

C. LuckyBot Unauthorized Access to Instacart's Servers

23. Each time LuckyBot is launched, it accesses Instacart's Shopper App and misuses code, features and functionality of the Shopper App. The software and services that support Instacart's Shopper App are located on AWS infrastructure. Because LuckyBot contains and misuses code, features and functionality of Instacart's Shopper App, it is also

accessing without authorization Instacart's AWS servers, which are physical computers located in Northern Virginia.

24. Instacart's investigation into LuckyBot has consumed significant company time and resources. For example, Instacart engineers have spent considerable time analyzing LuckyBot, its technical architecture, and attempting to identify Lucky Bot's developers.

D. LuckyBot Causes Harm To Instacart's Reputation, Brands, and Goodwill With Its Shoppers and the Public

25. LuckyBot harms Instacart and Instacart's Shoppers by damaging Instacart's proprietary Shopper App installed on Shoppers' mobile devices. LuckyBot is specifically designed to infect and run on mobile devices equipped with Instacart's Shopper App. In fact, LuckyBot cannot operate unless the user has at some point downloaded the Instacart Shopper App and created an account. The Instacart Shopper App is licensed by Instacart to its users. Once the Shopper creates an account with Instacart's Shopper App, LuckyBot will leverage the Shopper's credentials (e.g., credential harvesting) in order to operate the counterfeit, adulterated version of the Instacart Shopper App.

26. Instacart devotes significant computing and human resources to combating bots like LuckyBot . Instacart, as a provider of the Instacart Shopper App, as well as other products, must also incorporate security features in an attempt to stop installation of LuckyBot and other bots. Instacart has expended significant resources to investigate and track the LuckyBot and Shopper Helper Defendants' illegal activities and to counter and remediate the damage caused by Shopper Helper and LuckyBot to Instacart, its Shoppers, and the general public.

27. LuckyBot irreparably harms Instacart by damaging its reputation, brands, and Shopper goodwill. Defendants physically alter and corrupt Instacart's Shopper App.

28. In effect, once altered and controlled by LuckyBot, the Instacart Shopper App

ceases to operate normally and becomes a tool for Defendants to conduct their unauthorized access to batch information on Instacart's servers and automated processes. Yet, they still bear Instacart's trademarks. This misleads Instacart's Shoppers and the public generally into wrongly believing that Instacart condones, facilitates or somehow is associated with the use of LuckyBot. Instacart has invested substantial resources in developing high-quality products and services.

29. LuckyBot and Defendants' injure Instacart and its reputation, brand, and goodwill because Shoppers subject to the negative effects of this automated and malicious application incorrectly believe that Instacart and Instacart's Shopper App are the sources of their inability to obtain order batches that otherwise would be available. There is a great risk that users may attribute imbalance and inability to receive select orders to Instacart and associate these problems with Instacart's products, thereby diluting and tarnishing the value of the Instacart trademarks and brands.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 19th day of April 2024, in Seattle, Washington.

Like Liu

Like Liu