**HUNTON ANDREWS KURTH LLP**
Ann Marie Mortimer (State Bar No. 169077)
amortimer@HuntonAK.com
Jason J. Kim (State Bar No. 221476)
kimj@HuntonAK.com
Jeff R. R. Nelson (State Bar No. 301546)
jnelson@HuntonAK.com
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627
Telephone: (213) 532-2000
Facsimile: (213) 532-2020

Attorneys for Plaintiff
FACEBOOK, INC.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

| | |
|---|---|
| FACEBOOK, INC., a Delaware corporation,<br><br>Plaintiff,<br><br>v.<br><br>ILIKEAD MEDIA INTERNATIONAL COMPANY LTD., CHEN XIAO CONG, and HUANG TAO,<br><br>Defendants. | CASE NO.: 3:19-CV-07971<br><br>**COMPLAINT; DEMAND FOR JURY TRIAL** |

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Plaintiff Facebook, Inc. alleges the following:

## INTRODUCTION

1. Beginning no later than 2016 and continuing until at least August 2019, Defendants ILikeAd Media International Company Ltd., Chen Xiao Cong, and Huang Tao participated in a deceptive advertising scheme targeting Facebook and its users. Specifically, Defendants deceived internet users into installing software for their internet browsers that contained malware along with a plugin or browser extension ("the malicious extension"). The malicious extension was available on the internet and was not installed as a result of visiting or using Facebook. After the victims self-compromised their browsers, the malware enabled Defendants to access their victims' Facebook accounts and takeover their ad accounts, a practice known as "account take over fraud." Defendants then used the accounts to run ads without the Facebook users' knowledge or consent.

2. Defendants ran a number of deceptive ads on Facebook using a malicious technique known as "cloaking," which concealed the true nature of the ad from Facebook's ad review process and allowed Defendants to market goods in violation of Facebook's Terms of Service and Advertising Policy. Since April 2019, Facebook has notified hundreds of thousands of users that their Facebook accounts may have been compromised, and it has required those users to verify their identity and change their Facebook account passwords.

3. Accordingly, Facebook brings this action for injunctive relief to stop Defendants' misuse and abuse of the Facebook platform in violation of Facebook's Terms of Service and Advertising Policies. Facebook also brings this action to obtain compensatory, punitive, and exemplary damages in response to Defendants' violations of California Comprehensive Computer Data Access and Fraud Act, § 502, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and breach of contract.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

## PARTIES

4. Plaintiff Facebook, Inc., is a Delaware corporation with its principal place of business in Menlo Park, San Mateo County, California.

5. Defendant ILikeAd Media International Company Ltd. ("ILikeAd") was a Hong Kong-based advertising company that used the website ILikeAd.com.[1] Ex. 1 and 2. On its website, ILikeAd promoted itself as a "one-stop comprehensive solution to advertisers" providing advertising and marketing services to businesses interested in advertising on Facebook. *Id.* On information and belief, ILikeAd provided affiliate marketing services and profited from commissions for sales resulting from internet traffic that they delivered to their customers. *Id.*

6. Defendant Cong was a software developer located in Wuhan, Hubei, China.

7. Defendant Huang Tao was a marketing director at an entity called GuangZhou HongYi Technology Company Ltd. ("HongYi Technology") located in Guangzhou, Guangdong, China. Ex. 3. ILikeAd and HongYi Technology were affiliated entities that share the same Chief Executive Officer. Exs. 4 and 5. Tao used the aliases "staoism" and "staosim."

8. At all times material to this action, each Defendant was the agent, employee, partner, alter ego, subsidiary, or co-conspirator of and with the other Defendant, and the acts of each Defendant were in the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and the consent of each of the other Defendant, and each Defendant aided and abetted the other Defendant in the acts or omissions alleged in this Complaint.

[1] Defendants used the website ILikeAd.com between 2016 and 2017. The website is not presently used to promote marketing services by Defendants.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

## JURISDICTION AND VENUE

9. The Court has federal question jurisdiction over the federal causes of action alleged in this complaint pursuant to 28 U.S.C. § 1331.

10. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law causes of action alleged in this complaint because they arise out of the same nucleus of operative fact as Facebook's federal claims.

11. In addition, the Court has jurisdiction under 28 U.S.C. § 1332 over all causes of action alleged in this complaint because complete diversity exists and the amount in controversy exceeds $75,000.

12. The Court has personal jurisdiction over Defendants because they knowingly directed and targeted their conduct at California, individual California residents, and at Facebook, which has its principal place of business in California. By accessing Facebook, using Facebook, and running ads on Facebook, Defendants transacted business and engaged in commerce in California. Defendants also used computers located in California to facilitate their conduct and victimized California residents. Facebook's claims arise directly from and relate to Defendants' activities described in this Complaint.

13. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b), as the threatened and actual harm to Plaintiff occurred in this District. Venue is also proper with respect to each Defendant pursuant to 28 U.S.C. §1391(c)(3) because none of them reside in the United States.

14. Pursuant to Civil L.R. 3-2(c), this case may be assigned to either the San Francisco or Oakland division because Facebook is located in San Mateo County.

## FACTUAL ALLEGATIONS

### A. Background

#### 1. Advertising on Facebook

15. Facebook is a social networking website and mobile application that enables its users to create their own personal profiles and connect with each other on

their personal computers and mobile devices. As of October 2019, Facebook daily active users averaged 1.62 billion and monthly active users averaged 2.44 billion.

16. Anyone with a Facebook account and page can create an ad account, through which users can create and place ads on Facebook. Every week, users create millions of ads through the Facebook ad platform, which provides advertisers with many options for reaching their target audiences, so long as they comply with Facebook's Policies.

17. To pay for their ads, advertisers can input and maintain credit card or other payment information on file in their ad accounts. Financial information saved to a Facebook account, like credit card numbers, is stored securely and only the last four digits of the credit or debit card is visible to the user or others accessing a user's account.

18. To create and publish an ad, an advertiser must agree to Facebook's Terms of Service, Self-Serve Ad Terms, Commercial Terms, and Advertising Policies. Advertisers are also subject to Facebook's Community Standards, among other terms and conditions.

19. Ads are subject to Facebook's ad review system, which relies primarily on automated tools that review ads for compliance with Facebook's Advertising Policies. This automated review happens before an ad can run. Ads may also be subject to additional review after they are published, depending on user feedback and other indicators.

20. If the ad review process identifies a policy violation, the ad will be rejected and the advertiser will receive a rejection message. Some ads are flagged by the automated ad review system for manual human review. If the ad review system does not detect a policy violation, the advertiser will receive a notification confirming that the ad will begin running.

21. Facebook can also take a range of enforcement actions against an advertiser who violates the Advertising Policies, including banning an ad account

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

from running ads. To detect recidivism, Facebook analyzes the characteristics of ads and accounts to identify accounts that may be associated with previously identified bad actors.

**2. Cloaking**

22. One of the components reviewed by the ad review system is the website landing page a person will see if they click on an ad. If the landing page violates Facebook's Terms or Advertising Policies, the ad will be rejected.

23. "Cloaking" is a malicious technique used by advertisers to circumvent various ad review processes in order to show content on a landing page that violates Facebook's Terms and Advertising Policies.

24. In particular, cloaking disguises the true landing page for an ad and the actual content of the landing page, in order to circumvent Facebook's review process. A "cloaked" landing page used in an ad will display content to Facebook's automated and manual review systems that differs from that shown to actual Facebook users. The landing page displayed to the review system will promote content that falls within the bounds of the Advertising Policy, when in fact, the true landing pages displayed to users frequently promote deceptive products and services and display disallowed images. The true landing pages will frequently include ads for deceptive diet pills and cryptocurrency investments and images of sexual content.

**B. Facebook's Terms and Advertising Policies**

25. All Facebook users must agree to Facebook's Terms of Service ("Terms") (available at https://www.facebook.com/terms.php) and other rules that govern access to, and use of, Facebook. Those Terms include Facebook's Advertising Policies.

26. Section 3.2.1 of the Terms prohibits users from "do[ing] . . . anything unlawful, misleading, [ ] or fraudulent." Section 3.2.2 of the Terms, in turn, prohibits users from "upload[ing] viruses or malicious code," as well as "anything that could

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

disable, overburden, or impair the proper working or appearance of [Facebook] Products."

27. Section 3.2.3 of the Terms prohibits users from "access[ing] or collect[ing] data from [Facebook] Products using automated means (without our prior permission) or attempt[ing] to access data you do not have permission to access."

28. Under Section 4.2, Section 3 of the Terms stay in effect even if a user's account is disabled or the user deletes the account.

29. Advertising Policy 4.13 (available at https://www.facebook.com/policies/ads/) prohibits "ads, landing pages, and business practices" from "contain[ing] deceptive, false, or misleading content, including deceptive claims, offers, or methods."

30. Advertising Policy 4.28 prohibits "tactics intended to circumvent our ad review process or other enforcement systems," including "techniques that attempt to disguise the ad's content or destination page," as well as "[r]estrict[ing] Facebook's access to an ad's destination page."

31. Advertising Policy 4.32 prohibits ads that "promote products, services, schemes or offers using deceptive or misleading practices."

**C. Defendants' Scheme**

**1. Overview**

32. Beginning no later than 2016, Defendants jointly engaged in an account take over fraud scheme targeting Facebook and its users. Defendants' scheme proceeded as follows:

a. First, Defendant Cong developed the malware, which was designed to compromise computers and take over Facebook ad accounts. Defendant ILikeAd

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

registered two domains that were encoded in the malware as command and control servers[2] ("C2").

b. Second, between 2016 and 2019, Defendant Tao, on behalf of Defendant ILikeAd, promoted the distribution and installation of the malicious extension online through various forums and websites. When victims installed the malicious extension, they self-compromised their computers with Defendants' malware. In the case of Facebook users, the malware collected and exfiltrated Facebook login information from the victims' computers or browsers, thereby allowing Defendants to access the victims' Facebook accounts.

c. Third, Defendant Cong designed the malware to disable the accounts' security notifications in order to conceal Defendants Tao and ILikeAd's access and use of the Facebook accounts from the victim. The malware also enabled Defendants to run ads with the victims' Facebook ad accounts and paid for the ads using the victims' payment information. In some instances, Defendants ran deceptive ads using the images of certain types of celebrities.

d. Fourth, Defendants used cloaking software and services to avoid Facebook's ad review process. Defendants ran deceptive ads that redirected Facebook users to landing pages associated with counterfeit goods, male enhancement supplements, and diet pills, which violated Facebook's Advertising Policies.

**2. Development and Functionality of the Malware**

33. Beginning no later than May 2016, Defendant Cong used a Github repository to host and develop portions of the source code for the malware. Defendant ILikeAd registered two domains that were encoded in the malware to connect to the C2s. Exs. 6 and 7.

[2] A command-and-control server is a computer controlled by a malicious actor that is used to send commands to computers compromised by malware and serve other functions.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

34. Defendant Cong designed the malware to (a) compromise victims' computers and collect information from infected computers, and (b) access and take over Facebook ad accounts, if the victims had an ad account. After a victim installed the malicious extension, the malware executed unauthorized commands on the compromised computer in order to locate, copy, and exfiltrate user credentials, including Facebook credentials and cookies, saved to the compromised computer's internet browser (collectively "access information"). Defendants used this access information to access Facebook accounts without authorization of the victims or Facebook.

35. Defendants used their unauthorized access to the victims' accounts to run ads on Facebook and obtain unauthorized payments for the ads. Defendants used the malware to extract data that showed whether the victims had an ad account, had previously paid for ads, the amount spent on ads, and the balance on the victim's ad account. Defendants used the payment and ad account information to run ads on Facebook.

36. Defendants used multiple C2s to obtain data from compromised computers. Defendants' C2 domain names were encoded into the malware and included the following domains: api2019.com, api.new-api.com, api.kkkkdajlhlkjhsdewgtuv.com, api168168.com, pcmaps.net, and downmaps.com.

37. Defendant Cong designed the malware to execute a number of steps in order to maintain their control of the victims' accounts and to conceal their unauthorized activity. First, the malware turned off user notifications, which prevented victims from learning that (a) their account was accessed from an unrecognized device and browser; and (b) that their ad account had been used to run Facebook ads. Second, the malware locked in the changes made to the notification settings, preventing the victims from reverting or otherwise altering them.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

### 3. Distribution and Installation of the Malware

38. Defendants caused the installation of their malware on victims' computers when victims installed the malicious extensions online. The malware was not installed, nor were the victims' computers compromised, as a result of visiting, accessing, or using Facebook.

39. Defendants caused the malware to be installed by bundling it with other software downloads. To increase the likelihood that their malware was successfully installed on a victim's computer, the software bundles contained (a) the complete malware executable, and (b) a downloader and corrupted DLL (dynamic link library) file used to "hijack" the legitimate DLL process of chromium-based applications (e.g. Chrome, Opera), an attack called "DLL hijacking." DLL hijacking caused the malware to be downloaded and installed from a domain that hosted the malware executable, commonly referred to as the "payload." Domains that hosted the malware payload included: down.kaidandll.com, down.dll-biu.com, and down.biubiudown.com, among others.

40. Defendants also used a web-based code repository and hosting service to host the malware. The malware executables were added to the repository using two Google IP addresses physically located in the Northern District of California.

41. Between 2016 and 2019, Defendant Tao promoted the installation of Defendants' malicious extension on various forums and websites using the aliases "staoism" and "staosim." Exs. 8, 9, 10, 11, and 12.

### 4. Unauthorized Advertisements and Cloaking

42. If the compromised Facebook account had an ad account, Defendants used it to publish ads through the compromised account without the victim's knowledge or consent. Those ads were billed to the victim's ad account.

43. Defendants' advertisements used cloaking to circumvent Facebook's content policy and review process. As a result, certain users that clicked on the cloaked ads were redirected to a website that was different than the website shown in

the advertisement. Defendants' unauthorized advertisements marketed counterfeit goods, male enhancement supplements, and diet pills.

**D. Defendants Unjustly Enriched Themselves and Their Unlawful Acts Have Caused Damage and a Loss to Facebook.**

44. Defendants interfered with and continue to interfere with Facebook's computer network, and they have negatively impacted the Facebook experience for users whose accounts were affected by their fraud.

45. Defendants' breaches of Facebook's Terms and Advertising Policies, as well as their violations of state and federal law, have caused Facebook substantial harm.

46. Defendants' actions injured Facebook's reputation, public trust, and goodwill.

47. Facebook has suffered damages and a loss attributable to Defendants, including the efforts and resources it has used to address this Complaint, investigate and mitigate Defendants' illegal conduct, and attempt to identify, analyze, and stop Defendants' injurious activities. Facebook has paid over $4 million to Defendants' victims in order to reimburse them for the unauthorized ads purchased using their ads accounts.

48. Defendants have been unjustly enriched by their activities at the expense of Facebook in an amount to be determined at trial.

**FIRST CAUSE OF ACTION**

(Breach of Contract)

49. Facebook realleges and incorporates all preceding paragraphs.

50. Access to and use of Facebook's services is governed by Facebook's Terms and its related policies.

51. Defendants agreed to and became bound by Facebook's Terms and related policies through their use of Facebook and its services.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

52. Facebook has performed all conditions, covenants, and promises required of it in accordance with its agreement with Defendants.

53. Defendants knowingly breached Facebook's Terms and Advertising Policies.

54. Defendants' violations of Facebook's Terms and Advertising Policies have directly and proximately caused and continue to cause harm and injury to Facebook.

55. When Defendants agreed to, and became bound by, Facebook's Terms and Advertising Policies, both Facebook and Defendants knew or reasonably could have foreseen that the harm and injury to Facebook was likely to occur in the ordinary course of events as a result of Defendants' breach.

56. Defendants' breaches of Facebook's Terms and Advertising Policies have caused Facebook damages in an amount to be determined at trial, and in excess of $75,000.

## SECOND CAUSE OF ACTION

(California Penal Code § 502)

57. Facebook realleges and incorporates all preceding paragraphs.

58. Defendants knowingly accessed and without permission used Facebook's data, computers, computer system, and computer network in order to (A) devise or execute a scheme or artifice to defraud and deceive, and (B) to wrongfully control or obtain money, property, or data, in violation of California Penal Code § 502(c)(1).

59. Defendants knowingly and without permission used or caused to be used Facebook's computer services in violation of California Penal Code § 502(c)(3).

60. Defendants knowingly and without permission disrupted or caused the disruption of computer services and denied or caused the denial of computer services to one or more authorized users of Facebook's computers, computer systems, and computer networks in violation of California Penal Code § 502(c)(5). More specifically, as described above, Defendants' malware modified user notifications

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

without permission in order to prevent users from learning that their accounts were being used without permission.

61. Defendants knowingly and without permission accessed or caused to be accessed with Facebook access information obtained from the malware Facebook's computers, computer systems, and computer networks in violation of California Penal Code § 502(c)(7).

62. Because Facebook suffered damages and a loss as a result of Defendants' actions and continues to suffer damages as result of Defendants' actions, Facebook is entitled to compensatory damages, attorney's fees, and any other amount of damages to be proven at trial, and injunctive relief under California Penal Code § 502(e)(1) and (2).

63. Because Defendants willfully violated Section 502, and there is clear and convincing evidence that Defendants committed "fraud" as defined by section 3294 of the Civil Code, Facebook is entitled to punitive and exemplary damages under California Penal Code § 502(e)(4).

**THIRD CAUSE OF ACTION**

(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

64. Facebook realleges and incorporates all preceding paragraphs.

65. Facebook computers and servers were "protected computers" as defined by 18 U.S.C. § 1030(e)(2).

66. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with intent to defraud, accessed Facebook's protected computers and by means of such conduct furthered the intended fraud and obtained something of value. Defendants accessed Facebook protected computers purporting to be legitimate Facebook users when in fact they had compromised the users' computers with malware designed to transmit unauthorized commands to Facebook. Defendants used their unauthorized access for the purpose of furthering their fraudulent advertising campaigns, which included running deceptive ads and cloaking landing pages

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

contained in certain ads. As a result of the fraud, Defendants obtained money and unauthorized use of Facebook, the value of which exceeded $5,000.

67. Defendants violated 18 U.S.C. § 1030(a)(5)(A) because they knowingly and intentionally caused the transmission of a program, information, code, or command and as a result of such conduct intentionally damaged Facebook protected computers. More specifically, Defendants modified users' account notification settings to prevent users from receiving a notification that their Facebook accounts were being used without authorization and that they were being used to run advertisements.

68. Defendants violated 18 U.S.C. § 1030(b) by attempting and conspiring to commit the violations alleged in the preceding paragraph.

69. Defendants' conduct caused a loss to Facebook of at least $5,000 during a one-year period.

70. Defendants' actions caused Facebook to incur a loss and suffer damages as defined by 18 U.S.C. § 1030(e)(8) and (11), including the expenditure of resources to investigate and respond to Defendants' fraudulent scheme in an amount to be proven at trial.

71. Defendants continue to promote their malware online and Facebook has no adequate remedy at law that would prevent Defendants from continuing their unlawful scheme. Permanent injunctive relief is therefore warranted.

## FOURTH CAUSE OF ACTION

(Unjust Enrichment)

72. Facebook realleges and incorporates all preceding paragraphs.

73. Defendants' unjustly enriched themselves at Facebook's expense.

74. Defendants accessed and used Facebook's platform and computer network without authorization or permission.

75. Defendants used Facebook's platform and computer network to, among other things, defraud and deceive users, interfere with Facebook's operation, platform,

and computer network, and wrongfully obtain money through their advertising scheme.

76. Defendants received a benefit by profiting from their unauthorized use of Facebook's platform and computer network.

77. Defendants' retention of the profits derived from their unauthorized use of Facebook's platform and computer network would be unjust.

78. Defendants' unauthorized use of Facebook's platform and computer network has injured Facebook's reputation, public trust, and goodwill.

79. Defendants' unauthorized use of Facebook's platform and computer network damaged Facebook, including but not limited to the time and money spent investigating and mitigating Defendants' unlawful conduct.

80. Facebook seeks injunctive relief and damages in an amount to be proven at trial, as well as disgorgement of Defendants' ill-gotten profits in an amount to be determined at trial.

81. As a direct result of Defendants' unlawful actions, Facebook has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

## REQUEST FOR RELIEF

**WHEREFORE**, Plaintiff Facebook requests judgment against Defendants as follows:

1. That the Court enter judgment against Defendants that Defendants have:

   a. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. 1030;

   b. Violated the California Comprehensive Computer Data Access and Fraud Act, in violation of California Penal Code § 502;

   c. Breached their contract with Facebook in violation of California law; and

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

d. Been unjustly enriched at the expense of Facebook in violation of California law.

2. That the Court enter a permanent injunction enjoining and restraining Defendants and their agents, employees, successors, and assigns, and all other persons acting in concert with or conspiracy with him or affiliated with Defendants from:

a. Accessing or attempting to access Facebook's platform and computer systems;

b. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Facebook's platform and computer system, including developing malware that targets Facebook;

c. Engaging in any activity, or facilitating others to do the same, that violates Facebook's Terms and Advertising Policies, including the use of cloaking software to circumvent Facebook's ad review process; and

d. Engaging in activity that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1030) or the California Comprehensive Computer Data Access and Fraud Act (California Penal Code § 502).

3. That Facebook be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial.

4. That Facebook be awarded a recovery in restitution equal to any unjust enrichment enjoyed by Defendants in an amount to be determined at trial.

5. That Facebook be awarded its reasonable costs, including reasonable attorneys' fees.

6. That Facebook be awarded pre- and post-judgment interest as allowed by law.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

That the Court grant all such other and further relief as the Court may deem just and proper.

Dated: December 5, 2019

**HUNTON ANDREWS KURTH LLP**

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Jason J. Kim
Jeff R. R. Nelson
Attorneys for Plaintiff
FACEBOOK, INC.

Platform Enforcement and Litigation
Facebook, Inc.
Jessica Romero
Michael Chmelar
Nikkya Williams

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

**JURY TRIAL DEMAND**

Plaintiff hereby demands a trial by jury on all issues triable to a jury.

Dated: December 5, 2019

**HUNTON ANDREWS KURTH LLP**

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Jason J. Kim
Jeff R. R. Nelson
Attorneys for Plaintiff
FACEBOOK, INC.

Platform Enforcement and Litigation
Facebook, Inc.
Jessica Romero
Michael Chmelar
Nikkya Williams

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627