November 3, 2021

The Honorable Thom Tillis
113 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patrick Leahy
437 Russell Senate Office Building
Washington, DC 20510

Dear Senators Tillis and Leahy:

Thank you for your letter of September 30 about advertisements on piracy apps and websites. Facebook takes creativity, copyright, and protection of intellectual property rights seriously, and we understand that online piracy is an important problem. We take a comprehensive approach to addressing online safety, including with respect to advertisements for our business that current and non-users see on other platforms. We strongly oppose the placement of our advertisements on websites and apps that either infringe or pose a high risk of infringing copyright (including on commercial-scale pirate websites and apps). We maintain a robust framework to combat misplacement of Facebook ads on third-party websites and apps.

Advertisement Fraud Management Framework

The goal of our advertisement fraud management framework is two-fold: (1) to prevent from bidding or serving Facebook ads on fraud traffic sources and (2) to prevent payments for identified fraud traffic. To accomplish these goals, our general practice is to request third-party agencies with whom we contract to proactively identify and protect against fraudulent traffic.

Our current ad fraud management framework is divided into three activities: (1) prevention; (2) detection; and (3) mitigation.

1. **Prevention**: Fraud prevention begins during advertisement network selection. From this selection process, Facebook contracts with industry-leading third-party digital media agencies to place ads for our platforms and services on external websites and apps. Our general practice is to request direct, transparent placements, and request that fraud terms be included in our agreements. In negotiating these agreements, we generally request that vendors agree to actively monitor ad campaigns for signs of fraudulent activity, and agree to alert Facebook in the event that any such activity is detected or suspected. Our general practice also includes requests that vendors agree to ensure that our ads

do not appear on websites or adjacent to any content promoting subjects such as pornography, non-gaming violence, or infringement of intellectual property rights (including music and video piracy). While each agreement is unique, the foregoing reflects some of the terms that we strive to obtain in our agreements with vendors.

2. **Detection**: We utilize tools and fraud suites from third-party agencies, such as the Kochava Fraud Console and tools from Forensiq and DoubleVerify, to try to detect fraudulent placements (including advertisements on websites that either infringe or pose a high risk of infringing copyright). We continuously monitor these placements and try to identify any anomalies that may signal fraudulent or suspicious activity. We, in close collaboration with these third-party agencies, also develop custom, threshold-based signals to detect app and web traffic that lead to suspicious activity.

3. **Mitigation**: We maintain global blocklists intended to prevent our ads from appearing on apps and websites associated with fraud, fake actors, or sensitive content. Our partnership with third-party agencies allows us to try to permanently block identified fraudulent ad sources, such as websites and apps, and also identify potentially problematic traffic, which is flagged for investigation in partnership with the ad network/publisher. Further, our mitigation framework consists of utilizing automatic and manual blocking technology to investigate problematic traffic with ad networks. Finally, if any fraud or violations of the underlying agreement with the ad placement agency are identified, our practice is to request refunds for the ad impression.

We recognize that no matter our preventative measures, there must always be ongoing manual traffic reviews to spot and investigate suspicious signals. As such, we regularly assess and continue to make improvements to our detection and protection framework, to improve our detection of ads that appear on or are attributed to fraud traffic sources. Through partnership with third-party agencies, we strive to update our blocklists weekly. Additionally, these third-party agencies have advised us that they conduct regular audits (on the weekly and monthly level) to evaluate fraud safety measures.

Managing our ad placements globally can be challenging and is an iterative process. For example, for one of the ads referenced in the Breaking (B)ads report, which you cite in your letter, our teams determined that ten versions or variations of the piracy app already appeared on our permanent blocklist. Further, as a result of the information provided in the report, our teams added an additional four variations of the app to our permanent blocklist. As detailed above, we, in close partnership with third-party vendors, continue to proactively identify areas where we can improve in this area, and take steps to help protect current and non-users from seeing ads on inappropriate websites and

apps, including on those that either infringe or pose a high risk of infringing copyright advertisements.

Thank you again for the opportunity to answer your questions, and we look forward to working with you going forward.

Sincerely,

Meta, Inc.

575 7th STREET NW
STE 700
WASHINGTON, D.C. 20004

Meta