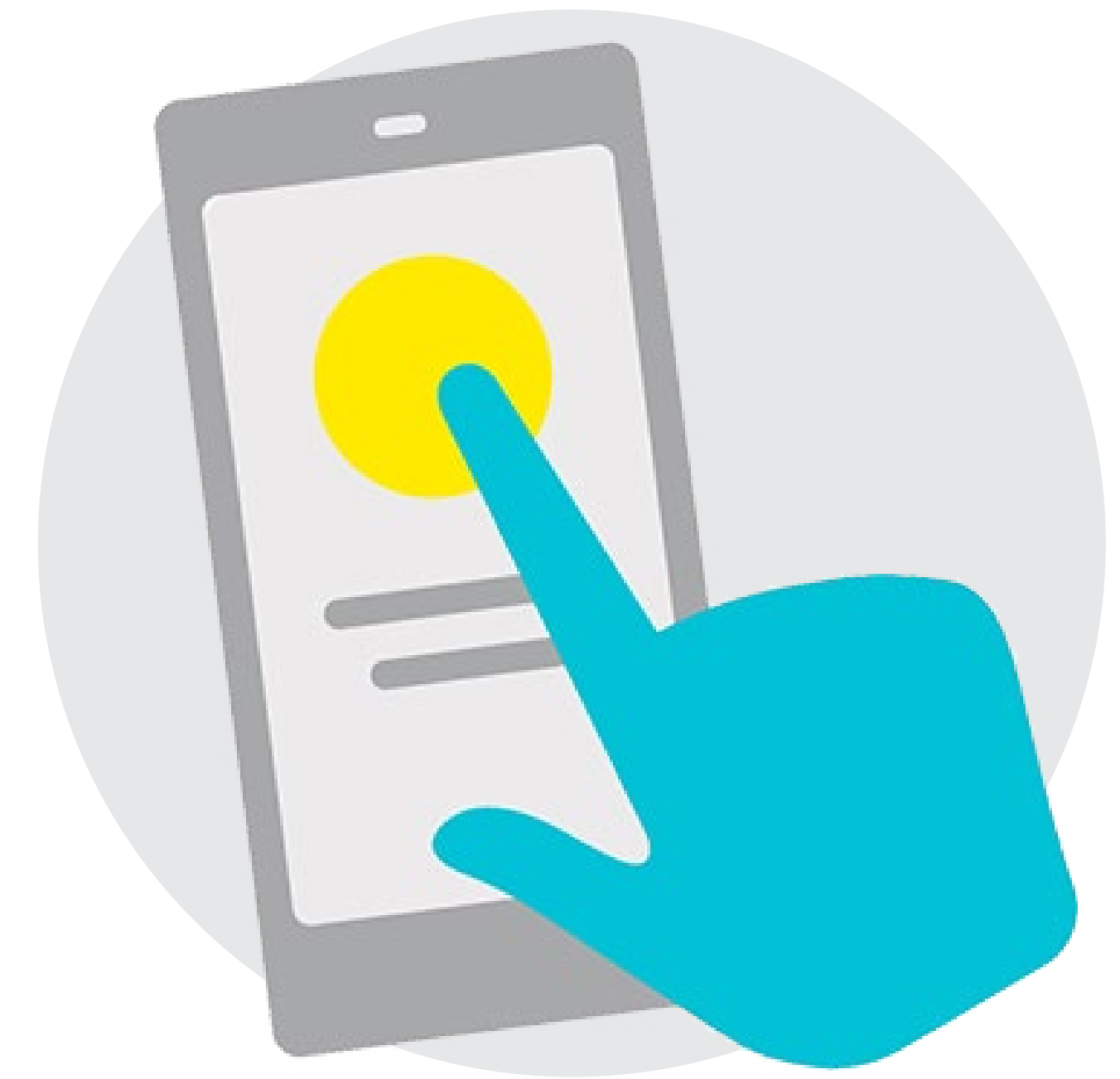




Mobile Ad Fraud Defense: A Three-Step Guide

If you run campaigns on mobile ad networks, you've probably worried about mobile ad fraud and how to detect it and prevent it.

In 2018, AppsFlyer estimated that the financial exposure to ad fraud in the mobile advertising ecosystem was as high as \$800 million per quarter. Many advertisers believe that the majority of mobile ad fraud happens when buying cheap Android installs in Southeast Asia, but advertising fraud in fact happens everywhere around the globe and on a variety of campaigns; as [eMarketer's Digital Ad Fraud 2019 report](#) details, **nearly 15% of total app installs in the U.S. in Oct. 2018 were fraudulent.**



KOCHAVA★

 **AppsFlyer**

 **singular**

 **adjust**

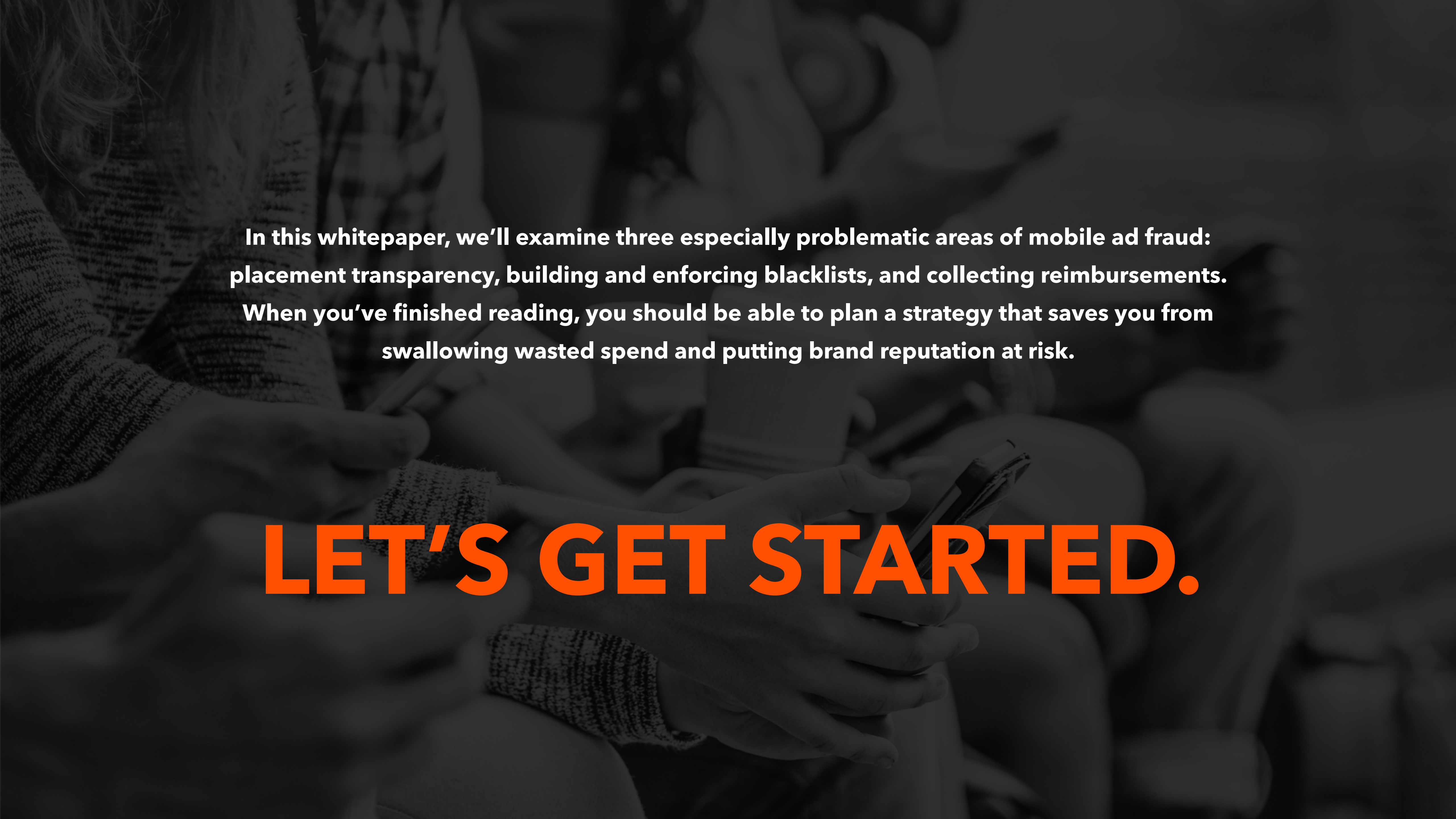
branch

There are many fraud prevention tools available, but a good place to start is the fraud prevention tool from your mobile attribution platform.

Kochava, AppsFlyer, Singular, Adjust, and Branch all have tools to help you spot potentially fraudulent activity in your campaigns.

Capabilities differ between fraud tools, but they all analyze raw campaign data at a publisher, site/app, and device level and identify traffic abnormalities that could be indicative of fraud. The most common traffic abnormalities that fraud tools seek out are high click counts per device, high click counts per IP address, suspicious types of IP addresses, low time between a click and install, low click-to-install ratio, and publishers or apps with a high volume of new devices in their audience.

Some tools will allow you to set rules to automatically block suspicious traffic in real time; others offer a combination of automated actions and manual actions. However, no matter which tool you choose, you will need to build your own processes to actually enforce the insights from the fraud tools, or you will not sufficiently protect yourself from ad fraud.



In this whitepaper, we'll examine three especially problematic areas of mobile ad fraud: placement transparency, building and enforcing blacklists, and collecting reimbursements. When you've finished reading, you should be able to plan a strategy that saves you from swallowing wasted spend and putting brand reputation at risk.

LET'S GET STARTED.