

# Stopping Ad Fraud at Scale

With marketing activity across the globe, Viber was able to stop performance ad fraud in its tracks.

Rakuten Viber

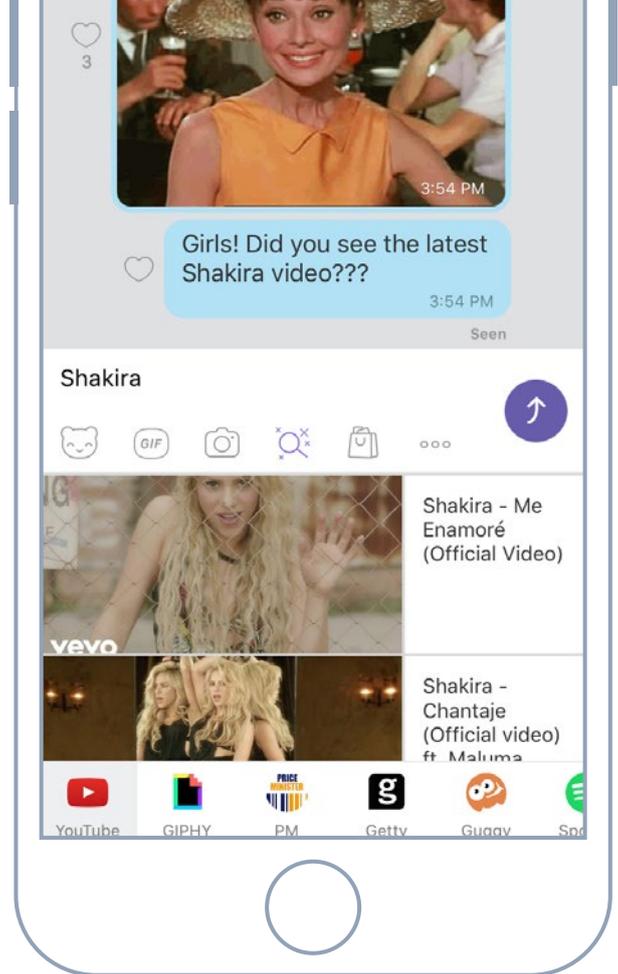


# Rakuten Viber

Viber is a free instant messaging and calling app that allows you to connect with friends and family no matter where you are. Founded by Viber Media in 2010, Viber initially launched its iPhone version in 2010, and released an Android version in 2012.

The app now has over 800 million users who can communicate with one another using several different features including Viber's VoIP video calls, one-on-one messaging and group chats, sticker packs, and much more.

In 2014, Viber was acquired by Japanese electronic commerce and Internet company, Rakuten, for \$900 million.



## Problem

Viber has a strong global footprint, but is still actively growing its user base across Europe, Asia and North America. In order to scale their paid activity, Viber decided to enlist an agency that would manage their media buying via ad networks. The agency was also responsible for onboarding and connecting Viber to new partners as well as guaranteeing high quality and legitimate traffic ensuring Viber wouldn't become a target of fraudulent behavior.

## Solution

Viber had been working with Adjust for over two years, and when they heard about the Fraud Prevention Suite (FPS) they were one of its earliest adopters. By enabling FPS, all of Viber's marketing campaigns were automatically protected from the most common and widespread fraud schemes.

Right after activation, Adjust automatically started cross-checking the IP addresses of all incoming traffic against a database of known datacenters, VPN providers, Tor exit nodes and previously attributed IP addresses. Any



## Results

**"I don't think any advertiser really understands the amount of fraudulent traffic they are dealing with until they activate the Fraud Prevention Suite. I can't imagine doing any media buying without it now."**  
(Moshi Blum).

"On the first month of onboarding the new network, we received premium quality traffic, whereas once we approved the network and scaled the budget, the network's traffic fraud rates rose from 2% to a whopping 40%," says Blum. "This was, surprisingly, something that repeated itself in several of the networks we worked with. FPS allows us to experiment with and test new sources so that we know our budgets are targeted towards legitimate users only."

### **The use of FPS also resulted in the following:**

- Most of the rejected installs came from distribution modeling.
- FPS meant no wasted budgets on fraudulent traffic and meant Viber could acquire users who would convert. On average they saved 10% of their marketing budget, which they could then reinvest in real users.
- FPS gave Viber more freedom with their agency so they could experiment safely.
- Viber has now changed their internal evaluating logic for network quality. They no longer just look at their top KPIs but also include fraud rate as an evaluator. Now, if a partner reaches more than 20% of fraud they discontinue working with that partner.

traffic coming from repeated or unusual IPs was rejected and attributed as untrusted and both Viber's servers and network partners were notified in real-time.

This screened out installs that came from untrusted sources, and eliminated simulated/emulated installs that were generated on server farms, or were fed into the internet via VPNs or the TOR network.

Distribution modeling and hyper engagement filters worked to protect Viber from two types of click spamming: 1 - low in frequency but high in active user/device count; 2 - high in frequency but low in active user/ device count.

To fight this fraudulent scheme during attribution, Adjust calculated the statistical correlation between the click engagement and the resulting install. If there was no correlation between clicks and installs for a particular source, Adjust started to deny attribution and both Viber's servers and network partners were notified in real-time.

"Since FPS protected our interests from the start, we were more confident about allowing them a free reign to onboard new partners and buy traffic," says Moshi Blum, User Acquisition Lead at Viber. "With FPS activated in our dashboard we could be more lenient with the agency knowing the data we received was filtered for mobile fraud schemes. This also meant our retargeting efforts were more efficient since the audience was genuine."



## About Adjust

Adjust is the mobile measurement company, providing the highest quality analytics and measurement solutions for mobile app marketers worldwide. With Adjust's open source SDK, app marketers can measure and analyze user behavior, user acquisition, marketing ROI, user lifetime cohorts and more. Adjust's platform proactively keeps datasets clean through the Fraud Prevention Suite, verifies in-app purchases in real-time, and provides streamlined reporting for understandable, actionable and comparable metrics. Adjust is a Facebook Marketing Partner and a Twitter Marketing Platform Partner, and dynamic Adjust integrations are in use by over 900 networks and analytics providers worldwide. Founded in Berlin in 2012, Adjust today has global offices in San Francisco, New York, Sao Paulo, London, Paris, Istanbul, Tokyo, Shanghai, Singapore, Jakarta and Moscow.

Adjust is trusted by clients across Asia, the EU and the Americas: including leading app developers like Zalando, Rovio and Zynga, major software companies like Salesforce, Microsoft and Yelp, and global brands like Universal Music and Warner Bros.

Adjust is the only mobile analytics company to meet stringent EU privacy compliance standards. Adjust is funded by Target Partners, Capnamic Ventures, Iris Capital, Active Venture Partners, and Highland Capital.

For more details, visit [www.adjust.com](http://www.adjust.com) or contact [sales@adjust.com](mailto:sales@adjust.com).