



Adjust GmbH Saarbrücker Straße 38a, 10405 Berlin, Germany
Adjust Inc. 535 Mission Street, San Francisco, CA 94105, United States of America
Phone +49 30 91 46 00 83, Fax +49 30 25 74 96 75 www.adjust.com

Report von Adjust zeigt: Ad Fraud-Rate verdoppelt sich im Vergleich zu 2017

Adjust sagt dem weltweiten Werbemarkt einen Schaden von mehr als 4,9 Milliarden US-Dollar voraus. E-Commerce ist am stärksten betroffen.

San Francisco und Berlin - Mai 10., 2018 - Der globale Marktführer für Mobile Measurement Adjust hat heute die Ergebnisse seines jüngsten Berichts zum Thema Mobile Ad Fraud veröffentlicht. Die Ergebnisse zeigen, dass Mobile Fraud auch im Jahr 2018 die zentrale Herausforderung für Werbetreibende sein wird. Im Vergleich zu 2017 hat sich der mobile Anzeigenbetrug prozentual fast verdoppelt. Insgesamt 7,3% aller bezahlten Installationen wurden von Adjusts Fraud Prevention Suite abgelehnt. Auf den gesamten mobilen Werbemarkt übertragen, lassen die Zahlen von Adjust somit einen Schaden von etwa 4,9 Milliarden US-Dollar für das Jahr 2018 erwarten. Die Kernaussagen des Reports sind darüber hinaus:

- E-Commerce ist durch Fraud am stärksten betroffen (Vergleich 2017: Gaming)
- Weltweites Aufkommen an Fraud lässt sich auf insgesamt 4 Methoden zurückführen
- Neu entdeckte Form des Ad Frauds macht gleichzeitig den größten Anteil aus: SDK-Spoofing verbreitet sich zunehmend

Für den **Mobile Fraud Guide** hat Adjust insgesamt 3,43 Milliarden App-Installationen und mehr als 350 Milliarden App-Events untersucht. Das entspricht einer Datenmenge von 125 Terabyte pro Tag von mehr als 20.000 Apps, die im Januar, Februar und März dieses Jahres untersucht wurden. Ziel der Untersuchung war es, herauszufinden, wie groß der Ausmaß von Fraud ist und wie stark die Mobile Branche im Jahr 2018 davon betroffen sein wird.

Weltweiter Schaden in Milliardenhöhe

Laut einer [Studie von eMarketer](#) werden die Ausgaben für mobile Werbung im Jahr 2018 in den USA um 20% auf mehr als 75 Milliarden Dollar steigen. Das Forschungsunternehmen schätzt auch, dass die Ausgaben für mobile Werbung im Jahr 2018 um 23,5% gegenüber dem Vorjahr steigen werden. Legt man diese Erkenntnisse den Fraud-Messungen von Adjust zugrunde (Ablehnungsrate von +7,0%), so ist im globalen Werbemarkt von einem Schaden von etwa 4,9 Milliarden US-Dollar auszugehen.

"Natürlich lässt die Menge an Fraud, die wir bei unseren aktiven Ablehnungen sehen, nur erahnen, welches Ausmaß Fraud im gesamten Ökosystem einnimmt. Die Menge an Fraud, die insgesamt verhindert werden könnte, ist sicher deutlich höher", sagt Andreas Naumann, Fraud-Spezialist bei Adjust.

Fraud betrifft alle Branchen - E-Commerce gerät immer mehr ins Fadenkreuz

Im vergangenen Jahr war die Kategorie "Games" mit einem Anteil von 35% aller abgelehnten Installationen am stärksten betroffen. Die nächste Kategorie im Fadenkreuz der Fraudster war E-Commerce mit einem Anteil von 20%. Im Jahr 2018 gab es jedoch eine dramatische Veränderung: E-Commerce ist heute die am stärksten betroffene Branche und macht 40% der von Adjust abgelehnten Installationen aus. Die Kategorie "Games" liegt mit 30% auf Platz zwei, gefolgt von "Travel" mit 10% auf Rang drei.

Aufkommen einer neuen Fraud-Art: SDK-Spoofing

Der dramatische Anstieg der jüngsten Fraud-Zahlen lässt sich durch das Aufkommen einer völlig neuen Form des Ad Frauds erklären: SDK Spoofing. SDK Spoofing ist das am schwierigsten aufzuspürende Betrugsverfahren und hat sich schnell als führende Variante etabliert. Erste Untersuchungen von Adjust ergaben, dass SDK Spoofing weltweit verbreitet und für 37% aller abgelehnten Installationen verantwortlich ist.

Die vier relevantesten Fraud Arten weltweit

Neben dem SDK Spoofing, sind vor allem drei bereits bekannte Arten, für die steigenden Betrugszahlen relevant:

- SDK Spoofing 37%
- Click Injection 27%
- Fake Installs 20%
- Click Spam 16%

Click Spam weist organische Nutzer im Tracking so aus, als seien sie über eine Plattform zum App-Kauf geführt wurden. Eine ausgeklügeltere Form des Click Spams sind Click Injections. Dabei werden Betrüger informiert sobald eine App aus dem Appstore heruntergeladen wurde und können sich vor dem ersten Öffnen durch den User mit einem Add-Klick zwischen schalten. Unter dem Begriff Fake Installs dagegen werden Techniken zusammengefasst, die Installationen vortäuschen, die nicht auf echten Geräten stattgefunden haben.

Weiterführende Informationen zu den relevantesten Arten des Add-Frauds bietet der Mobile Fraud-Guide. Der vollständige Guide kann kostenlos heruntergeladen werden: <https://www.adjust.com/resources/insights/sources-of-error-white-paper/>

Über Adjust

Adjust ist der global führende Anbieter im Bereich Mobile Measurement und Fraud Prevention. Das Berliner Unternehmen stellt weltweit höchst qualitative Analyse-, Mess- und Fraud Prevention-Lösungen für App Marketer bereit und ermöglicht ihnen schnellere, smartere Entscheidungen zu treffen. Mit *Adjusts* Open-Source SDK können App Marketer Nutzerverhalten, User-Acquisition, Marketing ROIs, User-Lifetime-Kohorten und weiteres messen und analysieren. Mit der Fraud Prevention Suite hält *Adjusts* Plattform Datensätze proaktiv sauber, verifiziert In-App-Käufe in Echtzeit und stellt ein vereinfachtes Reporting mit verständlichen, verfolgbaren sowie vergleichbaren Metriken zur Verfügung. *Adjust* ist Marketing Partner aller führenden Marketing Plattformen, einschließlich Facebook, Google, Snap, Twitter, Naver, Line, und WeChat. *Adjusts'* dynamische Integrationen werden von über 1.200 führenden Netzwerk- und Analytikanbietern weltweit genutzt. Insgesamt haben mehr als 20.000 Apps die Produktlösungen von *Adjust* integriert, um ihre Performance zu verbessern.

Adjust ist das einzige Mobile Analyse Unternehmen, das die strikten EU Datenschutz- und Compliance-Standards einhalten kann. Für weitere Informationen besuchen Sie unsere Website: www.adjust.com.