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 Add 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.

Die 4 wichtigsten Fraud Arten weltweit

1. **SDK Spoofing**

SDK-Spoofing ist wahrscheinlich das am schwierigsten zu erkennende Betrugsverfahren. Durch eine betrügerische App haben Betrüger Zugriff auf das Gerät von echten Nutzern und verwenden diese, um legitim wirkende gefälschte Installationen auszulösen. Die verwendeten Geräte existieren tatsächlich und sind als Installationsquellen glaubwürdig. Alles scheint real: die Verbindung, die Gerätedaten, das Gerät. Es gibt jedoch keine Interaktion zwischen dem Nutzer/Gerät und der Anzeige, und am wichtigsten ist, dass es keine tatsächliche Installation gibt. Die Performance der Kampagne scheint sehr gut zu sein, aber nur in den Statistiken. Die Werbetreibenden verlieren Geld und die Endbenutzer sind sich nicht bewusst, dass sie an einem Betrug beteiligt waren.

Alarmierende Zeichen: Wenn die SDK-Version und die App-Version von Installationen, die durchkommen, nicht mit der neuesten Version übereinstimmen, die Sie veröffentlicht haben. Die am stärksten betroffenen App-Kategorien sind: Games 29%, E-commerce 27%, Food & Drink 17%.

2. **Click Injections**

Erscheint nur auf Android und ist eine ausgeklügelte Form von Click-Spamming. Fast alle Daten sind echt, mit Ausnahme der letzten Ad Engagement. Durch den Zugriff auf eine Android-App auf dem Gerät eines echten Nutzers können die Betrüger direkt nach Abschluss der Installation und vor dem ersten Öffnen der App einen Klick auslösen. Der Betrüger erhält die Auszahlung für die Installation, obwohl diese organisch war oder über einen anderen Kanal kam. Dies liegt daran, dass die Attributionsmethode fast immer auf dem letzten Klick basiert (letzte Anzeigeninteraktion).

Alarmierende Zeichen: Attribution to click, nachdem der Nutzer sich entschieden hat, die App herunterzuladen. Die am stärksten betroffenen App-Kategorien sind: E-commerce 51%, Games 23%, Travel 8%.

3. Click Spam

Click Spam, auch als organic poaching bezeichnet, ist eine Art von Betrug, der auftritt, wenn ein Fraudster Klicks für Nutzer ausführt, die diese nicht getätigt haben. Click Spam fängt organischen Verkehr ab, beansprucht ihn und somit später auch die Auszahlung für den Benutzer. Fast alles ist real - Es erscheinen Installationen von echten Benutzern auf echten Geräten, die sich nach der Installation normal verhalten - weil dies echte Benutzer sind, die die App organisch heruntergeladen haben. Das einzige, was gefälscht ist, ist die Anzeigenschaltung. Stattdessen hat der Betrüger, der für die Installation bezahlt wurde, tatsächlich die Zuweisung einer legitimen Installation gestohlen, ohne je Werbung gezeigt zu haben. Die Performance der Kampagne sieht gut aus, aber die Daten sind ungenau und bedroht somit zukünftige Entscheidungen. Wenn ein Werbenetzwerk organische Nutzer beansprucht und diese Nutzer innerhalb einer App gut abschneiden, wird der Werbetreibende offensichtlich entscheiden, in diesen Kanal zu investieren, um mehr von der gleichen Art von Nutzern zu erwerben.

Alarmierende Zeichen: bezahlte Installationen aus bestimmten Quellen, die sich unheimlich ähnlich verhalten wie organische Gegenstücke. Eine flache oder besser zufällige Verteilung der "Klick-zum-ersten-App-Start-Zeit" über den Attributionszeitraum und niedrige bis extrem niedrige Conversion-Raten. Top-Kategorien sind E-Commerce mit 38%, Games mit 29% und Food & Drink mit 7%.

4. Fake Installs

Eine gefälschte Installation ist ein weit gefasster Begriff. Er meint zusammengefasst die Situation, in der Betrüger dafür sorgen, dass Attributionspartner Installationen tracken, die nicht auf echten Geräten stattgefunden haben. Dies sind vollständig konstruierte Benutzer, die nur existieren, um Installationen basierend auf betrügerischer Werbung auszulösen. Normalerweise können sie durch eine hohe Anzahl von Installationen mit einem sofortigen Abfall von Nutzer-Interaktion (mit der heruntergeladenen App) nach dem Klick entdeckt werden. Nutzer, Geräte und Anzeigen sind gefälscht und stammen in der Regel aus Rechenzentren oder Geräte-Farmen und werden versucht, via VPNs zu vertuschen.

Alarmierende Zeichen: eine hohe Anzahl von Installationen mit einem sofortigen Abfall von Nutzer-Interaktion (mit der heruntergeladenen App) nach dem Klick. Top-Kategorien sind Gaming mit 42%, E-Commerce mit 14% und Entertainment mit 14%.