



Adjust GmbH Saarbrücker Straße 37a, 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](http://www.adjust.com)

## Adjust entwickelt Lösung für neueste Form von AdFraud

*Sogenannter SDK-Spoofing Fraud greift auf Endgeräte von Nutzern zu und täuscht App-Installationen vor*

**SAN FRANCISCO / BERLIN - 25. Januar 2018** - Fraud-Experten von Adjust, dem weltweit führenden App-Measurement Unternehmen, haben eine Lösung für eine völlig neue Form von AdFraud entwickelt, die sich im Laufe des Jahres 2017 rapide verbreitet hat.

Beim sogenannten SDK-Spoofing, auch Replay-Angriffe genannt, greifen Betrüger ohne das Wissen der Nutzer auf deren Endgeräte zu und täuschen App-Installationen vor. Der Betrugsangriff wird vom Endnutzer nicht erkannt und kann jedes Gerät betreffen. App-Installationen finden auf diesen Geräten nicht wirklich statt sondern werden lediglich simuliert - so investieren Werbetreibende Budget in scheinbare Installationen. Da die genutzten Geräte tatsächlich existieren und als Quellen glaubwürdig sind, ist SDK-Spoofing nur schwer identifizierbar und der nächste Schritt in der Evolution von AdFraud.

*"Die Verbindung ist real, die Gerätedaten sind real, das Gerät ist real. Es ist schlimm genug, dass es keine Interaktion zwischen dem Nutzer und der Werbung für die beworbene App gibt. Das noch größere Problem ist jedoch, dass es nicht einmal eine tatsächliche Installation gibt."* kommentiert Andreas Naumann, Fraud Specialist bei Adjust, die Entdeckung des SDK-Spoofing Fraud.

Um SDK-Spoofing zu verhindern, hat Adjust einen sogenannten **Signatur-Hash** entwickelt, der mit der Veröffentlichung der SDK-Version 4.12 jetzt für alle Kunden unabhängig von der Nutzung der kostenpflichtigen Fraud Prevention Suite verfügbar ist.

### **Die nächste Evolutionsstufe von AdFraud - So relevant ist SDK-Spoofing**

SDK-Spoofing ist ein gewaltiger Sprung in der Evolution von Fraud. Erste untersuchte Kampagnen weisen eine unterschiedliche Verbreitung von SDK-Spoofing auf. Weltweit machen die betrügerischen Installationen in einzelnen Kampagnen bis zu 80% aus, wobei die Werbetreibenden mit den größten Budgets und den höchsten Auszahlung pro Install am

stärksten betroffen sind.–Nach Einschätzungen von Adjust ist SDK-Spoofing noch nicht an seinem Limit angelangt und wird ohne geeignete Gegenmaßnahmen rapide wachsen.

Seit 2017 ist der Trend zu erkennen, dass Betrüger vermehrt reale Gerätedaten sammeln. Sie tun dies, indem sie eigene Apps entwickeln, die einen echten Nutzen bieten und von den betroffenen Nutzern verwendet werden. Je mehr Nutzer die betrügerische App herunterladen, desto Größer ist der Bestand an Gerätedaten, die den Betrügern als Anbieter der App zur Verfügung stehen.

Mit Hilfe der Gerätedaten können Betrüger nun Installationen anderer Apps vortäuschen, indem sie entsprechende Events auf dem Endgerät des nichtsahnenden Nutzers auslösen und diese als App-Installationen ausweisen. Das Marketing-Budget der App-Entwickler fließt somit in scheinbare Installs von echten Geräten, die in Wirklichkeit gar nicht stattfinden.

### **Adjust Entwickelt Verfahren zum Schutz vor SDK-Spoofing**

Der sogenannte **Signatur-Hash** erweitert die URL um einen neuen dynamischen Parameter, der nicht erraten oder gestohlen werden kann und jeweils nur einmal verwendet wird. Dieser zusätzliche Parameter, kann für jede App im Dashboard von Adjust generiert werden. Marketer haben auch die Möglichkeit, die Signatur für verschiedene Versionen ihrer App zu erneuern. Dadurch können sie die Verwendung alter Signaturversionen im Laufe der Zeit ablehnen und sich so vor Fraud schützen.

Diese Lösung wurde mit der Veröffentlichung der SDK-Version 4.12 (<https://www.adjust.com/support/product-updates/released--new-sdk-for-ios-windows-and-android/>) verfügbar und ist jetzt für alle Kunden unabhängig von der Nutzung der kostenpflichtigen Fraud Prevention Suite verfügbar.

### **Über Adjust**

Adjust ist ein Mobile Measurement Unternehmen, das höchst qualitative Analyse- und Messlösungen für App Marketer weltweit bereitstellt. Mit Adjusts Open-Source SDK können App Marketer Nutzerverhalten, User Acquisition, Marketing ROIs, User Lifetime Kohorten und weiteres messen und analysieren. Adjusts Plattform hält Datensätze mittels der Fraud Prevention Suite proaktiv rein, verifiziert in-App Einkäufe in Echtzeit und stellt ein vereinfachtes Reporting mit verständlichen, verfolgbaren und vergleichbaren Metriken zur Verfügung. Adjust ist sowohl Facebook Marketing Partner, als auch Twitter Marketing Plattform Partner und wird von über 900 Netzwerk- und Analytikanbietern weltweit genutzt. In 2012 gegründet, unterhält das Startup neben dem Hauptsitz in Berlin weitere Büros in San Francisco, New York, São Paulo, London, Paris, Peking, Istanbul, Tokio, Shanghai, Singapur, Jakarta und Moskau.

Kunden von Asien, der EU bis hinzu den USA vertrauen in Adjust: So zum Beispiel führende App Entwickler wie Zalando, Rovio und Zynga, größere Software Unternehmen, wie

Salesforce, Microsoft und Yelp, aber auch globale Brand, wie Universal Music und Warner Bros.

Adjust ist das einzige Mobile Analyse Unternehmen, das die strikten EU Datenschutz- und Compliance-Standards einhalten kann. Target Partners, Capnamic Ventures, Iris Capital, Active Venture Partners und Highland Capital haben in Adjust investiert.