

# How Fraudsters Are Moving Their Tricks In-App

The bad guys are tweaking how they utilize malware

**INTERVIEW** | **MAY 2018**

**Ross Benes**





An interview with:

## **Amit Joshi**

Director, Product and Data Science  
Forensiq



**A**d fraud is prevalent, but often misunderstood by marketers. Amit Joshi, director of product and data science at [Forensiq](#), spoke with eMarketer's Ross Benes about how fraudsters are adjusting their tactics to take advantage of the in-app ad spend surge.

**eMarketer:**

What is a common misconception that people have about ad fraud?

**Amit Joshi:**

People will always say there's mobile fraud and then there is desktop fraud. But really you should think about it as mobile web and desktop in one bucket, and then in-app in a completely separate bucket.

**eMarketer:**

Why do you categorize fraud that way?

**Amit Joshi:**

When you're analyzing fraud, you're thinking about the environment that you're analyzing—regardless of whether it is on a phone or computer. The device itself is less important than the fact that you're looking at a webpage vs. in-app in a completely different environment.

**eMarketer:**

How has the state of ad fraud changed in the past few years?

**Amit Joshi:**

Compared to two years ago, there has been a very heavy shift toward fraud being committed in-app specifically. As the money flows to in-app, obviously that is where the fraud is going to go since that's where they can profit the most.

“When you’re analyzing fraud, you’re thinking about the environment that you’re analyzing—regardless of whether it is on a phone or computer. ”

**eMarketer:**

Have you seen a shift in the types of tactics fraudsters use?

**Amit Joshi:**

Over the last year we have seen a shift in how fraudsters work the malware. The old model is infecting someone’s device and then opening invisible windows in the background to load ads and steal ad revenue.

The new model uses very light malware. Instead of doing all of the fraud on the device itself, they commit fraud on a server somewhere. Instead of sending requests from the server, they pass the fraud through the device so it looks like the requests are coming from the device.

**eMarketer:**

A knock on in-app ad measurement is that it often relies on software development kits [SDKs], which **publishers are hesitant to integrate** since each SDK they add to their app slows down load times. Does this dynamic make in-app fraud detection an uphill battle?

**Amit Joshi:**

I highly disagree with the notion that SDK-based detection is necessary.

**eMarketer:**

Go on.

**Amit Joshi:**

There are a lot of problems around that. Not many folks understand how to integrate SDKs correctly. The other issue is reach. Even if we integrate our SDK, we have to wait for everybody to update the app that they're using so that they get the newest version of the SDK. It can take up to a year to get an actual good level of reach.

That's why we built non-SDK solutions to catch fraud in the in-app world. We don't really use SDK very often unless it is required by the client. We use a combination of JavaScript and server-side based detection.

Interview conducted on May 31, 2018