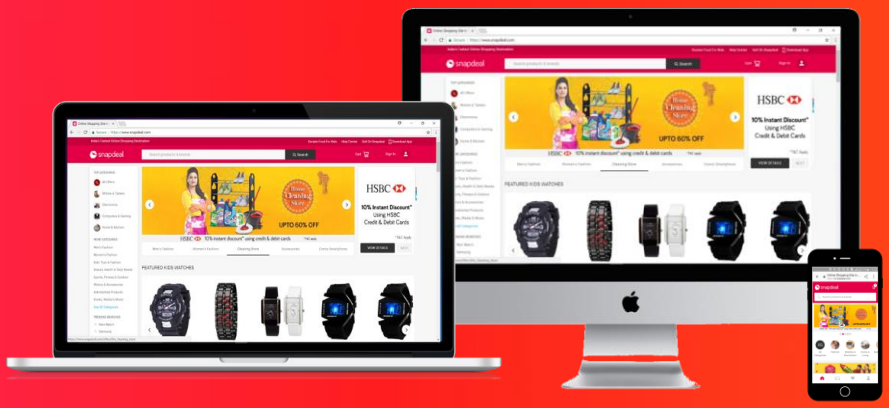


# Snapdeal: Improving Sales Performance Through Reliable Fraud Solution

## Summary


- 31% of the transactions analysed were found to be highly suspicious / fraudulent.
- Two main kinds of fraud found - Click spam and click injection for apps, or cookie stuffing and incorrect attribution for web


## The Brief

Snapdeal a leading e-commerce platform in India, approached MfilterIt with their inorganic sales data. They suspected fraud from a few of their online advertising publishers and wanted a neutral third party Ad Fraud service so as to optimise their advertising spend.

## Our approach

On receiving the Snapdeal's data, Mfilterit's operation team applied advanced algorithms to identify any abnormalities in the sales transactions. Two kinds of frauds were identified: Click Spam and Click Injection.

Due to the offline nature of the analysis, limited algorithms were executed. Mfilterit's additional algorithms estimate a further 5% click fraud.

## Fraud Category 1: Click Spam/ Cookie Stuffing

For this category, this fraud is referred to as click spam for mobile apps, and cookie stuffing for web. This fraud involves the following steps:

**Step 1:** When a user visits a fraudster's website or app, a click is fired in the background towards Snapdeal.

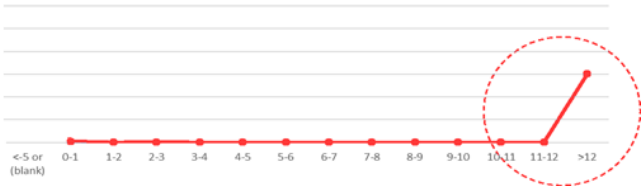
**Step 2:** The click is registered with the fraudulent sub-publisher who then drops a third-party cookie without the user's knowledge.

**Step 3:** When the user actually visits the Snapdeal site and places an order, this organic order is converted to Affiliate.

**Step 4:** The cookie stuffer is hence paid a commission by Snapdeal for assisting a sale, even though the sub-publisher hasn't encouraged a sale.

### Example 1: Large click-to-order-time

One indication of this fraud is the large time gap between the click generated and the order placed. For example, the graph below shows that, out of the given cases that were analysed, about 31% transactions had Click-to-Order time difference greater than 12 hours. This indicates that clicks were generated, but many orders actually took more than 12 hours to convert. Thus, this raises a very serious suspicion of fraud for the given publishers.




## Fraud Category 2: Click Injection/ Incorrect Attribution

This category of fraud is referred to as click injection in the case of mobile apps and incorrect attribution for web. An exception to this may be Coupon sites and re-targeting sites.

This fraud involves the following steps:

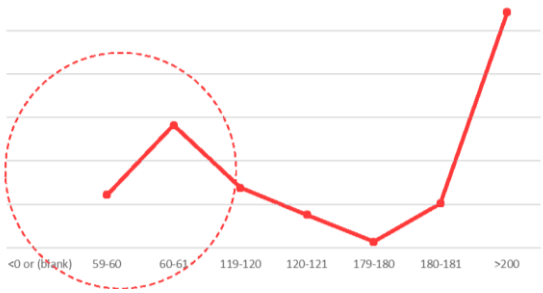
**Step 1:** When a malicious publisher notices that Snapdeal is being used by the customer, a click is injected in the background.

**Step 2:** Now when the customer makes a purchase, the publisher is attributed with the sale.

**Step 3:** The publisher is thus paid a commission by Snapdeal, even though the publisher did not help with the sale.

### Example 2: Low click to order time

One example of this fraud is when the time between the click and order is very low. In the below graph, a strong possibility of fraud is raised when a significant number of transactions have click to order time less than one minute.




> *"We have found MfilterIt to be a very useful solution, helping us reduce and prevent fraud in digital marketing. We have been using their services to specifically identify device and click fraud. Since their technology aggregates data from multiple sources to identify such frauds, we are quite confident of relying upon their solution and optimizing our marketing investments accordingly."*
>
> *- Snapdeal's User Growth Team*

## Results

With MfilterIt's analysis, Snapdeal could confirm its suspicion of fraud in many instances. By identifying a significant chunk of transactions as malicious by many leading advertising partners, Snapdeal was able to take corrective action and better utilise their marketing budget to attract quality customer and thereby increase ROI.