Comprehensive Anti-fraud Kit

To Monitor & Prevent

Ad Fraud

Offer18

Index

Types of Ad Fraud and Ways to Avoid Them

Anti-Fraud Toolkit by Offer18

What is Ad Fraud?

Ad fraud can be any intentional attempt to deceive digital advertising networks for personal benefit. It is an attempt to interrupt the appropriate delivery of advertisements to real users, frequently using bots to commit ad fraud. But this is not the only way, fraudsters use a wide range of tactics to trick advertisers and ad networks.

The Digital Ad Industry grows at a fast pace, and so does the rate of fraud. To combat this, it is imperative to think outside the box and make use of all the tools available. That is why Offer18 comes with a variety of advanced features. The use of these features allows you to monitor fraudulent traffic and prevent it from negatively impacting your business.

Who are Fraudsters?

A fraudster is someone who generates fake traffic, artificially inflates the number of views on an advertisement, or performs similar tactics to make money by fraudulent means. This not only costs advertisers money, but it also harms legitimate publishers trying to make a living in this industry.

Generally they accomplish this by:

- Making payouts for bogus advertising clicks
- Earning money for misleading conversions (installations / subscriptions)

Types of Ad Fraud and Ways to Avoid them

1. Click-Flooding / Click Spamming

In this type of fraud, fraudsters perform bogus clicks for credit on organic app downloads. Since ad networks usually pay those whose ads lead to the last click, they attempt to capture the last click.

Prevention

The **Fraud Fender** makes it possible to monitor click flooding. If you are receiving large numbers of clicks from the same Batch IP / ISP / Unrecognized devices/browsers, then it could be bot traffic.

By using **Click Spamming Defender**, you can prevent spam clicks. Another way to block multiple clicks from the same IP address is with a **Unique Click Limit** Filter. You can set a limit of one click, and more than one click from the same IP will be rejected automatically.

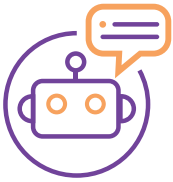
2. Click Injection

This is a form of last-click attribution. In this type of fraud, fraudsters install malware on the mobile phones of individuals. Once it detects a user installing an advertiser app and a click is just triggered before the app installation, fraudsters claim credit for it.

Prevention

The time gap between installation and click usually remains very short in such kinds of frauds. So it can be prevented using **CTIT** by setting a minimum duration for installation. Any conversion that occurs before the specified time will be marked as per the chosen status.

3. Bot Traffic/Invalid Traffic



Any non-human traffic on the website or app is referred to as "bot traffic." Bot traffic is often interpreted negatively, but it doesn't necessarily mean that it's bad or good; it just depends on what it is used for.

Prevention

Numerous tools can be used to monitor and prevent bot traffic. You can evaluate it in the **Fraud Fender** to see if you're receiving traffic from the same IP/ISP/location. Also, you can use **Conversion Risk Monitor** to see how long it takes between clicks and conversions.

4. Spoofing

It is an act where fraudsters gain the trust of customers and later on acquire access to the critical information of their system to harm them with malware, hack sensitive data, or else end up causing turmoil. Generally, there are three types of spoofing :

- **SDK Spoofing** - Commonly known as "traffic spoofing," where fraudsters use an actual device to make fake installs. This category includes the act of creating valid-looking installations with real information, but no actual installations are included.
- **Domain Spoofing** - Fraudsters use domain spoofing to fake a high-value domain that is worthy of more money. Although the impressions and users are genuine, the site's quality remains low.
- **User Agent Spoofing** - Bad actors modify the header in the web page request to hide details about the user's browser. This tactic is frequently used by fraudsters to conceal bots.

Prevention

It can be prevented using **Proxy Block,** because in this case, conversions come from proxy servers. Once you select "enabled" from the drop-down of the proxy block feature, any traffic obtained from the proxy browsers or servers will be automatically blocked. This will make sure that advertisers receive high-quality traffic.

5. Fake Install

Here, a fraudster misleads the affiliate by showing an app install that never happened in reality, or when the install is completely synthesized. This could lead an advertiser or marketer to believe that they've discovered a brilliant publisher. This type of fraud can be done through:

Malicious App Fraud / Code Injection - Using bogus apps, fraudsters set up subscriptions/ installations. Although it looks like a genuine app, it contains malware that processes an installation in the background.

Device Farms - A device farm is made up of a huge multitude of devices that perform repetitive tasks like installs, sign-ups, and engagements. In most cases, advertisers pay for it, but there are no authentic users.

Cookie Stuffing - is one of the most common types of ad fraud because it is intended to deceive and reduce audience information, thereby messing up the outcomes of a whole campaign.

Prevention

Such kinds of malicious app fraud can be monitored with the **Conversion Risk Monitor** tool because in this case, conversions occur within a few seconds of the click, which can be blocked using **CTIT**.

Device Farms and cookie stuffing can be prevented using **Proxy Block** to stop numerous installations from the same ISP/Proxy IP all at the same time.

6.1 Incentive Traffic

To improve the app rating, advertisers sometimes offer monetary rewards to people for making installs. This is not fraud, but fraudsters use it to mix incentives with genuine traffic to meet daily download limits.

6.2 Misleading Incentive

In this type of fraud, a customer responds to an advertised incentive, but the end result is not what was intended. For example, users click on messages like “You have won a prize! After clicking, the fraudster forces the user to complete more steps.

Prevention

Generally, in the case of incentive traffic, the conversion ratio remains very high and the CTIT remains almost the same. To avoid this type of traffic, the ideal practice is to set a general CR value in **Offer Automation**.

7.1 Hidden Ads / Ad Stacking / Pixel Stuffing

Here, the ad is displayed in such a manner that the visitors do not see it. This type of malfeasance aims at ad networks that pay for views rather than clicks.

7.2 Click Hijacking

A malicious actor redirects a click from one ad to another. Clicks are stolen, while the user believes he has tapped a certain button but hasn't. Unintentionally, he clicked elsewhere.

Prevention

There is a way to block this with **Proxy Block** Feature because in this case, the majority of the clicks come from proxy servers. Alternatively, you can also make use of an **IP Range Filter** to filter out known anonymous IP addresses.

8.1 Misinformation

In this case, the merchant offers all the details that regulators require. However, they represent it as insufficient or misleading, which ultimately results in the required action.

8.2 Disinformation

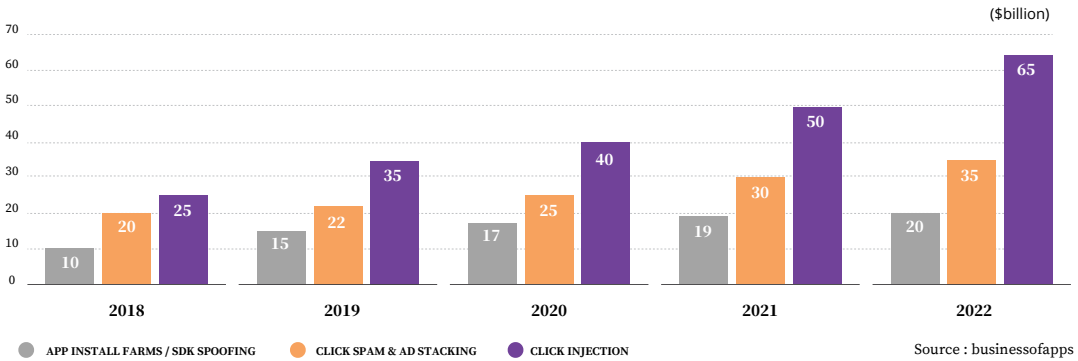
Appropriate action details are lacking here. Fraudulent sellers conceal the price or purchase-critical details. Untrustworthy sellers also hide billing invoices, making it impossible for users to unsubscribe if they find a fraudulent subscription.

Prevention

It is possible to prevent this through the use of **Offer Automation**, since the CR in this case, will remain very high. Depending on the setup, you can set a certain range of CR at the source/sub-source level and block traffic from them if the Conversion Ratio exceeds the limit set.

Ad Fraud Statistics

There has been an increase in the three major types of online ad fraud in recent years. As per the study, App Install Farms/SDK Spoofing has a likelihood to reach $20 billion by the end of 2022. Furthermore, the study predicts that it will reach $35 billion for Click Spam and Ad Stacking along with $65 billion for Click Injection.

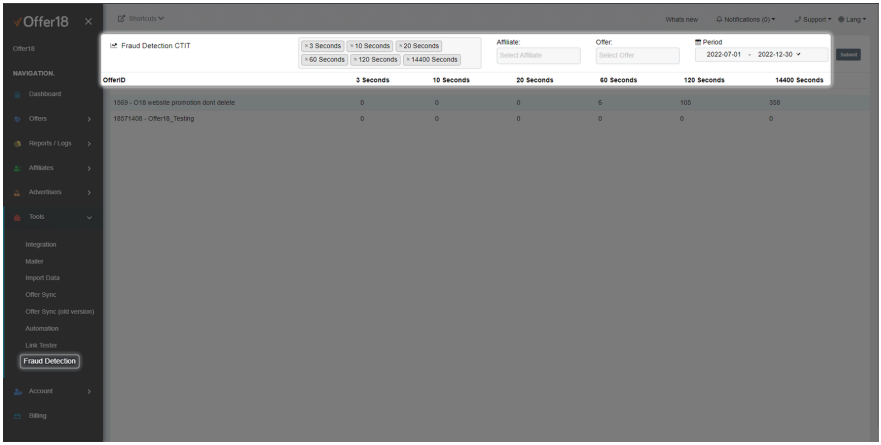


Source : businessofapps

Anti-Fraud Toolkit

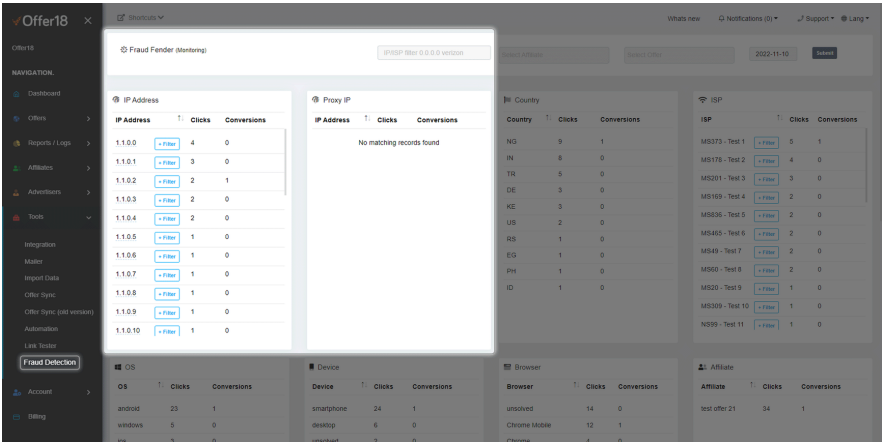
- **Conversion Risk Monitor**

CTIT is one of the first and most relevant variables to look at when investigating suspected fraud attempts on your traffic. It is a vital part of fraud identification and attribution fraud. A Conversion Risk Monitor helps you detect conversions that occur within a certain period of time that must be fraudulent. So, this is a very effective method to minimize the impact of bot traffic.



- **Fraud Fender**

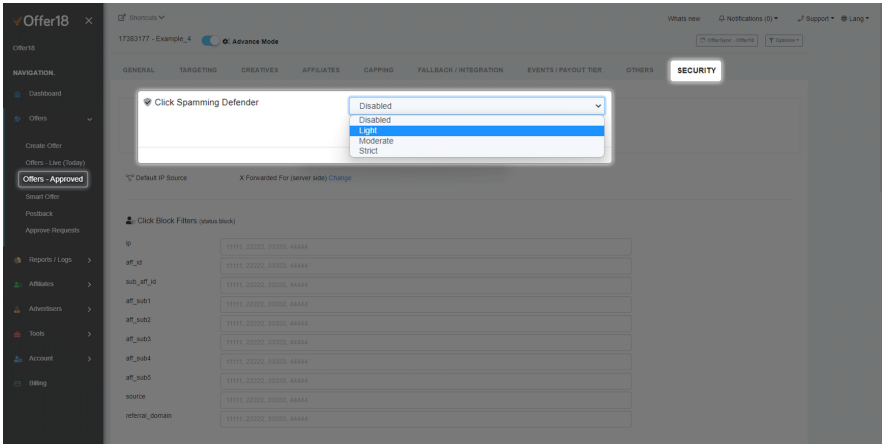
Fraud Fender is a fraud/bot monitoring tool that gives you an overview of your traffic quality. Clicks from the batch of IP/ISP, a Referrer with a bad reputation, multi-conversions from the same IP, and unrecognized devices or browsers lead to bot traffic. With the help of this tool, you can detect this kind of traffic as well as filter out the sources that are sending you repeated clicks.



- **Click Spamming Defender**

  To tackle Click Spamming ad fraud, Offer18 comes with Click Spamming Defender to continuously monitor traffic trends. When users enable this option, spam traffic based on their traffic sources starts to filter out. It functions on the predefined algorithm that automatically stops click flooding.

  It could be evidence of ad fraud if you're not receiving the conversions you desire or if you're getting traffic that seems too good to be real. A security algorithm gives you 3 modes based on the user's requirements, i.e., Light, Moderate and Strict.

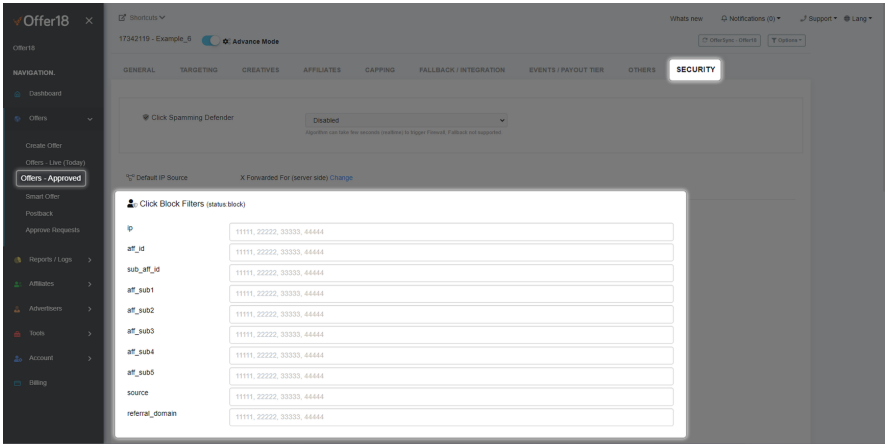


- **Click Block Filters**

  You can use the below listed filters to block clicks that you suspect will lead to fraud.

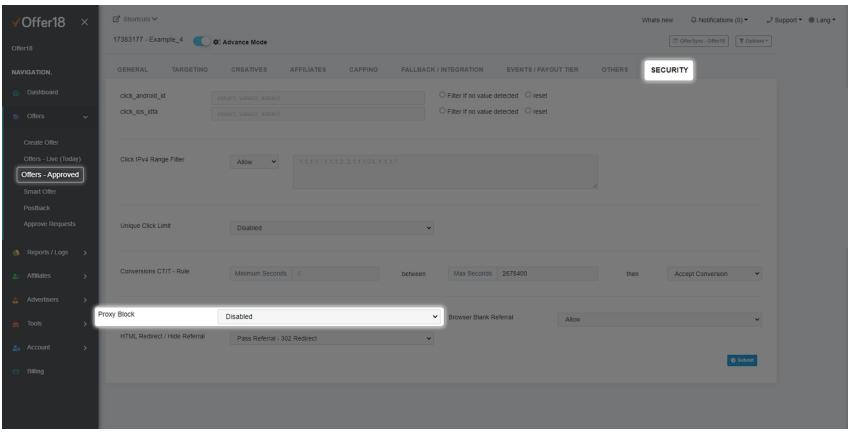
  - IP Address
  - Affiliate
  - Sub Affiliate
  - Aff Sub1 to Aff Sub5
  - Source
  - Referral Domain

  For example, if you are getting bot clicks from the same IP address, you can block that IP address, and the click will be rejected.



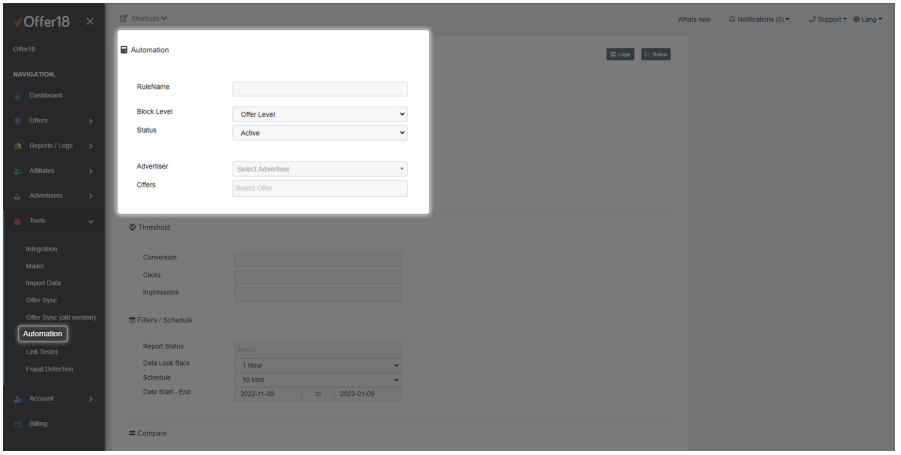
- **Bot/Proxy Block**

  With the help of browser proxy blocks, traffic sent from different locations or user agents by using a proxy can be rejected. Through this, you will receive traffic from the exact location from which you want to receive it and can increase customer lifetime value.



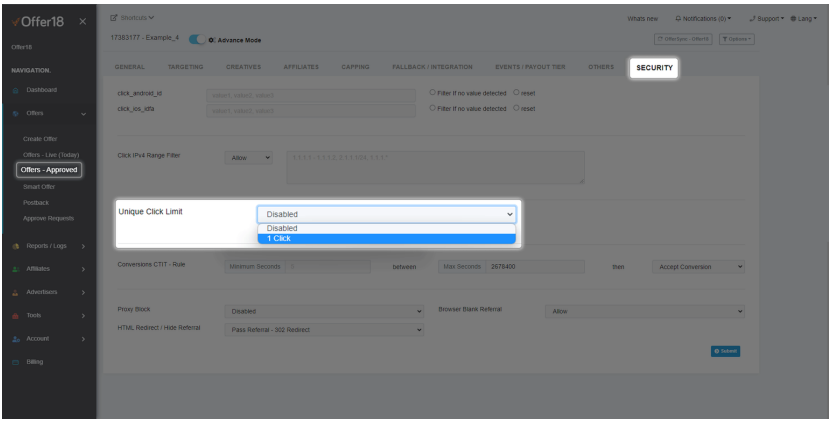
- **Offer Automation**

  If you know the expected CR, CTR, eCPM, etc. then you can block the source that is not fulfilling your expected value of performance metrics. You don't need to do it manually; it can be done automatically with the help of Offer Automation.



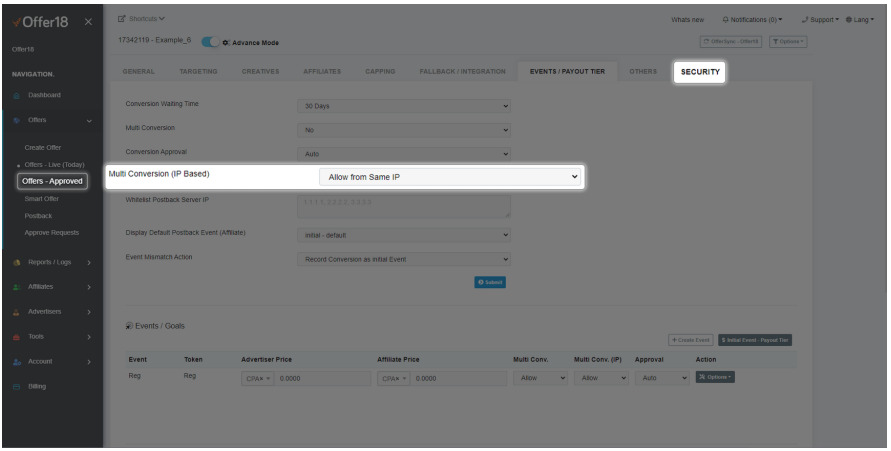
- **Unique Click Limit**

  Unique Click Limit allows you to receive only one click from one browser session ID and prevents click stuffing or click spamming. This is the best practice to block traffic from bots or emulators.



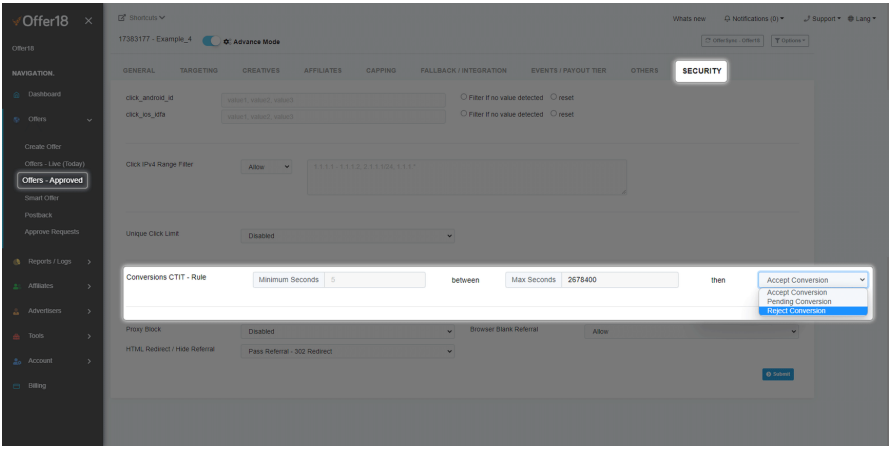
- **Multi Conversions (IP Based)**

  You can allow or prevent multiple conversions having the same Click IP on a campaign level. Those conversions will remain in pending status at your end if you select the "Multi Conversion (IP Based)" option from its drop-down.



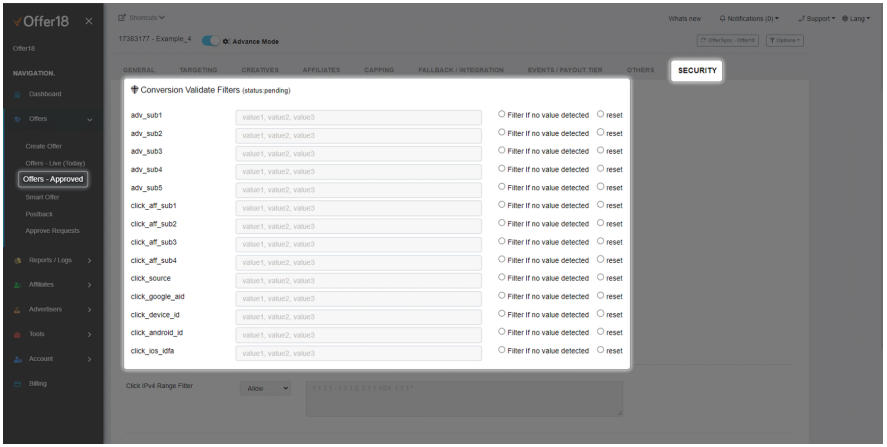
- **CTIT Rule**

  You can set here the minimum or maximum time, which according to you must be the difference between your click and the conversion time. If any conversion gets recorded in between the set time period, then you can choose your action for the conversion status from the given options.



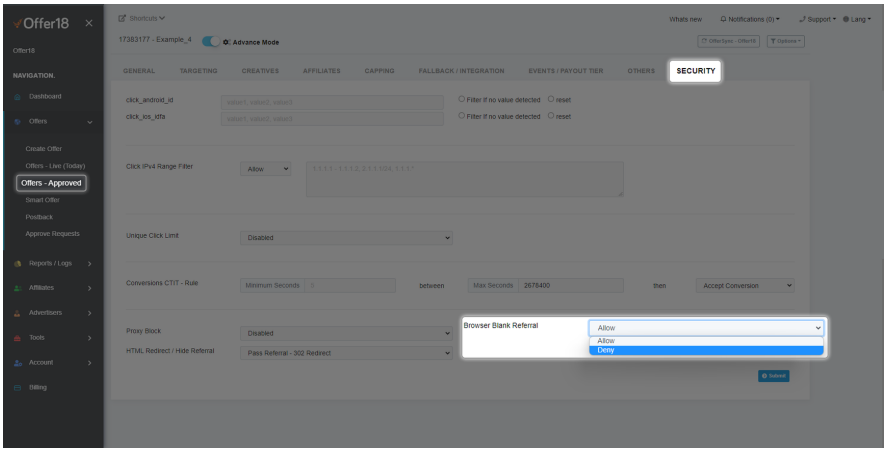
- **Traffic Source/Conversion Validate Filters**

  You can also keep conversions in a pending status until they receive validation from the advertiser end with the help of conversion validation filters. It can also be done either based on a specific value or if no value is detected in particular parameters.



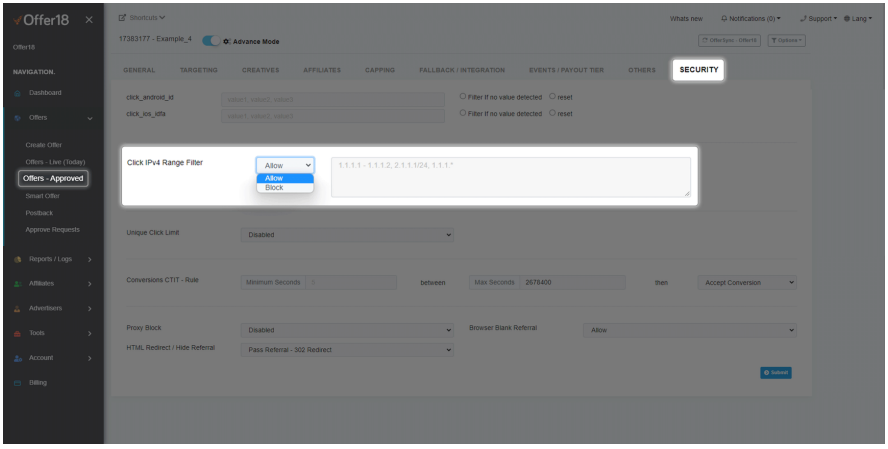
- **Browser Blank Referrer**

  Referrer hide is really common, in which publishers hide their source referrer and send traffic from restricted referrer domains, but the hide referrer block option helps you prevent this kind of technique.



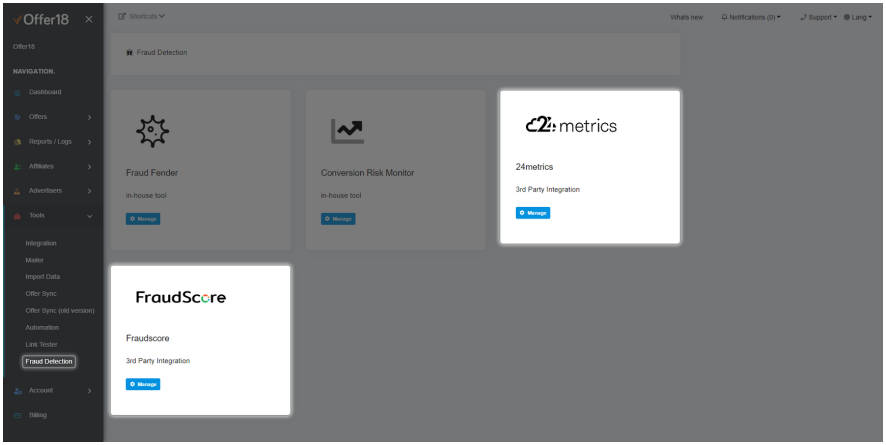
- **IP Range Filter**

  IP-Targeting entails assured advertising. IP targeting allows digital advertisers to pinpoint the precise audience for their ads. You can identify who is engaging when you know who you're targeting. It is possible to analyze the effectiveness of your digital advertising more directly when you are clear on who your targets are and who is seeing your ads. Here it is possible to allow or block certain IP ranges so that fraudulent traffic cannot be routed across specified IP ranges.



- **3rd Party Integration**

  Offer18 is also compatible with other major 3rd party fraud detection tools like 24metrics and FraudScore. You just need to get the API key, and the rest will be done automatically.



Want to Learn More?

Well, knowledge isn't confined to this manual. We have made a collection of sources from which you can learn and apply the provided information to achieve more effective results.

- **How to Use it?**

  From our comprehensive knowledge base in which each and every feature of the dashboard is explained in an understandable manner, along with key steps and useful GIFs on how to use it.

  Knowledge base

- **[Video] Affiliate Fraud Prevention - Offer18**

  In addition to reading, videos are a great way to learn about fraud and prevention. An internal toolkit of fraud detection tools along with third-party tools provided in the dashboard saves your ad campaigns and ultimately your profits.

  Watch the Video

- **How are Others Using Offer18 to Combat Ad Fraud?**

  Our valued clients have been using Offer18 for many years and are extremely satisfied with the results. They confirm that such tools provided protection to their campaigns against fraudulent conversions and boosted their revenue.

  Case Study

In the Final Analysis

Ad fraud is a substantial concern for all marketers. They are committing such fraud on a massive scale, which has a significant impact on the company's revenue and reputation. Despite this, most marketers do not take ad fraud very seriously and hence face immense losses in a later stage.

Ad fraud speedily exhausts ad budgets, which is obviously a major stumbling block to marketers' efforts. The more funds spent on fraudulent leads and conversions, the less budget there is to invest in effective marketing areas.

So, in order to prevent such frauds and guide marketers in implementing best practices, we formed this user guide of dominant frauds and Offer18's power pack tools to combat such frauds. This will assist you in defeating such fraudsters' tricks and providing a healthy solution to safeguard your ad campaigns.

Reach Us

hi@offer18.com

www.offer18.com