

THE KAMA
INSIGHT
SERIES

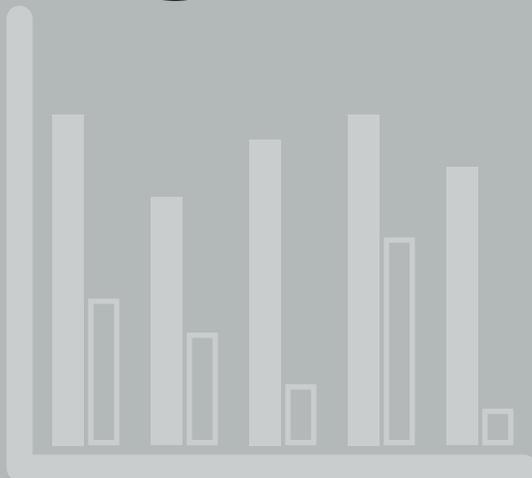
**FIGHTING
FRAUD
IN USER
ACQUISITION**

“It is unsurprising that with over 1.5 million apps currently available via the Play Store and App Store, that it is becoming more challenging for developers to get their app noticed in such a saturated, “red ocean” market place - and that’s just the first step in building a sustainable gaming business”



ANA

whiteops



KamaGames 2017

In a recent Newzoo report, it was reported that gamers worldwide generated over \$99.6 billion in revenue in 2016, an increase of 8.5% compared to 2015. For the first time, mobile games were also taking a larger share than PC based games at \$36.9 billion, up 21.3% globally. The global games market is expected to grow with a compound annual growth rate of +6.6% going into 2019 which will see the overall market reaching \$118.6 billion and mobile gaming \$52.5 billion.

When looking specifically at the social casino games market, the most recent Eilers & Krejcik report estimated an increase of +13.6% y/y growth to \$3.81 billion in CY16. Combined, the top 3 companies accounted for 41% of the total social casino games market, while the top 15 companies accounted for roughly 82% of the total market.

Mobile games revenue accounted for 71% of all social casino game revenues generated in CY16 versus 64% in CY15 showing a very clear growth in the sector.

In addition to the compound nature of the market when it comes to the top 3 companies, research also showed that the top 10 apps generated \$481 million in Q416 and accounted for nearly half of all the social casino revenues generated worldwide. When using a “rule of thumb” formula that states in order to get an app into the Top 25 Apps on the US App Store, it would need to acquire 38,000 new users every day – and that’s a lot!



THE IMPACT OF FRAUD

According to research carried out by the Association of National Advertisers and White Ops, advertising fraud would have cost digital advertisers well over \$7.2 billion in 2016.

ANA/WhiteOps study reveals bot fraud will cost marketers more than \$7B in 2016 without increased focus.

Keeping this significant figure in mind, it is surprising that the topic of the impact of fraud on user acquisition and that of fraudulent traffic, has not received more attention than it has done and is still, in many cases, being overlooked.

The subject of fraud has always been some what taboo, but recently the topic has started to be discussed more openly. KamaGames recently covered this topic at a talk given at the Pocket Gamer Connects conference in London. The amount of attention the talk drew led us to expand upon it further here.

“Mobile in-app advertising is one of the youngest and fastest growing parts of online marketing and so there is very high competition combined with low market regulation”



KamaGames 2017

Mobile in-app advertising is one of the youngest and fastest growing parts of online marketing and so there is very high competition combined with low market regulation. This means there are an ever growing range of opportunities for publishers and developers to be cheated. In 2015, a report from VentureBeat stated that the number of games publishers and developers who said they were victims of fraud increased by almost two thirds.

Two-thirds of mobile developers find themselves victims of mobile user acquisition fraud.

In 2016, VentureBeat again reported that games publishers and developers stood to lose up to a staggering \$100M as a direct result of fraud.

THE ROUTES OF FRAUD

Unsurprisingly the level of fraud is significantly higher for countries with higher Life-Time Value and where the competition for quality paying players is significantly higher. These countries are referred to as “Tier 1” countries which feature the United States and the countries in Western Europe at the top of its list.

Mobile app marketers will lose \$100 million to fraud this year.

At KamaGames, we encounter fraud attempts from multiple routes on a daily basis. One of several routes that are seen more regularly is the fraud via traffic from affiliate networks and 3rd party agencies where it is more complex to see where their traffic is coming from as it's far from transparent. This is mostly due to the multiple entities between the traffic source and the publisher.



“The easiest way to detect incentivized traffic is to monitor the player’s early metrics which happen just after install, no more than 1-2 days, and also metrics with high probability, metrics based around consistency of what 80-90% of organic users do”



INCENTIVIZED OR MIXED TRAFFIC INSTEAD OF NON-INCENTIVIZED

This is a common example to explore. A target user is playing a match-3 style game and sees a pop up that offers him: *“Watch a video ad, get 3 bonus lives”*. Most users will, of course, watch the ad not because they are interested in the video or the app which they need to install, but because they are interested in getting the 3 bonus lives. This type of incentivized traffic is more than 10 times cheaper than non-incentivized which makes this type of fraud extremely profitable for some fraudulent networks as a lot of publishers and developers think they are buying non-incentivised traffic when it is the exact opposite.

So, how best to tackle it?

INCENTIVIZED TRAFFIC

The easiest way to detect incentivized traffic is to monitor the player’s early metrics which happen just after install, no more than 1-2 days, and also metrics with high probability, metrics based around consistency of what 80-90% of organic users do. For example, some games have *“achieve level 3”*, in other games it’s the *“completed tutorial”* event being triggered.

KamaGames know what the normal conversion rate for this metric is across their users and therefore any significant deviations (more than 10-15% for such high probability



metrics) are an indicator of incentivized/mixed traffic.

INCENTIVIZED EVENTS

To detect an incentivized event such as *“Play 5 levels and get X in rewards”*, KamaGames monitors the deeper metrics that happen less often and not as soon as the ones mentioned previously to detect incentivised traffic. There are events such as *“Achieve level 10”* or *“Open 2nd location”* which our average user will trigger on the 3rd or maybe 4th day after the install (with the probability of around 45-55%). By cross checking several metrics, we can identify if this traffic has come from an incentivized event and is a result of a *“Play 5 levels and get X”* type incentive.



“To minimise the effect of such fraud, publishers should continually check the distribution of paying players by tiers and analyse their actions and routines after they made a payment. Most likely, these newly acquired players will not continue to play”



IMITATION OF HIGH PERCENTAGE OF PAYING PLAYERS

This is the hardest variation of incentivized traffic to detect. Typically, the publisher will see expected metrics for their user's activity, including as well as good or even above average conversion to paying players. Due to these early encouraging results, the publisher is likely to be tempted to increase its spend into this "high performing" network - only to find out that while conversion rates were high, total payments and the average payment amount (and consequently, revenues) were abnormally low.

This is actually mixed traffic as one part is non-incentivized traffic and the other part is incentivized purchases traffic. Typically - there will be a lot of minimal spend purchases (e.g. \$1).

To minimise the effect of such fraud, publishers should continually check the distribution of paying players by tiers and analyse their actions and routines after they made a payment. Most likely, these newly acquired players will not continue to play.

GEO CHEATING

The last of the more common types of fraud is the selling of cheap traffic disguised as expensive traffic. Fraudsters are aware of the users' Life-Time Value across the different countries and are manipulating the tracking platforms by altering the country of install (which is typically validated by IP). Fortunately, there are few other indicators which can help to define the actual origin of install such as language, location and a mobile carrier of a phone collected by the trackers (or a combination of those).



“The automated system monitors a wide number of metrics to help minimise the impact of fraud on UA activity. Currently, fraudulent traffic is being detected within 2-3 hours of the test campaigns going live. In 2016 alone, the system saved hundreds of thousands of marketing Dollars due to the early detection of fraudulent traffic”



KamaGames 2017

FIGHTING FRAUD

For the past few years, KamaGames has invested resources in developing its own anti-fraud analysis and optimisation system, which is based on years of experience and huge data collected over time.

The automated system monitors a wide number of metrics to help minimise the impact of fraud on UA activity. Currently, fraudulent traffic is being detected within 2-3 hours of the test campaigns going live. In 2016 alone, the system saved hundreds of thousands of marketing Dollars due to the early detection of fraudulent traffic.



“Installing suitable solutions to minimise the impact of fraudulent traffic is a ‘must have’ for any publisher planning to spend on acquiring users”



KEY TAKEAWAYS

- The level of fraud in the mobile app industry, and specifically in the gaming industry, is increasing year by year. Installing suitable solutions to minimise the impact of fraudulent traffic is a ‘must have’ for any publisher planning to spend on acquiring users
- A significant amount of the source of fraud is coming from non-transparent 3rd party agencies and affiliate networks. This is why working with agencies you trust is imperative
- Incentivized and/or mixed traffic instead of non-incentivized is the cheapest and the most popular type of fraud. Tracking and

monitoring the early metrics in real or near-real time will help to significantly reduce the threat

- Monitor a number of metrics during the lifetime of a campaign and pay attention to all deviations or irregularities
- Work with the larger and well known networks who work directly with the publishers and get the traffic via SDK and then pass the names or ID’s of sources straight to the publisher
- Monitor any significant deviations or irregularities such as a group of users having the US as a country of origin but they are using an Indian carrier, or it uses Vietnamese language for example



“KamaGames is a global developer and a publisher of social casino hits designed for mobile, social and smart TVs”



KamaGames 2017

ABOUT KAMAGAMES

KamaGames is a global developer and a publisher of social casino hits designed for mobile, social and smart TVs.

Bringing together creativity, proprietary technology and a passion for games, KamaGames has built a premium portfolio designed to deliver real-life entertainment to the masses.

KamaGames' Random Number Generator (RNG) is certified by iTech Labs and meets the highest standards to guarantee fair play.

The award winning flagship game, Pokerist(R) Texas Poker, was named one of the Best Apps by Apple, #1 Top Grossing App on the Apple App Store in 89 countries as well as being in the Top 5 Google Play Grossing Apps in 24 countries.



**POKERIST
TEXAS POKER**

www.pokerist.com



ROULETTIST

www.roulettist.com



BLACKJACKIST

www.blackjackist.com



BACCARIST

www.baccarist.com



**OMAHA
POKER**

Coming Soon



To learn more about KamaGames visit :
www.KamaGames.com



Like us on
Facebook



Follow us
on Twitter

THE KAMA INSIGHT SERIES
**FIGHTING FRAUD IN
USER ACQUISITION**

For more information contact:
Sam Forrest, Director of Global PR,
KamaGames.

S.Forrest@KamaGames.com