ADDRESSING AD FRAUD THROUGH MULTIPOINT ANALYSIS & MACHINE LEARNING

trafficguard

JUNIPER RESEARCH

Contents

1. Digital Advertising Fraud: The Current Pain Points

1.1 Fraud & Mobile Advertising

As consumers spend more time on mobile, ad spend and ad fraud have also been growing on mobile channels. Spend on mobile advertising exceeded spend on desktop advertising for the first time in 2015, with 60% of global digital advertising budgets anticipated to be attributable to mobile advertising in 2018.

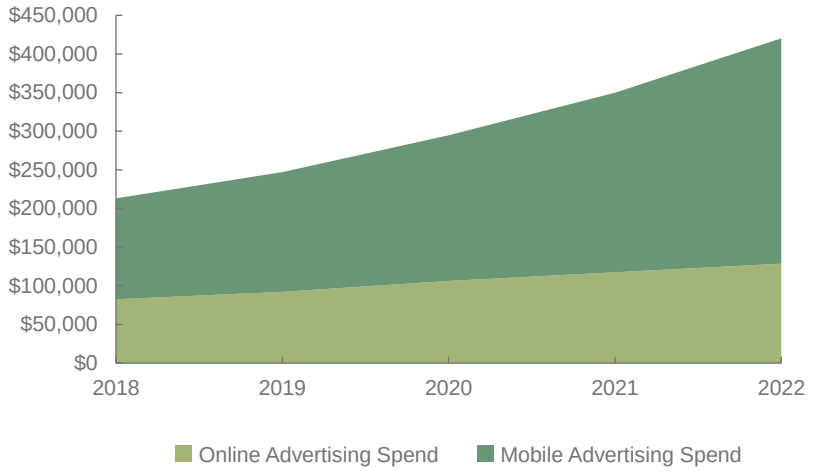
Increasing mobile advertising budgets have created a compelling opportunity for perpetrators of ad fraud.

In 2017, digital advertisers lost US$39 million per day to fraudulent activities, as these undergo continuous innovation to avoid detection.

Advertisers in the APAC region will lose US$17 million per day. There are a number of tools and solutions app developers and advertisers can adopt to mitigate the prevalence of fraud in their advertising campaigns. However, the capabilities of these solutions differ; leaving stakeholders open to varying levels of loss due to fraudulent activities.

These solutions must also be able to adapt to the changing advertising fraud landscape. As fraudsters innovate to evade detection, fraud detection solutions must remain vigilant against new types of ad fraud.

Figure 1.1: Global Online & Mobile Advertising Spend (US$m), 2018-2022



Source: Juniper Research

1.2 Ad Fraud Pain Points & Their Impact

Brands and app developers expect that when they advertise their products, they are communicating with legitimate consumers that have the potential to become their customers. Unfortunately, that is not always the case. IVT (Invalid Traffic) occurs when interactions with advertising are not from legitimate consumers. In cases where IVT is intentionally created to attract ad spend, it is commonly referred to as ad fraud.

For simplicity in this White Paper, the terms ad fraud and IVT are used interchangeably.

Fraud can occur in various forms and fraudsters are using increasingly sophisticated techniques to evade detection and trick attribution platforms.

The ingenuity of advertising fraudsters in evading detection is a constant challenge for advertisers to reduce ad fraud and maximise ROAS (Return on Ad Spend). This problem is further compounded by the sheer volume of advertising engagements. It is becoming increasingly evident that advertising fraud will continue to hamper app developers and advertisers' efforts to secure a return on their advertising spend. If stakeholders do not implement effective controls, then they risk losing business to competitors.

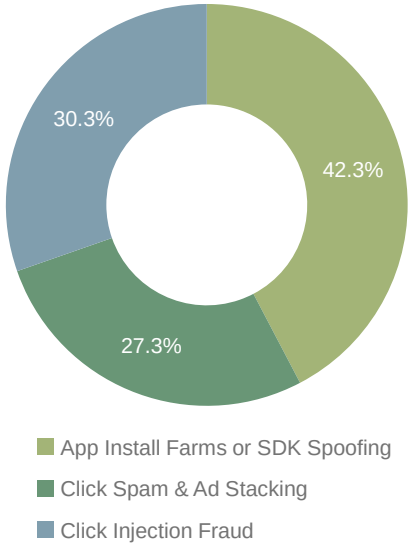
1.2.1 Direct & Indirect Costs of Ad Fraud

Dependent on the capabilities of fraud detection and mitigation tools adopted, advertisers are susceptible to varying degrees of advertising fraud. The adoption of IVT reporting tools, blocking fraud at a single level (ie attribution) or multipoint analysis and mitigation tools, will dictate the level of recovered advertising spend that could be lost to fraudulent activities. Whilst GIVT (General Invalid Traffic) is often easy to detect and eliminate; SIVT (Sophisticated Invalid Traffic) is perpetrated by fraudsters who implement processes to evade detection. By tracking each app install or ad transaction through its journey, multipoint prevention tools are able to efficiently analyse traffic and remove increasingly sophisticated fraudulent ad activity. Failure to do so will inevitably lead to wasted advertising spend and impact performance; limiting advertising returns and effectiveness.

Juniper calculates that globally, 1 in 13 app installs will not be from genuine users in 2018.

SDK Spoofing and Install App Farms will continue to be a major concern for mobile app advertisers. This issue is expected to increase, with 1 in 10 app installs expected to be fraudulent by 2022.

Figure 1.2: Proportional Wasted Advertising Spend Owing to Common Fraud Tactics in 2018 (US$25.8bn)



Source: Juniper Research

The direct and indirect impacts of fraud, along with their associated costs, vary based on the strategies employed by the advertiser to protect their ad spend. The key impacts that advertisers are likely to face for any given anti-fraud strategy, from only having reporting in place (detection) to deploying solutions with sophisticated means of removing IVT (prevention), are outlined in the next section.

1.2.2 The Effectiveness of Ad Fraud Mitigation Strategies

The degree of loss to which advertisers are subject to will vary depending on their approach to managing IVT. The matrix below summarises possible strategies and the potential each offers for mitigating the various impacts of ad fraud.

Table 1.3: Ad Fraud Mitigation Strategy Impact Matrix

	No reporting	Reporting only	Single level blocking	Multi-level blocking
Wasted media spend	🔴	🟡	🟡	🟢
Downstream wasted media spend	🔴	🔴	🟡	🟢
Investment in fraud inflated sources	🔴	🟡	🟡	🟢
Time wasted & poor investments	🔴	🟡	🟡	🟢
Loss to chargebacks & refunds	🔴	🔴	🟡	🟢
Threat of litigation	🔴	🔴	🟡	🟢
Diminishing campaign optimisation	🔴	🔴	🟡	🟢
Damaged reputations & lost trust	🔴	🔴	🟡	🟢
Multiple levels of fraud	🔴	🔴	🔴	🟢

Source: Juniper Research

Figure 1.4: Ad Fraud Mitigation Strategy Impact Matrix Key

Source: Juniper Research

No reporting: When an advertiser chooses to turn a blind eye to IVT.

Reporting only: When an advertiser has tools in place to detect and report on IVT. This reactive approach enables the advertiser to take some action after the fraud has occurred.

Single level blocking: Rudimentary fraud prevention, where fraud is blocked at a specific stage in the user journey. When fraud is blocked, many of its impacts are reduced. However, this approach means that fraud can still skew performance data and impact optimisation.

Multi-level blocking: Proactively blocking fraud as soon as it is detected resulting in the most comprehensive level of protection.

i. Wasted Media Spend

This is the most obvious and commonly reported impact of ad fraud, the cost of each invalid media purchase. Juniper estimates that an advertiser with no detection or protection in place running a US$10 million advertising campaign will, on average, waste US$2.6 million of this spend to fraudulent activities.

Adoption of detection tools will allow visibility of IVT, however additional actions must then be taken to recover wasted ad spend or dispute valid traffic volumes with suppliers.

Multipoint fraud prevention will analyse hundreds of fraud indicators per ad transaction across both the click and attribution levels to detect and block IVT. Only blocking can truly stem the flow of ad spend to fraudulent IVT.

ii. Downstream Wasted Media Spend

In addition to the advertiser, many networks and agencies can be involved in each advertising trade. Downstream media spend is defined as the ad spend which these intermediaries incur in the process of acquiring traffic for advertisers.

Intermediaries are players involved in the advertising transaction aside from the advertisers, including ad networks and agencies. These stakeholders typically operate on shorter payment terms than advertisers. When an advertiser only detects fraud, often in the time it takes them to report IVT to intermediaries, the latter have already unknowingly paid their sources, leaving them out of pocket for the IVT. With little transparency afforded to intermediaries, ultimately their own efforts to limit IVT in their supply can be restricted; perpetuating the cycle of fraud.

By using tools that block at a single level, this can be mitigated to an extent. However multipoint analysis will enable the highest degree of efficiency by blocking IVT as it is detected; reducing wasted media spend downstream.

iii. Investment in Fraud Inflated Sources

There are two key characteristics that drive an advertiser or intermediary to increase operations with particular traffic sources; quality of ad traffic and the success rate of conversions. With no fraud detection in place, it is hard to get a timely insight into quality to guide these decisions. Fraud inflates volume metrics, making low quality sources appear to be high performing. The result is advertisers unknowingly increasing investment in sources of IVT, compounding their losses further.

Using ad fraud detection tools, an advertiser can manage their own optimisation decisions but, unless IVT is blocked, the intermediaries in the supply chain are unable to optimise the quality of their advertising media until they receive feedback from the advertiser. This ultimately restricts advertising potential for the advertiser.

Juniper estimates that an advertiser displaying 1 million ads in a 24 hour period will pay for more than 100,000 fraudulent ads on average before detection.

Blocking IVT at the attribution level is a substantial improvement as the potential for an intermediary to be misattributed credit is reduced. This means when they optimise according to the number of valid attributions, they are looking at data that has had IVT filtered out. However, blocking at the attribution level only means that there is still a significant level of IVT present at the click level.

With a multipoint approach, IVT is blocked as it is detected, as opposed to waiting for the attribution after the fact. Reporting from a multipoint

analysis tool ensures the most accurate and timely understanding of quality for fast and effective optimisation.

iv. Time Wasted & Poor Investments

Loss due to advertising fraud is not limited to the financial loss of media spend. Advertisers that can detect, but not block IVT, spend considerable time interpreting IVT reporting and taking subsequent actions based on the insights gained, then reconciling media volumes with intermediaries to try to claw back their misplaced ad spend.

The time recovered by blocking IVT in real-time can then be used on proactive projects that promote growth and improve the performance of advertising campaigns, rather than focusing efforts on limiting loss to ad fraud.

v. Loss to Chargebacks & Refunds

In cases where IVT blocking has not been used, negotiations to resolve volume disputes are time consuming for both advertisers and intermediaries. When it comes to reconciling conversion volumes, often the resolution is issuing some type of refund or credit to the advertiser.

By employing tools to effectively block IVT, time wasted on these disputes is eliminated.

vi. Threat of Litigation

Unresolved conversion volume disputes can expose advertisers and intermediaries to costly and time-consuming litigation cases over the prevalence of fraudulent advertising. For companies relying on reporting to drive conversion volume reconciliation processes at invoice time, this risk is particularly relevant. Disputes between advertisers and ad networks on the level of fraud and misrepresentation of ad reach diminish the value of the product on all sides.

Employing multipoint prevention enables real-time blocking of fraud before spend is attributed to incorrect sources; reducing the need for conversion volume reconciliation and therefore mitigating the risk of litigation.

vii. Diminishing Campaign Optimisation

When considering the capabilities of an ad fraud detection solution, the coverage level of the detection platform is important. Many platforms may limit their assessment of traffic to a sample to minimise costs. However, this can lead to an inaccurate representation of the level of fraudulent traffic over entire advertising campaigns, which in turn can also lead to ill-informed strategic decisions in the future.

Fraud detection only goes part way to addressing diminishing campaign optimisation as the advertising industry continues to operate ‘walled gardens’ with regards to information transparency. Only the advertiser gets access to the levels of exposure to IVT and they share quality reporting on a periodic basis.

However, for a campaign to reach its potential, intermediaries need access to real-time fraud reporting, as well as advertisers. Where IVT is blocked in

real-time, sources with fraud are naturally optimised out of the supply, in favour of genuinely higher performing sources.

Multipoint prevention tools provide the level of transparency for real-time, actionable quality insights that drive full campaign optimisation; not just from the advertiser but also from their suppliers.

viii. Damaged Reputations & Lost Trust

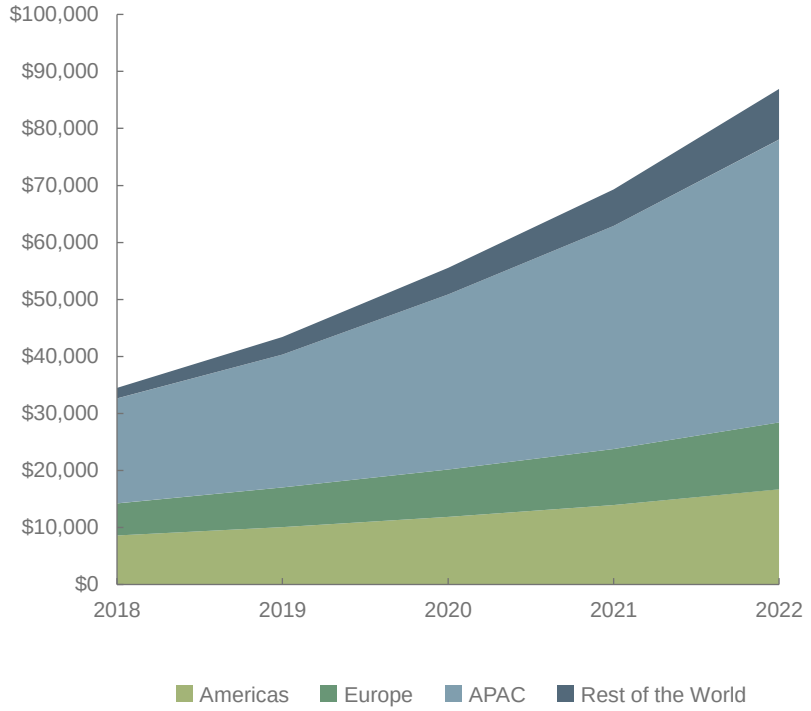
This cost is largely the burden of intermediaries which unknowingly supply IVT to their clients. Over time, the trust between these traffic suppliers and advertisers will diminish. Once damaged, it can be a lengthy process to rebuild a reputation tarnished by fraud and IVT.

This impact is very common, particularly when advertisers employ detection tools that are opaque to their intermediaries. This approach begins to resemble a witch hunt in a time when the industry is calling for collaboration and transparency to fight fraud.

By 2022, the total loss to mobile advertising fraud is forecast to reach US$87 billion, rising from US$34 billion in 2018.

In the APAC region, Juniper Research anticipates that loss to reach US$56 billion in 2022, from US$19 billion in 2018.

Figure 1.5: Total Loss of Mobile Advertising Spend to Fraud (US$m) Split by 4 Key Regions 2018-2022



Source: Juniper Research

2. Anti-Ad Fraud Service Comparison

2.1 Ad Fraud Detection & Mitigation: Solutions Comparison

Only ad fraud prevention solutions which both detect and prevent IVT can fully address advertising fraud to reduce the scale of misplaced ad spend. If the correct platform is not deployed, advertising budgets will continue to be subject to fraud in all its evolving forms; leaving advertisers further out of pocket.

The important considerations when implementing fraud mitigation solutions are outlined below:

- Stage in the Journey – This is the stage in the advertising journey when IVT detection or prevention takes place, including impression, click and attribution. As anti-fraud capabilities tend to be an add-on to other products, many solutions available today have a restricted focus on a small proportion of the advertising journey dictated by what their technology was initially developed to do. Some fraud prevention specialists detect and prevent fraud at multiple stages of the advertising journey.
- Detection Capabilities – Automated rule engines filter IVT based on a relatively static set of rules. More sophisticated solutions employ some level of statistical algorithms. These approaches have a limited ability to detect fraud that has not been encountered before; the unknown unknowns. As fraud is constantly mutating to avoid detection, this does leave ad spend exposed. Companies that specialise in multipoint fraud prevention, dedicate resources to evolving, testing and validating the application of ML in their fraud prevention efforts. Ultimately, this offers protection against known fraud tactics, as well as emerging unknown fraud tactics.
- Blocking Capabilities – Blocking capabilities vary across different solutions. The ability to block in real-time is essential to minimising the loss to fraud that can occur at multiple levels of the advertising chain. Thus, it is in the best interests of advertisers to review the extent of their chosen platform's abilities. Best practice is to block IVT as early as reliably detected and to enable blocking at various stages. As fraud tactics become increasingly sophisticated, early stage prevention can be more easily evaded, making later stage detection at the click or attribution level vital in defending against SIVT.
- Reporting Capabilities – Some tools are more transparent than others in terms of what they report and to whom they report it. Sophisticated reporting provides clear reasoning for IVT diagnosis. Tools which extend reporting to intermediaries, as well as advertisers, give power to the whole supply chain to mitigate IVT, rather than just giving refunds when IVT is reported.
- Coverage Level – Coverage level refers to whether a tool processes every transaction or just a sample of transactions. Sample level coverage is common for impression level solutions that deal with high volumes.
- Fraud Tactics Mitigated – An evaluation of the solution's potential to mitigate fraudulent traffic itself. The most comprehensive solutions will block IVT in real-time at multiple levels of the advertising ecosystem.
- Conflict of Interest – Some tools may have a conflict of interest. This might manifest in a conflicting pricing model, where pricing is tied to

volumes of IVT. This incentivises fraud detection and may lead to false positives. Another type of conflict is where measurement platforms which are responsible for attribution, also provide fraud protection. In this case, they could be incentivised to measure poorly and misattribute conversions, in order to process higher volumes through their anti-fraud tools.

- Integration Methods – How an anti-fraud tool integrates dictates its compatibility with different types of advertisers. For example, systems relying on measurement SDKs rely on having their SDK installed on an app. For agencies that run campaigns for hundreds of apps, this integration type is infeasible. Solutions with a greater variety of integration methods provide greater flexibility and are able to offer services to different types of clients.

Multipoint analysis mitigates all these concerns for app developers and advertisers whilst ensuring that IVT is removed swiftly and reliably.

Table 2.1: Fraud Prevention Methodologies, Capabilities & Functionality Comparison

Criteria	Brand Safety/Viewability Tools	Mobile Measurement Platforms' Anti-Fraud Tools	App Install Fraud Detection	Multipoint Fraud Prevention
Specialisation	Brand Safety/Viewability	Attribution (with anti-fraud tools)	App install fraud detection	**Ad fraud prevention**
Stage in journey	Impression. Available only to a direct advertiser at their DSP level.	Install attribution. Available to the app publisher only.	Install attribution. Available to the app publisher only.	**Click and install attribution. Available for agencies, ad networks, app publishers and direct advertisers.**
Detection methodologies	Typically rule-based filter and simple analysis of just impression level data. Solutions experimenting with ML, but impression level data only.	Typically identified by automated rules engine. Varying levels of ML sophistication.	Some rudimentary ML applications used for detection only.	**Fraud prevention specialists with resources dedicated to ML evolution in addition to automated rules engines and sophisticated algorithms.**
Blocking capabilities	Blocking can be implemented in the pre-bid stage through pre-defined parameters. Post-bid reporting will not provide blocking capabilities.	This can only be done at the install attribution level.	No blocking capabilities, only detection of ad fraud at the attribution level.	**Click and install attribution**
Reporting capabilities	Only to the client	Only to the client	Only to the client	**Client and traffic sources**
Coverage level	Sample-based coverage is often necessitated by the high volume of impressions.	Full coverage	Full coverage	**Full coverage**
Fraud tactics mitigated	• Domain Spoofing • Hidden Ads/Ad Stacking • Known Bots & Servers • Malware Engagement	• Known Bots & Servers • Ad Stacking • Click Spam • Click Injection • App Install Farms	None	**• Known Bots & Servers • Ad Stacking • Click Spam • Click Injection • App Install Farms**
Conflict of interest	No	Yes	No	**No**
Integration methods	Javascript Tags	Attribution SDK and Measurement URL Combination	Postback data from MMP or API integration with MMP	Measurement URL Measurement Postback URL Measurement Tag Measurement Proxy
Suitability	• Often the first line of defence against advertising fraud. • Suited to managing brand safety and ad viewability.	• Suitable for those assessing advertising campaigns for a single app (ie not an ad agency or network). • If client is not concerned with misattribution.		**• Clients operating on both CPC and CPI; those safeguarding advertising campaigns for multiple apps. • Clients wanting independent validation of attribution and to hasten campaign optimisation.**

Source: Juniper Research

2.1.1 The Importance of ML (Machine Learning) in Reducing Ad Fraud

ML will be essential in the detection and mitigation of advertising fraud at multiple levels. The speed at which bad actors modify techniques to evade detection and the increasing sophistication of fraud tactics renders conventional, rules-based fraud prevention ineffective.

Only ML is capable of analysing the volumes of data required to predict the likelihood of fraud in real-time. For example, TrafficGuard's ML ingests hundreds of datapoints across each click and attribution; building score profiles for validation. This means that when an invalid click is blocked, the diagnosis is based on as many as 200 indicators of fraud.

Using a combination of unsupervised, semi-supervised and supervised ML gives fraud tools the ability to detect anomalies, perform predictive modelling and find clusters to identify new and earlier indicators of fraud.

Given the real-time nature of the digital advertising market, it is important to note the need for the ongoing evolution of ML models to remain vigilant against fraudsters and emerging fraudulent activities. The speed, efficiency and accuracy of these solutions mean they are able to handle the vast amounts of data that need to be processed to detect fraudulent activities.

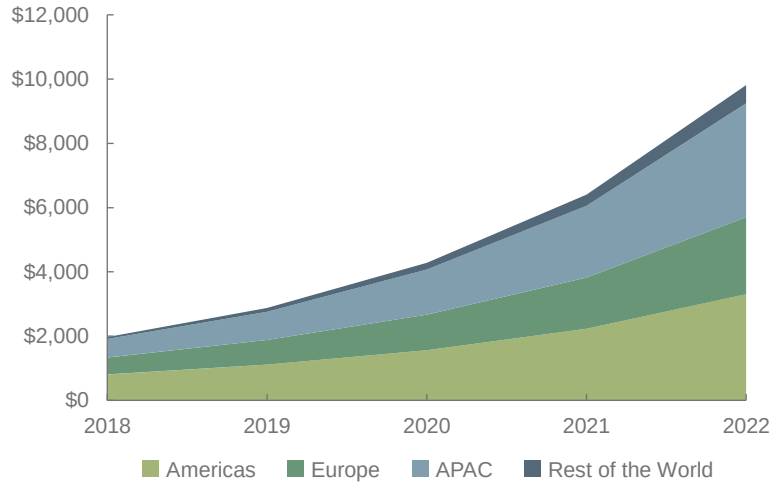
ML tools, such as those used by TrafficGuard, will enable the fight against ad fraud to move from detection to proactive mitigation in real-time.

The ability to block in real-time shifts the primary reporting functionality to the amount of fraud that has been mitigated, rather than detected.

ML is forecast to save app developers and advertisers over US$10 billion in 2022, rising from US$2 billion in 2018. As ML is fed more data, the efficiency of fraud detection and mitigation from these services will increase.

In the Asia Pacific region, Juniper expects this saving to equate to US$3.5 billion in 2022, rising from US$576 million in 2018.

Figure 2.2: Potential Savings from Machine Learning Mobile Ad Fraud Mitigation Solutions (US$m) Split by 4 Key Regions 2018-2022



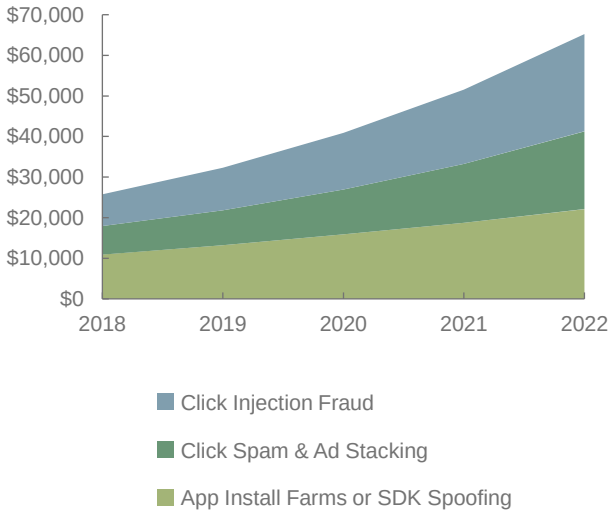
Source: Juniper Research

3. Market Sizing & Future Opportunities

3.1 Quantifying the Advertiser Loss

By 2022, global loss to ad fraud across mobile applications will reach US$65 billion. In the APAC region alone, this is anticipated to grow to US$44 billion. Given that advertising fraud techniques will continue to evolve, it is imperative that app developers and advertisers adopt services that are able to adapt to changing market conditions and practices.

Figure 3.1: Total Loss of Mobile Advertising Spend to Fraud (US$m), Split by 3 Fraud Sources 2018-2022



Source: Juniper Research

Juniper has analysed 5 factors in assessing the market conditions that appeal to fraudsters. Countries with high smartphone penetration and app engagement provide a high addressable base of users and thus the potential for IVT. Additionally, we assessed the anticipated smartphone growth in the APAC region through to 2022. GDP per capita has also been evaluated to assess the level of affordability for app developers and advertisers when adopting fraud mitigation tools. Additionally, countries that command lower CPMs will continue to attract fraudsters using basic or unsophisticated techniques, owing to capabilities of current fraud detection capabilities.

Table 3.2: Mobile Ad Fraud Risk Factor Assessment Heatmap for 10 APAC Countries

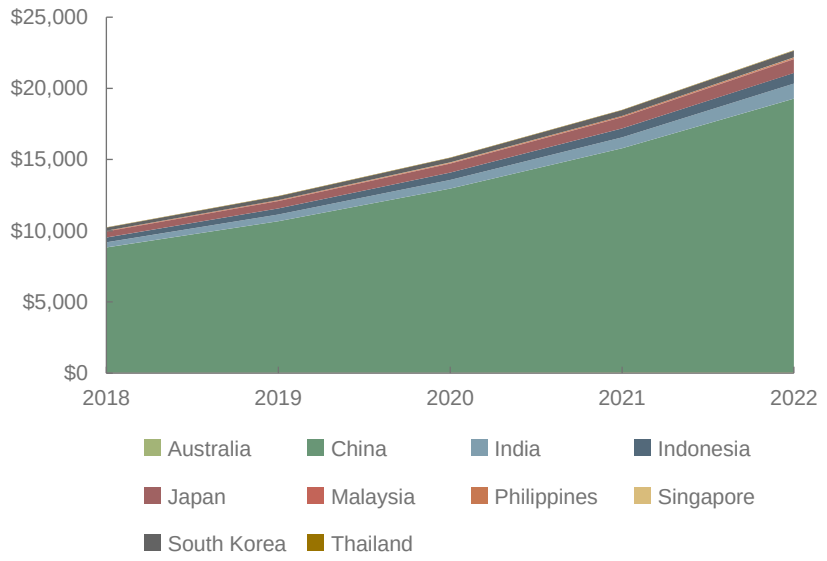
	Smartphone Penetration (20%)	Smartphone Growth (25%)	Smartphone App Usage (25%)	GDP per Capita (US$) (15%)	CPM (US$) (15%)	Score
Malaysia						
Thailand						
India						
Indonesia						
South Korea						
Australia						
Japan						
Singapore						
Philippines						
China						

LOW RISK HIGH RISK

Source: Juniper Research

When analysing the top target countries, fraudsters have historically focused on developed regions where smartphone penetration and app usage is high and install rates are sufficient to ensure fraud is profitable. However, as smartphone penetration is anticipated to grow in a number of other regions, fraudsters will begin to exploit regions where smartphone penetration and app usage are both increasing. Regions that are forecast to experience these market conditions are primed for higher exposure to fraud in the future, thus must prepare to detect and mitigate this rise in fraud.

Figure 3.3: Total Loss of Mobile Advertising Spend to Fraud (US$m) Split by 10 APAC Countries 2018-2022



Source: Juniper Research

Solutions such as TrafficGuard's are well placed to mitigate the anticipated rise in advertising fraud in these countries. Juniper Research forecasts that US$19 billion will be lost to ad fraud through mobile advertising in 2022 in China alone. As smartphone penetration in India grows, fraudsters will look to exploit this expanding user base through advertising fraud.

It is in the best interest of app developers and advertisers to adopt solutions that are able to mitigate the anticipated rise of fraud at multiple levels to maximise their protection against fraud.

3.1.1 High App Usage

The countries above are examples of places where high app usage presents fraudsters with opportunities, notably at the click level. With rising app engagement levels, the prevalence of in-app advertising as a monetisation model for app developers is high.

For trusted brands, such as eCommerce and OTT messaging apps, monetisation is not accomplished through advertising. However, smaller app developers are likely to be entirely dependent on in-app advertising both to advertise their app and for advertising within their own application.

Therefore, it is in the best interest of app developers and advertisers to choose platforms that can detect ad fraud and block traffic in real-time.

Smartphone users in South Korea, China, Japan, Australia and Indonesia spend between 3 and 5 hours on app usage during the day. The majority

of mobile applications will have advertising as a monetisation model (over 95% of installed apps in 2018) and are likely to show ads frequently.

Furthermore, ad spend can also be directed at advertising on the web and mobile browsers, which must also be taken into consideration. As smartphone penetration grows in a country, browsing on these devices will also increase.

3.1.2 High Smartphone Growth

As the proliferation of smartphones increases, so will the total number of apps downloaded. As a result, fraudsters are likely to move attention to emerging regions to capitalise on growing ad spend through fraudulent activities. Fraudsters using sophisticated means will continue to operate in regions where smartphone usage has been long-established, as fraud will continue to remain profitable.

Countries with high smartphone growth (2018-2022) include the Philippines (33%), India (14%), Malaysia (14%) and Thailand (10%). These countries, alongside Singapore, will be open to install-level advertising fraud.

App developers will be drawn to publishers which have a high proportion of fraudulent media inventory owing to their lower CPM. These app developers must not underestimate the ability of ad fraud prevention solutions to eliminate IVT and increase their ROAS.

3.2 How TrafficGuard Mitigates Fraud

Brands, agencies and app developers using TrafficGuard for fraud detection and mitigation position themselves well to tackle this anticipated rise of loss to advertising fraud. Using multipoint analysis, TrafficGuard is able to provide greater insights into the level of ad fraud over a given ad campaign. The data collected at all levels of the ad ecosystem is able to inform each level's own insights to help detect a great deal of fraud.

In regions where app engagement or app usage is forecast to rise, the adoption of a platform that can remain vigilant and mitigate new types of ad fraud is essential.

Leveraging ML technology, TrafficGuard's platform is able to monitor advertising traffic in real-time, blocking the traffic deemed fraudulent using sophisticated ML.

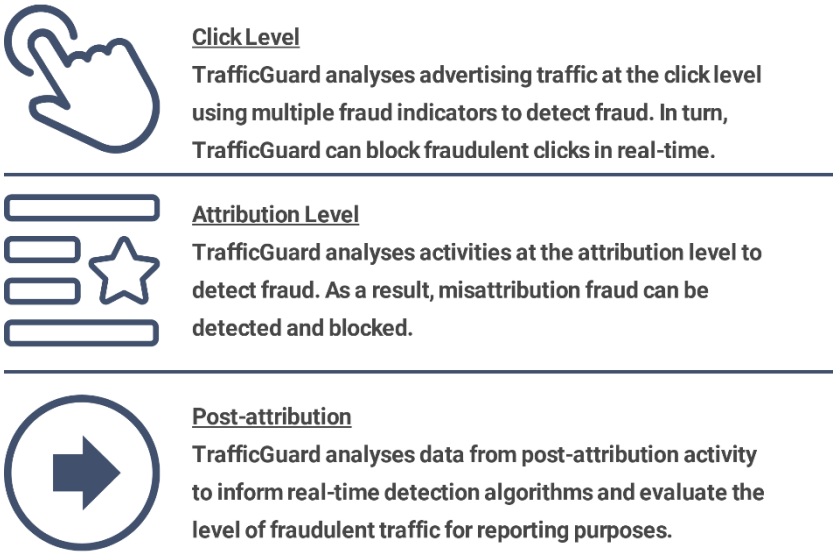
TrafficGuard is able to block IVT at both the attribution and the click level; enabling both advertisers and app developers to maximise their ROAS.

4. A New Approach – The TrafficGuard Solution

4.1 TrafficGuard – A New Approach

TrafficGuard is a comprehensive ad fraud prevention solution which detects, reports and mitigates ad fraud in real-time.

Figure 4.1: The Triple Layered TrafficGuard Solution



Source: Juniper Research

TrafficGuard analyses advertising traffic at multiple points in the advertising journey including the click level, the attribution level and post-attribution level. This enables TrafficGuard to block IVT as soon as it is detected and also find earlier indicators of tactics that are conventionally diagnosed at the attribution level.

Specialising in ML-driven fraud prevention, as opposed to just detection, TrafficGuard is able to limit the impact of fraud by ensuring performance data stays clean and fraud is blocked in real-time.

4.1.1 TrafficGuard's ML (Machine Learning) Services

In order to accomplish this level of fraud mitigation, TrafficGuard has developed ML to detect advertising fraud at multiple levels of the advertising ecosystem. ML processes data from three levels of ad traffic, which are analysed to create a deep understanding of the origins of, and mechanisms used by, fraudulent traffic.

This level of detection enables the solutions to block IVT at the click and install attribution levels in real-time. Solutions which only analyse a single level of IVT have often been designed to tackle a specific issue of advertising fraud, whereas TrafficGuard has been built to analyse and mitigate multiple levels of fraud. The multipoint analysis of ad fraud will become essential to the mitigation of evolving sophisticated ad fraud.

TrafficGuard's ML solutions enable multipoint analysis of advertising fraud traffic. As a result, TrafficGuard can detect early indications of emerging fraud tactics, thus is

able to block new ad fraud tactics earlier to minimise losses to ad fraud.

TrafficGuard also leverages the data it has collected to monitor post-attribution activity.

Luke Taylor

Chief Operations Officer and Founder of TrafficGuard

In every other industry, specialists are enlisted to combat fraud and safeguard security but, for some reason, in digital advertising that hasn't been the case. The main options for fraud mitigation to date have been companies that perform some other related digital advertising function, extending their offering to also offer ad fraud protection. Fraud is an expensive and growing problem for digital advertising and it calls for purpose built protection.

TrafficGuard has been built from the ground up specifically to mitigate ad fraud. We have a dedicated team of data scientists developing cutting-edge ML-driven fraud mitigation and a variety of integration methods to provide fraud prevention to a variety of businesses in the supply chain.

Since TrafficGuard's inception in 2016, our vision for the technology has been to create a solution that benefits the entire digital advertising ecosystem. Transparency is key to this; that means not just reporting on fraud so that the advertiser can reclaim media spend, but proactively blocking invalid traffic and reporting mitigation to both the advertiser and their suppliers in real-time.

True transparency maintains trust between advertisers and their traffic suppliers to **build a stronger digital advertising ecosystem.**

5. Stakeholder Recommendations

5.1 Stakeholder Recommendations

5.1.1 Multipoint Prevention Needed to Provide the Most Comprehensive Ad Fraud Protection

Reporting tools must be adopted to evaluate the prevalence of IVT in advertisers' activities. However, in isolation, reporting lacks the essential ability to block fraud. Multipoint analysis and real-time blocking of fraud at multiple levels of the advertising journey are required to adequately protect the business from all the direct and indirect impacts of ad fraud. There is a range of direct and indirect impacts that advertisers must guard against, including the common reporting of wasted media spend.

5.1.2 Both Direct & Indirect Ad Fraud Impacts Must be Considered when Choosing a Fraud Mitigation Solution

Wasted media spend is often the most publicised impact of fraudulent traffic for advertisers. However, the capabilities of varying fraud detection and mitigation solutions have far wider-reaching impacts than lost advertising spend to fraud. Advertisers must also consider the impact of investment in fraudulent sources, diminishment of campaign optimisation and damage to reputations and trust. With such a wide range of solutions whose capabilities vary, it is essential that advertisers consider the mitigation of all impacts, both direct and indirect, on their advertising activities.

5.1.3 The Digital Advertising Ecosystem Requires Collaboration & Transparency from all Stakeholders

Other impacts, such as downstream wasted media spend, can only be mitigated by increased transparency between advertisers and intermediaries in the advertising ecosystem. Not only will this increase trust between the various stakeholders, but fraudulent traffic can be identified at all levels of the advertising journey, thus negating associated costs such as loss to chargebacks and refunds. When choosing a fraud detection and mitigation solution, a tool that enables transparency of ad traffic data between advertisers and intermediaries is essential.

5.1.4 ML is Vital to Maximising Detection Solutions

As rules-based detection adapts to new fraud tactics, fraud continues to evolve to evade detection, creating an ongoing cat-and-mouse scenario.

ML will be vital to the detection of IVT to arrest this cycle. Given the vast amounts of advertising traffic, solutions that leverage ML effectively will be able to process the huge volumes of data to deliver a faster and more reliable diagnosis of IVT.

By blocking IVT, an advertiser and intermediaries in the supply chain can optimise high quality traffic sources in real-time; driving overall campaign performance. Additionally, time saved in managing IVT reporting and invoice reconciliation with intermediaries can be invested in activities that deliver further ROAS.