DIGITAL ADVERTISING FRAUD IN NORTH AMERICA

trafficguard

JUNIPER RESEARCH

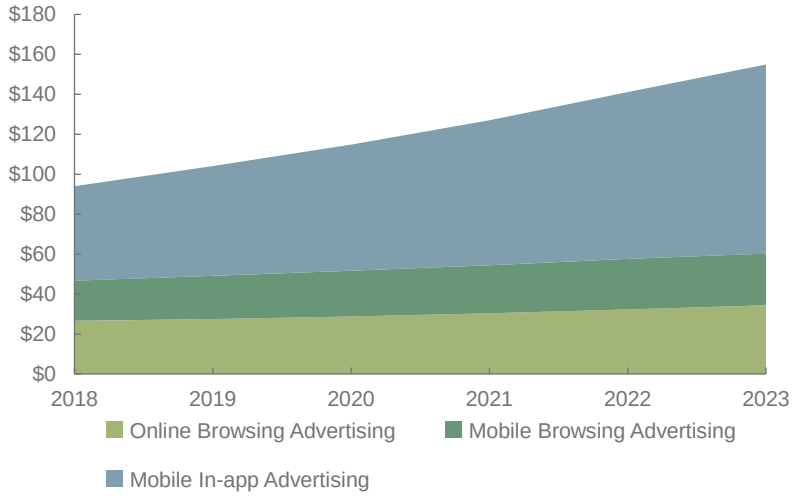
Contents

1. The North American Digital Economy

1.1 The North American Digital Economy

The digital ecosystem in North America is changing rapidly, with increasing proportions of advertising budgets being spent on mobile advertising. As can be seen in figure 1.1, in-app advertising spend is forecast to be the fastest growing sector over the next 4 years, growing 72% over this period. Indeed, total ad spend across online browsing, mobile browsing and mobile application is anticipated to grow 49% in the same period, reaching $155 billion worth of ad spend by 2023.

Figure 1.1: Total Advertising Spend on Online & Mobile Channels in North America ($bn) Split by Online Browsing Ads, Mobile Browsing Ads & In-app Ads 2018-2023



Source: Juniper Research

This high amount of advertising spend will continue to attract fraudulent players aiming to exploit the digital advertising ecosystem for monetary gain.

In 2018, advertisers lost $44 million of advertising spend per day to fraudulent traffic in North America. This loss is only forecast to increase, and is anticipated to reach $100 million a day by 2023.

Marketers invest in advertising to reach real people with the intention of making them customers, however activities from fraudulent operations impede this. Fraudulent traffic is often present on premium and non-premium traffic sources and networks; failure to adopt suitable fraud detection and mitigation solutions leaves advertisers exposed to fraud that consumes budgets and restricts advertising performance.

There are a variety of fraud detection and mitigation solutions available to combat this increasing threat of fraud to advertising budgets. However the capabilities of these solutions vary considerably. The choice of a fraud detection and mitigation solution has direct implications on the amount of ad spend that can be mitigated or recovered from ad fraud, as well as the extent of other financial and non-financial impacts of fraud.

Fraud in the digital advertising ecosystem can be committed in numerous ways. Fraud operations are becoming innovative and employing increasingly sophisticated methods to evade detection from attribution,

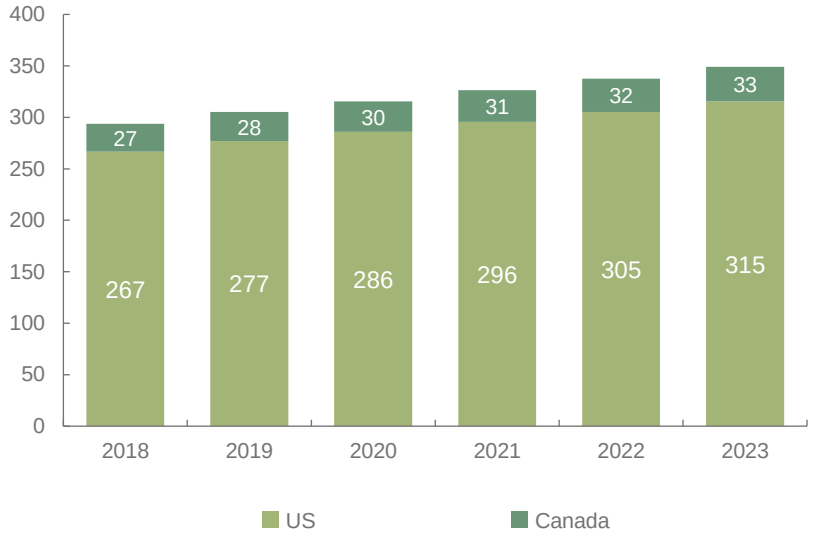
measurement and mitigation platforms. Comprehensive mitigation will leverage machine learning to analyse advertising traffic data to detect these new fraud tactics and block Invalid Traffic (IVT) to minimise advertisers' loss.

Rules-based migitation can be effective in combating known fraud tactics, but when it comes to defending against new and evolving fraud tactics, a more sophisticated approach is required. The introduction of machine learning to fraud mitigation processes has enabled the much more thorough, multi-dimensional analysis that is required to detect fraud as it evolves. Machine learning, supported by expertise, infrastructure and data requirements, provides a proactive and formidable fraud defence.

Machine learning is of the utmost importance in maintaining vigilance against innovative fraud tactics by efficiently evaluating anomalous traffic and detecting indicators of fraud early. A failure to adopt a suitable platform will lead to increased losses to emerging fraudulent techniques.

The adaptability of these solutions is key for future success in maximising Return on Advertising Spend (ROAS) through minimising the impact of fraudulent traffic on advertising budgets.

Figure 1.2: Total Number of Internet Users (m) (US & Canada) 2018-2023



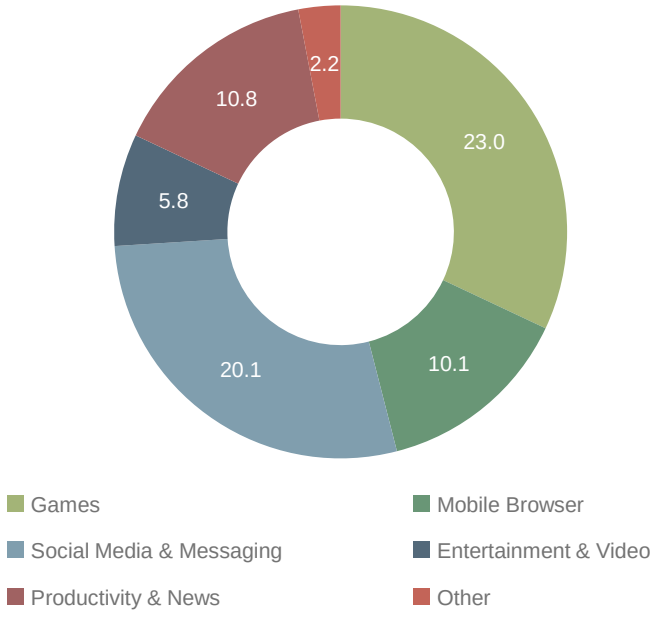
Note: An Internet user is defined as an individual who accesses the Internet through at least one connected consumer device (smartphone, tablet, PC, Connected TV) per annum.

Source: Juniper Research

1.1.1 The Average North American Internet User

As shown in figure 1.3 below, the average North American mobile device user spends over 70 hours per month accessing mobile applications (including mobile browsers). The largest categories accessed (Games, and Social Media & Messaging) are app categories that are most dependent on advertising for monetisation.

Figure 1.3: Average Mobile Device Usage per North American User per Month in 2018 (Hours) Split by Category



Source: Juniper Research

Given the large number of Internet users in the region and the high usage of advertising-rich services, fraudulent players will continue to be attracted to the potential monetary gains that can be obtained from their activities.

In 2019, the average North America user will account for:

- **Over 31,000 attributable online browsing ad impressions per annum**
    - **Of which 5,400 (17.4%) can be attributed to fraudulent traffic**
- **Over 21,000 mobile browsing ad impressions per annum**
    - **Of which 3,900 (18.8%) can be attributed to fraudulent traffic**
- **Over 69,000 attributable in-app ad impressions per annum**
    - **Of which, over 12,000 (17.5%) can be attributed to fraudulent traffic**
- **$407 of advertising spend per Internet user per annum**
- **$61 of wasted advertising spend per Internet user per annum**

As a result of this significant time spent on connected devices, Internet users in North America will be shown over 9 trillion ads on desktops and PCs in 2019, 6 trillion via browsing on mobile devices and 21 trillion in-app adverts.

Countries in North America can be considered established in terms of their digital ecosystem, including device adoption and usage. As a result, fraudsters will gravitate to advertising traffic in the region.

In comparison, the average Internet user in Latin America will only account for $25 of advertising spend per annum, only 6% of the same figure for the US. Additionally, Juniper Research anticipates that the average Latin

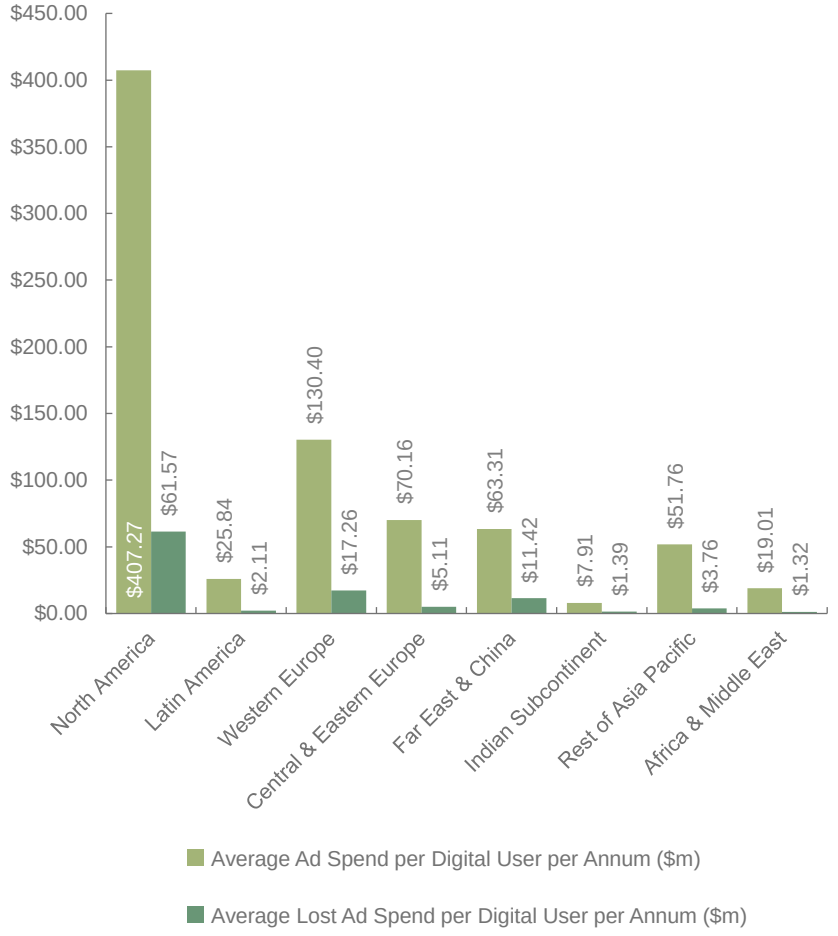
American user will only view 14,500 online browsing ads, over 4,200 mobile browsing ads and over 5,400 mobile in-app ads.

1.1.2 Average Ad Spend per Internet User in North America

North America's digital ecosystem provides large areas of attack for fraudulent operations. A large number of people online, with high device usage and a propensity to shop, leads to a high advertising spend per Internet user. As a result, Juniper anticipates that fraudsters will continue to invest their activities in North America. Thus, advertisers will have to contend with the most innovative fraudulent tactics and must adopt an anti-fraud solution that can contend with the rapidly changing fraud landscape.

Advertising spend per Internet user is greatest in North America; estimated to be over $407 in 2019. This figure represents 455% of the global average of $90.

Figure 1.4: Average Ad Spend per Internet User per Annum in 2019 ($) Split by 8 Key Regions



Source: Juniper Research

2. The Issue of Ad Fraud in North America

2.1 Fraudulent Traffic

The Media Rating Council (MRC) classifies IVT as General or Sophisticated based on the means required to detect it. General Invalid Traffic (GIVT) is identified by rudimentary filtration including blacklists, whereas Sophisticated Invalid Traffic (SIVT) requires more advanced analytics, co-ordination and corroboration of multiple signals to identify. Advertisers are therefore vulnerable to a variety of different fraud tactics which can occur at multiple points throughout the advertising journey. Therefore the choice of adoption of a fraud detection and mitigation platform is key to tackling the rising threat of advertising fraud.

For the purposes of this White Paper, we define IVT as traffic that is not from legitimate sources. In cases where IVT is intentionally created to attract ad spend, it is commonly referred to as ad fraud. We use the terms fraudulent traffic and Invalid Traffic (IVT) interchangeably.

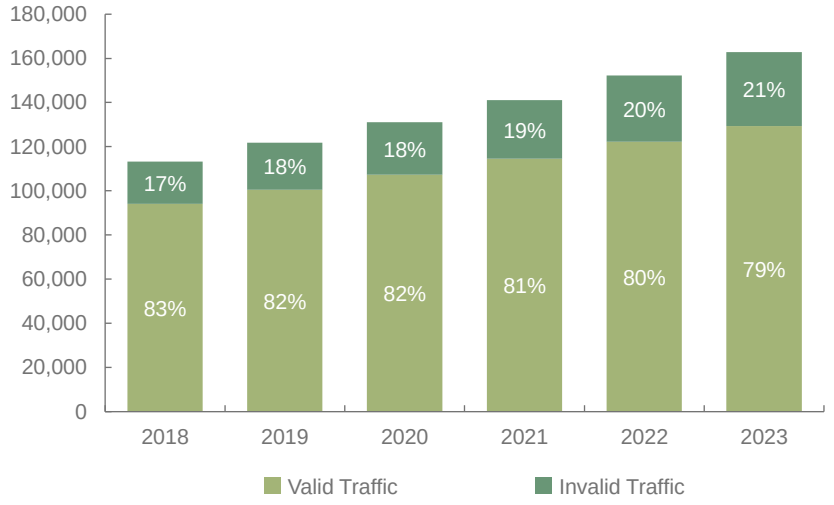
There are fraud detection solutions that offer just reporting, some that prevent fraud at a single stage of the advertising journey, and others that protect at multiple stages. Multipoint analysis (ie analysing advertising traffic data on multiple stages) examines hundreds of indicators of fraud for each ad transaction at the impression, the click and attribution level. This enables fraud to be mitigated as early as it can be identified, as opposed to waiting for a specific stage in the journey, and also provides more data to facilitate reliable detection.

Multipoint analysis provides the only efficient method of detecting and blocking SIVT. As fraud tactics become more complex, assessing ad traffic on multiple levels becomes essential to maintain vigilance against new types of advertising fraud.

Fraud in the advertising industry is anticipated to continue to innovate. Previous methods of analysing advertising traffic data, such as IP blacklists and rules-based mitigation, are too simple for fraudsters to reverse engineer and evade.

As we can see from figure 2.1, the volume of valid, human derived advertising traffic and IVT are both anticipated to increase for the forecast period. However, annual IVT volume per North American Internet user is set to grow 57% over the next 4 years; almost twice the growth of genuine advertising traffic in the same period. Already today, almost 1 in 5 ad transactions are derived from fraud.

Figure 2.1: Advertising Traffic per Internet User per Annum in North America, Split by Valid & Invalid Traffic 2018-2023

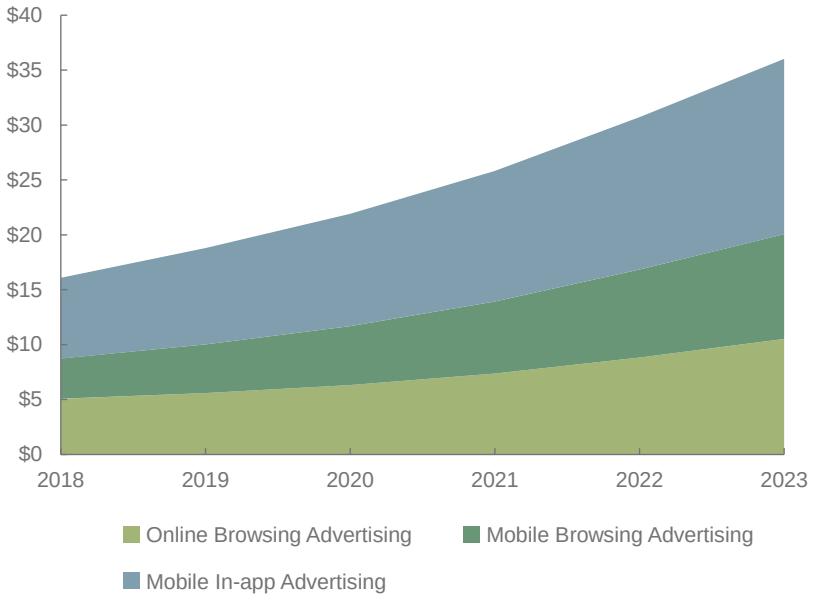


Source: Juniper Research

2.1.1 Advertiser Loss in North America

Juniper Research anticipates that the total loss to advertising fraud in North America will equate to $18.7 billion in 2019, rising to to $36 billion by 2023. This represents a compound annual growth rate (CAGR) of 17.8%. In the US, total lost spend to advertising fraud will reach $17.9 billion in the US in 2019 and rise to $34.1 billion in 2023 with a CAGR of 17.5%.

Figure 2.2: Total Loss Revenue Through Advertising Fraud in North America ($bn) Split by 3 Internet Access Types, 2018-2023



Source: Juniper Research

The digital advertising ecosystem can be considered highly fragmented, with multiple layers of aggregation and arbitration on each digital advertising transaction. These layers create complexity that allows fraud to infiltrate traffic sources, exploiting the attribution process to steal ad spend. Current tactics, including click injection techniques, bots, install farms, app SDK spoofing, and ad stacking, are all used to create fake ad engagements, or steal attribution of genuine ad engagements. Advertisers in North America will waste $61 on average per Internet user on fraudulent advertising traffic in 2019. This is set to rise to $103 per user by 2023.

Fraud follows advertising spend. As a result, those advertising in North America must put the correct tools in place to monitor and block fraudulent traffic. To highlight the extent of this, Juniper Research anticipates that 36% of global advertising spend lost to advertising fraud by 2023 will be from North American advertisers, however the region will only account for 9% of Internet users globally.

2.1.2 The Impacts of Fraud on Digital Advertisers

The most apparent impact of fraud is the loss of advertising spend on fraudulent traffic. However, there are many other costs that are often not considered by advertisers when looking at the total impact of ad fraud. Such costs include:

- **Wasted downstream media spend**; downstream media spend is defined as the ad spend which intermediaries incur in the process of acquiring traffic for advertisers. When fraud is not removed in real-time, intermediaries with shorter payment terms on their traffic sources bear the costs of fraud. This leaves them out of pocket and also means that the fraud perpetrators get paid, enabling the cycle to continue.

- **Continued investment in sources containing high levels of fraud**; fraud inflates volume metrics, enabling low quality sources to appear high performing. As a result, advertisers increase investment in these sources, unknowningly buying more and more IVT. Without the proper detection tools, advertisers continue to invest in these sources.
- **Time wasted investigating fraudulent sources**; without the ability to block IVT in real-time, the time taken to reconcile media volumes with supply intermediaries must also be taken into consideration. Blocking in real-time will enable the time that would have been spent on this to be used for proactive projects, rather than focusing efforts on reacting to fraud. Additionally, disputes on any reconciliations can delay the process and create additional costs. In the worst scenarios, this may lead to costly litigation cases.
- **Diminishing campaign performance**; while IVT is present and undetected in digital advertising, it is near impossible for traffic sources to effectively optimise campaigns. Real-time fraud mitigation enables fast camapign optimisation that strengthens campaign performance.

It is essential that advertisers are aware of the full spectrum of costs involved in ad fraud, including the direct cost of wasted advertising spend and the indirect costs involved after-the-fact. When equipped with the knowledge of all the ways ad fraud impacts a business, it is easier to identify the solution that addresses it comprehensively.

2.1.3 Strategic Recommendations for Advertisers in North America

Adoption of fraud detection and mitigation tools by advertisers is essential in mitigating any lost spend. These should include the following capabilities:

- **Real-time detection and mitigation of fraudulent traffic**; this ensures budget is not wasted on ad fraud and also enables better campaign performance with faster optimisation driven by clean performance data. It also mitigates further expenditure not directly related to the lost spend on fraudulent advertising traffic, including further investment in fraudulent sources and the cost of litigation and disputes over advertising traffic volumes. Blocking capabilities vary across the solutions on the market; as fraud can occur at multiple levels of the advertising chain, advertisers must ensure that their choice of platform is able to mitigate fraud at multiple stages, enabling the earliest reliable mitigation and ensuring detection of tactics that evade earlier stages.
- **Machine learning**; this technology enables more granular analysis of transactions for detection of emerging, unknown fraud tactics, and more reliable detection of known tactics. As a result innovative fraud tactics can be identified and mitigated earlier, thus reducing further loss to the advertiser.
- **Timely insight on the quality of advertising traffic**; this, enables advertisers to effectively evaluate the impact of the advertising expediture and assess ROAS. Reporting should be granular and available to both the advertiser and ad network. By granting visibility of quality to traffic sources, the potential for mitigating IVT and reducing the overall cost of fraud is increased.

- **Blocking at multiple levels of the advertising journey**; multipoint analysis will analyse traffic and block IVT in real-time, and as early in the journey as it can be reliably detected. Attribution should be verified before traffic sources receive their post-backs for more confident optimisation. This also mitigates the need for volume reconcilliations and disputes about traffic volumes after attribution – saving time and reducing risk.
- **Full analysis of advertising traffic**; analysing a sample of advertising traffic to detect fraud is ineffective. In order to minimise advertisers' exposure to fraud, full analysis of advertising data is essential.
- **Independence**; using a third party vendor to identify and remove IVT eliminates any conflict of interest, providing unbiased validation of measurement and attribution to advertisers, traffic sources and attribution vendors. As exploiting attribution is key to ad fraud success, it is important that attribution be independently verified.

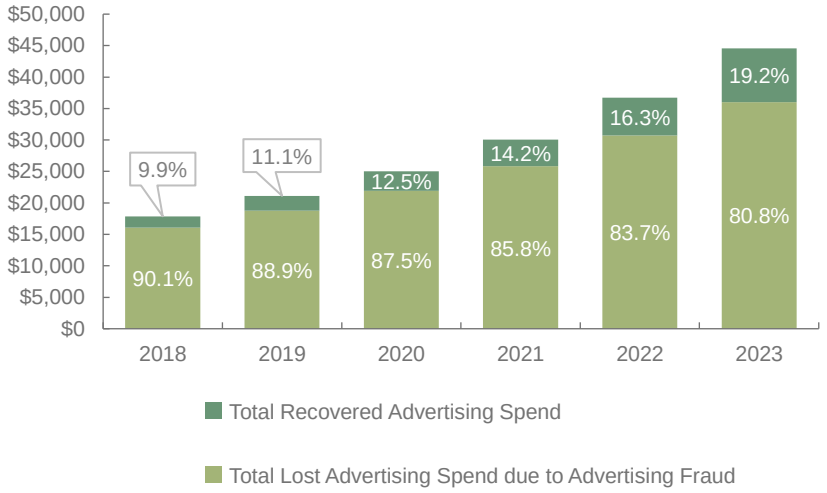
In isolation these factors will enable advertisers to detect, report and mitigate fraud to a limited extent. However, to maximise the impact of fraud detection and mitigation solutions, advertisers must adopt a solution that can offer all these capabilities. In doing so, advertisers position themselves best to defend against the growing threat of advertising fraud.

2.1.4 Recovery of ad spend from fraud through both reactive and proactive measures

It is of note that stakeholders in the advertising industry are becoming more aware of the potential threat that advertising fraud can have on their advertising budget. As such, many advertisers and supply chain parties are using proprietary or third party tools to recover ad spend from fraud periodically, or proactively prevent fraud from taking their ad spend.

Recovered advertising spend includes spend on fraudulent traffic that has either been blocked in real-time or spend recovered by fraud detection solutions after payment.

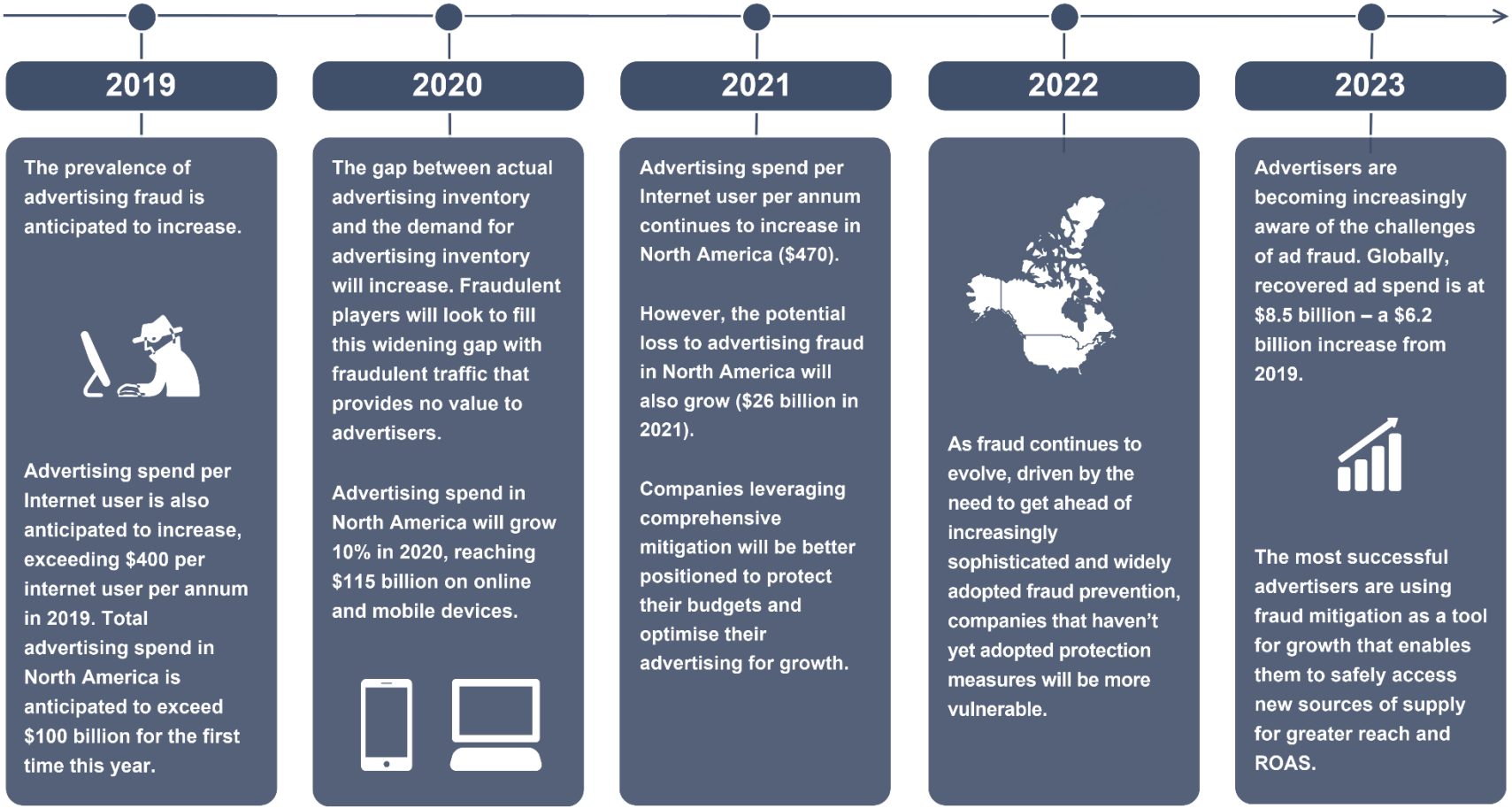
Figure 2.3: Advertising Spend Expsosed to Fraud in North America ($m) Split by Spend Lost to Fraud and Recovered Ad Spend 2018-202



Source: Juniper Research

Whilst Juniper Research forecasts that the total loss to advertising fraud will grow 111% over the next 4 years, efforts in detecting and mitigating this fraud will lead to growing proportions of spend recovered, with almost 20% of potential annual loss to fraud being recovered by 2023.

Figure 2.4: Digital Advertising in North America: The Next 5 Years



Source: Juniper Research

3. TrafficGuard & Fighting Digital Advertising Fraud

3.1 TrafficGuard – Stop fraud. Drive growth.

The most significant impact of ad fraud is often the opportunity cost it consumes. Unlike legacy fraud prevention that focuses on recovery of yesterday's ad spend, TrafficGuard has been built from the ground up to maximise the performance of today's. TrafficGuard prevents ad fraud in real-time; meaning that your campaigns generate genuine advertising engagement, lifting ROAS and helping your business meet its growth objectives.

3.1.1 TrafficGuard's Growth Drivers

1. **Faster advertising optimisation**: Removal of fraud in real-time ensures that performance metrics stay free of fraud; enabling faster and more confident campaign optimisation.
2. **Strengthened growth partnerships**: Traffic quality is one of the most common reasons an advertiser will stop working with an ad network. By removing fraud, network turnover is reduced; enabling each campaign to build on the learning and optimisation of the previous campaign.
3. **Full budget utilisation**: According to Figure 2.1, 20% of ad budgets are wasted on fraud. This means that without real-time fraud prevention, only 80% of your ad budget has the potential to deliver a return.
4. **Waste mitigation**: Fraud wastes ad budget and leads to time-consuming media volume reconciliation. Real-time prevention stops the flow of money to fraud and allows marketers to focus on activities that deliver growth.

Working together, these four drivers grow and compound the earning potential of digital advertising efforts.

3.1.2 What Does TrafficGuard's Growth-Focused Fraud Prevention Look Like?

- Real-time and surgical**:** TrafficGuard's Growth Drivers rely on their ability to prevent fraud surgically. This means unlike aggressive legacy solutions, TrafficGuard doesn't rely on blacklists, but layers of sophisticated analysis that reliably mitigate fraud before it impacts advertising campaigns.
- Machine Learning**:** Fraud is constantly evolving. Machine learning builds on layers of behavioural analysis and rules to provide a deeper understanding of traffic for protection against known and unknown types of fraud.
- Multi-point**:** By analysing multiple stages of the advertising journey, TrafficGuard can mitigate fraud earlier than legacy solutions. It can also mitigate sophisticated fraud that typically evades single level detection.
- Transparent**:** TrafficGuard diagnoses fraud with science, not a magical blackbox. Clients can access full and granular reporting on fraud mitigated by campaign, source and sub-ID.

Luke Taylor

Chief Operating Officer and Founder of TrafficGuard

The North American digital advertising market is very sophisticated. The businesses we talk to have a great understanding of the challenges that ad fraud poses for their advertising efforts. These include difficulties in finding new sources of traffic to scale with, declining returns, and time wasted reacting to fraud. Some businesses want only to recover ad spend wasted on fraud each month.

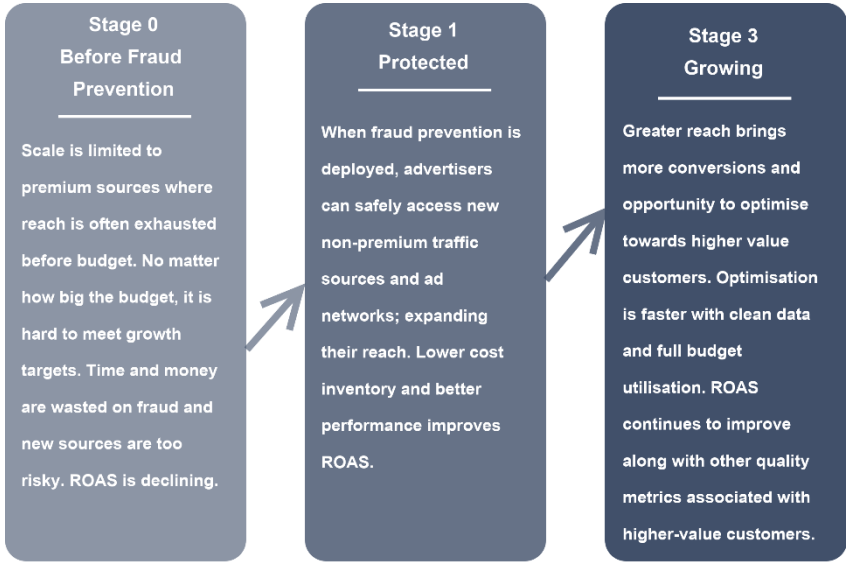
However, the most successful digital advertisers look at fraud mitigation as a tool for growth.

This is where our surgical fraud prevention comes in. TrafficGuard's 4 growth drivers work together to grow the earning potential of digital advertising.

Safe in knowledge that TrafficGuard is proactively protecting them from fraud, our clients have been able to achieve

1. Greater reach and accelerated user acquisition by working with more traffic sources
2. Faster optimisation enabled by greater scale and fraud-free performance data
3. Higher value customer acquisition through better optimisation
4. Improved ROAS through both the reduction in ad spend wasted on fraud and the improved advertising performance
5. Time saving in management of fraud such as reconciling media volumes at billing time or analysing traffic quality for optimisation.

Figure 3.1: Growth Example



Source: Juniper Research

If you ask anyone in user acquisition or growth marketing, "do you want to grow your return on ad spend?"; the answer should be a resounding yes! Real-time, surgical fraud prevention is one of the easiest ways to achieve growth.