PubMatic

UNDERSTANDING INVENTORY QUALITY

THINKING BEYOND BOTS

UNDERSTANDING INVENTORY QUALITY

THINKING BEYOND BOTS

As brands funnel more of their ad budgets to digital, they have been demanding greater transparency across the digital advertising supply chain and the definition of quality has evolved. Our industry must move beyond ad fraud alone.

Digital advertising provides marketers with targeting precision and comprehensive analytics that they are hard-pressed to find with any other medium. This is why digital is expected to account for approximately half of all global media ad spend by 2020[1], and why programmatic has become increasingly favored as the channel of choice for accessing these in-demand ad impressions. However, the mechanics that made digital automation so popular also introduced challenges for buyers that do not exist in traditional media.

Since the inception of programmatic a decade ago, the concept of inventory quality (IQ) has been most closely associated with fighting fraud. The assumption was that inventory is at its best when all bots and non-human traffic are excluded from monetization. Sophisticated operations like 2016's "Methbot" scam, which siphoned millions of dollars in fraudulent impressions from advertisers, shined a spotlight on the quality challenges that exist within the digital ecosystem, and some of the world's largest advertisers mandated a clean supply chain as a result.

While true that, all things being equal, human traffic is preferred to non-human traffic, the industry is moving towards a new view of inventory quality that is more comprehensive than just fraud. IQ will also require being more selective in the value of the visitors consuming advertising and moreover, inventory quality must also include activities that site operators conduct to manipulate traffic designed specifically to increase ad spend.

This white paper will provide insights into what both buyers and publishers should be aware of to thrive within the new programmatic future. While brand safety and viewability are incredibly important considerations for marketers seeking to improve the ROI of their ad campaigns, the focus of this paper is on fraud and the activities and practices that encompass inventory quality.

Our goal is to shed light onto the evolving definition of inventory quality by examining the following concepts:

NON-HUMAN TRAFFIC

Computer-generated activity that inherently delivers fraudulent ad impressions

LOW-VALUE HUMAN TRAFFIC

Ad impressions that are viewed by human users, but against low value content or in a context less valuable to advertisers

PRACTICES THAT DECEIVE AND OBFUSCATE

Domain spoofing, ad injection and other practices designed to increase ad revenue in ways that buyers may perceive as legitimate traffic activity and can be either human or non-human

MOBILE IN-APP INVENTORY QUALITY

Uncharted territory that serves as the next frontier for inventory quality innovation

THE FUTURE STATE

Where our industry is heading with regards to inventory quality, and what buyers and sellers need to do to ensure they remain protected

NON-HUMAN TRAFFIC

The concept of inventory quality is often equated with non-human traffic within the digital advertising industry.

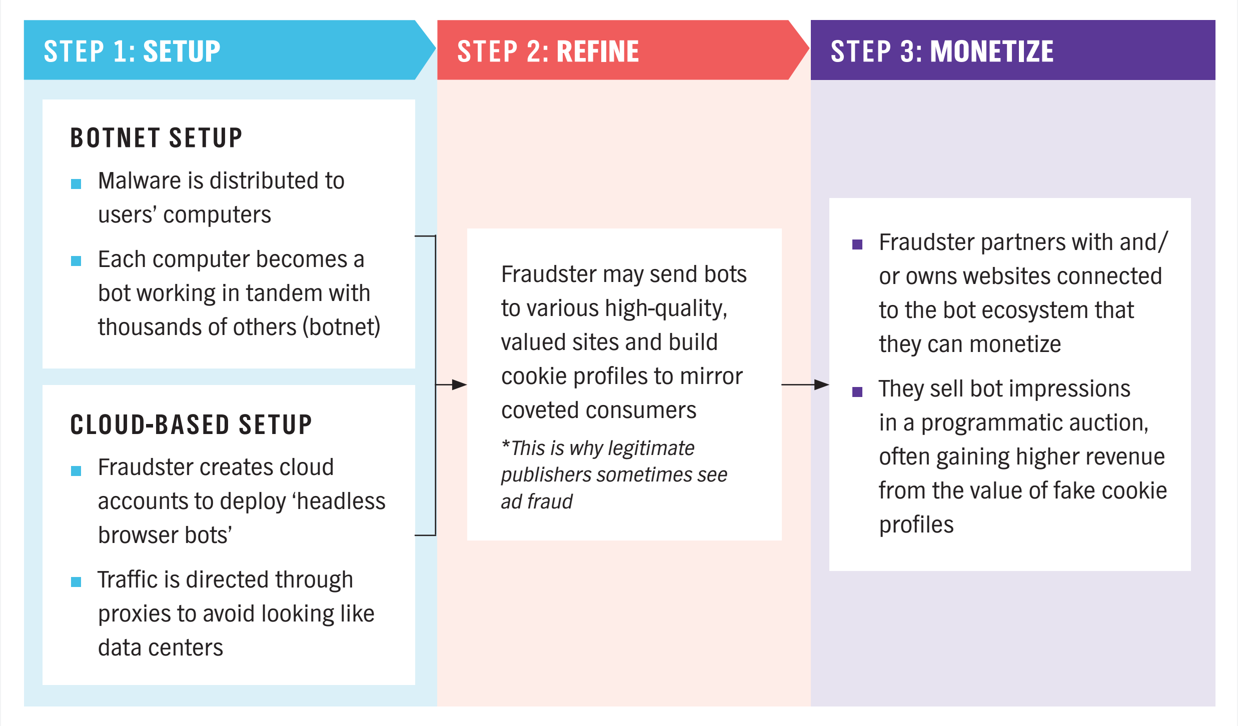
Before today's landscape of fraud tech vendors hit the scene, non-human traffic (e.g. bot fraud) ran rampant, filling the coffers of bad actors. Despite the investment in identifying and preventing non-human traffic across the digital ecosystem, the ANA and White Ops found that economic losses from digital ad fraud reached $6.5 billion in 2017.[2] To make progress towards the industry's goal of eradicating bot fraud, it is important for advertisers and publishers alike to have a baseline understanding of what non-human traffic is and how it works.

WHAT IS NON-HUMAN TRAFFIC?

Also known as invalid traffic (IVT), non-human traffic includes any website traffic that is generated from sources other than a real person. This can include fraudulent traffic, such as malicious bots, as well as traffic generated by unnatural consumer browsing behavior. There are two primary types of IVT:

	MRC DEFINITION[3]	EXAMPLES
GENERAL INVALID TRAFFIC (GIVT)	GIVT "consists of traffic identified through routine means of filtration executed through the application of lists or with other standardized parameter checks"	■ Known data-center traffic ■ Self-identified bots and other crawlers ■ Unknown browsers ■ Browser pre-rendered traffic
SOPHISTICATED INVALID TRAFFIC (SIVT)	SIVT "consists of more difficult to detect situations that require advanced analytics, multi-point collaboration/coordination, or significant human intervention, etc., to analyze and identify"	■ Bots masquerading as legitimate users ■ Hijacked devices ■ Hidden/stacked ad serving ■ Adware and malware

HOW SIVT WORKS



STEP 1: SETUP

BOTNET SETUP

- Malware is distributed to users' computers
- Each computer becomes a bot working in tandem with thousands of others (botnet)

CLOUD-BASED SETUP

- Fraudster creates cloud accounts to deploy 'headless browser bots'
- Traffic is directed through proxies to avoid looking like data centers

STEP 2: REFINE

Fraudster may send bots to various high-quality, valued sites and build cookie profiles to mirror coveted consumers

**This is why legitimate publishers sometimes see ad fraud*

STEP 3: MONETIZE

- Fraudster partners with and/or owns websites connected to the bot ecosystem that they can monetize
- They sell bot impressions in a programmatic auction, often gaining higher revenue from the value of fake cookie profiles

HOW TO PROTECT YOURSELF

While the industry's goal is to find a way to stop bad actors from perpetrating bot fraud altogether, the reality is that avoidance and mitigation are the best tools to minimize waste.

1 AVOIDANCE

Avoidance commonly occurs with a fraud tech vendor making decisions about fraud before the ad request from the publisher enters the auction and/or the ad impression is purchased and served. Once an impression can be recognized as fraudulent, it can be discarded.

2 MITIGATION

Mitigation comes after the ad is delivered, where reporting surfaces the percentage and distribution of ad fraud. At that point, the buyer's best recourse is to ask the supplier for a refund, which is becoming a more common practice. For example, PubMatic launched a Fraud Free Program for demand partners, so if fraud is detected, buyers don't have to pay for it. Additionally, buyers should pull offending domains, apps and supply sources from future media spend.

LOW-VALUE HUMAN TRAFFIC

‘Not fraud’ is not enough in today’s digital ecosystem. It is imperative to seek quality in content and audience as well.

In the context of ad fraud, quality is black and white. An ad impression was either consumed by a human on the site indicated in the advertiser’s bid request, or it was not. However, the immense opportunity and rapid growth of the programmatic industry—which has grown at a 28 percent CAGR over the past five years and is expected to reach over $70 billion globally in 2018[4]—has created an environment ripe for less savory activity.

Theoretically, aside from explicit fraud, ad investment should be dedicated to websites with original content and loyal audiences. Yet, given the amount of money flowing through the digital ecosystem, incentives have been corrupted and participants have learned they can reverse the “natural order.”

There are millions of websites that sell advertising. Many sites offering original and attractive content have risen out of advertising-based revenue business plans. Other sites offer a poor-quality content and user experience, but at first glance appear to be legitimate publishing endeavors.

Understanding how sites are created, designed and operated opens the door to making smart IQ policy decisions.

WHAT IS LOW-VALUE HUMAN TRAFFIC?

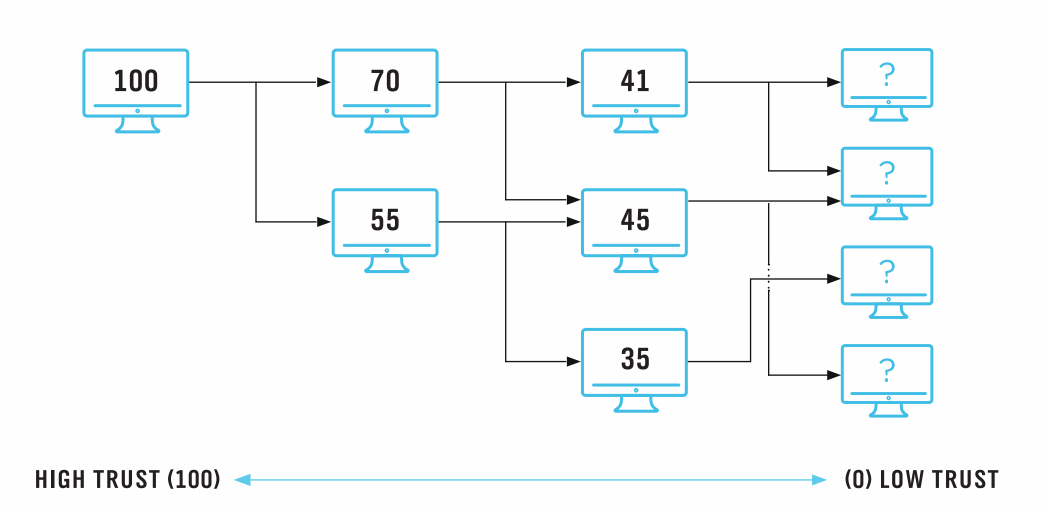
Low-value or undesirable human traffic refers to situations when users have not fully self-selected to visit the sites in question. Often, they click on ‘click bait’ links, only to find the actual content to be less attractive than expected, existing only as a backdrop for selling advertisements. Other times, users are redirected without their consent. These users simply bounce and never return.

This problem is becoming increasingly important as brand advertising spend continues its rapid shift to digital. Direct response advertisers can measure the success of campaigns based on some consumer-driven action (i.e. sales, installs, sign-ups, etc.). Brand advertisers, on the other hand, often have less easily measurable success metrics, making them more susceptible to this type of quality breach.

CASE STUDY

THE POWER OF BACKLINKS TO IDENTIFY UNDESIRABLE AUDIENCES AND CONTENT

To get a better indication of audience intentionality, it is helpful to analyze all the backlinks to a particular site. By assigning each site a score, one can measure a domain's quality by calculating the density and influence strength of the sites linking to it. Illustrated below, as links flow from highly-trusted sites upstream, each site along the chain picks up a portion of that trust. Sites with more trusted link sources are given higher scores.



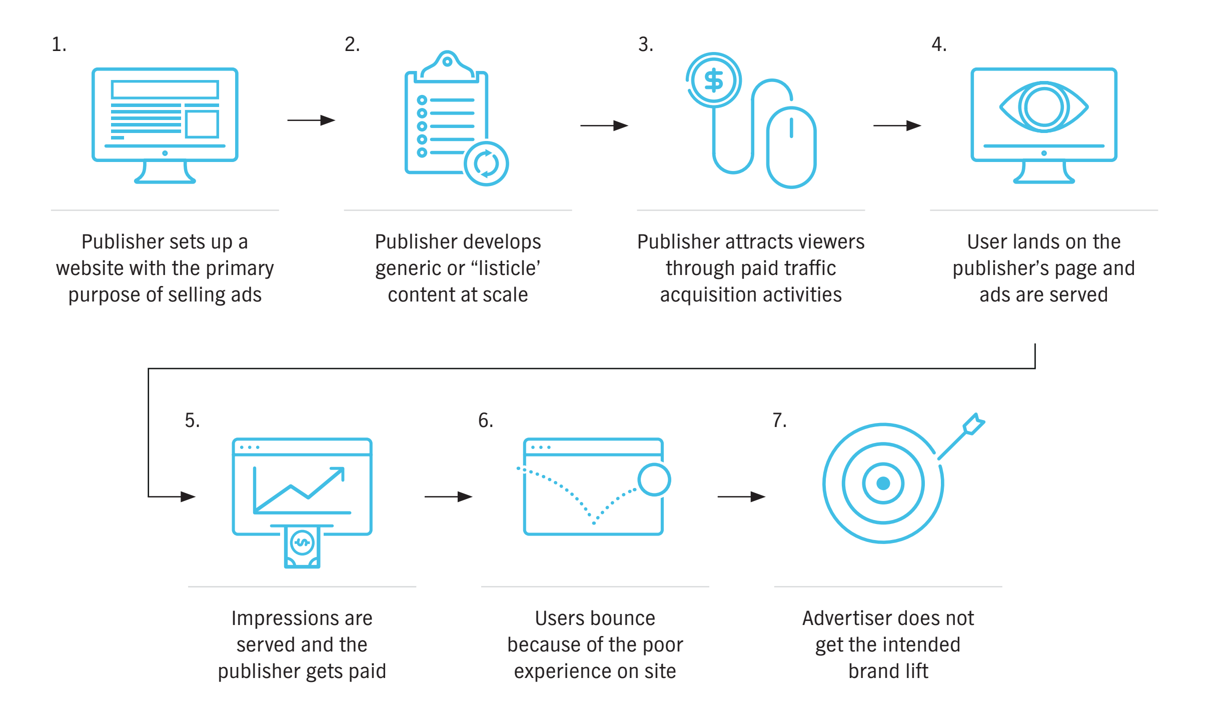
These scores are based on reputation, not on traffic. There is a strong correlation of low scores to 'ghost sites,' that are created for the sole purpose of generating advertising revenue. If a website has built an organic, loyal audience, one would expect a percentage of that audience to promote the site by linking to it, thus increasing a site's score.

A low score is not only a great indicator that a site has poor quality content and audience, but it is also immune from manipulation since backlinks must 'flow' from trusted sites (often respected news or media properties). Unless the backlinks are rooted in trusted environments, they will be discounted as quantity over quality.

IQ PRO TIP

Traffic metrics are just one of many metrics that should be measured as part of a site's quality assessment. By analyzing backlinks, it is possible to get a more accurate depiction of the intentionality of an audience. Reach out to your SSP partners to learn about the third-party tools available to help conduct this analysis in a scalable way.

HOW LOW-VALUE HUMAN TRAFFIC WORKS



1. Publisher sets up a website with the primary purpose of selling ads

2. Publisher develops generic or “listicle” content at scale

3. Publisher attracts viewers through paid traffic acquisition activities

4. User lands on the publisher’s page and ads are served

5. Impressions are served and the publisher gets paid

6. Users bounce because of the poor experience on site

7. Advertiser does not get the intended brand lift

HOW TO PROTECT YOURSELF

Until recently, this activity has been unchecked by the marketplace. However, things are changing due to several factors including an industry-wide focus on supply chain efficiency, the demand for transparency, the introduction of privacy related regulations, such as The European Union’s General Data Protection Regulation (GDPR), and the realization that targeting a single individual wherever they may appear does not work as hypothesized.

Buyers should be aware of common tactics used by these less-desirable publishers, so they can identify potential problem sites. It is important to work with programmatic partners who are diligent about digging into the quality of a site’s content and audience in order to protect buyers.

Some common signals to look for to identify low-value human traffic:

1 **NO REAL AUTHORS FOR CONTENT**

When content is created for the sole purpose of providing real estate for ads, publishers will often use a stock photo for the content writer. These authors may show up on a variety of ghost sites with similar characteristics.

2 **INCONSISTENT TRAFFIC PATTERNS**

Odd spikes in traffic can indicate an increase in traffic acquisition activities. If these spikes don't trigger fraud detection technology, the publishers are incentivized to continue to add visitors, since they keep making money.

3 **GENERIC 'ABOUT US' PAGES**

Since ghost sites don't have a core driving principle other than generating revenue for themselves, they will often have generic about us or contact pages. It is unlikely that you will be able to identify an actual person to contact.

4 **MASKED DOMAIN REGISTRATION**

It is typical for these domains to be registered with a privacy mask, so it is difficult to find out who is behind the site. Some may also choose to be registered in countries with protection guards against US law enforcement, such as Panama.

PRACTICES THAT DECEIVE & OBFUSCATE

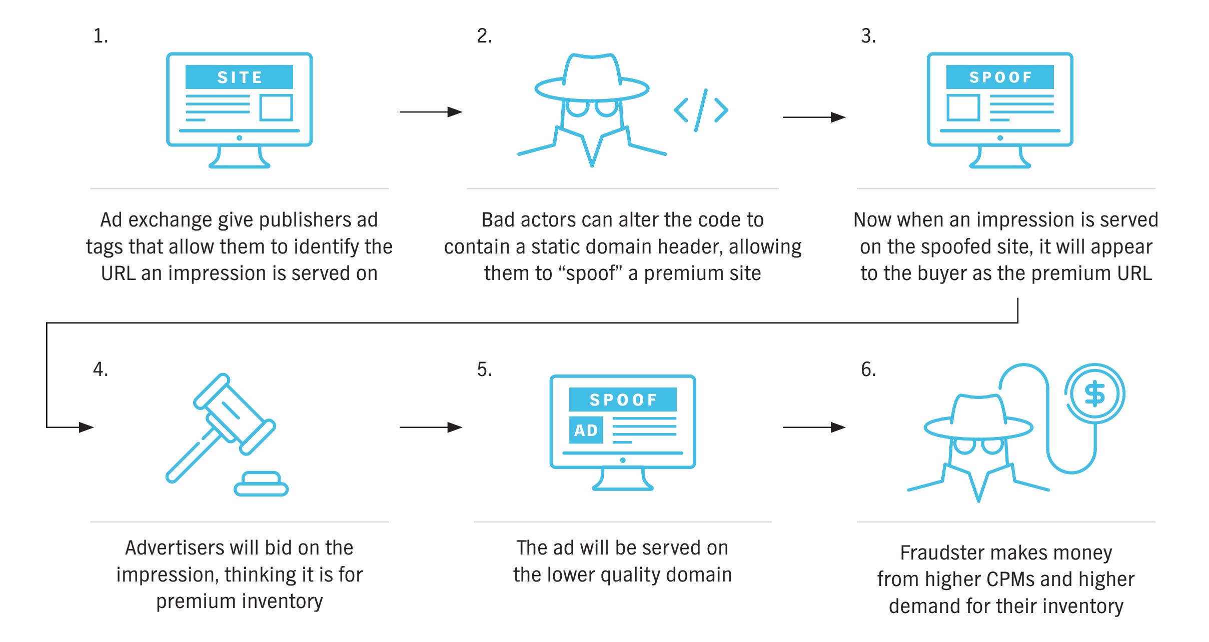
As the fight against fraud wages on, there are many ways that the source and value of an impression can be laundered, obfuscated and made to appear legitimate.

The programmatic industry has been awakening to the realities of quality in the ecosystem and has made progress towards delivering a more transparent, higher quality digital supply chain. However, bad actors are able to dedicate the full breadth of their time, effort and capital into developing ways to circumvent the system. While domain spoofing is, perhaps, the most widely discussed, there are many ways that the illegitimate sellers of inventory can make their activity look less suspicious and thereby make the impressions appear more attractive and valuable to buyers.

WHAT IS DOMAIN SPOOFING?

Domain spoofing is the method of laundering traffic to make bid requests appear more valuable to advertisers. For example, traffic from a ghost site is 'spoofed' and made to look like inventory from a premium domain. Buyers therefore may place more value on this inventory and implicitly trust its quality.

HOW IT WORKS



1. Ad exchange give publishers ad tags that allow them to identify the URL an impression is served on

2. Bad actors can alter the code to contain a static domain header, allowing them to "spoof" a premium site

3. Now when an impression is served on the spoofed site, it will appear to the buyer as the premium URL

4. Advertisers will bid on the impression, thinking it is for premium inventory

5. The ad will be served on the lower quality domain

6. Fraudster makes money from higher CPMs and higher demand for their inventory

HOW TO PROTECT YOURSELF

Domain spoofing is one form of digital misconduct that is on a path to extinction, thanks in large part to industry's swift adoption of the Interactive Advertising Bureau (IAB)'s ads.txt initiative. Ads.txt is a simple solution that allows publishers to identify and broadcast all of the companies in the programmatic ecosystem who are authorized to sell their inventory.

With ads.txt, buyers can quickly and easily validate the authenticity of a bid request and protect themselves. Likewise, publishers who implement ads.txt files on their properties can ensure the legitimacy of the supply chain. Analysis conducted by PubMatic earlier this year confirmed that marketers continue to drive ad spend towards ads.txt compliant inventory. Over the course of a four-month period, the analysis found:

+31%

spend on ads.txt compliant inventory

-16%

spend on inventory with no ads.txt file

Many technology providers, including PubMatic, have announced policies whereby publishers can only monetize inventory that has been authorized via their ads.txt files.

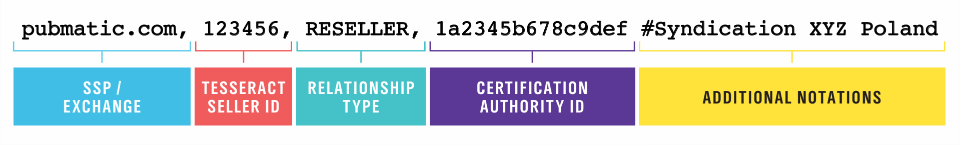
It is, however, important for both buyers and sellers to understand the current limitations of ads.txt:

- It does not cover mobile app inventory, an environment where domain spoofing continues to run rampant
- Publishers are not able to differentiate between ad formats within the spec, so cannot authorize a specific reseller for display only (vs. video)
- Risk of human error remains, particularly with spelling errors, leading to drop-offs of legitimate inventory sellers
- Some nefarious resellers are employing social engineering to scam their way into publishers' ads.txt files

CASE STUDY
ADS.TXT FILE MANIPULATION

A PubMatic supply partner, referred to throughout as Tesseract, was found to be arbitraging inventory on a premium property, buying from third-parties rather than through a direct or reseller relationship with the publisher. This arrangement had the potential to remain unnoticed for some time, since the publisher's ads.txt file includes an entry listing Tesseract's PubMatic supplier ID. However, while verifying, we found some concerns.

Under the section heading #Syndicated Video, the publisher's ads.txt entry showed the following:



```
pubmatic.com, 123456, RESELLER, 1a2345b678c9def #Syndication XYZ Poland
```

The question arose: what does a media company in Poland have to do with the Israeli-based company, Tesseract?

Pulling Tesseract URL data for its highest volume day revealed that nearly half of the unique URLs were from the publisher, representing 97 percent of the total volume for that day (totaling over 500 million ad requests). The specific URLs had nothing to do with Poland, and 95 percent of the publisher's ad requests flowed through US data centers. There was nothing to indicate that the content could warrant the volume of ad requests seen.

The investigation ultimately found that Tesseract did not, in fact, have a direct relationship with the publisher. Instead, they relied on XYZ Poland's influence with the publisher to get listed in the publisher's ads.txt file to legitimize their arbitrage efforts (which included serving carousel type video units in display ad slots). PubMatic began the termination process immediately upon confirmation.

IQ PRO TIP

Ads.txt should be viewed as the first line of defense against domain spoofing and fraud. It is important to work with vendors that are vigilant in their efforts to uncover malicious or suspicious activity. Ask your technology partners what they are doing to address these concerns.

OTHER PRACTICES THAT DECEIVE & OBFUSCATE

1 PAGE-LEVEL SCRIPTING

The same sites that resort to deceptively acquiring human traffic rather than building an organic audience often manipulate the mechanics of their sites to increase the ad revenue per user. These types of activities encompass subversive actions like 0x0 transparent i-frames, which allow a publisher to count impressions without ever displaying viewable ads on site, and ad sizing, which can increase ad impressions per user by order of magnitude.

Page-level scripting is especially rampant with mobile in-app inventory. Unless measurement vendors have their own SDKs integrated into mobile apps, the signals upon which they can make decisions are limited, resulting in an environment where manipulation of app inventory is less likely to be identified and flagged. The IAB's Open Measurement (OM) SDK eliminates the need for multiple SDKs (one for each measurement provider) to be integrated into apps. See more about OM-SDK in the Mobile In-App Inventory Quality section.

2 AD INJECTION AND ADWARE

Whether delivered by toolbars, hidden within software installations or dropped by maliciously coded ads, malware allows bad actors to sell inventory against sites with which they have no relationship. Often, as in the case of ad injection, illegitimately sold ads cover the existing ad units perfectly or appear on pages where the site offers no ad opportunities. The bad actors profit from this, taking revenue from the publisher, and trading on the target site's good name. This inventory often hides under the cover of domain spoofing and works its way into the ecosystem through ad networks, aggregators and other entry points.

The IAB's ads.cert initiative, which will work with RTB 3.0, was designed to help solve this issue. Ads.cert goes beyond the protection of ads.txt by using a digitally-secure signature to create an unbroken chain of custody between the original ad placement and the buyer. This digital signature serves as a type of 'authorization key' to prevent fraudsters from masking a bid request by wrapping it in a legitimate domain, which is possible with the malware used in ad injection.

3 POOR USER EXPERIENCE

These “land grab” activities include all the ways a publisher pushes the envelope of user experience to increase ad revenue, including:

- Cluttering a page with multiple ads of various sizes
- Forcing users to click through a slide show to increase ad impressions
- The liberal use of auto-play video, often with audio enabled

None of these methods can nor should be considered fraudulent; after all, in this category, everything is transparent and visible.

The quality issue at play here is two-fold: consumers get annoyed by the excess of advertising, and any brand associated with these methods may be left feeling soiled. Moreover, the massive bombardment of messages decreases the impact and value for any single one. PubMatic, as well as most exchanges and platforms, have policies in place designed to avoid these types of environments.

MOBILE IN-APP INVENTORY QUALITY

Mobile app is the ‘Wild West’ of inventory quality due to the lack of tag-based detection. Fraud is very difficult to identify and content is hard to verify.

Unlike the desktop environment, where online advertising grew and matured with the industry, mobile app ad inventory has a host of challenges pertaining to measurement and fraud detection.

Desktop tracking uses cookies; mobile apps track via device IDs. IP addresses represent individual computers and servers connected to the internet in the desktop environment, while with mobile, IPs may represent the cell towers to which thousands of devices can connect. The signal set for mobile is very different and can’t be used the same way for non-human fraud detection by third parties. Contributing to the difficulty is accessing the signals that are available within the app itself. Software Development Kits (SDKs) are needed to ‘tunnel into’ the app and access the available data that would allow for fraud (and viewability) detection.

Moreover, evaluating the content and user experience of apps is difficult given the device environment. While it’s easy to load a web page and peruse the content for quality checks, apps need to be loaded on devices, which can be difficult to monitor at scale.

IN-APP INVENTORY QUALITY CHALLENGES

The app environment facilitates the passing of falsified data, given the current difficulties in accessing quality signals and information within the app itself. There are various types of spoofing behavior, but they all share the desired objective of generating more ad revenue for the bad actor by making the ad inventory and audience opportunity appear much larger and more valuable than it is.

This spoofing behavior can come in various flavors, and each behavior results in either non-human, low quality or inflated metrics.

DEVICE SPOOFING

Unethical, rogue apps falsify or misrepresent the device information that is included in the outgoing bid request. By injecting a wide range of data representing different device IDs (e.g. IMEI), IP addresses, hardware make and model, etc., bid requests can appear to be originating from a large pool of unique, diversified users.

APP SPOOFING

Most similar to domain spoofing, which ads.txt solved for in the desktop environment, app spoofing injects the name of well-known app IDs so they appear more attractive to buyers. However, the creative is served into the app doing the spoofing.

LOCATION SPOOFING

Rogue apps will insert falsified latitude/longitude data into the bid stream. This increases the value of that bid request due to geo-targeting (e.g. bid request comes from Timbuktu but is falsified to show the user is in New York City). This practice is also used in conjunction with other spoofing practices to avoid detection (e.g. making the bid requests look like they originate in the UK, hiding the fact that they may be originating out of a farm of pre-programmed devices in a Sri Lankan warehouse).

HOW TO PROTECT YOURSELF

In 2017, the IAB Tech Lab introduced Open Measurement (OM), with OM-SDK as the centerpiece of this initiative. Acting as a 'universal translator', the OM-SDK will allow verification and measurement providers to 'listen' and collect signals originating within the app through a single SDK implementation for publishers. If widely adopted, the OM-SDK will create a standard allowing advertisers to better measure app inventory for fraud and viewability.

Additionally, in June 2018, the IAB unveiled a proposal that would create the equivalent of the ads.txt standard for mobile apps. Once rolled out and adopted, this solution would prevent much of the app spoofing in mobile, similar to what ads.txt has done for domain spoofing on the web.

Until these industry standards are adopted widely, mobile app inventory fraud is hard to identify. Technology providers can point buyers in the right direction, where they can take a closer look at specific apps that are either rogue, bad actors or whose reputation for quality is being used to mask bad actor activity.

1 **USE THIRD-PARTY FRAUD DETECTION**

Though mobile app fraud detection isn't as robust as desktop, third parties are a first line of protection, and offer reporting that serves as a signal indicating which apps should be more closely investigated and/or blocked from campaigns.

2 **CHOOSE APPS WHERE USERS CONSUME CONTENT**

Avoid flashlight apps, anti-virus, and other utility apps where users simply don't spend time interacting with the content. These types of apps are often used to generate high volumes of bid requests where users aren't engaged.

3 **STICK TO APPS FROM THE ANDROID AND IOS STORES**

Though these most popular app stores don't evaluate apps specifically for ad fraud, they do have basic requirements that are non-existent from other app stores.

4 **WHITELIST APPS FROM THE TOP 1,000 IN POPULARITY**

Curating from lists of Android and iOS apps, indexed by popularity, create a whitelist that includes only apps that have strong, verified user bases. Rogue apps are likely to lurk in the tail of the supply chain and benefit from the open auction structure of the advertising ecosystem.

FUTURE STATE

Imagine you could snap your fingers and ad fraud instantly disappeared. What would this fraud-free future look like?

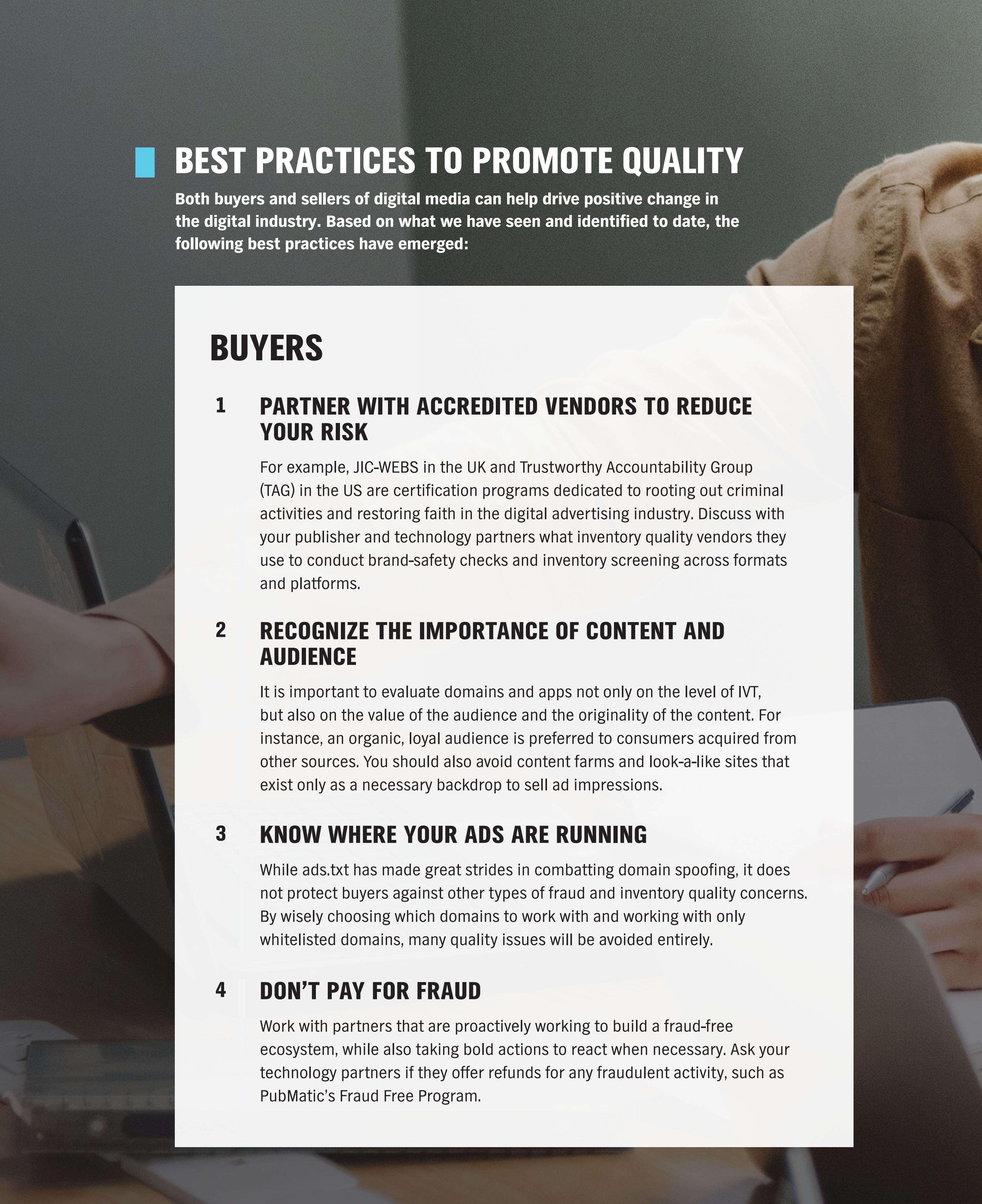
The current focus on cleaning up ad fraud, though critical to ensuring the long-term health of the digital advertising ecosystem, serves as a distraction from other issues important to the industry. New industry initiatives, such as ads.txt and ads.cert from the IAB, provide a strong foundation for the direction forward. As programmatic professionals, we must all identify the next area where resources will be needed to continue improving inventory quality.

THE DECLINE OF TARGETING

Consumers are increasingly voicing their discomfort with cookies marking them and bundling them into audiences and segments that advertisers then target (via ad tech) to deliver marketing messaging. Regulations like the European Union’s GDPR create obstacles for cookie and audience targeting. This is leading quality content and contextual targeting to become increasingly important.

QUALITY STARTS WITH CONTENT

Third-party fraud detection vendors convince the marketplace that by deploying their solutions, advertisers can put a stop to fraudulent traffic. While there is value in identifying and filtering out non-human traffic, we have been lulled into believing that this is the best and only solution. Quality content, developed by legitimate and trusted sources, allow for an additional layer of filtration.



BEST PRACTICES TO PROMOTE QUALITY

Both buyers and sellers of digital media can help drive positive change in the digital industry. Based on what we have seen and identified to date, the following best practices have emerged:

BUYERS

1 PARTNER WITH ACCREDITED VENDORS TO REDUCE YOUR RISK

For example, JIC-WEBS in the UK and Trustworthy Accountability Group (TAG) in the US are certification programs dedicated to rooting out criminal activities and restoring faith in the digital advertising industry. Discuss with your publisher and technology partners what inventory quality vendors they use to conduct brand-safety checks and inventory screening across formats and platforms.

2 RECOGNIZE THE IMPORTANCE OF CONTENT AND AUDIENCE

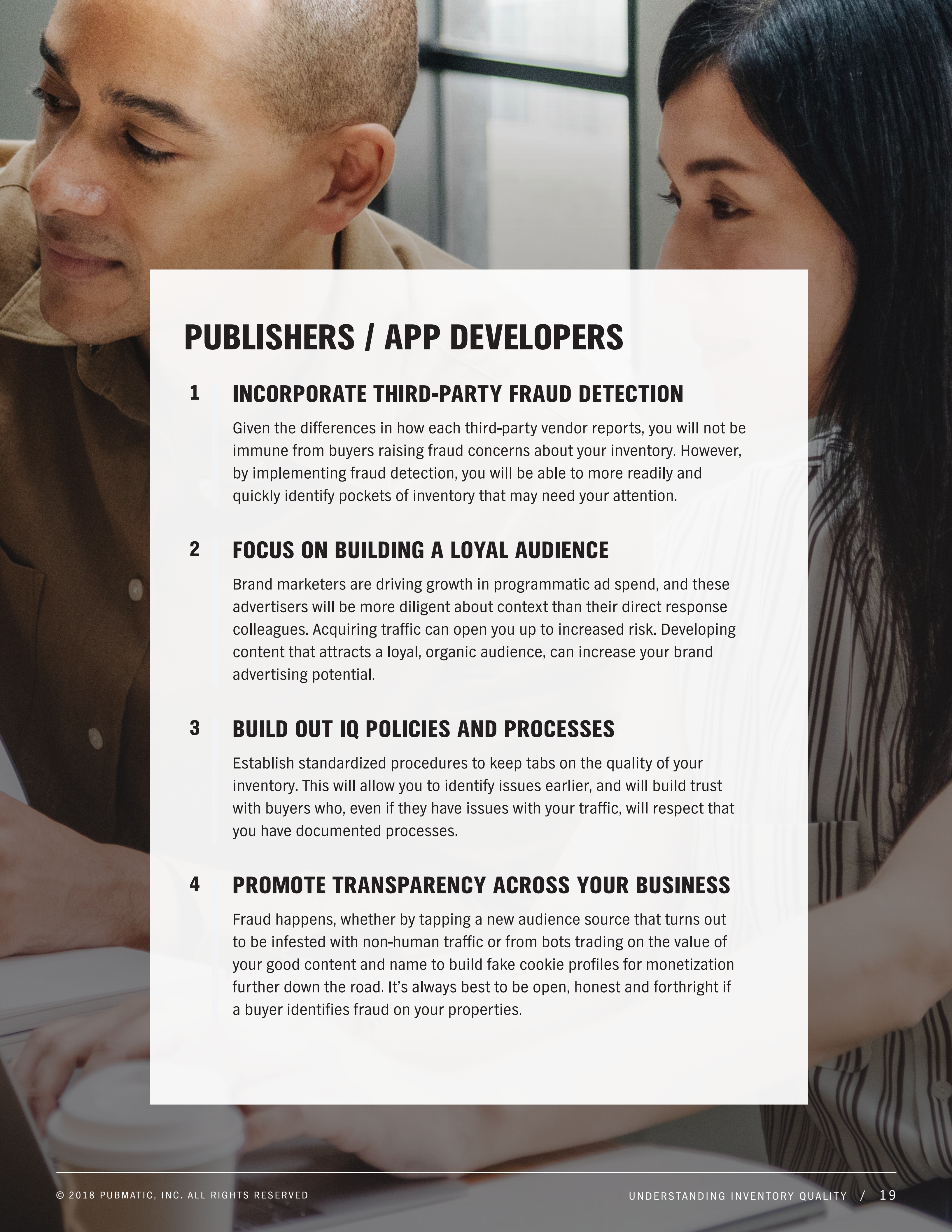
It is important to evaluate domains and apps not only on the level of IVT, but also on the value of the audience and the originality of the content. For instance, an organic, loyal audience is preferred to consumers acquired from other sources. You should also avoid content farms and look-a-like sites that exist only as a necessary backdrop to sell ad impressions.

3 KNOW WHERE YOUR ADS ARE RUNNING

While ads.txt has made great strides in combatting domain spoofing, it does not protect buyers against other types of fraud and inventory quality concerns. By wisely choosing which domains to work with and working with only whitelisted domains, many quality issues will be avoided entirely.

4 DON'T PAY FOR FRAUD

Work with partners that are proactively working to build a fraud-free ecosystem, while also taking bold actions to react when necessary. Ask your technology partners if they offer refunds for any fraudulent activity, such as PubMatic's Fraud Free Program.



PUBLISHERS / APP DEVELOPERS

1 INCORPORATE THIRD-PARTY FRAUD DETECTION

Given the differences in how each third-party vendor reports, you will not be immune from buyers raising fraud concerns about your inventory. However, by implementing fraud detection, you will be able to more readily and quickly identify pockets of inventory that may need your attention.

2 FOCUS ON BUILDING A LOYAL AUDIENCE

Brand marketers are driving growth in programmatic ad spend, and these advertisers will be more diligent about context than their direct response colleagues. Acquiring traffic can open you up to increased risk. Developing content that attracts a loyal, organic audience, can increase your brand advertising potential.

3 BUILD OUT IQ POLICIES AND PROCESSES

Establish standardized procedures to keep tabs on the quality of your inventory. This will allow you to identify issues earlier, and will build trust with buyers who, even if they have issues with your traffic, will respect that you have documented processes.

4 PROMOTE TRANSPARENCY ACROSS YOUR BUSINESS

Fraud happens, whether by tapping a new audience source that turns out to be infested with non-human traffic or from bots trading on the value of your good content and name to build fake cookie profiles for monetization further down the road. It’s always best to be open, honest and forthright if a buyer identifies fraud on your properties.

[1] "Global Ad Spending: The eMarketer Forecast for 2018," eMarketer, May 2018

[2] "Bot Baseline 2016-2017," ANA and WhiteOps, May 2017

[3] "Invalid Traffic Detection and Filtration Guidelines Addendum," Media Ratings Council, Inc. (MRC), October 2015

[4] "Programmatic Ad Spending Worldwide, 2012-2019," eMarketer, November 2017

About PubMatic

PubMatic is a publisher-focused sell-side platform for an open digital media future. Featuring leading omni-channel revenue automation technology for publishers and enterprise-grade programmatic tools for media buyers, PubMatic's publisher-first approach enables advertisers to access premium inventory at scale. Processing over 12 trillion advertiser bids per month, PubMatic has created a global infrastructure to drive publisher monetization and control over their ad inventory. Since 2006, PubMatic's focus on data and technology innovation has fueled the rise of the programmatic industry as a whole. Headquartered in Redwood City, California, PubMatic operates 13 offices and six data centers worldwide.

PubMatic is a registered trademark of PubMatic, Inc. Other trademarks are the property of their respective owners.

PUBMATIC CONTACTS

Press Contact:

BLAST PR
pubmatic@blastpr.com

Inventory Quality Contact:

ERIC BOZINNY
Director, Inventory Quality
eric.bozinny@pubmatic.com

Sales Contacts:

JEFFREY HIRSCH
Chief Marketing Officer &
Head of US Publisher Development
jeffrey.hirsch@pubmatic.com

BILL SWANSON
Chief Revenue Officer, EMEA
bill.swanson@pubmatic.com

CRAIG CHINN
VP, Chief Customer Success Officer
craig.chinn@pubmatic.com

JASON BARNES
Chief Revenue Officer, APAC
jason.barnes@pubmatic.com

KYLE DOZEMAN
VP, Advertiser Solutions, US
kyle.dozeman@pubmatic.com

PubMatic