PROGRAMMATIC
INSIGHTS
REPORT
SPOTLIGHT ON QUALITY

JUNE-SEPTEMBER 2017 DATA UPDATE

1R

1R RHYTHMONE

Contents

Introduction

Advertisers and brands have been contending with inventory quality and brand safety since the advent of programmatic buying. While sources vary in their estimates of the problem — and their assessment of its impact — everyone agrees that fraud is a multibillion-dollar issue. According to Adobe*, media quality is still the number one challenge for digital marketers when buying advertising.

This situation is further complicated by technology itself. The power of programmatic buying is in its ability to allow advertisers to purchase audiences — not just specific publishers or apps as a proxy. While this opens up vast quantities of supply, it also makes transparency and quality assessment challenging.

ENSURING QUALITY

RhythmOne's advertising marketplace processed over 28.7 trillion raw ad opportunities in the last 12 months, ending in September 2017 — an average of 2.4 trillion opportunities per month, overall. This number is only increasing: in the last four months, June to September (i.e., the time period of this report), our platform saw on average nearly 2.7 trillion ad opportunities per month.

While this volume allows us to provide multi-channel, multi-format inventory at scale for demand-side platforms, agencies and brands, it also puts RhythmOne on the front line of combatting fraud. We take this imperative seriously.

That is why we developed RhythmGuard, our proprietary filtering technology that uses first- and third-party data and machine learning algorithms to identify and block all types of suspicious inventory in fractions of a second before, during, and even after a bid request is made. The blocking rates you see detailed in this report are a result of RhythmGuard.

On average, RhythmGuard blocks 30-60% of raw ad opportunities (i.e., bid requests) which have

> ## Online ad fraud will cost brands $16.4 billion in 2017.
> — Adloox

underperformed, in some respect, based on our traffic quality scans. This does not mean that 30-60% of our inventory is fraudulent, rather, it represents the portion blocked based on specific filtering parameters. As a result, we are proud to offer one of the industry's largest footprints of targetable, verified, and pre-filtered inventory.

A DYNAMIC REPORTING ENVIRONMENT

Covering North America (US and Canada) in the period of June through September 2017, this report focuses on our inventory blocking rates as a barometer of supply quality. It offers transparency into trends in our marketplace around the traffic we block by device, ad size, type, and IAB category.

In addition to real-time filtering, we also monitor and make adjustments to the supply we allow to enter our marketplace in the first place. We dynamically increase or decrease inventory we get from certain providers. We may go so far as to temporarily suspend or permanently terminate relationships in order to remediate consistent quality concerns. As such, the overall amount we block from reporting period to reporting period may change significantly – as evidenced in the callout on page 5, "Beyond Blocking: Ensuring Quality at the Source."

*Adobe Digital Insights, "Advertising Report," March 2017

Getting Clear on Quality

It's helpful to start by defining terms. Ad fraud, or the practice of falsifying traffic or traffic-related activities in order to charge advertisers for impressions, engagements, or conversions that did not actually occur, is currently classified in two main categories by the Media Rating Council (MRC):

GIVT General Invalid Traffic

GIVT is non-human traffic. This is typically considered the most basic type of fraud and is somewhat easier to identify and combat.

TYPES OF GIVT:
- Bots
- Spiders
- Crawlers
- Invalid domains
- Invalid IPs

SIVT Sophisticated Invalid Traffic

Sophisticated invalid traffic includes more advanced deception techniques that aren't picked up by typical botnet filters. This classification of fraud can be more complicated to detect and eliminate.

TYPES OF SIVT:
- Bots or crawlers pretending to be legitimate
- Ads delivered via hijacked or malware-infected devices
- High frequency of impressions from same user, cookie, or device
- High click-through rates from the same user, cookie, or device
- Domain and URL spoofing
- Publisher fraud including falsified sites, stacked, or popup ads
- Invalid completes or conversions

Combatting Techniques

- Global IP, domain, User Agent, and device ID block lists derived from first- and third-party data sources
- Manual verification of publisher quality, including domain history, privacy policies, and content quality
- Real-time verification leveraging multiple third-party verification data
- GIVT and SIVT scoring algorithms
- Ad creative verification
- Contextual content checks
- Post-bid verification to check on domain spoofing
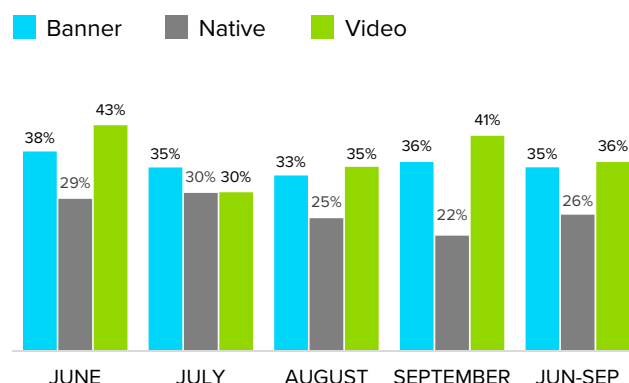- Monitoring and eliminating publishers that consistently underperform

Trends by Type

RhythmOne categorizes its inventory into three main types: banners, video, and native.

In June-September 2017, the average blocking rate for video advertising slightly edged out banner advertising (36% vs. 35%).

Video advertising comes in different forms including in-stream, outstream, in-banner, and interstitial delivered by different players, either in-app or in browser, which makes the identification and elimination of suspicious traffic all the more challenging — and necessitates enhanced implementations of both GIVT and SIVT measurement. In mid-2017, we enabled new third-party monitoring features and made enhancements to our RhythmGuard offering to better combat fraud on the video front.

Banners as an ad type have the longest history and greatest volume in our marketplace. Those who combat fraud have had time to develop sophisticated detection and elimination techniques to keep suspicious banner inventory from reaching advertisers.

BLOCKING RATE BY AD TYPE (June – September)

Banner   Native   Video

|	JUNE	JULY	AUGUST	SEPTEMBER	JUN-SEP
Banner	38%	35%	33%	36%	35%
Native	29%	30%	25%	22%	26%
Video	43%	30%	35%	41%	36%

Native advertising, in general, is blocked with less frequency. There is a lower volume and demand for native advertising — factors that make it a less attractive target for fraudulent activities. Requests for true native inventory typically originate from web servers before the content is rendered to the device, making it much more difficult to forge inventory of that media type.

Beyond Blocking: Ensuring Quality at the Source

This report primarily addresses the blocking of inventory once it enters the RhythmOne marketplace. Another important lever we have to control quality is the inventory we allow to enter our marketplace in the first place. Which supply partners we work with, and the quality they bring to the marketplace, are variables we constantly scrutinize. We may add new partners or suspend relationships that require quality remediation. This is why over time, the average amount of inventory we block may vary. For example, as detailed to the right, our blocking rates among video and banner advertising decreased by 12% and 20%, respectively, when compared with the previous reporting period. This is because we've reviewed and adjusted certain supply partners' contribution to the marketplace. As demand for different types of inventory varies over time, the overall blocking average may go up or down based on efforts to normalize quality across our supply. This way, our partners can rest assured that we will provide the scale they need and the quality they expect.

BLOCKING RATE AVERAGES BY REPORTING PERIOD (2017)

Banner   Native   Video

	MAR-MAY	JUN-SEP
Banner	55%	35%
Native	34%	26%
Video	48%	36%
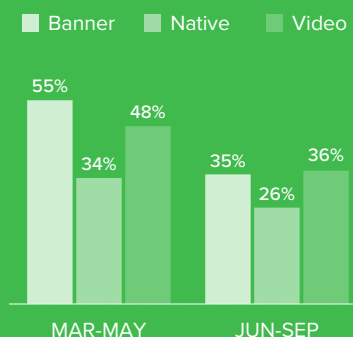
Trends by Device

In July-September 2017, we blocked more inventory on desktop vs. mobile devices, with minor fluctuations on a month-to-month basis. As the data illustrates, suspicious and underperforming traffic generally results in blocking nearly one-half of overall ad opportunities on desktop devices and more than one-quarter on mobile devices. While this traffic is eliminated before it is sent to demand partners, these figures underscore the challenge.

MOBILE WEB VS. IN-APP

With mobile ad spending accounting for 70.3% (US) of total digital advertising spending*, many of the techniques used to perpetuate fraud as well as detect it have migrated from desktop to mobile. Mobile advertising is broken into two broad categories — mobile web (including mobile-optimized versions of websites) and mobile app. Fraud on mobile web is similar to desktops since ads are delivered via a browser.

The rate at which we blocked ad opportunities on mobile web (avg. 40%) and mobile app (avg. 20%) showed little month-to-month fluctuation. Fraud on mobile apps is inherently complicated and can be committed in multiple ways, including:
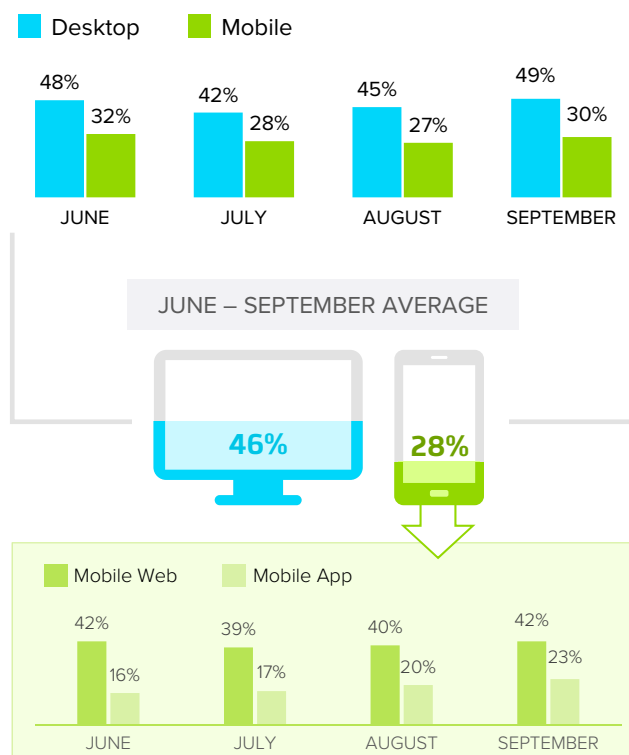
- Malicious apps (typically found outside trusted marketplaces) designed to commit impression and click fraud

*eMarketer Comparative Estimates, August 2017

- Botnets similar to the desktop world
- User session hijacking to drive installs

This makes fraud detection on mobile apps more varied, and therefore more challenging.

BLOCKING RATE BY DEVICE (June – September)

Desktop / Mobile

	JUNE	JULY	AUGUST	SEPTEMBER
Desktop	48%	42%	45%	49%
Mobile	32%	28%	27%	30%

JUNE – SEPTEMBER AVERAGE

Desktop: **46%** Mobile: **28%**

Mobile Web / Mobile App

	JUNE	JULY	AUGUST	SEPTEMBER
Mobile Web	42%	39%	40%	42%
Mobile App	16%	17%	20%	23%

Ads.txt Increases Transparency

Ads.txt (Authorized Digital Sellers) is an IAB initiative to eliminate the ability of fraudsters to profit by misrepresenting inventory in the open digital advertising ecosystem. Ads.txt provides a means for content owners to declare who is authorized to sell their inventory. RhythmOne is a strong proponent of the initiative. Since mid-September 2017, we have aggressively marketed the initiative — and as of early November 2017, a rapidly growing percentage of our partners have adopted ads.txt and have verified in their site code that RhythmOne is a trusted seller of their inventory.
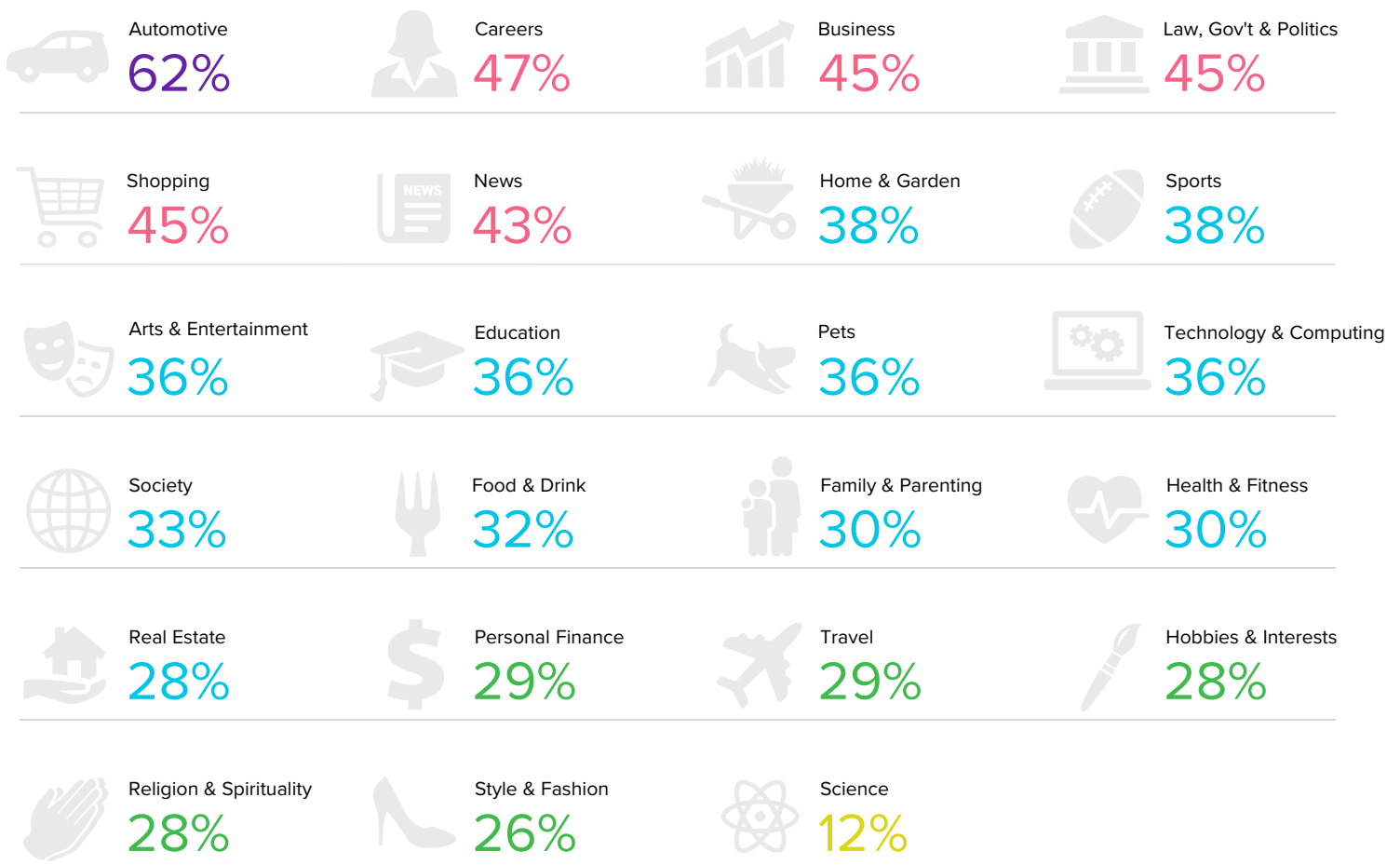
Trends by IAB Category

Another lens through which to view blocking levels is by IAB category. IAB categories are assigned to publishers and are associated with the types of content that a site or mobile app serves. The higher levels of blocking by IAB category are typically associated with retail and/or consumer products, or those with higher CPMs — like automotive, business, and shopping. There is a good deal of fraud directed at consumers spending online or perhaps applying for a new job (e.g., careers). For example, phishing attacks seek to capture consumer information to make fraudulent purchases.

The same processes can infect consumer systems. Those same compromised devices can then originate fraudulent requests for advertisements, siphoning additional revenue into the pockets of criminals.

The amount of blocking by IAB category is also affected by seasonality and volume, as evidenced in our June-September 2017 averages. For example, according to comScore, more than one-half (51.5%) of the total US digital population visited Automotive sites in September 2017 – compared with just 22.8% of the total US digital population visiting Religion/Spirituality sites in that same month.

Automotive	Careers	Business	Law, Gov't & Politics
62%	47%	45%	45%

Shopping	News	Home & Garden	Sports
45%	43%	38%	38%

Arts & Entertainment	Education	Pets	Technology & Computing
36%	36%	36%	36%

Society	Food & Drink	Family & Parenting	Health & Fitness
33%	32%	30%	30%

Real Estate	Personal Finance	Travel	Hobbies & Interests
28%	29%	29%	28%

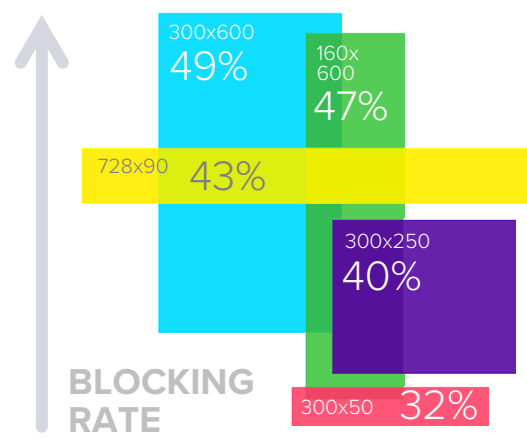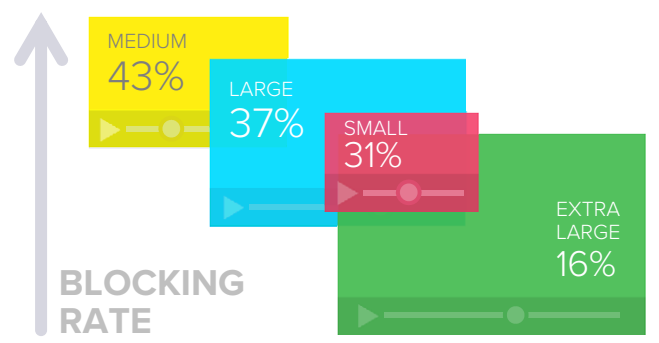| Religion & Spirituality	Style & Fashion	Science
28%	26%	12%

Trends by Creative

Advertisers might wonder if there are some ad sizes that tend to be a greater target of fraud. The answer? Yes.

The likely rationale for this variation is the hardcoded methods used to perpetuate fraud. For example, a malicious program (malware or adware) may only be programmed to look for certain sized content containers to override and inject. Moreover, some fraudulent inventory is generated using pop-under windows that have static content in them, resulting in skewed data by size. Finally, fraudulent inventory is often sold on a tag basis, which focuses on a single ad size.

BLOCKING RATE BY VIDEO SIZE (JUNE – SEPTEMBER)

MEDIUM
43%

LARGE
37%

SMALL
31%

EXTRA LARGE
16%

BLOCKING RATE

BLOCKING RATE BY BANNER SIZE (JUNE – SEPTEMBER)

300x600
49%

160x 600
47%

728x90
43%

300x250
40%

300x50
32%

BLOCKING RATE

With video sizes, we generally see lower blocking rates across ad sizes compared with banner sizes. The extra large video size in particular experiences a low block rate compared with its smaller-sized peers.

This is attributable to the lower volume of ads purchased at this size, and because the smaller sizes are typically "standard," so they tend to represent a more attractive target to those looking to perpetrate fraud.

Private Marketplaces as a Conduit to Quality

Our Private Marketplaces (PMPs) have seen a significant increase in volume over the past year. From November 2016 to June 2017, our PMPs processed 3.4 trillion opportunities at an average of 430 billion per month. From July to September 2017, we processed 3.8 trillion PMP opportunities at an average of 1.28 trillion per month. Compared to OpenRTB, RhythmOne's PMPs have stricter IVT thresholds than base DSPs and typically have higher block rates.

This is largely attributable to the select inventory we offer through our PMPs, either owned or exclusive header bidder supply, or supply that meets specific data or targeting criteria. As PMP volume grows, we will continue to explore this issue further as we seek to help advertisers and brands tap into quality in a programmatic environment.

Conclusion

RhythmOne strongly believes in creating an ecosystem that is respectful to consumers, impactful for advertisers, and sustainable for publishers. We will continue to provide transparency into trends we're seeing around inventory quality and brand safety — major components of our mission to provide the most efficient and effective marketplace for digital advertising and content distribution.

While great strides have been made in assuring brand safety, the industry has a long way to go. For the ecosystem to continue to thrive, we must:

- Agree to universal quality standards and measurement criteria
- Eliminate fraud at its source rather than just monitoring and measuring – fix the problem, not the score
- Encourage supply partners to adopt ads.txt in order to enhance transparency and eliminate fraudulent representation
- Collaborate on both supply and demand sides, and commit to operating in a manner to not promote or stimulate fraud

HOW YOU CAN USE THIS INFORMATION

Seasonality, volume, and other factors, such as evolving DSP restrictions and IVT benchmarks, directly affect blocking rates. Advertisers need to be aware of the constantly changing programmatic landscape. They should ask questions of their partners regarding the supply they're accessing – and the measures their underlying platforms are taking to combat fraud at the source.

When it comes to blocking trends by type, device, and creative, advertisers should consider:

- Setting expectations appropriately about what will be measured in mobile (web and app) and desktop campaigns
- Consider leveraging non-standard ad sizes, such as the extra large unit – especially in video
- Running campaigns in Private Marketplaces (PMPs) to ensure a high-quality and transparent environment with greater control over placement

What Advertisers Should Look For in Their Partners

So, what should advertisers look for in their supply and verification partners? Some key considerations:

- Work with partners that can analyze and provide transparency based on multiple approaches
- Look for supply providers and technology platforms that can offer real-time evaluation and elimination of suspicious traffic vs. after-the-fact reporting
- Work with providers that offer transparency into their methodology and inventory quality
- Confirm that verification takes place both pre- and post-bid
- Look for supply platforms that own and operate web properties and apps — they have a real stake in successfully eliminating fraud, and have the added benefit of being able to test new detection methods at the source
- Make sure you work with technology partners that rank highly on independent, objective quality measures, like Pixalate's Global Seller Trust Index™

RhythmGuard

STANDING BEHIND OUR INVENTORY

RhythmGuard is our proprietary brand safety technology that actively combats fraud by leveraging our own unique detection technology coupled with data and measures from some of the leading third-party providers in the industry — ensuring uniform quality across our supply and demand partners.

#1
PIXALATE
GLOBAL SELLER
TRUST INDEX
US

#2
PIXALATE
GLOBAL SELLER
TRUST INDEX
International
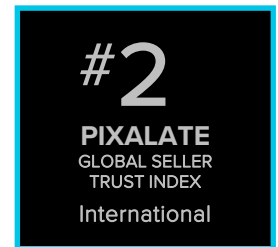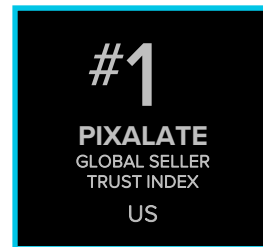
RHYTHMGUARD IN ACTION

From the moment we partner with a publisher to the microseconds before we serve an ad, RhythmGuard is at work filtering traffic and ensuring we maintain the highest quality standards.

Block Lists (GIVT)*
Extensive block lists based on:
- Domain
- Device ID
- User Agent
- IP Address

SIVT Scoring**
Proprietary scoring algorithms combine the data from our exchange with top third-party verification providers.

Contextual Brand Safety
Review of contextual placements and keywords to ensure ads do not appear near suspicious or unwanted sites or news.

Publisher and Creative Verification
After the bid, but before the impression is served, RhythmGuard verifies the creative ID and checks for domain spoofing.

VERIFICATION PARTNERS

pixalate   whiteops   CONFIANT   DV DoubleVerify

grapeshot   IAS Integral Ad Science   MOAT   THE MEDIA TRUST

ASSOCIATIONS AND CERTIFICATIONS

DTSG UK BRAND SAFETY   JIC WEBS   VV OPEN VIDEO

tag   iab.

---

* GIVT: General Invalid Traffic — Includes traffic identified through routine and list-based means of filtration — such as bots, spiders, other crawlers; non-browser user agent headers; and pre-fetch or browser pre-rendered traffic.
** SIVT: Sophisticated Invalid Traffic — Includes traffic identified through advanced analytics, multipoint corroboration, human intervention — such as hijacked devices, ad tags, or creative; adware; malware; misappropriated content.

About RhythmOne

We Make Connections that Matter, Driving Real Business Outcomes.

RhythmOne provides streamlined, transparent connections between advertisers and audiences through a combination of differentiated supply, innovative technology and insights-driven data.

Our end-to-end platform provides more direct, efficient, and effective connections, driving ROI for advertisers and publishers.

BRAND/AGENCY → CMP → DSP → DMP → EXCHANGE → SSP → WEBSITES/APPS → CONSUMER

James Murphy | VP, Programmatic

James Murphy is Vice President, Programmatic at RhythmOne. He oversees RhythmOne's programmatic division, including business development and operations. With over 20 years' experience in digital media — and over five in developing world-class programmatic platforms — his insight and operational knowledge ensure RhythmOne is constantly exceeding the expectations of our supply and demand partners alike.

What Makes Us Different

- Proprietary Analytics
- Viewability and Verification Guarantees
- Unique Targeting Opportunities

- Quality, Brand-Safe Inventory
- Creative Innovation with Personalized Campaigns

- Automated Optimization
- Unparalleled Reach
- ROI-driven Programmatic Influencer Marketing

Learn More and Contact Us   Visit us at RhythmOne.com

RHYTHMONE