WHITE PAPER

IronNet™

Cybersecurity for your brand

How to fight the cybercrime of digital ad fraud

SECTION 1

Feasting on a complex digital ad ecosystem

Digital ad fraud is a well known but little understood problem. While seemingly simple on the surface, in reality the underlying networks and techniques employed to perpetrate this fraud are incredibly complex. Digital ad fraud can be defined as the deliberate attempt to prevent the proper delivery of an ad to a human user.

$51 million each day lost to ad fraud

—JUNIPER RESEARCH

There are three main forms that this fraud can take:

- Shady publishing practices, such as buying in traffic or stacking ads, to inflate their ad revenues.
- Ghost sites set up by fraudsters for the specific purpose of laundering ad impressions.
- The falsification of bid requests to attract bids that were intended for reputable sites and apps.

Bots that inflate

Ghost publishers

Domain & app misrepresentation

THREE PRIMARY DRIVERS OF DIGITAL AD FRAUD

Even with a clear sense of what digital ad fraud is, the fundamental problem on hand is that the digital ad supply chain is a complex, multi-player system that isn't systematically incentivized to root out all sources of fraudulent activity. The problem is widespread. In its study of its clients' web traffic, Adobe found that "about 28% of the traffic likely came from bots and other 'non-human signals.'"

> **In its study of its clients' web traffic, Adobe found that "about 28% of the traffic likely came from bots and other 'non-human signals.'"**

For marketers, it can be tempting to ignore fraudulent traffic. The appeal of high impression volumes and the pressure to spend budgets often win out over the desire to scrutinize any potential fraud. After all, the rationale is layered and typically sounds like this:

- Recorded fraud rates are usually pretty low (<5%).
- The cost of fraud is minimal and already baked into ad rates.
- Enough traffic eventually will reach some human eyeballs.

So why bother? Well, here are three compelling reasons: *brand, brand, and brand*. Several brand-inspired questions can help shift the collective mindset:

- Do you really want all your brand-building efforts to be dismantled by bad bots unleashed by those criminal groups?
- And what if your well-intentioned ads appear on illegitimate domains where they could become a vehicle for malware?
- Are you comfortable overlooking the bigger picture that ad fraud is a source of funds for organized crime?

Most Fortune 500s have adopted impressive sustainability, corporate social responsibility, and other positive-change initiatives. Now is the time to take a fresh look at digital ad fraud through this same lens of accountability.

The first step is to take a deep look at fraudsters' ever-changing tactics and then learn how to spot and stop them in their tracks.

SECTION 2

The ad fraud problem *is* a cybersecurity problem.

When you think of cybercrime, financial systems such as bank accounts or shopping apps immediately come to mind. But cybercrime is happening everywhere, and it no longer is easy to ignore. Some of the most unexpected and unusual vulnerabilities from the last several years reveal the extent to which cyber attacks are creeping into the day-to-day fabric of our lives.

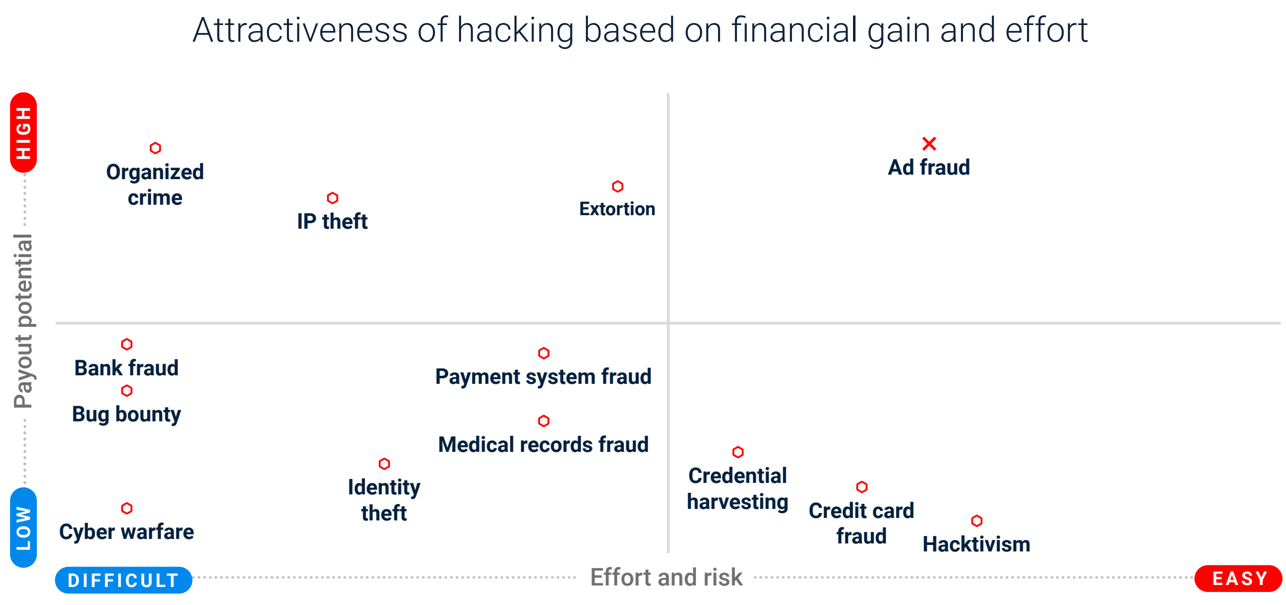
Cybercriminals are lurking ...

- **In doctors' offices**, where malware reigns supreme among healthcare targets, along with a spike in the proverbial cockroach of the threat landscape: ransomware;
- **Within music streams**, such as the exposure of some Spotify user passwords;
- **In popular online games**, as illustrated by 46 million records stolen from Animal Jam adolescents; and
- **Even at gas stations**, where hackers are taking advantage of default password settings to loot 120,000 liters of fuel.

Just as unsettling is the fact that attackers are becoming more and more egregious. Given the time and resources, hackers have the ability to breach even some of the strongest and most secure digital systems in the world, as evidenced by the SolarWinds/SUNBURST supply chain attack that affected 18,000 entities — including some of the most secure systems in the world. And when money becomes the cybercriminal's end-all-be-all payload, watch out!

Reporter Tara Seals notes in *Infosecurity Magazine* that, "Cybercrime is a lucrative business, with relatively low risks compared to other forms of crime. Cybercriminals are rarely caught and convicted because they are virtually invisible."

Therein lies the accelerating risk of digital advertising: the digital ad supply chain is a complex system that confounds even the most sophisticated and well-intended marketers, leaving it unprotected from money-driven hackers.



In Hewlett Packard Enterprise's *The business of hacking*, X marks the spot on ad fraud as both the most lucrative hacking activity and the easiest one for cybercriminals to carry out. It continues to be the one that gets away: from detection, from consequence, and, quite frankly, from systemic complacency.

It's clear that no brand strategy or decision-making around ad spend includes knowingly filling the pockets of organized criminal groups and other seedy players. It's equally as clear, however, that the industry needs a major mindshift in the way ad fraud is perceived and, more important, how it is combated.

Indeed, fraudsters are going where the money is. Worldwide spending on digital advertising has grown to about $390 billion. Gaining a better sense of where the siphoned money is going and who is behind the fraud prompts a necessary wakeup call for the industry to approach ad fraud as a cybersecurity problem.

So where is the money going?

15% of digital marketing spend is "unattributable"

—PWC AND ISBA, THE TRADE BODY FOR UK ADVERTISERS

Not all this money is being lost to fraud, but this number highlights the extent to which proper oversight is lacking in the digital supply chain. It is precisely this barrier to visibility that fraudsters are continuing to exploit in their pervasive efforts to drain more and more money out of digital advertising.

There seems to be an industry-wide tacit acceptance that seeing 2-3% fraud on a campaign is normal and doesn't merit any form of investigation as to its source. In reality, if even this relatively small percentage of spend is being lost on every campaign then the industry has at least a $12bn fraud problem. And how can we be confident that the true scale of the losses isn't much bigger than the existing, standardized fraud detection tools are reporting?

Who is behind the fraud?

As far back as 2016, the World Federation of Advertisers (WFA) co-authored a "Compendium of Ad Fraud" report highlighting the fact that ad fraud was on course to be "second only to cocaine and opiates as a form of organised crime." Five years later, this is still the elephant in the room.

Even now, with widespread awareness of ad fraud's prevalence, the industry continues to whistle past the graveyard rife with illicit activities the stolen ad budgets are actually funding. Yet stories about new ad fraud discoveries abound, and as marketers shift budgets into new channels the fraudsters follow.

Although there have been one or two well-publicized takedowns of fraud operations, these instances unfortunately are a drop in the ocean compared to the money that is being lost. The harsh truth is that there is still very little risk to — *and a huge profit for* — the criminals behind the fraud.

Looking at fraudsters through the lens of cybersecurity defense reveals a new and better way for companies to detect malicious activity and shut it down. How? By looking at the perpetrators' behaviors on back-end networks. You can't directly see the them, but the truth is in the network traffic, detected by advanced behavioral analytics designed to take down even nation-state level hackers.

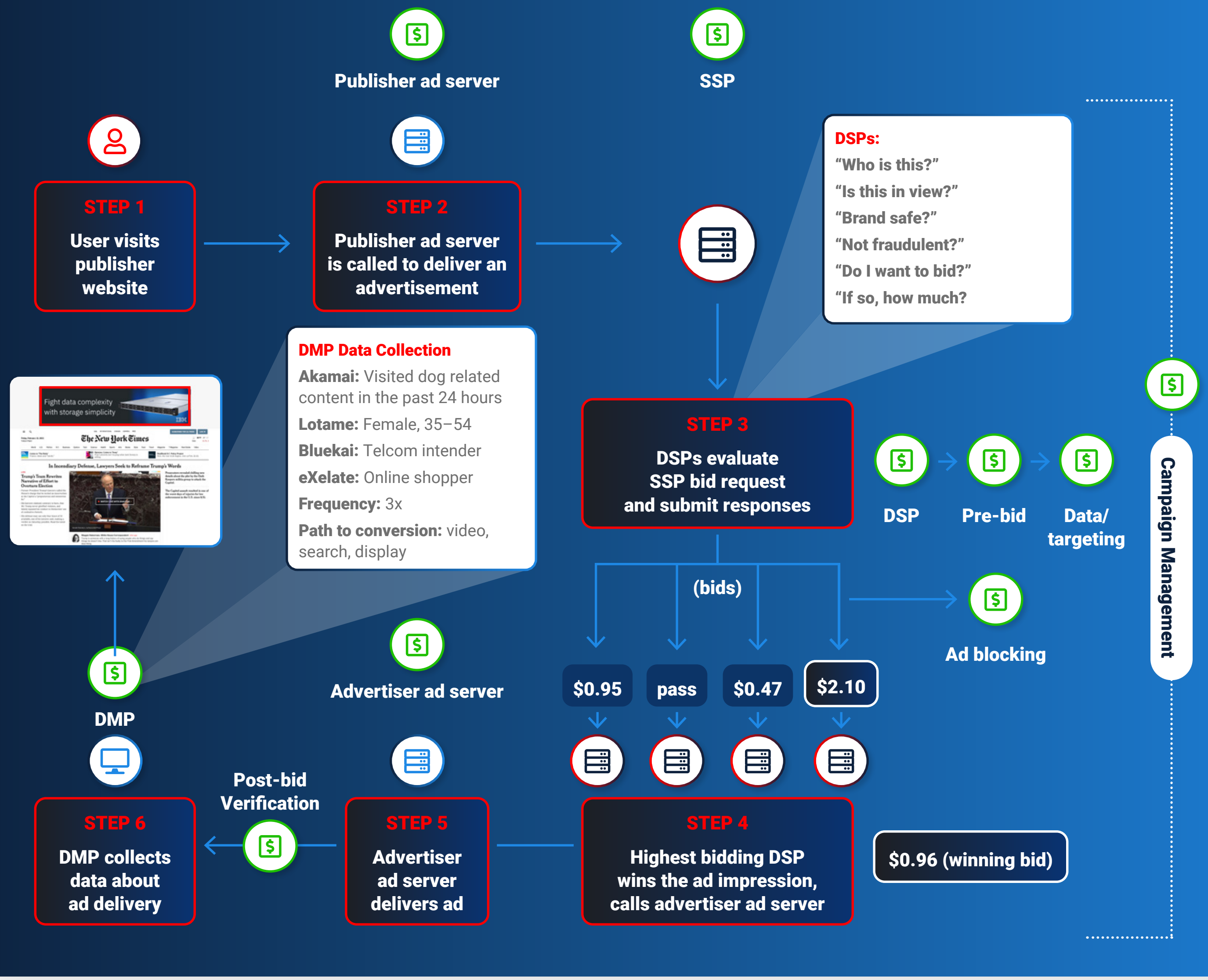
The harsh truth is that there is still very little risk to — and a huge profit for — the criminals behind the fraud.

SECTION 3

How does digital advertising fraud happen?

To better understand where the fraudsters are pouncing, let's first take a look at the complex digital ad supply chain. While the process is much more nuanced, this diagram helps to demystify the process and shed light on how such a huge volume (about 40% of ad impressions annually) are considered fraudulent.

The digital ad supply chain, based on the Interactive Advertising Bureau's *The Programmatic Supply Chain*



STEP 1 User visits publisher website

STEP 2 Publisher ad server is called to deliver an advertisement

STEP 3 DSPs evaluate SSP bid request and submit responses

STEP 4 Highest bidding DSP wins the ad impression, calls advertiser ad server

STEP 5 Advertiser ad server delivers ad

STEP 6 DMP collects data about ad delivery

DSPs:
"Who is this?"
"Is this in view?"
"Brand safe?"
"Not fraudulent?"
"Do I want to bid?"
"If so, how much?"

DMP Data Collection
Akamai: Visited dog related content in the past 24 hours
Lotame: Female, 35–54
Bluekai: Telcom intender
eXelate: Online shopper
Frequency: 3x
Path to conversion: video, search, display

As you can see, your media budget flows through a variety of different supply vendors and take many different paths to reach your target audience. Unfortunately, this complexity also creates multiple vulnerabilities and hiding spots where fraudsters can insert themselves into the supply chain. Given how convoluted (and profitable) the digital ad supply chain is, it's no wonder that it is an easy target.

Ad fraudsters have many tricks up their sleeves. Some specific tactics include:

- Publishers using bots to inflate user visits and sell the ad impressions they generate
- Compromising users' devices by injecting malware that generates fake ad impressions and clicks
- Misrepresenting domains to disguise the true source of the ad impression at Step 3
- Using bots to collect desirable cookies, passing themselves off as authentic human users and attracting higher CPMs in the bidding stage
- Hijacking click-throughs to steal credit for driving affiliate referrals
- Conversion-spoofing to gain credit for events that never happened
- Lat/long-spoofing to attract the higher CPMs paid to reach users in specific locations

Across the ad ecosystem, fraudsters' current tactics are continually evolving. They now have been shown to use techniques associated with large, organized crime syndicates, as well as calculated and prolonged attack techniques like those of Advanced Persistent Threat (APT) groups.

It is clear that the digital ad fraud problem is a cybersecurity problem.

A snapshot of adversarial techniques found in ad fraud analysis shows the cybercrime tactics now at play in the underworld of digital advertising:

Advanced phishing

Sophisticated attacks customized to a particular person or business, unlike large scale email campaigns

Command & control

A remote computer controlled by a cybercriminal sending data-stealing commands to compromised machines via malware

Domain generation algorithms

Domains fabricated to be used as communication nodes with a command and control server, hidden within the digital supply chain

Sites with extreme rate traffic

A seemingly safe domain covertly moving large amounts of data, such as personally identifiable information (PII) of customers

Complex and suspicious traffic patterns

Using calculated and prolonged attack techniques, consistent with large, organized, and well-funded adversaries

The criminals perpetrating the fraud are using advanced techniques to do more than generate fake ad impressions. So while protecting the brand should remain a top reason to take on digital ad fraud, it's imperative to address fraud directly as a cybersecurity concern.

Fighting digital ad fraud head on

Because such huge brand risk remains as hackers go after weak links, it makes sense to turn to cybersecurity experts, with an established track record of identifying and mitigating their customers' exposure to other forms of digital threats.Most organizations already make significant investments in cybersecurity to protect their critical digital assets and back-end infrastructure. Now front-end, marketing efforts need the same attention. And since cybersecurity experts have no vested digital supply chain interests, they can provide impartial insight into the level and types of fraud affecting digital ad campaigns. As a cybersecurity company that uses behavioral analytics to detect the type of sophisticated techniques the fraudsters are now using, IronNet views potential threats to ad budgets through a different lens. In response to the clear similarities between cyber attacks and ad fraud, IronNet looks for cyber invalid traffic (CIVT), going deeper than traditional general invalid traffic (GIVT) and sophisticated invalid traffic (SIVT) to detect more fraud. IronNet's unique vantage point into attacks on financial, healthcare, energy, and government networks has enriched its detection analytics above those used to find typical ad fraud. Accordingly, IronNet's CIVT detections allow brand stakeholders to see the bigger picture.

For example, in one global customer environment, IronNet detections found:

- Proof that 13% of existing traffic volume was invalid: 6x more than previously believed present
- Discovery that nearly half of that fraudulent traffic (6%) was hostile: that is, it originated from a nation state or sophisticated criminal actors specifically targeting the customer's ad spend

6x more
fraud found
with CIVT tool

FIND MORE DIGITAL AD FRAUD.

As the only CIVT detection platform on the market, IronNet's Digital Detect was built by cybersecurity experts who have spent years studying malicious traffic that targets high risk entities such as political bodies, intellectual property, financial enterprises, and personal information databases. It's time for a better way to protect your customers and maximize your digital efforts, effectively.

Find fraud more quickly — and more accurately — to protect your ad spend, campaign impact, and brand reputation.

IronNet™