Ad Fraud = Money Down the Drain

What buyers of media need to know about ad fraud, why it occurs and how to mitigate its risks.
The pervasive and egregious nature of ad fraud has been receiving significant attention of late. How did it become such a substantial issue?

Programmatic workflow is fueling the ad fraud fire.

Ad fraud has been an issue since the commercialization of advertising on the web in the 1990s. However, dramatic growth in programmatic workflow processes has added significant fuel to the ad fraud fire. Programmatic buying, which has grown by over 350% in the past two years, has introduced considerable efficiencies and scalability to the digital media purchasing process. Advertisers now have access to a multitude of media sources and to robust targeting with 3rd party data and contextual vendors, allowing them to find their audiences throughout the web – at scale and with cost efficiencies. These features, combined with ease of access and promise of performance, have helped drive double-digit growth rates; the Internet Advertising Bureau (IAB) estimated that 52% of display advertising was transacted programmatically in 2014. However, along with the benefits of programmatic buying also came the issues of loss of insight into traffic sources, concerns about publisher quality, and issues related to brand safety – all of which were previously kept in check via premium purchasing relationships.

Fraudsters are hijacking your advertising budget!

Loss of insight into traffic sources, mainly due to obfuscated or highly generalized publisher names (e.g. “News and Entertainment site” instead of “Huffington Post”) on RTB exchange bid requests, has quite literally swung the door wide open to ad fraud and malware. Ad fraud – specifically referring to non-human traffic (bot traffic), low quality traffic (generally individuals who are compensated for repeatedly clicking on links) and malicious URLs – introduces bottom line impacts to marketing’s #1 success metric ROI. Simply put, fraudsters – who, by the way, are not clever, rebellious teenage hackers in their parents’ basement, but rather organized criminal networks – are defrauding marketers. In essence, fraudsters are hijacking your advertising budget. When an advertising opportunity is purchased that turns out to be fraudulent, those brands and their advertising agencies are investing marketing dollars on campaigns that will NEVER reach the intended audience. Ad fraud is truly introducing risk to the sustainable growth of digital advertising.

Ad fraud cost is estimated at over $6 billion in 2015.

Clearly ad fraud is a very big issue for marketers - eroding campaign performance by impacting ROI and ROAS, reducing trust, exposing consumer audiences and brands to fraudulent activities, and enabling criminals. Ad fraud is conservatively estimated at over $6B2 in 2015 with non-human traffic representing up to 50% of page views. Regardless of the exact numbers, ad fraud is clearly impacting marketing investment results.
All in the Family - Ad Fraud and its Cousin, Malware

To better understand the roots of ad fraud, let’s go back to the origins of revenue-driven malware (malicious software). Ad fraud certainly existed before programmatic ad tech platforms were utilized. In fact, affiliate advertising and click fraud were early and easy targets for ill-gotten gains. When the money making power of the web was in its infancy, fraud and malware players were generally amateurs. However, as consumer adoption of the internet grew and the commercial power of the web became apparent, organized crime networks saw the potential to generate revenue. These criminal networks then employed sophisticated programmers who generated complex and often difficult to detect malware, spam and phishing exploits.

Spam was the first real monetization of the bots.

Ad fraud methodology actually originated in spam. Malware writers used various tactics to infect the computers of end users including viruses, Trojans (malware that misrepresents itself as useful), drive-by downloads, and infected websites.

How does this happen? At a high level, an infected web page will scan the visitor’s browser or system for vulnerabilities and once it finds one, it uses technology to place malware onto the visitor’s computer.

Once installed, the malware can steal sensitive personal information and/or make the consumer’s computer part of a botnet, which from a “crowdsourced” perspective can have the processing power of supercomputers. A botnet is simply a network of computers that have been infected with malicious exploits which allows them to be controlled remotely - a “robot network.”

Wonder how ad fraud monetization happens?

While there are a multitude of methods, here are a few fraudster favorites:

- **Spam**: Advertiser pays the fraudster for delivery of the spam.
- **Traffic**: The publisher pays the fraudster for the delivery of traffic to the site.
- **Pirate Site Generation**: Advertiser pays for displaying ads on fake sites which are visited by bots.
- **Conversions**: Advertiser pays for fake clicks and/or conversions on PPC or CPC campaigns.
Interestingly, most of the time the end user is completely unaware that their machine has been compromised or that it has become part of a botnet. An infected botnet computer can be used by the consumer while simultaneously making undetected outbound web calls for criminal gain. Computers can become infected if software – including browsers, operating systems, multimedia tools, and anti-virus solutions – are not kept up-to-date; or if the user downloads software without being certain of the software provider. Botnet computers are “managed” by criminals that are referred to as “command and control operators”, orchestrating and allocating computers in the botnet for various criminal purposes. The scope of botnet usage can include not only ad fraud, but also spam, identity theft, Distributed Denial of Service (DDOS) attack which involves flooding the bandwidth or resources of a target system to compromise cyber security and allow access, malware distribution points for ad fraud, or more. In fact, ad fraud is a gateway for your consumer audience to become implicit contributors to this epidemic.

Money has been pouring into digital advertising with global digital ad spend expected to grow to $250B by 2018\(^3\). Crime follows money and opportunity. For the fraudsters, this has meant unprecedented opportunities for unprecedented wealth. In the network security industry, solutions were created to block malware and spam. These were successful for a while. Then the malware writers changed their tactics. New solutions were developed by the security industry, and for a time they held their own. Then again, the fraudsters changed their tactics. The foe that the ad tech industry is up against is clever, relentless, and knows technology.

As long as there is money to be siphoned, there will be criminals trying to get as much of it as they can.
Every day, zvelo technology enables clients to block hundreds of millions of pages containing malicious content.

30% website traffic can be impersonators or hacking tools.

In fact, research by zvelo shows that upwards of 15% of all URLs in the active web contain malicious or objectionable content. Bad bots such as impersonators and hacking tools make up around 30% of total website traffic.

Understanding ad fraud is just the beginning of learning how to protect your brand or client against it.

Are you evaluating an anti-fraud solution? If so, insist on understanding how they propose to prevent ad fraud.

Here are some data points to consider as you evaluate ad fraud solutions:

- What different fraud methodologies does the solution utilize?
- How does the vendor stay on top of ever-changing tactics?
- Does the provider have a threat Lab? Are cyber security, as well as ad tech experts, on staff?
- Does their expertise include dynamic malicious detection and ad fraud prevention?

zveloSHIELD™ Ad Fraud Prevention & Botnet Detection is a real-time dual decisioning pre-bid solution that looks at both IPs (traffic) and URLs to determine if an impression opportunity is from a known botnet or whether the URL is fraudulent, malicious, or dangerous.

zveloSHIELD™ also includes flexible, transparent campaign level reporting.
As the proven market leader for content and contextual categorization, as well as malicious and botnet detection, zvelo is the trusted partner of choice for the market's preeminent ad tech, cyber security, mobile service providers and subscriber analytics vendors. zvelo solves a diverse range of client business needs including: brand safety, web filtering, contextual targeting, subscriber analytics and ad fraud prevention.

zvelo delivers best-in-class categorization and malicious detection accuracy, coverage, language speed and responsiveness by combining artificial intelligence and human-supervised machine learning. zvelo customers, who represent over 500 million end users, benefit from 99.9% coverage of the active web, 489 categories of granularity, and support for over 200 languages. The processing power, reach and speed of zvelo technology delivers the fastest real-time updates available today.

Beyond the technology, innovation and datasets, zvelo is committed to their customers as partners. The zvelo team settles for nothing less than the best, with a company-wide commitment to responsiveness. zvelo is headquartered in Denver, Colorado with offices in the Philippines, New York, Spain, Florida and Michigan.

zvelo - your trusted partner, making the web safer, relevant and more profitable.

Learn more at: www.zvelo.com

Sources:

1. http://www.iab.net/media/file/PwC_IAB_Programmatic_Study.pdf
2. http://www.ana.net/content/show/id/botfraud