DEV/CON

AD FRAUD

State of the Industry 2017

Maggie Louie, CEO DEV/CON DETECT

AD FRAUD

State of the Industry 2017

Maggie Louie, CEO DEV/CON DETECT

- How much is being lost?
- Loses by category
- Common Symptoms
- Glossary of ad fraud
- Peer-to-peer discussion
- What is the industry doing?
- What can I do?

DEV/CON

How Much Is Being Lost?

$8B

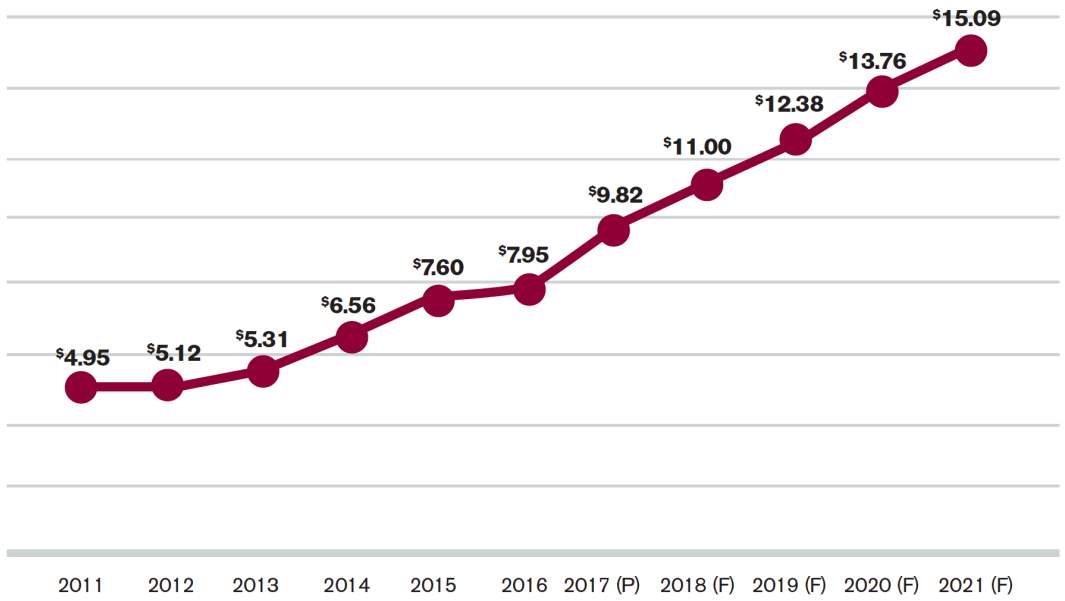
Ad tech fraud is rampant in the digital publishing world, costing over 8 billion in annual losses.

Source: 2016, ANA

DEV/CON

How Much Is Being Lost?

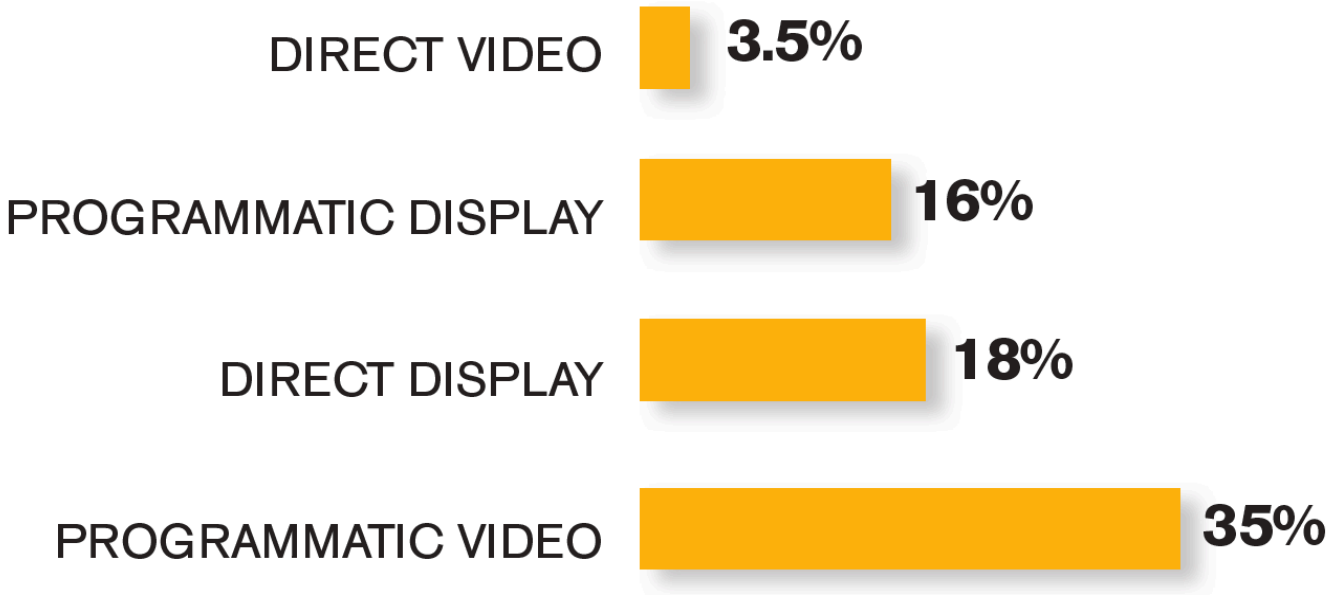
FIGURE 6: **ESTIMATED/FORECAST TOTAL U.S. DIGITAL AD FRAUD**
IN $ BILLIONS, 2011-2021
Source: Borrell; 2017.



Losses By Category

FIGURE 2: **MEDIAN BOT SERVED TRAFFIC PERCENTAGE**
BY TYPE OF DIGITAL AD TRANSACTION

Sources: White Ops, Borrell; 2017.



Common Symptoms

- Serving blanks in many positions
- Spammy ads popping up on desktop and mobile
- Reports from publisher ad server vary by as much as 20% from network reports
- Slow page load
- Numerous errors related to ad calls
- Slow lulling of publisher revenue month over month

DEV/CON

Glossary of Ad Fraud

- AD INJECTION
- AD STACKING
- AFFILIATE AD FRAUD
- BOTS/AD BOTS
- CMS FRAUD
- DOMAIN SPOOFING
- FAKE PAID TRAFFIC
- A FAKE/GHOST SITES AD STACKING
- HIDDEN IMPRESSIONS BOTS/AD BOTS
- HIDDEN VIDEO DOMAIN SPOOFING
- LEAD AD FRAUD
- PIXEL STUFFING
- RETARGETING MIMICS
- SCRIPT KIDDIE
- SEARCH AD FRAUD
- SITE BUNDLING
- TAG HIJACKING

DEV/CON

Glossary of Ad Fraud

AD INJECTION. Consumers are offered a free incentive – often a web browser tool bar or extension. A covert part of the incentive injects ads that deliver no revenue to the publisher's site, only to the incentive creator. The ANA/WhiteOps study counted 50,000 injected ads during every day of their two-month study.

AD STACKING. The process of placing multiple ads on the top of each other in a single ad slot. With ad stacking, only the ad on the top is viewable. Another ad stacking practice is to place two or more ads immediately next to each other with no content between them.

AFFILIATE AD FRAUD (AKA COOKIE STUFFING). Bots manufacture fake cookies to stuff a consumer computer. When that consumer calls up an affiliate site, the criminal collects the commission payment.

BOTS/AD BOTS. Bots are specific software applications. They typically run scripts (or automated tasks) in a repetitive fashion. In the realm of ad fraud, they are usually malicious bots that can perform any number of fraudulent behaviors. These could include unleashing viruses/worms, scraping websites for content and re-distribution, harvesting emails, generating views, etc.

CMS FRAUD. Bots hack a publisher's CMS (content management system) and add their own pages to a legitimate domain. These fake pages are placed on ad exchanges, but the criminal receives payment instead of the publisher.

Glossary of Ad Fraud

DOMAIN SPOOFING. Criminals change the URL of sites, to make advertisers believe these fake sites are legitimate publishers. This camouflage lures advertisers to pay for placements on them.

FAKE PAID TRAFFIC. Many publishers buy digital traffic from third parties to generate additional unique visitors. The ANA/WhiteOps study found that more than half of this purchased traffic is bot-generated.

FAKE/GHOST SITES. Some of these websites contain only ad slots, while others contain only generic content which is often duplicated from one page to the next. In order to avoid suspicion, a single ghost site may draw only a few impressions a day. However, since they act as networks, the net number of fraudulent impressions offered can be massive.

HIDDEN IMPRESSIONS. Also called “ad stuffing,” is the placement of ads in invisible 1X1 pixel spaces throughout a bot-infected website. It can also be the stacking of several ads on the same site so that only the top one is visible. An investigation by Advertising Age uncovered one site that offered 30 million impressions per day on a single exchange.

HIDDEN VIDEO. The growing use of video advertising online has brought with it ingenious application of hidden impressions specific to it. Most commonly “stacked,” these frauds are much more lucrative than that perpetrated on other digital ads, because of the higher CMP’s offered

Glossary of Ad Fraud

LEAD AD FRAUD (AKA CONVERSION FRAUD). This began as a cottage industry, where criminals employed cheap foreign labor to fill out forms. Now totally automated, bots can produce thousands of lead forms per minute and totally overpower most publisher anti-fraud systems.

PIXEL STUFFING. The process of serving one or multiple ads in a single 1X1 pixel frame. Pixel stuffing is typical kind of ad fraud as served ads are invisible to the naked eye. Pixel stuffing is often done through a 1x1 pixel frame at the bottom of a page.

RETARGETING MIMICS. Bots can be programmed to impersonate highly sought customer behavior – like home or car purchase activity. When the mimic bot goes to websites and behaves like an interested consumer, an avalanche of retargeted ads will be directed at this “hot prospect.” The ad targeting company can make money from this useless ad traffic.

DEV/CON

Glossary of Ad Fraud

SCRIPT KIDDIE. Fairly unskilled criminals who use scripts and programs developed by other people to attach and exploits sites and computers. Also known as Skid, Skiddie, Script Bunny and Script Kitty.

SEARCH AD FRAUD. Criminals build ghost websites loaded with high value keywords. Advertisers buy inventory on these sites. When bots click on these ads, the advertiser gets a report that shows the activity as legitimate.

SITE BUNDLING. When publishers and exchanges bundle entire networks of domains under single site IDs. So an advertiser might think they are buying abc.com but end up with ads served on xyz.com. Happens mainly on the supply side.

TAG HIJACKING. Publisher's tags are hijacked by a skid aka script kitty/skiddie who deploys exploits via plugins and code injections through various site vulnerabilities.
As the volume and complexity of digital marketing grows, no doubt this list will lengthen.

What Is The Industry Doing?

- **IAB**: Ads.txt – initiative to create transparency for the ad buyer
- **LMC:** Created Ad Quality Committee to identify leading companies addressing the publisher-side issues
- **Mather Economics:** Listener, benchmarking industry ad performance
- **DEV/CON:** Tags.id, indexing & mapping bad actor tags

DEV/CON

What Can I Do?

- **Audit Tags**: Daily or weekly auditing of the tags that are appearing on your site
- **Traffic Validation:** Daily or weekly auditing of non-human traffic on your site
- **Cookie Audit:** Regular auditing of cookies your site and ads are dropping
- **Revenue:** Daily or weekly reconcile of server reported revenue and network actual revenue

Q&A

Maggie Louie
mlouie@devcondetect.com

Jay Horton
jhorton@devcondetect.com

What We Do

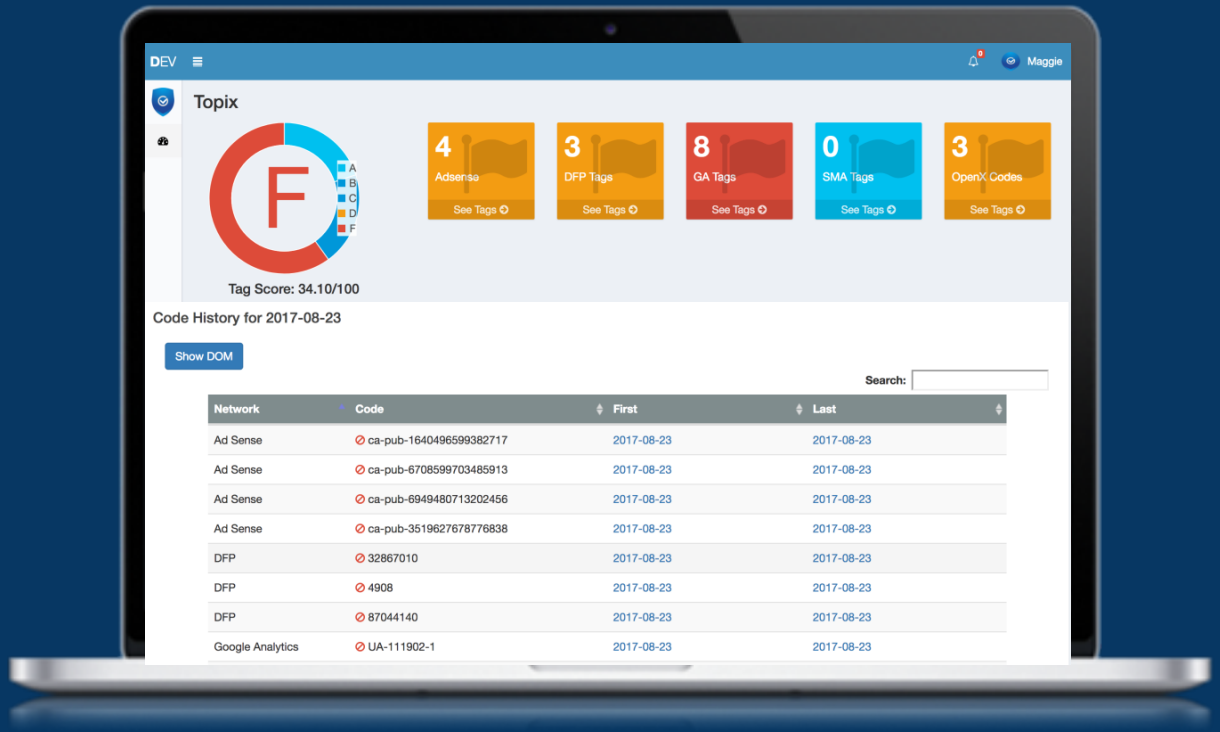
SECURITY SCAN

FORENSIC HEATMAP

YEILD DASHBOARD

DEV/CON

Security Scan



Yield Dashboard

View ad server numbers compared to your network numbers

Tracks variance and sends alerts according to your setting

Easily add any network of your choice

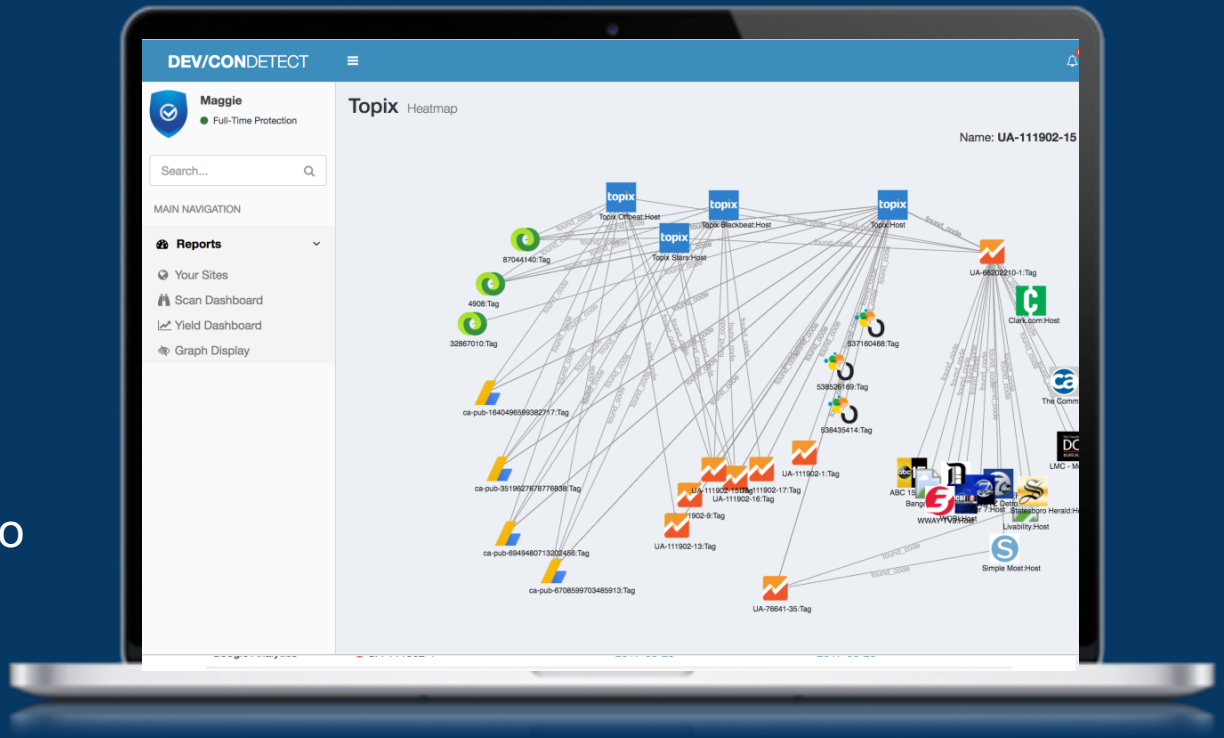
Heat Map

FORENSIC HEATMAP

View your tags and other sites using your tags

Connected relationships make tags easy to manage

Graph views make it easy to trace origins of all tags



Fully integrated with most major ad servers, ad networks and CMS platforms

amazon

Drupal™

Google AdSense

OpenX®

DoubleClick for Publishers

Joomla!™

centro®

smart AD SERVER

Our Suite of Services

DETECT

Ad Network Analysis

Ad Tech Recommendations

Ad Tech Consulting

PROTECT

Situation Management

Safe Exploit Removal

Revenue Reporting

DETECT + PROTECT

Code Monitoring

Revenue Security

Revenue Optimization

We are creating a massive database of known partner tags, server tags, network tags, analytics tags and monitoring the sites they are being used on.

Pricing Table

SELF-SERVE

Scan

10 Security Scans per month

LImited Dashboard

Limited Risk Heat Map

$399/month

PRO-PLAN

Publisher

Daily Security Scan

Risk Monitoring

Full Dashboard

Yield Dashboard
(Network Limit: 5)

Risk Heat Map

$2,000/month

ELITE

Enterprise

10 Site Minimum

Daily Security Scan

Risk Monitoring

Full Dashboard

Yield Dashboard
(Network Limit: 30)

Risk Heat Map

$1,700/month

DEV/CON