

The BuzzFeed News logo, featuring the words "BuzzFeed" and "News" in a sans-serif font, with a small orange dot above the "N" in "News".

BuzzFeed
News

Investigating Ad Fraud

Craig Silverman, BuzzFeed News | @CraigSilverman

REPORTING
TO YOU



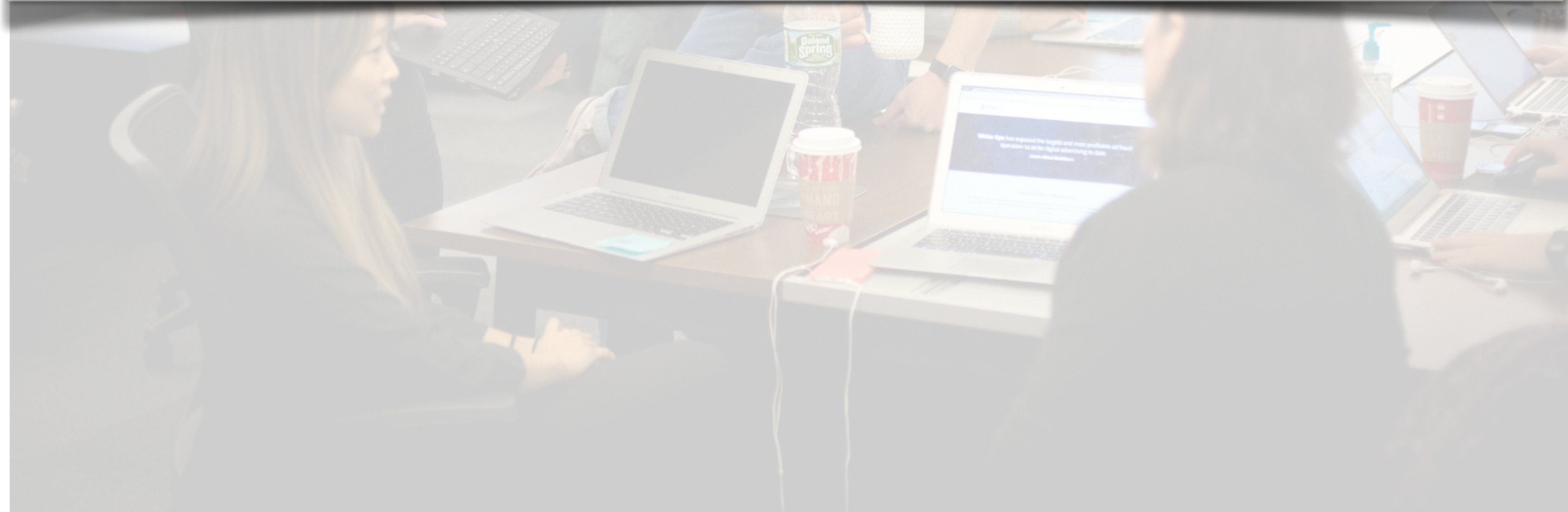
The New York Times

Russian Cyberforgers Steal Millions a Day With Fake Sites



Russian Cyberforgers Steal Millions a Day With Fake Sites

White Ops said the thieves received high prices for the fake ad views, garnering an average price of \$13 per 1,000 video views. Over all, the botnet delivered 200 million to 300 million fake ad views per day and brought in \$3 million to \$5 million in daily revenue, according to the company's analysis.



\$20 Billion in 2019



What I've Been Up To

- Almost two years, more than a dozen stories
- More than \$10 million credited back to advertisers
- Dozens of apps and websites removed from the Google Play store or taken down
- One publisher under investigation by the Manhattan District Attorney in New York
- Two letters sent to the Federal Trade Commission by a US Senator
- **Too many lies told by publishers, ad tech companies, brands and others to count**

A Bunch Of Digital Publishers Bought Cheap Traffic And Later Found Out It Was Fraudulent

Ad Industry Insiders Profited From An Ad Fraud Scheme That Researchers Say Stole Millions Of Dollars

The Publisher of Newsweek And The International Business Times Has Been Buying Traffic And Engaging In Ad Fraud

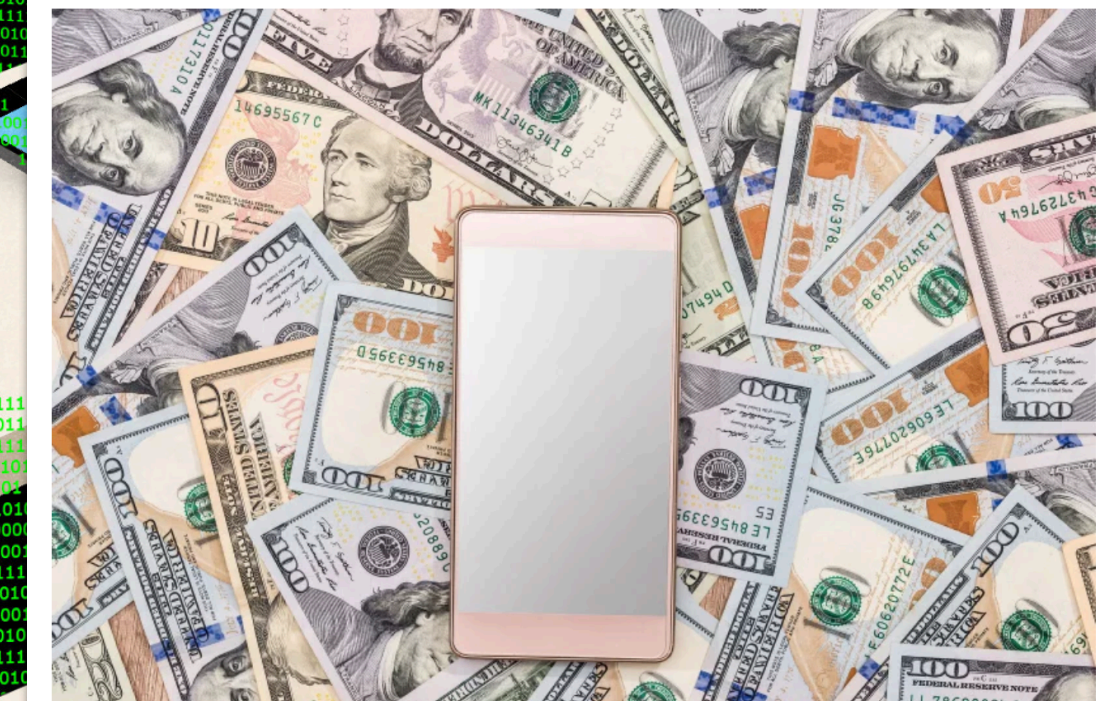
This Ad Fraud Scheme Stole Millions, But Almost No One Wants To Own Up To It

"Nobody knows how bad it is and nobody wants to know," said one critic of the ad industry.

Craig Silverman
BuzzFeed News Reporter

Posted on October 31, 2018, at 2:19 p.m. ET

[Tweet](#) [Share](#) [Copy](#)



Siphotography | Getty Images

Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme

A BuzzFeed News investigation uncovered a sophisticated ad fraud scheme involving apps and websites, some of which were targeted at kids.

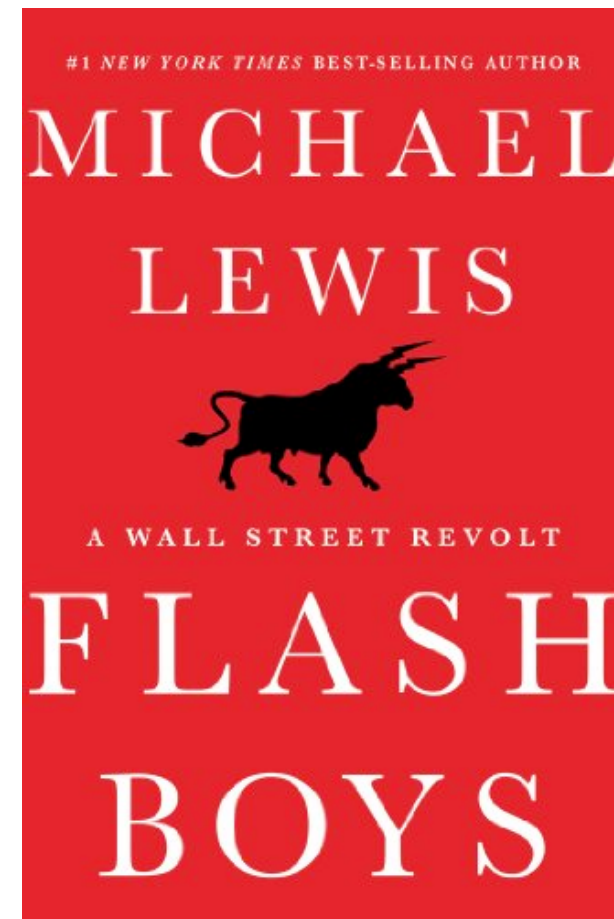
Craig Silverman
BuzzFeed News Reporter

This Is How Visiting A Porn Site Can Make You A Pawn In An Ad Fraud Scheme

This Giant Ad Fraud Scheme Drained Users' Batteries And Data By Running Hidden Video Ads In Android Apps

Contact me securely: tips.buzzfeed.com or +1-647-949-7610

“The deep problem with the system was a kind of moral inertia. So long as it served the narrow self-interests of everyone inside it, no one on the inside would ever seek to change it, no matter how corrupt or sinister it became.”



“The deep problem with the system was a kind of moral inertia. So long as it served the narrow self-interests of everyone inside it, no one on the inside would ever seek to change it, no matter how corrupt or sinister it became.”

Three Stories About Insider Ad Fraud

Contact me securely: tips.buzzfeed.com or +1-647-949-7610

Zombie Websites

[Getty]



**“ZOMBIE WEBSITES”
HAVE POTENTIALLY STOLEN
MILLIONS FROM SOME OF THE
WORLD’S BIGGEST BRANDS**





KYLIE JENNER'S POST INSTAGRAM POSTS A FASCINATING SELECTION OF SHIRTS

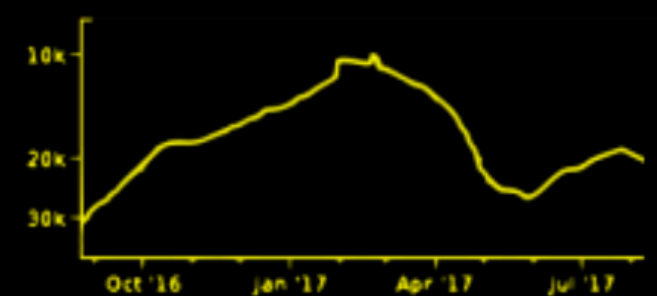
SARA BREWER • OCTOBER 10, 2017

CELEBRITIES FASHION 0 COMMENTS

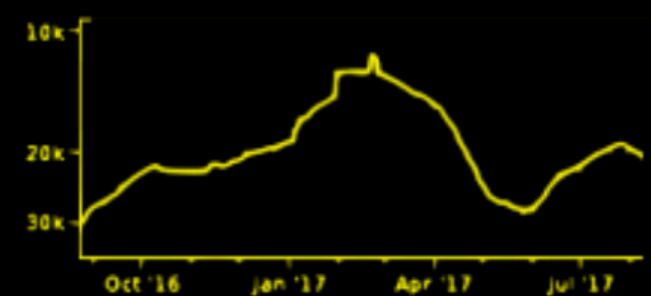
Don't assume rumored baby bump of Kylie Jenner anytime soon. In one of the first non-return photos she posted since her pregnancy was reported, she wears a loose shirt that leaves no trace of what she can keep underneath.

MONKEY FROG MEDIA

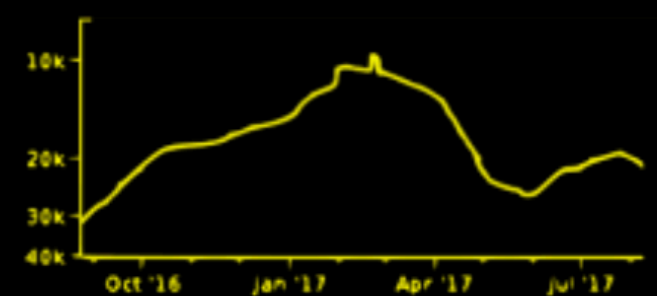
Trendyrecipe.com



Rightparent.com



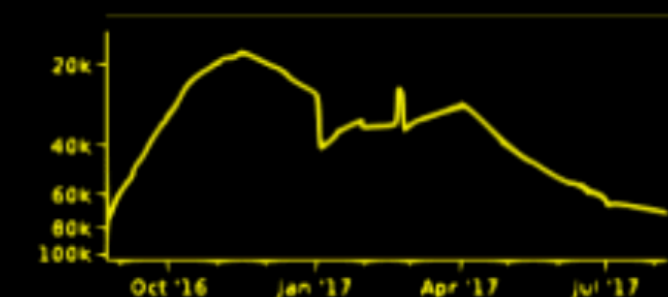
Momtaxi.com



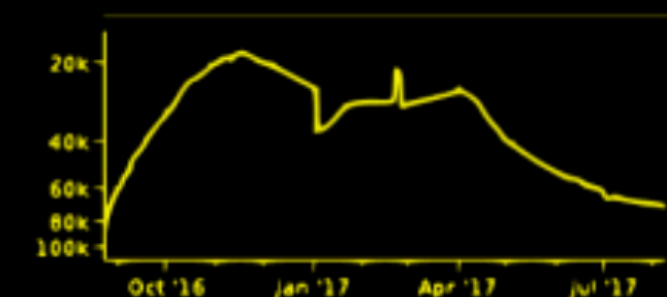
Social Puncher

ORANGE BOX MEDIA

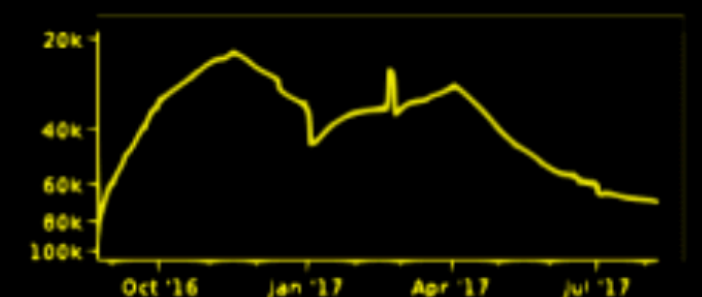
Smartergadget.com



Countnews.com



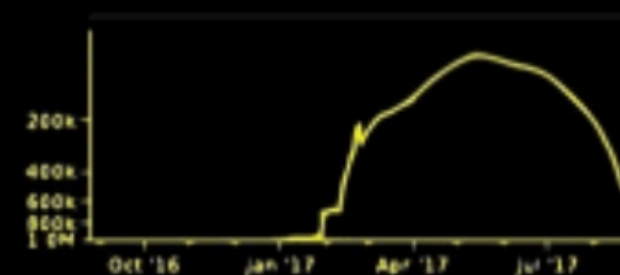
Scorebench.com



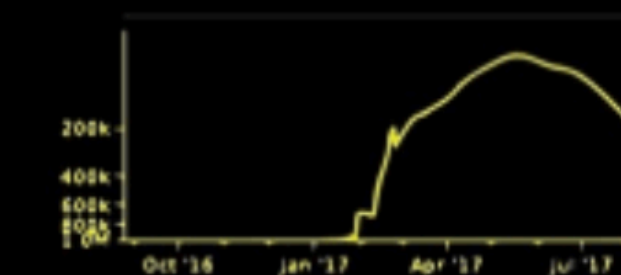
Social Puncher

KVD BRANDS

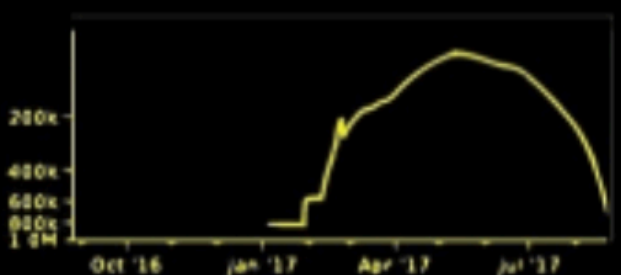
Hollywoodbug.com



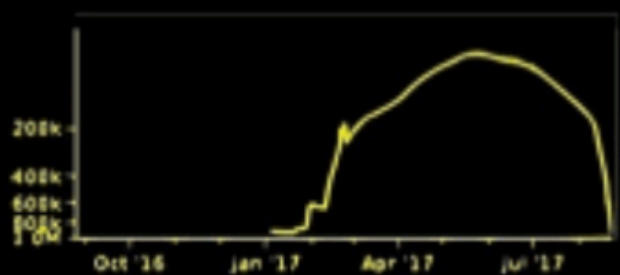
Upcomingbeauty.com



Beautytips.online

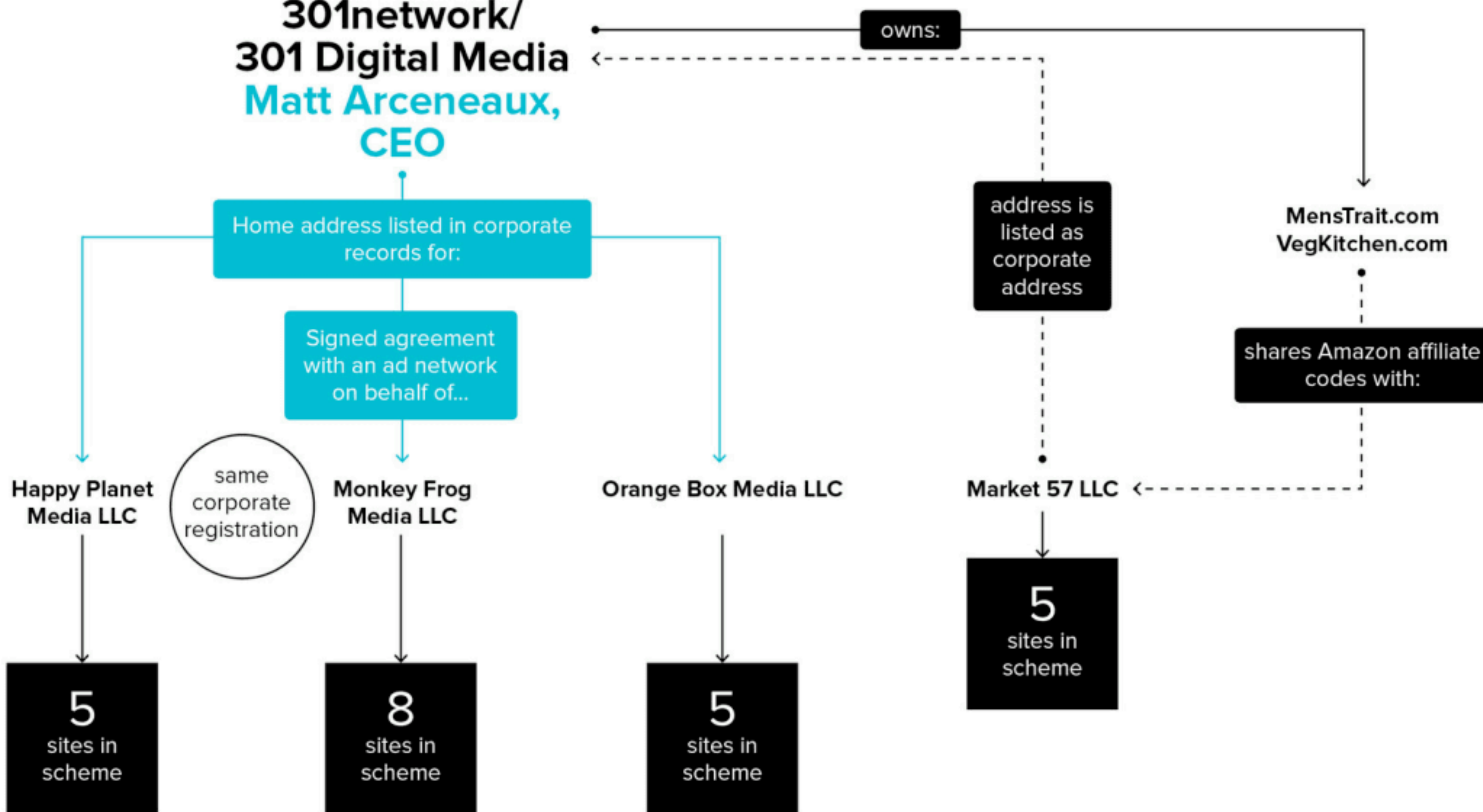


Recipegreen.com



Social Puncher

**301network/
301 Digital Media**
Matt Arceneaux,
CEO



100+ AFFECTED BRANDS

Lactaid

GOLD BOND
ULTIMATE

Aveeno
ACTIVE NATURALS

BEN & JERRY'S
CHOCOLATE

talenti.
glaze 3 varieties

Aria
RESORT & CASINO
LAS VEGAS

PELLAGIO
LAS VEGAS

MGM GRAND

Reese's

KitKat

JOLLY
rancher

ICE BREAKERS

Twix

m&m's

Dove

Milky Way

General
Mills
Morning Blend
Peanut Butter

Wendy's

Jimmy Dean

XYZAL
ALLERGY 24HR

ICYHOT

Nasacort
Allergy 24HR

Nexium
24HR

Allegra

Compound W
Antiseptic

Mucinex

Walt Disney World
Resort

Disney Cruise Line

Disney

GEICO

Prudential

Oppenheimer Funds

State Farm

citi

Lincoln
Financial Group

FARMERS
INSURANCE

PNC BANK

Liberty
Mutual

WELLS
FARGO

DISCOVER

Nationwide

Capital One

CHASE

NISSAN

Ford

TOYOTA

CHEVROLET

SUBARU

KIA

ACURA

Volkswagen

MASERATI

mazda

always
Gillette

ARIEL

Secret

Charmin

Febreze

Bounty

OLAY

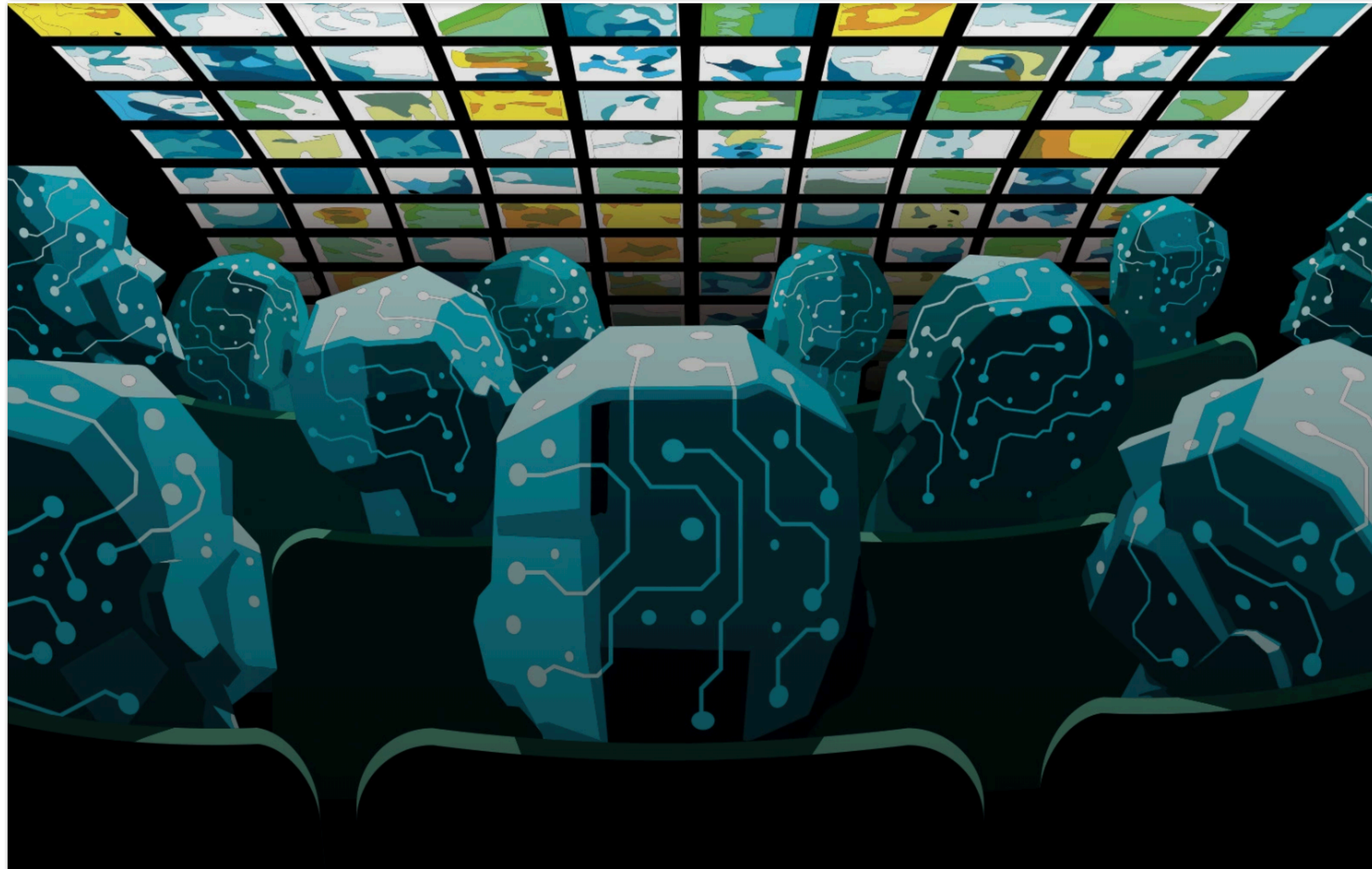
Oral-B

Luvs

BRAUN

Cascade
DISPOSABLE

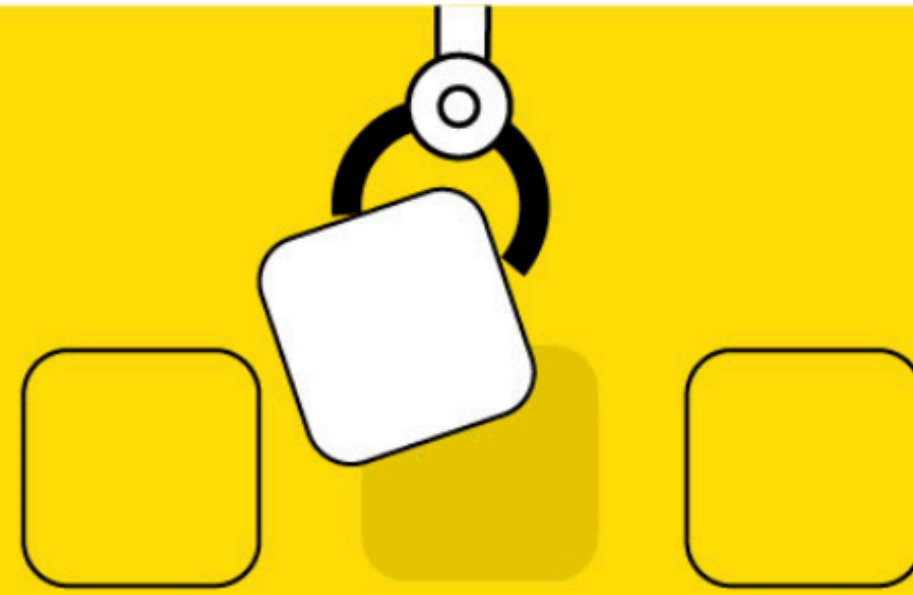
orgullosa



**Ad Industry Insiders Profited
From An Ad Fraud Scheme That
Researchers Say Stole Millions Of
Dollars**

Recorded Attack

How This App Fraud Scheme Works



Acquire an Android app that has real users, favorable reviews, and an overall positive reputation



Shift ownership to a shell company to obscure its true ownership and to hide its links to other apps in the scheme

Utilize developer access to the app to analyze the behavior of its existing human audience



Tarik Markow

Video Support Specialist



Dilan Pas

Executive Monetization Officer



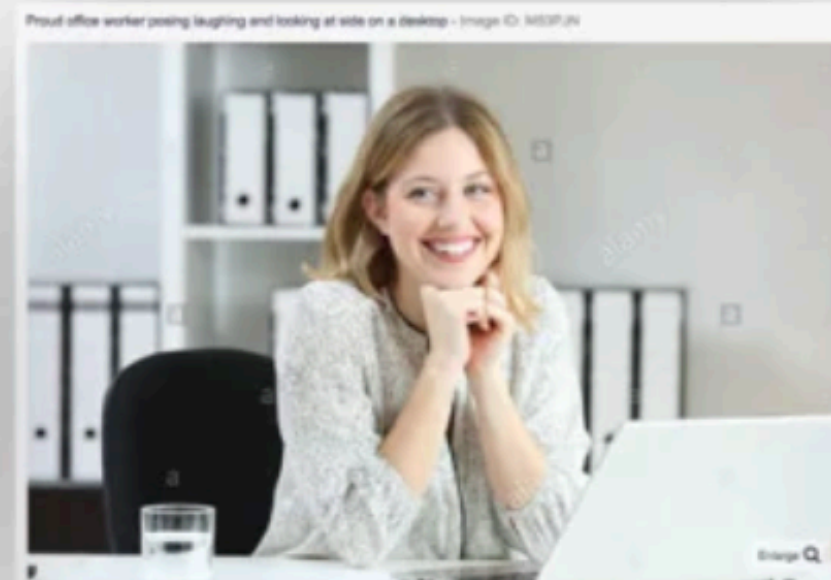
Iris Castello

Finance Officer



Natalia Bishop

Finance Assistant



Nika Kolar

Senior Key Account Manager



Martin Malek

Integration engineer



Julian Popovski

HR Manager



Maximilian Todorov

Recruiter



Sarah Hajek • 3rd

Account Manager at Quaret Digital

Cyprus

Message



Quaret LTD

European University Cyprus

See contact info

99 connections

If you need a publisher who creates and monetizes video portals , feel free to contact me

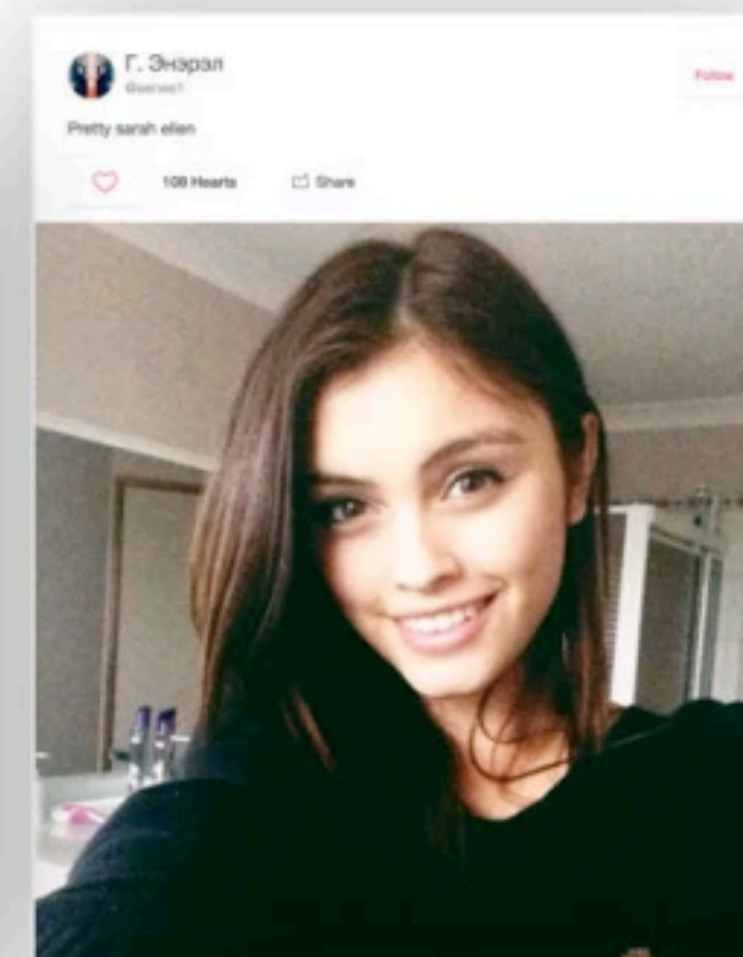
Experience

Account Manager

Quaret LTD

Jul 2017 – Present · 1 yr 4 mos

Serve as the lead point of contact for all customer account management matters
Build and maintain strong, long-lasting client relationships
Negotiate contracts and close agreements to maximize profits
Develop trusted advisor relationships with key accounts
Ensure the timely and successful delivery of our solutions
Clearly communicate the progress of monthly/quarterly initiatives
Develop new business with existing clients and/or identify areas of improvement



Client testimonials

What our partners think about our partnership



Gabriella Byrd

HEAD OF SALES

No Ad campaign - no sales. And in today mobile-first world there's no other way to reach target audience, but to get into their smartphones. And TapTapVideo is the best partner for this opportunity.



Kristi Grassi

@kristigrassi

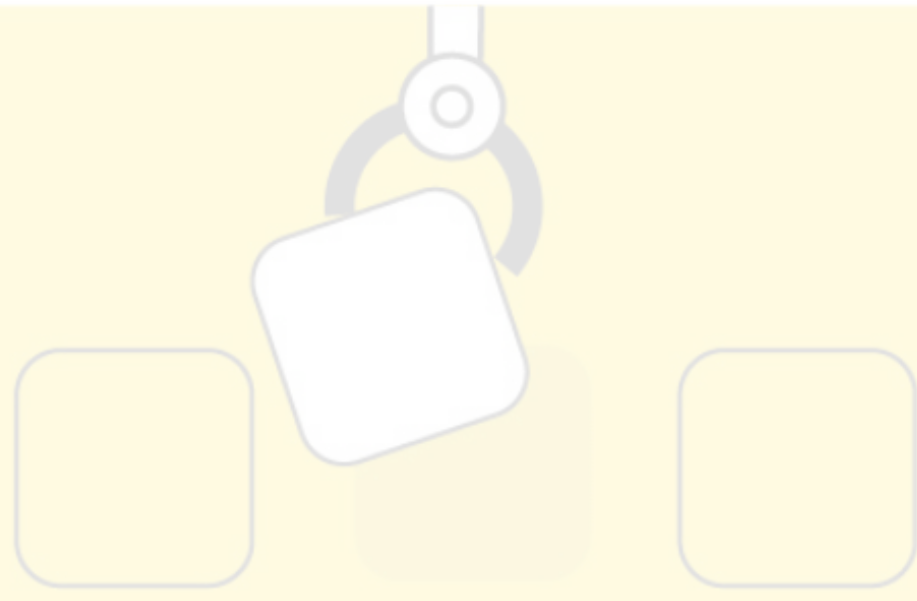
Product Design at Pivotal Labs

Los Angeles, California

kristigrassi.com

Joined January 2011

How This App Fraud Scheme Works

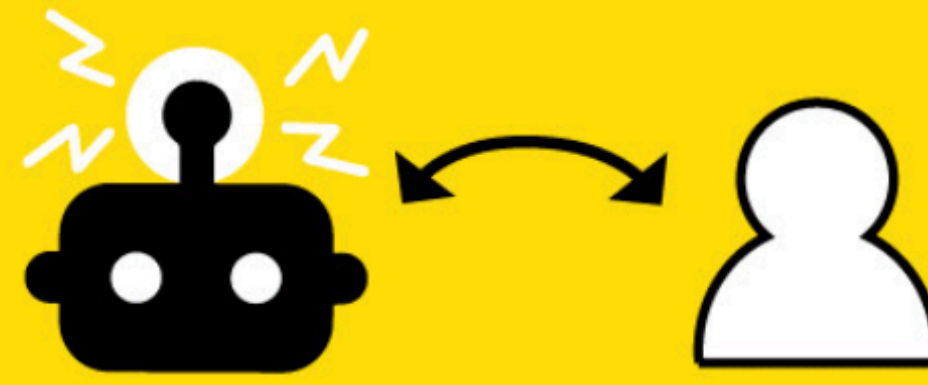


Acquire an Android app that has real users, favorable reviews, and an overall positive reputation

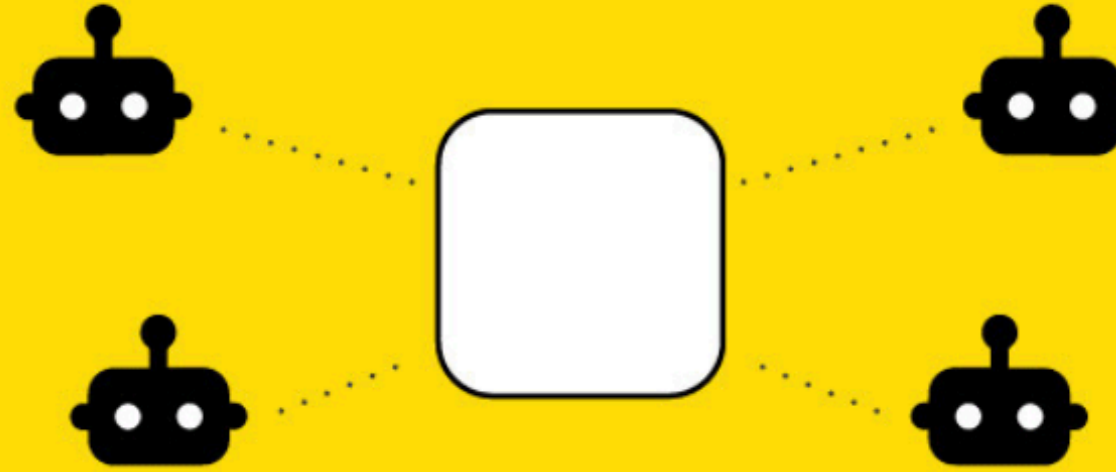


Shift ownership to a shell company to obscure its true ownership and to hide its links to other apps in the scheme

Utilize developer access to the app to analyze the behavior of its existing human audience



Program that behavior into bots running from dedicated servers so they can mimic the human audience

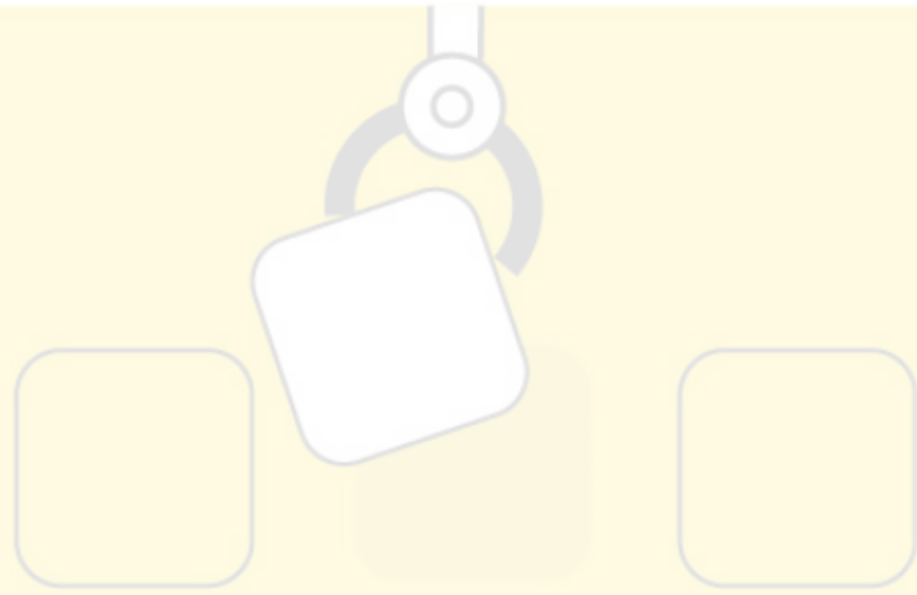


Direct bot traffic to the app



Blend bot traffic with existing human traffic to disguise it from fraud detection

How This App Fraud Scheme Works

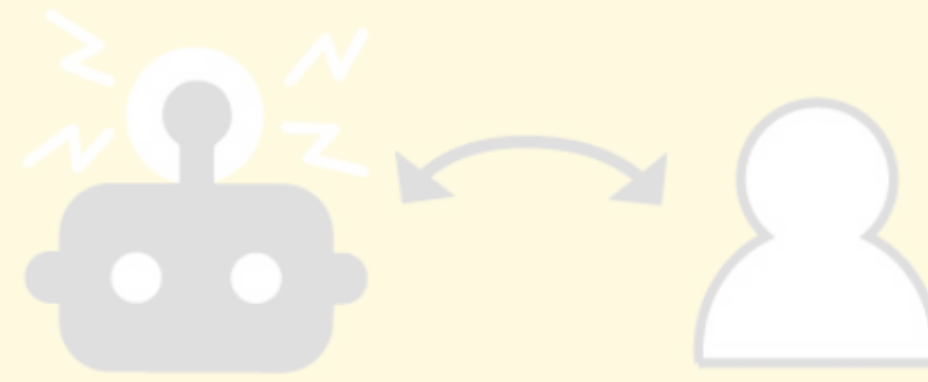


Acquire an Android app that has real users, favorable reviews, and an overall positive reputation



Shift ownership to a shell company to obscure its true ownership and to hide its links to other apps in the scheme

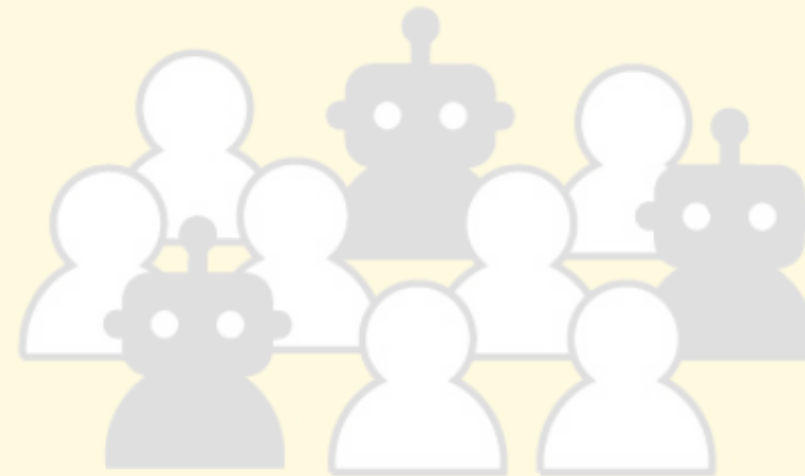
Utilize developer access to the app to analyze the behavior of its existing human audience



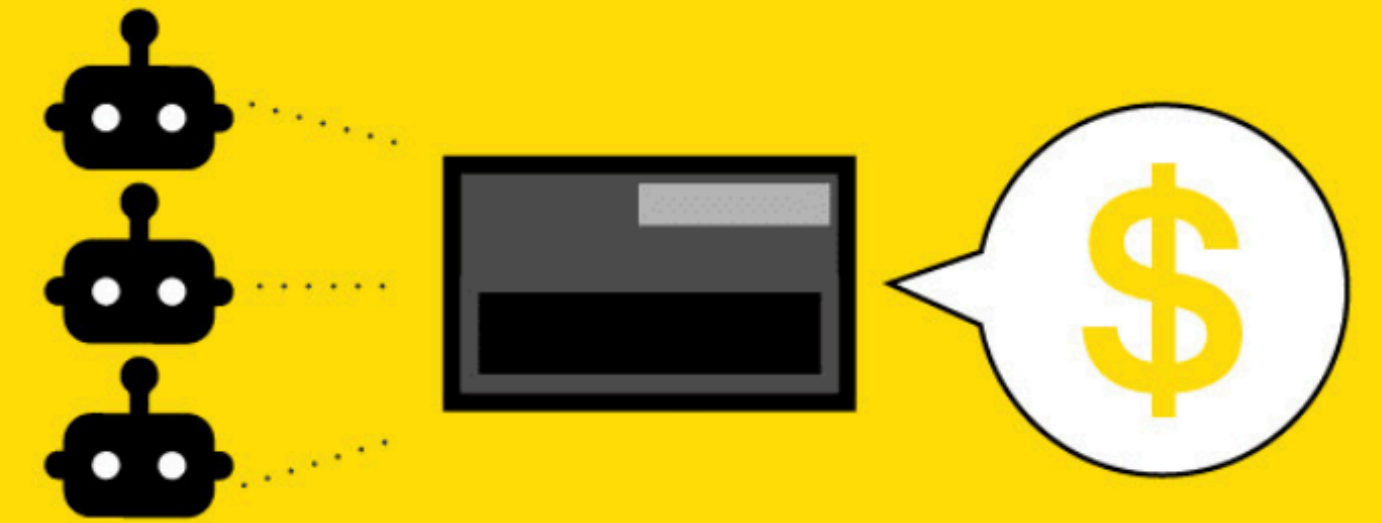
Program that behavior into bots running from dedicated servers so they can mimic the human audience



Direct bot traffic to the app



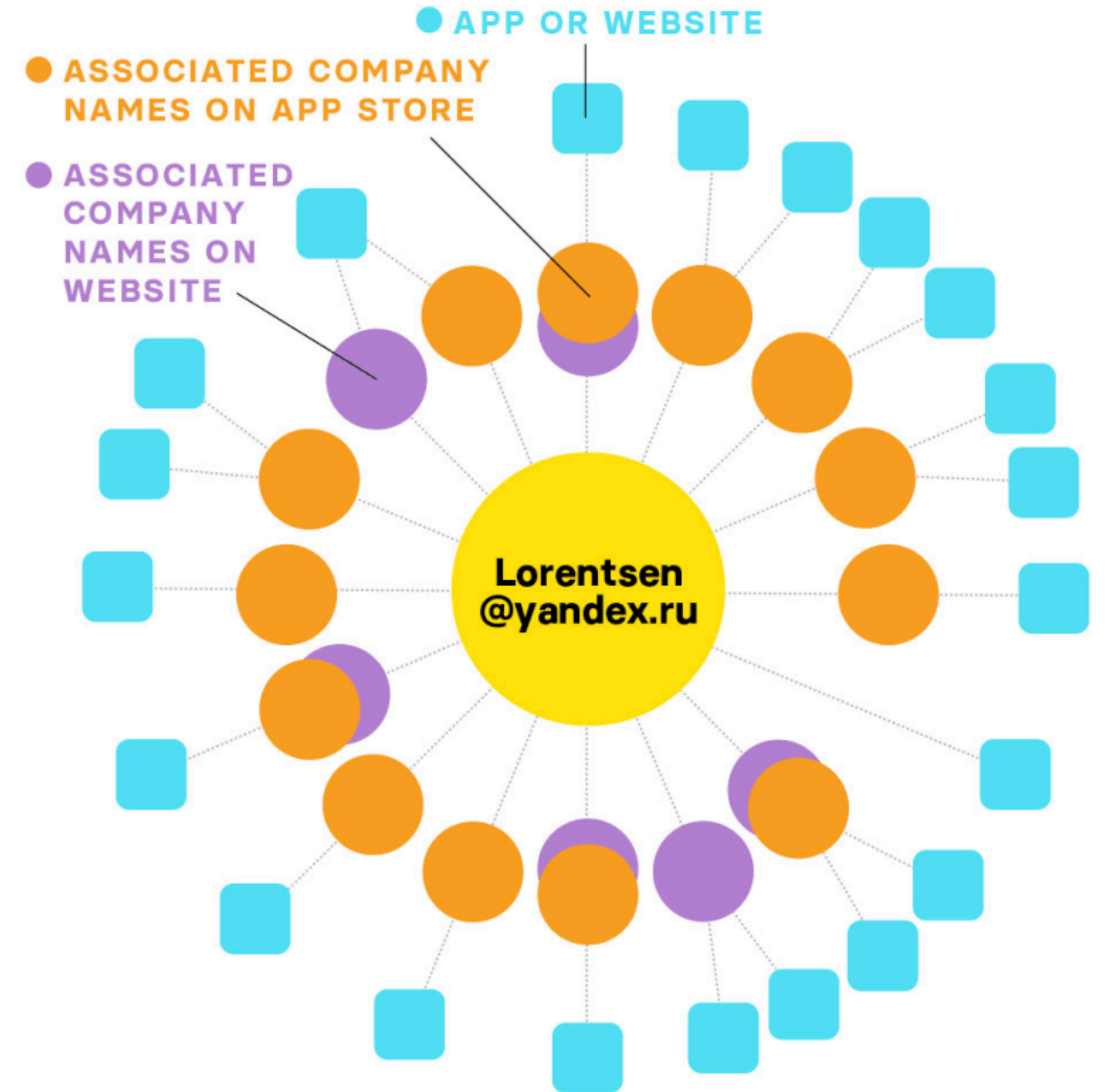
Blend bot traffic with existing human traffic to disguise it from fraud detection

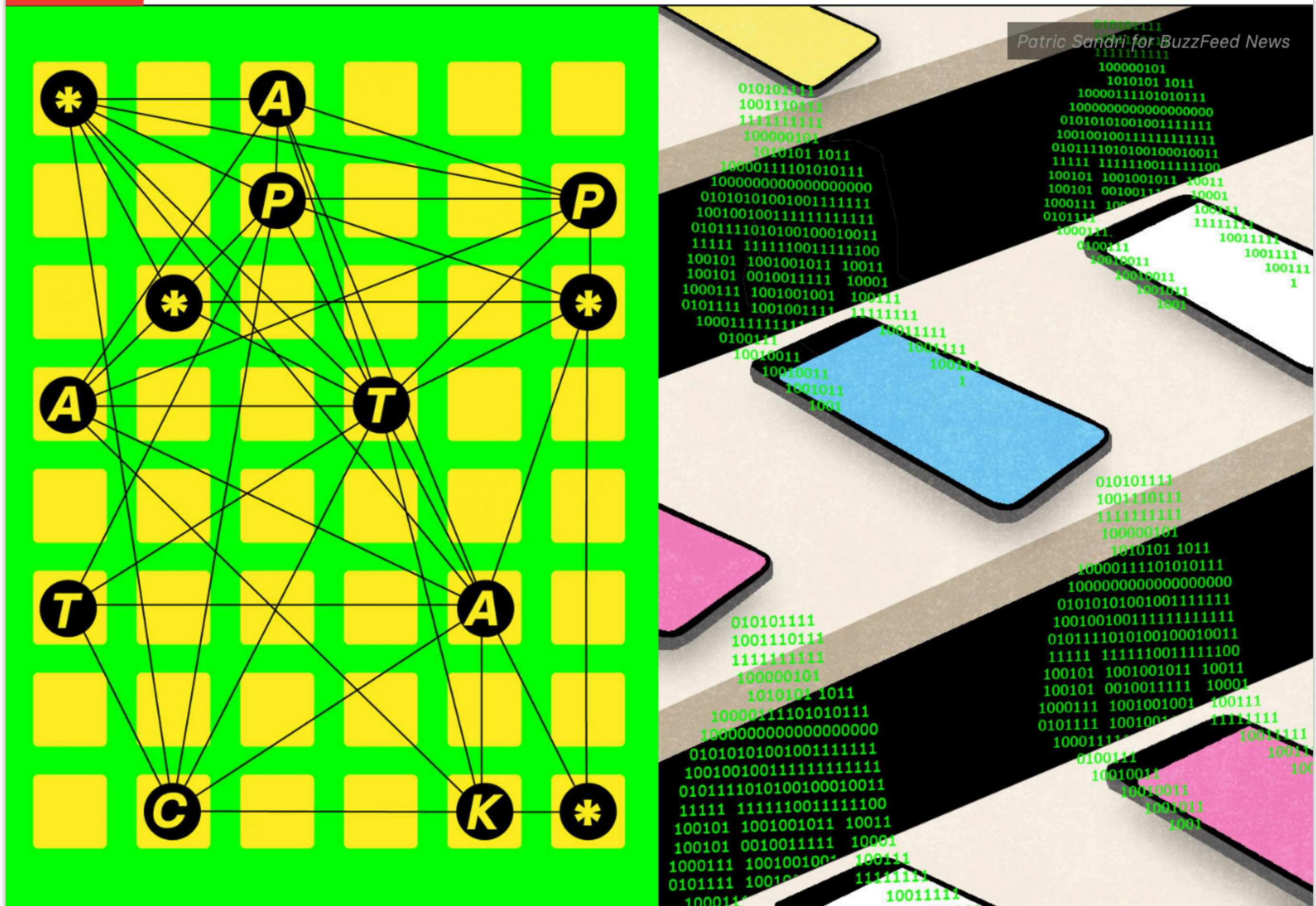


Earn additional revenue thanks to ads being viewed by bots

“I will explain you the technologies to create traffic on android, how to distribute it, how to sell the created traffic, the business structures needed, but most of all how to partner with the biggest partners to ensure the ongoing flow of advertisers and money. And by the way, your estimation of \$75 [million] accumulated damage is probably 10% of the real numbers. But that just explains how unaware or just cooperative the industry is with this growing ‘business.’”

–Fraud scheme insider





Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme

A BuzzFeed News investigation uncovered a sophisticated ad fraud scheme involving more than 125 Android apps and websites, some of which were targeted at kids.



Craig Silverman
BuzzFeed News Reporter

Posted on October 23, 2018, at 1:07 p.m. ET

These Digital Ad Fraudsters Went To Court To Try To Get Their Earnings Back. It Didn't Work Out Well For Them.

Rather than fearing the law, these fraudsters tried to use it to go after a legitimate company.




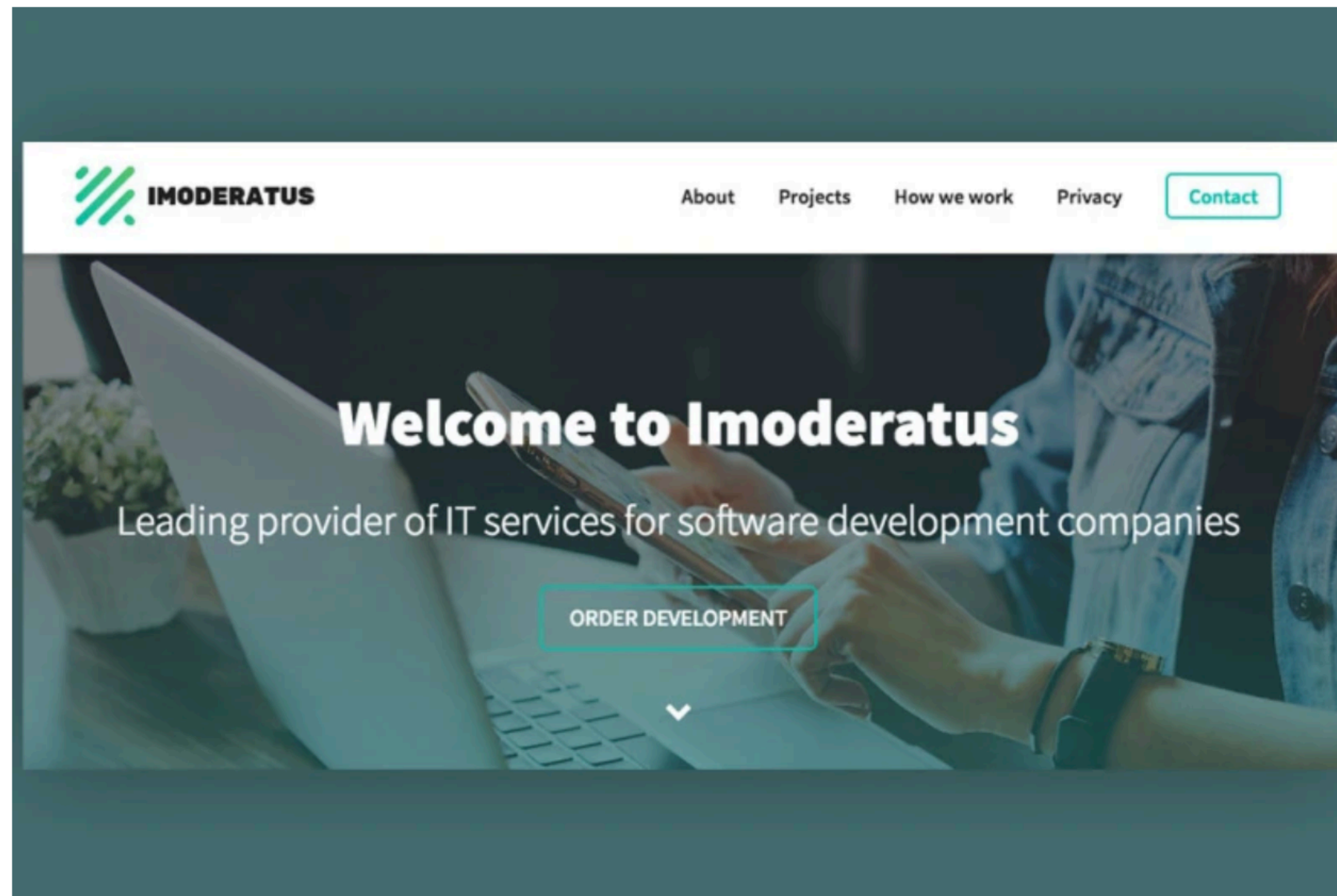
Craig Silverman
BuzzFeed News Reporter

Posted on January 7, 2019, at 3:29 p.m. ET

 Tweet

 Share

 Copy



In-Banner Video



Elements Console Sources Network Performance Memory Application Audits Security AdBlock

104 7

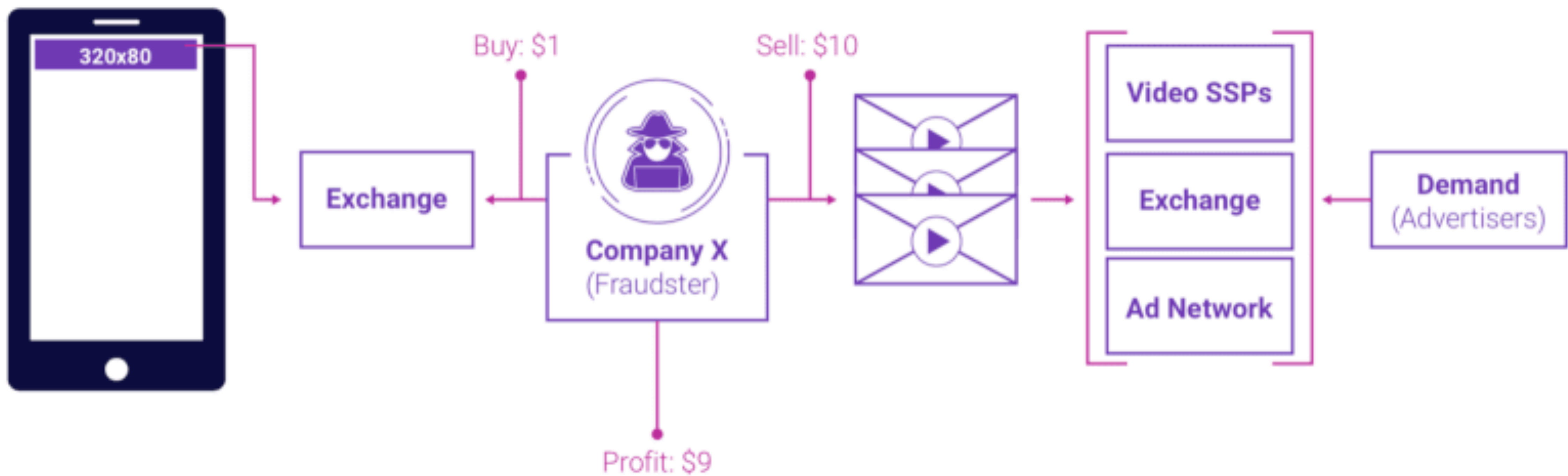
Styles Computed Event Listeners DOM Breakpoints

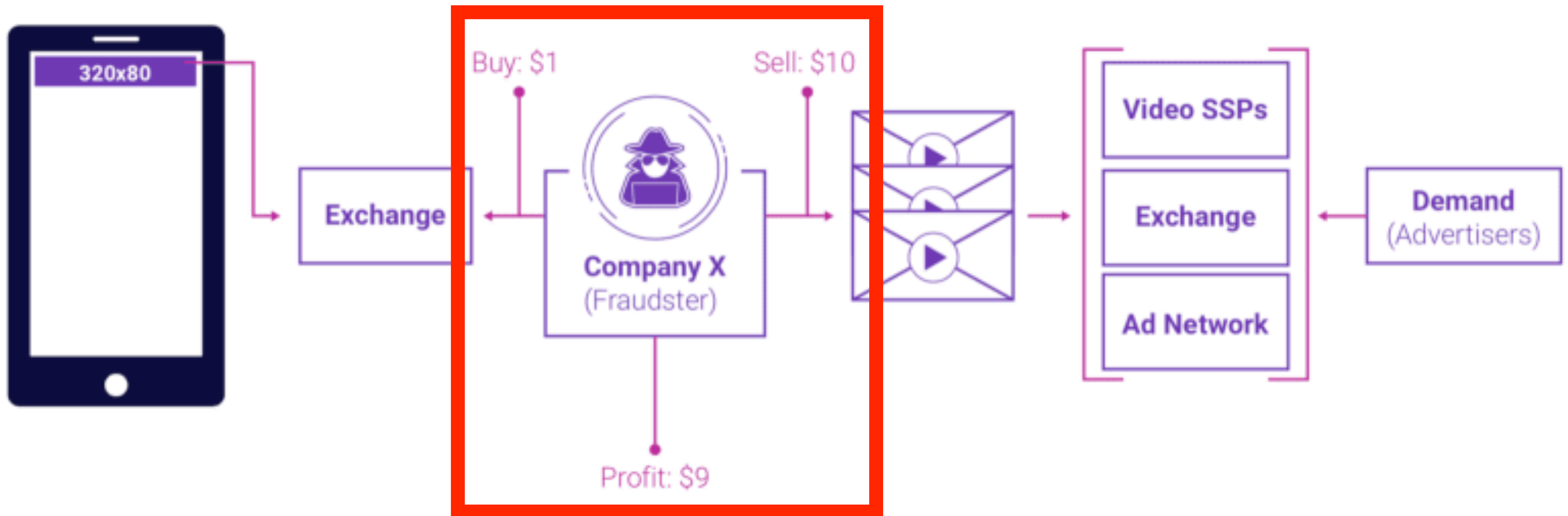
Filter :hov .cls +

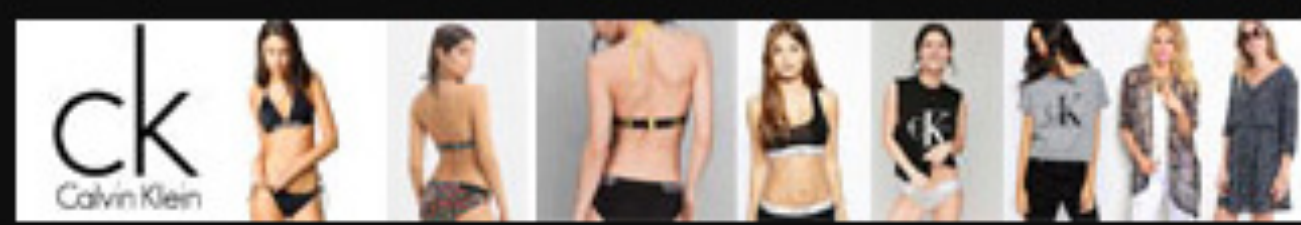
```
element.style {  
}  
  
body {  
    display: block;  
    margin: 8px;  
}
```

margin 8
border -
padding -
1248.550 x 347.642
8 8

html body





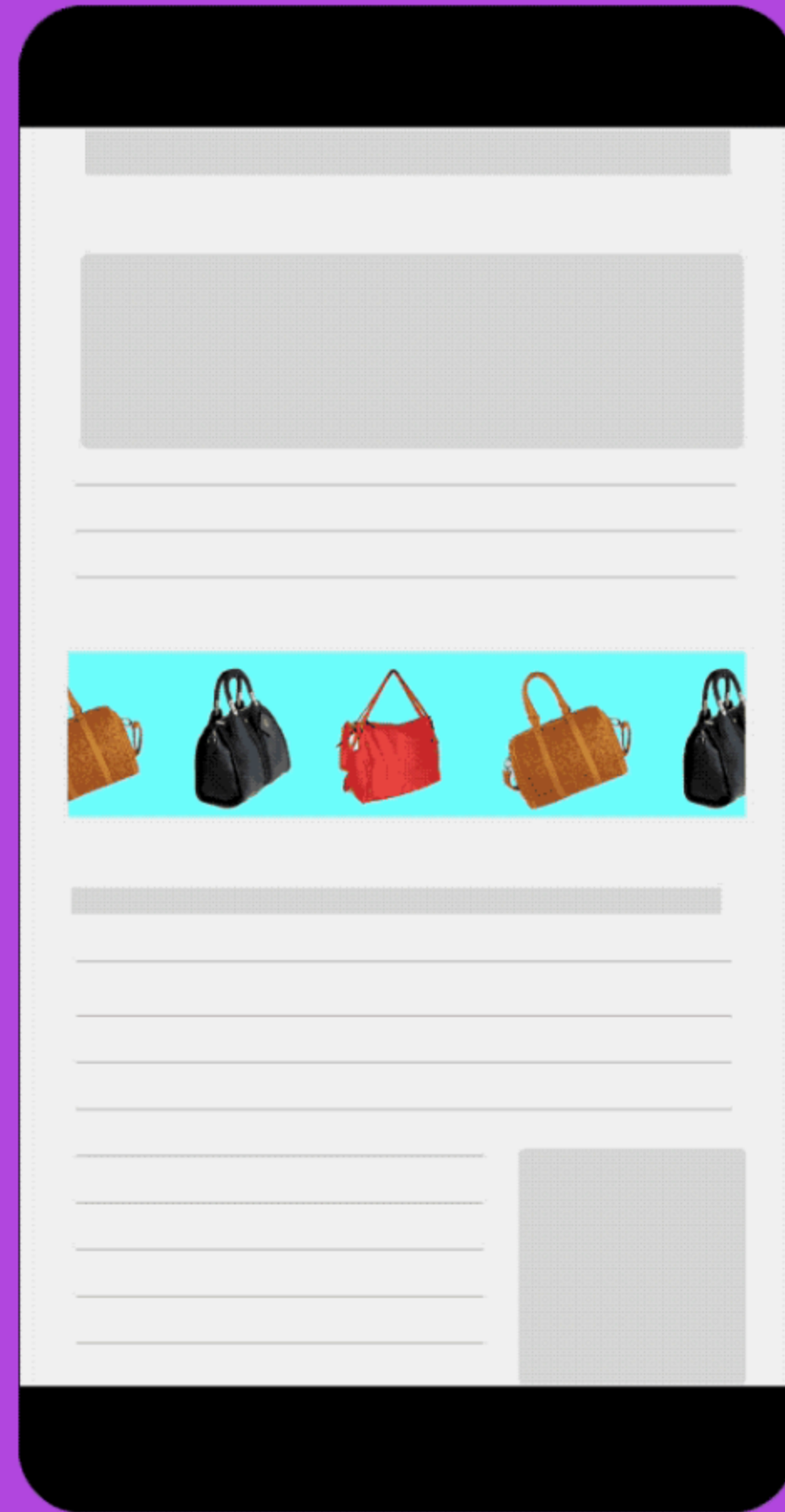


“I don’t even think about me being ripped off. All I think about is them damaging the app’s reputation. It can cost money to [a user] and drain his battery. This is the thing that makes me really mad.”

–Julien, app developer

“One of them spoke to my VP of sales and said everybody does it, why are we picking on them. It’s something we hear too often, unfortunately.”

–Asaf Greiner, Protected Media



This Giant Ad Fraud Scheme Drained Users' Batteries And Data By Running Hidden Video Ads In Android Apps

FBI probes media trading practices in the US

8 People Are Facing Charges As A Result Of The FBI's Biggest-Ever Ad Fraud Investigation

ANA Confirms FBI Criminal Investigation On Ad Transparency

As FBI agency probe heats up, marketers express concern over cooperating

Contact me securely: tips.buzzfeed.com or +1-647-949-7610

Mark R. Warner
US Senator from the Commonwealth of Virginia

Newsletter Signup

[f](#)[ig](#)[tw](#)[yt](#)[...](#)

[Meet Mark](#)[Services](#)[News](#)[Contact](#)[Priorities](#)[Español](#)[Q](#)

PRESS RELEASES

Warner Calls on FTC and Google to Address the Prevalence of Digital Ad Fraud

Oct 25 2018

WASHINGTON – U.S. Sen. Mark R. Warner (D-VA), Vice Chairman of the Senate Select Committee on Intelligence and a member of the Banking Committee, wrote a letter to the Federal Trade Commission (FTC) Chairman Joseph Simons expressing concern following a [report published by BuzzFeed](#) detailing continued prevalence of digital advertising fraud and inaction by Google to curb these efforts. According to *BuzzFeed*, this scheme has generated hundreds of millions of dollars in fraudulent advertising revenues, with operations spanning more than 125 Android apps and websites.

In July 2016, Sen. Warner and Sen. Chuck Schumer (D-NY) [wrote](#) to FTC Chairwoman Ramirez calling on the agency to protect consumers from the growing digital ad fraud phenomenon. Since then, [reports](#) have estimated that digital ad fraud has only grown to \$7.4 billion in 2017 – and projected to rise to \$10.9 billion by 2021.

At the center of *BuzzFeed's* report is Google, the only tech company absent for the Senate Intelligence Committee's September hearing on social media's role in protecting elections from misinformation and disinformation. The extent to which many popular online communications technologies have been exploited – and their providers caught repeatedly flat-footed – has been continuously highlighted in the course of investigating Russia's unprecedented interference in the 2016 election. In the same way that bots, trolls, click-farms, fake pages and groups, ads, and algorithm-gaming can be used to propagate political disinformation, these same tools can – and have – been used to assist click fraud in digital advertising markets and efforts to convince large numbers of users to download malicious apps on their phones.

What to do

- Make it a c-suite priority.
- Stop the silence. When you discover a bad actor, notify everyone you possibly can and look at how information can be made public.
- Take responsibly. It's not enough to simply pay for fraud detection/verification. Who on your team is responsible to stamping it out? What resources do they have? Can they stop a deal when it means losing money?
- Brands: stop accepting make-goods and credits without raising an issue. Build your own ad fraud team and check where your ads are running.
- Can there be a universal place to report fraud and bad actors?
- Recognize that either you do it, or law enforcement and regulators will do it for you.

Contact me securely: tips.buzzfeed.com or +1-647-949-7610

Thanks!

**Contact me securely: tips.buzzfeed.com
+1-647-949-7610**