BEYOND THE **APP**

THE EVOLVING NATURE OF MOBILE FRAUD

BLUE CARBON
CONSULTING INC.

$5,000,000,000

It’s estimated that advertisers, globally, will have lost upwards of $5 billion in 2019. Other estimates suggest it may even be more.

That’s a lot of money.

*Based on a 2019 Appsflyer Study

BLUE CARBON
CONSULTING INC.

Some more stats…

- 2019 global app install fraud: 22.6%[1]
- Q2 '19, mobile in-app ad fraud rate: 25%[2]
- Q2 '19, fraudulent mobile ad traffic: 11.6%[3]

Some leading experts argue that mobile fraud may be affecting as much as 90% of campaigns.*

1. 2019 Appsflyer Study , 2. Pixalate Q2 Ad Fraud Update 3. Q2 '19 Fraudlogix Report *According to Dr Augustine For, Ad Fraud investigator and Andreas Naumann, Head of Fraud, Adjust

BLUE CARBON
CONSULTING INC.

And in Canada…

Looking at fraudulent devices in the market:

- Total fraudulent devices in 2019: ~400 million
- 5-7 million fraudulent active devices are detected on a weekly basis

*Blue Carbon / Applied Post 2019 analytics study

When we talk about mobile fraud, we think of fraudulent apps or, perhaps, click farms like this.

What is mobile fraud?

Mobile ad fraud is the attempt to defraud advertisers, publishers or supply partners by exploiting mobile advertising technology. The objective of fraudsters is simply to steal from advertising budgets.

$5 Billion was the cost to the industry in 2019. Monetary loss is just part of the story with advertisers paying for fake impressions, clicks, and installs. It also impacts data and analytics - skewing the ability for marketers to make strategic decisions for their business.

Organized crime.

Let’s be clear: This is organized crime.

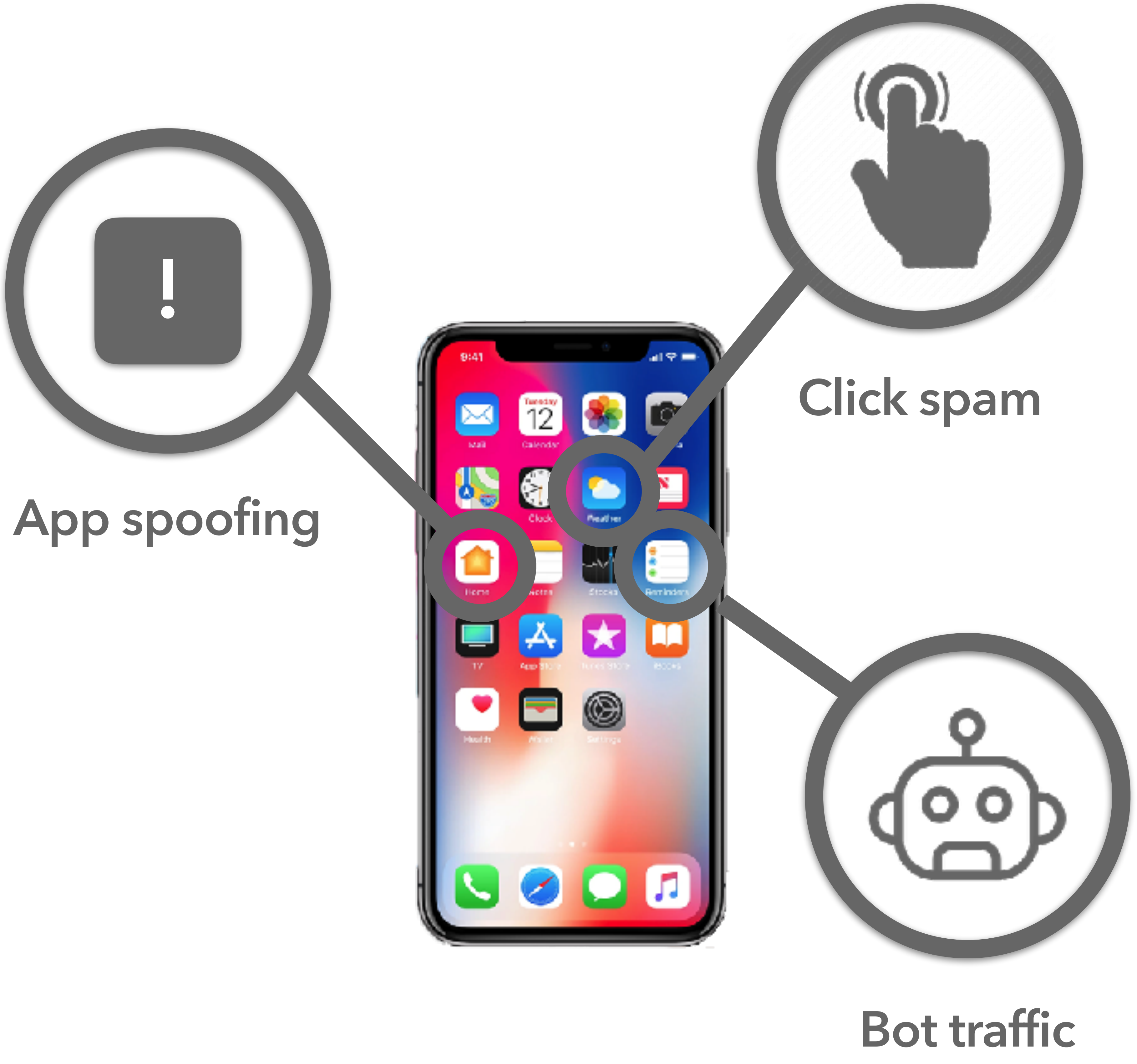
“Ad fraud is the second-largest organized-crime scheme globally, in terms of revenue generated” - and that includes narcotics - according to the CEO of CHEQ, an Ad Verification provider. And it’s understood that its proceeds fund other illegal industries, including drugs and human trafficking.

This issue goes well beyond business.

Mobile fraud encompasses a number of things.

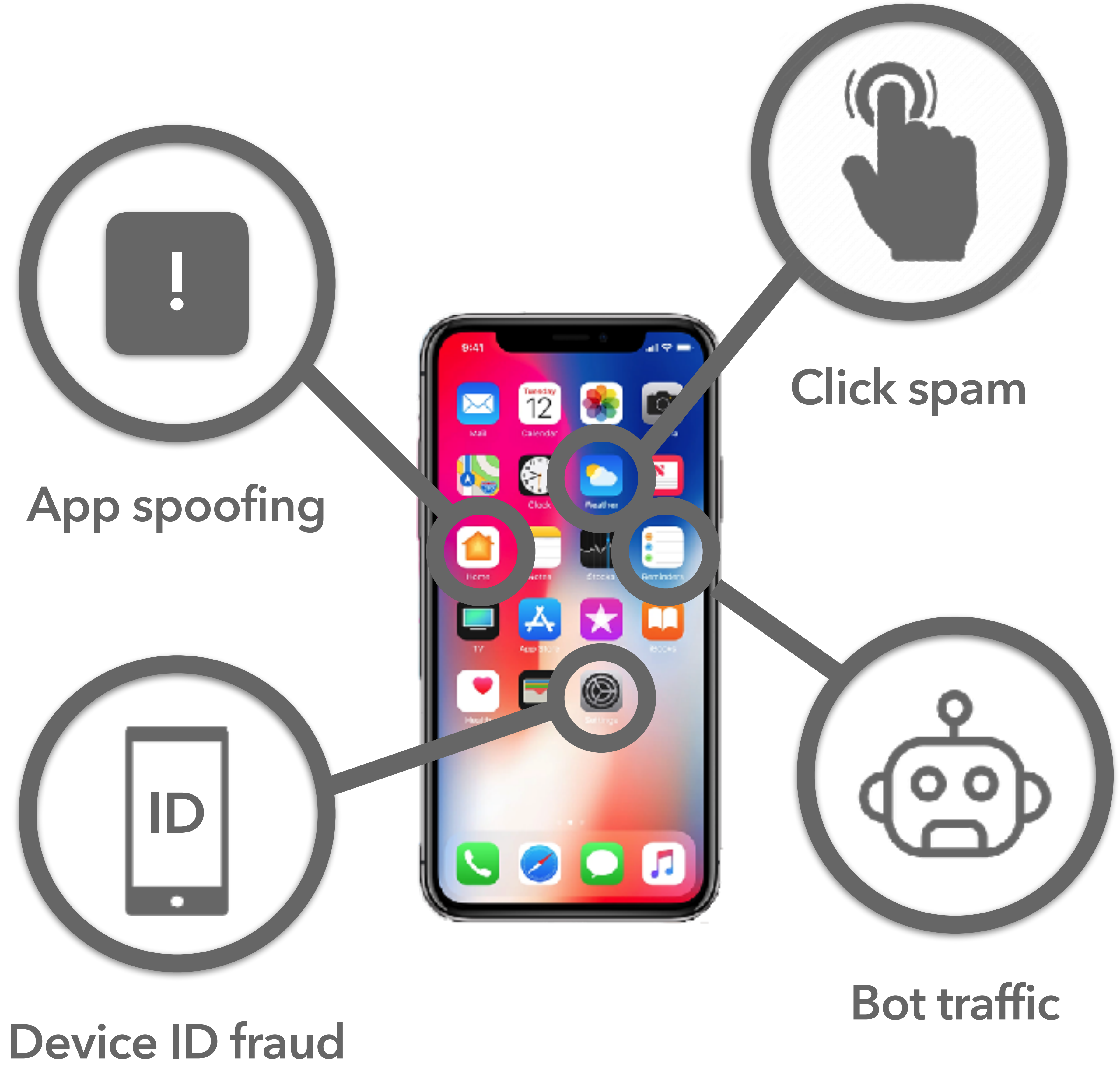
Examples include:

- **App Spoofing:** Mobile app spoofing occurs when a rogue app fakes or misrepresents the app information sent through the bid request. Fraudsters use this tactic to pose as a high-value app in order to boost CPMs.
- **Bot traffic - or IVT (**Short for invalid traffic) - that's any traffic not coming from human beings. For that reason, it's also referred to as 'non-human traffic'. The impact of IVT are clicks or impressions that artificially inflate an advertiser's budget or a publisher's earnings.
- **Click spam.** Click spam occurs when a large volume of clicks are faked on a mobile device, even though the user never clicked the ad. These are fake clicks generated by the app itself. The user may not have even seen the ad. This is also known as 'click flooding'.



BLUE CARBON
CONSULTING INC.

What we don’t hear as much about is fraud committed at the device level - by way of **Device IDs**..



BLUE CARBON
CONSULTING INC.

Mobile Ad Identifiers.

The mobile advertising ID, also known as a MAID - or simply device ID - is a sequence of alphanumeric characters assigned to a mobile phone or tablet. They're used by marketers, advertisers and app publishers to anonymously identify, understand, and target mobile device and app users.

Apple and Google have their own naming system:

- Apple: IDFA, short for ID for advertisers
- Google: AAID, short for Android advertising ID.

These identifiers are important because **investigating mobile fraud begins with the device.**

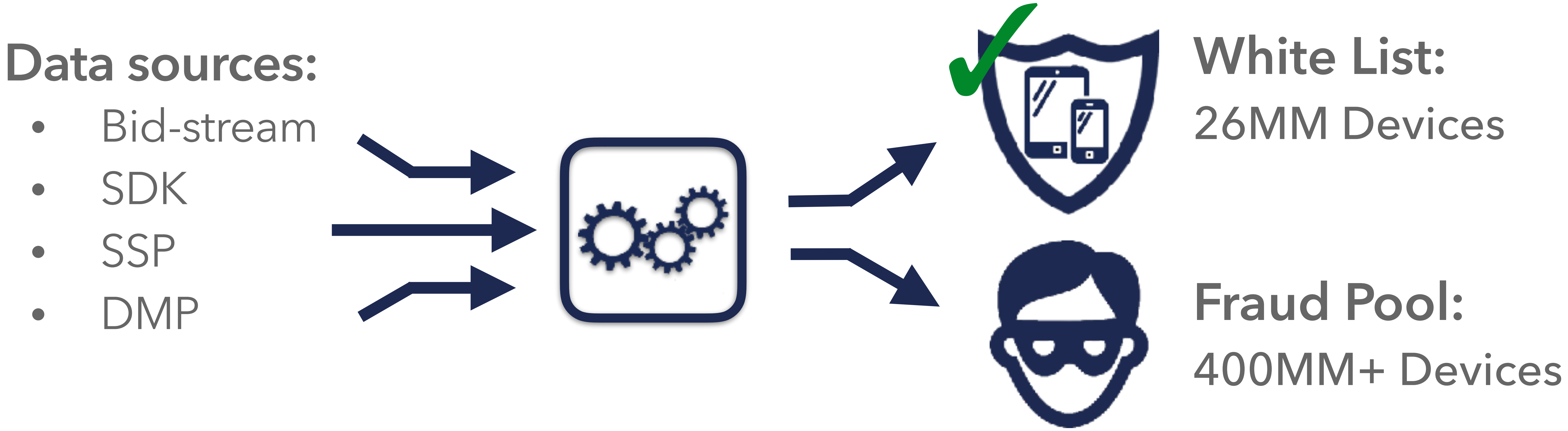
BLUE CARBON
CONSULTING INC.

DETECTING
DEVICE FRAUD

BLUE CARBON
CONSULTING INC.

How do we detect fraud? First a bit on the methodology:

It begins with our data sources - including bid-stream data, SDKs, Supply Side Platforms and Data Management Platform(s). Device IDs are initially quarantined for up to 14 days to be examined and determined whether fraudulent - to be added to the Fraud Pool - or whether legitimate, and released to the "White list".



Data sources:

- Bid-stream
- SDK
- SSP
- DMP

White List:

26MM Devices

Fraud Pool:

400MM+ Devices

So what happens in the little box with the gears?

It's where we use machine learning and big data algorithms to analyze vast numbers of metrics and the interrelations between them. It involves using a set of 46 filters, form more routine checks - to more difficult to detect situations that require advanced analytics and multi-point corroboration.

BLUE CARBON
CONSULTING INC.

Fraudsters can randomly match real device IDs. They’re often siphoned off from ad exchanges and other sources. To combat this kind of fraud, we monitor for anomalous behaviours, including some behaviours we refer to as ***Popping*, *Swarming*, and *Spoofing*…**

Popping. This is when a device is observed at one point (in terms of latitude & longitude) - and moments later - the same device is seen in another location, that would be physically impossible to get to in the time between calls.

Swarming. This is when an unusual level activity is observed at a single location - such as a middle of a forest or a lake - where large numbers of legitimate devices are unlikely to be. This traffic is filtered out until the device can be confirmed authentic or confirmed as fraudulent.

Spoofing. Fraudsters that run click farms with actual devices will continuously change their device IDs. These phones are changing their identity regularly. We monitor for these flurries of activity and when observed, the device ID gets sequestered.

BLUE CARBON
CONSULTING INC.

And click farms aren’t just in other parts of the world. They’re here in Canada.

Based on cluster analysis, potential click fraud farms have been identified here in Canada, including one being identified just outside of Ottawa.

BLUE CARBON
CONSULTING INC.

An example of swarming is occurring within Lake Ontario, adjacent to the island airport, where thousands of device IDs are regularly tracked.

Metro Toronto Convention Centre
Scotiabank Arena
Pacers vs Raptors · 6 p.m.
DON LANDS
ENTERTAINMENT DISTRICT
King St W
Front St W
Rebel
The Westin Harbour Castle, Toronto
Fort York Blvd
Harbourfront Centre
Quay W
IAGARA
erry Beach
WARD'S ISLAND
Centre Island
MUGGS ISLAND
Hanlan's Point Beach
Toronto Islands
Centreville Amusement Park
CENTRE ISLAND

BLUE CARBON
CONSULTING INC.

Fraud is constantly evolving.

Reshef Mann, co-founder and CTO at AppsFlyer, said:

"We often refer to fraud as a game of cat and mouse.."

Where in 2018 it was massive bot attacks, in 2019, it was massive app install fraud as the fraudsters evolved from physical device farms to device emulators and other sophisticated schemes "capable of unlimited scale".

"The speed at which fraudsters adapt is also accelerating, from one to two months in 2018 to as little as two to three days today." But as the types of fraud continue to expand and evolve, so, too, do our processes for identifying it.

WHAT **CAN** YOU DO?

BLUE CARBON
CONSULTING INC.

What you can do.

- **Use proven platforms**. Every day, there is a new marketing tool or service provider that promises great results. Advertisers should focus on platforms that have a proven track record of providing results through validated case studies, white papers and other third-party reviews
- **Have a 3rd party audit your ad performance.** Don't allow end vendors to evaluate their own work. Use industry trusted third parties to audit performance and to help hold your advertising dollars to the highest standard. Investigate when the Cost Per Thousands (CPMs) are too good to be true. Once investigated via a third party, the effective cost to reach non-fraudulent traffic often tells a different story
- **Manually monitor your ad data**. Manually monitoring your ads and data is important to ensure your ads aren't generating any bad traffic or scammers. Specifying campaign tactics beforehand – like your target audience, budget or metrics you want to monitor can help you learn which parts of your ad campaigns to tweak and better achieve your campaign targets.

BLUE CARBON
CONSULTING INC.

What you can do.

- **Pay For Action, Not For Traffic.** Advertising networks suffer from very basic fraud-protection mechanisms. They rarely disclose detailed campaign information to advertisers, so sorting through fake traffic is often not an option. The main metric for marketers' performance should change from pushing traffic to generating measurable values.
- **Demand Transparency From Your Ad Tech Provider.** Don’t trust someone who offers new "ad tech," or who just says that they are high quality. Demand transparency. Ask to understand how the technology works, not just what it is. Ad fraud isn't hard to avoid if you do it right, working with the right partners.
- **Combine The Right Tools With The Right Human Talent.** Technology alone can only do so much to uncover and protect against ad fraud. Often, fraudulent results are created by sophisticated methods and can be difficult to spot. However, a trained eye with experience managing campaigns for results can typically point out fraudulent data quickly. Even with the best tools, human oversight helps ensure quality and remains vital in our industry.

What you can do.

- **Understand Early Warning Signs From Your Data.** Data is one of the most powerful tools advertisers can use to combat fraud. Businesses should regularly audit and analyze data for warning signs. If expensive campaigns yield minimal results, it may be a sign of foul play. Additionally, advertisers should look at bounce rates, site times and click rates for any dramatic changes or suspicious activity.
- **Establish A Pre-Bid Suppression Strategy.** Establishing a pre-bid suppression strategy may entail working with a third-party pre-bid fraud suppression or block list vendor - one that runs pre-bid filtering on inventory where brands plan to place ads.
- **Utilize a White List of Devices.** Consider targeting against a cleansed, "white list" of devices.

While mobile fraud continues to be a major issues in our business, there's lots of progress being made and great products and services available to advertisers.

ABOUT **BLUE** CARBON

About Blue Carbon

Blue Carbon is a Toronto digital consulting firm helping agencies, advertisers, & publishers gain a competitive edge through marketing technology, insights, and data.

Recognizing the need to address mounting fraud in the mobile ad space, and in conjunction with our mobile partners, Blue Carbon set out to compile the most comprehensive database of fraudulent mobile device IDs in Canada. We now make that list available to advertisers for ad campaigns and for auditing purposes.

BLUE CARBON
CONSULTING INC.

THANK YOU

jason.cox@bluecarbonconsulting.com

416.272.1589 | bluecarbonconsulting.com

BLUE CARBON
CONSULTING INC.