iab. TECH LAB

Best Practices for Ad Fraud Disclosure

Released May 2022

Please email support@iabtechlab.com with feedback or questions. This document is available online at https://iabtechlab.com/ad-fraud-disclosures/

The Best Practices for Ad Fraud Disclosures document was developed by the IAB Tech Lab Programmatic Supply Chain Working Group. The following IAB Tech Lab member companies contributed to the creation of this document:

- Magnite
- HUMAN
- Google
- Pixalate
- Integral Ad Science
- Oracle's Moat
- Double Verify
- The Trade Desk

https://iabtechlab.com/working-groups/programmatic-supply-chain-working-group/
The IAB Tech Lab lead on this initiative was Jill Wittkopp.
Please contact support@iabtechlab.com if you have any questions or comments about this document.

Table of Contents

1. Executive Summary

The digital advertising industry continues to battle ad fraud in various ways, including through targeted collaboration in response to emerging ad fraud attacks. Typically, this collaboration occurs in response to a) observations shared (often informally) between organizations or b) a publicly reported attack. This type of collaboration is valuable, yet there is room for improvement, especially in consolidation of efforts and standardization of information sharing.

2. Overview

This proposal aims to improve how ad fraud attacks are disclosed, by consolidating a set of best practices that will drive alignment and consistency across the industry. The best practices comprise a set of guiding principles that can be expanded and updated as the industry evolves.

Rationale

There are multiple types of ad fraud attacks that can negatively impact the digital advertising industry at scale. These attacks include (but are not limited to) botnets and "bot farms," malicious applications on mobile and CTV apps, and sketchy browser extensions. In light of ongoing attacks that have emerged and that will likely emerge in the future, there is a need for the industry to better address and respond to an attack when it is disclosed. Currently ad fraud attacks are disclosed in bespoke and sometimes fragmented ways, leading to both a lack of consistency and clarity in what is disclosed, as well as potential gaps in both understanding and verification of attacks. By implementing the best practices included in this proposal, disclosing entities will help the industry to better address and respond to ad fraud attacks in a mutually beneficial way.

Disclosure and Reporting

A disclosure can be either a) informal and private or b) formal and public. Informal and private disclosures typically are conducted among organizations that share information ad hoc with each other. Formal and public disclosures are facilitated by credible third parties (e.g., industry bodies), or directly by the organization(s) that identified the attack, with the intent of reaching a broad audience. These two types of disclosures are not exclusive of each other, as informal and private disclosures can precede an eventual public disclosure.

The following criteria should be considered and applied when a disclosure is made:

Further protection of the ecosystem	Disclosures should materially and demonstrably help protect the digital ads ecosystem.
Verification and corroboration	Disclosures should be able to be verified and corroborated by third parties, especially with regard to the nature and impact of an ad fraud attack (see Information Sharing below). Reports should include relevant information that enables verification and corroboration of analyses and observations included in a disclosure. Exceptions, whether for proprietary or other reasons, should be clearly identified.
Avoidance of undue harm	Disclosures should not cause undue harm to other organizations, including through unsubstantiated claims. Care should be taken when identifying legitimate third parties or organizations in a disclosure (i.e., "naming names"). Disclosures should avoid presenting organizations as implicated in an ad fraud attack, as the risks pertaining to assertions of culpability often outweigh the benefits. (e.g., it is often difficult to determine whether an organization is a knowing participant in an attack or an unwitting victim. Generally, perceived victim organizations should be informed in private.
Reporting channels and mediums	Disclosure of an ad fraud attack (privately or publicly) can occur through various channels and mediums. When possible and appropriate, it is recommended that organizations use established channels and mediums.

Timing	An ad fraud attack should be reported as soon as practicable and when appropriate, such reporting should take into consideration the other criteria listed in this document.
Accuracy	Opinions expressed in reports should reference foundational facts wherever possible and avoid conjecture.
Origin	Reports shared through a third party should link to or reference a canonical source of data/information (see Information Sharing below).
Confidentiality	Confidential information should be explicitly marked as such. Any party receiving confidential information should take reasonable and appropriate steps to protect confidentiality (see Confidentiality below).

Information Sharing

Effective data and information sharing are critical aspects of a disclosure because this sharing enables targeted collaboration to defend against an attack. Including the information listed in the table below (when appropriate and possible) will maximize the value of a disclosure.

IP addresses	Server IPs are integral for initial analysis. Receipt of client/user IPs requires caution so that disclosures don't violate user privacy.
User agents	User agents represent request headers that can be used to analyze characteristics such as purported browser, browser version, operating system, etc.
Domains / URLs	Can be C2s involved in Botnets, intermediary domains or monetized pages.
Network	ISP, ASN, or mobile carrier network information.
App IDs	Used to accommodate cases where the apps themselves are determined to be integral to the ad fraud scheme or operation. Ideally,

	these IDs should be consistent with the IAB Tech Lab's App Identification Guidelines.
Compromised Entity ID	This would be an identifier of the entity that may be infected or perpetrating the fraud, identifiers could include seller ID or buyer IDs
Binary hashes	As a standard information security practice, binary hashes should be provided for malware.
SDKs	Whether any SDKs are used, and if so, the name and version of the SDK.

Confidentiality

The disclosure of ad fraud attacks is sensitive and nuanced, and confidentiality is an important element in both the disclosure and the receipt of disclosed information. The following factors should be considered and evaluated with each disclosure:

Proper identification of confidentiality	Organizations should clearly and explicitly mark which sections or elements of a disclosure are confidential and with whom they may be shared. Organizations should consider utilizing the Traffic Light Protocol (TLP) developed by the U.S. Cybersecurity & Infrastructure Security Agency (CISA), as it is a widely adopted sharing protocol that provides recipients with clear boundaries and expectations. If a briefing is presented using the TLP protocol, recipients must agree and comply with the protocol, otherwise they forfeit eligibility to receive briefings.
Onward data sharing	Organizations receiving confidential information must not share confidential

	information with other third parties without prior and explicit approval from the original disclosing organization.
Applicable laws and jurisdiction	Organizations should work with legal counsel prior to making a disclosure to understand reasonable legal safeguards (e.g., NDAs), applicable laws, as well as legal risks and constraints.
Maintenance of confidentiality	Any party receiving confidential information must take appropriate steps to protect confidentiality.
Legal vehicles	Legal vehicles, such as NDAs, should be used when reasonably necessary and appropriate (subject to guidance from legal counsel if/as needed).

Objections and Corrections

While it is understood that an organization disclosing an ad fraud attack has taken reasonably adequate and necessary steps to disclose accurate information and assertions, there may be instances whereby other parties may raise objections or identify errors in a disclosure. Disclosing organizations should be prepared to address potential objections or corrections. The following guidelines are meant to facilitate effective reconciliation of objections and corrections.

Submitting objections	Objections to a disclosure should be provided directly to the disclosing party.
Public communication	Public communication about objections and corrections should be aimed at constructive dialog, rather than criticism or reproach.

Communicating corrections	Updates and/or corrections for a prior disclosure should use the same channel(s) as those used for the initial disclosure.
Accuracy and clarity of corrections	Corrections should clearly indicate what is new or what has been revised.

3. Additional Considerations

The disclosure of ad fraud attacks is an important element in the digital advertising industry's efforts to combat ad fraud. Despite their value and utility, these disclosures also have the potential to negatively impact industry efforts to stop bad actors. There are several caveats that should be considered when disclosing an ad fraud attack, especially if it is a public report.

Personal Information

In order to protect the privacy and security of users, personal information should not be shared or distributed in any way that contravenes applicable laws.

Law Enforcement

Companies may also consider disclosing information to law enforcement, as law enforcement efforts play a role in combating ad fraud. Disclosing companies should evaluate whether sharing information with law enforcement is appropriate.

Risk of Misinformation of Disinformation

While disclosures of ad fraud attacks can help the digital advertising industry in many ways, there is a risk that an inaccurate or misleading disclosure could lead to a cycle of misinformation or disinformation across the industry. Disclosing organizations should take reasonable and deliberate steps to minimize this risk by ensuring that information that they share is accurate and verifiable.

Duplicate or Disparate Efforts

Given the sensitive nature of disclosing an ad fraud attack, there is the potential that the same ad fraud attack(s) may have been identified, observed, and analyzed independently yet concurrently by different organizations (or groups). Organizations should be aware of this

potential, and they should be prepared to actively engage more broadly to better understand similarities and/or differences in what has been disclosed.

Timing and Status

The determination of when an attack emerged and whether it is still occurring will allow for ongoing attacks to be prioritized and/or actioned against before they potentially increase in impact. It should be noted that collaboration and corroboration will be needed among organizations to better understand how extensive an attack may be and by how much mitigation measures have reduced or eliminated an attack (e.g., blocklisting by one organization vs. underlying infrastructure taken down or disrupted vs. perpetrators identified and caught).

Conclusion

When choosing to disclose information about an ad fraud attack, using these best practices will help the ecosystem by providing clear, useful and timely information that allows the ecosystem to combat ad fraud in an effective manner. Despite the challenges that ad fraud represents across various dimensions, collaboration and responsible disclosures will enable the industry to further secure and harden the ecosystem against attacks.