**NexFort Data Limited: response to the Fraudulent Advertising Codes consultation**

---

**Cover sheet**

- **Consultation title:** Fraudulent Advertising Codes Consultation
- **Name of respondent:** [redacted]
- **Representing:** NexFort Data Limited
- **Confidentiality:** Nothing
- **How I came across this consultation:** Found it on Ofcom's website

---

**About this response**

NexFort Data Limited is a UK company working on the security of the online advertising supply chain. We measure that supply chain from the outside: what a device is actually made to contact when a page loads, and what a domain's public supply-path files declare about who is authorised to sell its inventory. We do not hold client data, we do not see the bid stream, and we cannot see inside walled gardens. We have never measured a government or military estate.

I am answering three questions where I think we hold something Ofcom does not, and leaving the rest to people better placed to answer them.

---

**Volume 1: Online advertising ecosystem**

**Is there any information or evidence you hold that could enhance our understanding of the online advertising ecosystem?**

Yes. Rather than describe it, or offer to produce it, I have run the measurement and the result is below.

**The specific gap.** Volume 2, paragraph 2.3 states that "most providers of Category 1 and Category 2A services use owned-and-operated supply chains (sometimes known as 'walled gardens') to place paid-for advertisements on their services". Paragraph 2.8 then concludes that the intermediaries measure will apply "only in limited circumstances because we understand that there is a greater prevalence of owned-and-operated supply chains among categorised services".

That conclusion carries a great deal of weight. It determines how often the intermediaries measure bites, and therefore how much of the open-display market the Codes reach in practice. Its evidential basis, at footnote 5 to Volume 2, is a set of formal and informal information requests to the services themselves. Across the four volumes I count 169 citations to such requests, every one with the respondent redacted.

I want to be careful here. Information requests are the right instrument, the redaction is proper, and I am not suggesting any provider has been anything other than accurate. The observation is narrower and I think it is useful: **the question of which advertising pathways a categorised service uses does not have to be asked. It can be measured from outside.**

**How, concretely.** Two public, machine-readable artefacts already answer most of it.

- **ads.txt and app-ads.txt**, published at a known path on a publisher's own domain, declare which companies are authorised to sell that publisher's inventory, and whether each is a direct seller or a reseller. A service placing advertising purely through an owned-and-operated pathway has a very different file, or no file, from one selling through the open-display market.
- **sellers.json**, published by exchanges and intermediaries, declares the sellers on whose behalf they are authorised to transact.

Both are IAB Tech Lab standards, both are already ubiquitous, and neither requires anyone's permission to read. Read together across the categorised services register, they give an independent, repeatable and dated answer to the question Volume 2 paragraph 2.3 answers from self-report. A page load from an instrumented browser adds the other half: which third parties a service actually causes a user's device to contact, as opposed to which ones it declares.

**So I have run it, rather than offering to.** On 9 September 2026 I read the ads.txt of every Category 1 and Category 2A service on your register: fifteen entries resolving to fourteen distinct domains, since Facebook appears both as a Category 1 service and as Category 2A in respect of Feed Deep Dive. One request per domain, nothing entered, nothing clicked, no page rendered. I read all fourteen again on 1 October 2026, the day before submitting: every verdict and every ad-system count below was unchanged.

| Service | Cat | Verdict from its published file | Ad systems |
|---|---|---|---|
| Pinterest | 1 | authorises third-party sellers | 7 |
| Quora | 1 | authorises third-party sellers | 86 |
| Roblox | 1 | authorises third-party sellers | 6 |
| TikTok | 1 | authorises third-party sellers | 1 |
| X | 1 | authorises third-party sellers | 6 |
| Bing | 2A | authorises third-party sellers | 143 |
| Facebook | 1, 2A | declares it authorises none | 0 |
| Instagram | 1 | declares it authorises none | 0 |
| YouTube | 1 | declares it authorises none | 0 |
| Reddit | 1 | no published file | 0 |
| Snapchat | 1 | no published file | 0 |
| WhatsApp | 1 | no published file | 0 |

| Service | Cat | Verdict from its published file | Ad systems |
|---|---|---|---|
| Google Search | 2A | no published file | 0 |
| ChatGPT Search | 2A | no published file | 0 |

**Six of the fourteen domains publish a file authorising named third parties to sell their inventory. Three declare in terms that they authorise none. Five publish nothing.**

The six are not marginal. Quora authorises 86 ad systems across 241 records on 1 October (263 on 9 September). Bing authorises 143, across 1,241 records of which 78 per cent are reseller entries. Pinterest, Roblox and X each name several of the largest programmatic exchanges with seller identifiers and TAG certification identifiers: Rubicon Project, PubMatic, OpenX, Index Exchange, TripleLift, Sharethrough, Amazon Publisher Services and others.

The three that declare the opposite are worth as much. Facebook, Instagram and YouTube each serve a comment-only file stating that their inventory cannot be purchased programmatically through open exchanges. Those are positive declarations and they support paragraph 2.3 for those services. I would rather report that than only report what supports my argument.

**What this does not establish, stated plainly.** An ads.txt sits at a domain, not at the categorised part of a service. It cannot show which surface of that domain the authorised sellers serve, so Pinterest authorising OpenX does not by itself establish that the Category 1 user-to-user feed carries open-display inventory, and Bing's 143 systems do not establish that search advertising specifically is transacted that way. Nor does it establish volume or revenue share by pathway, which is genuinely invisible from outside and for which your information requests remain the only route. And "no published file" is not evidence in either direction: Reddit and ChatGPT answer the path with an ordinary web page, and Snapchat, WhatsApp and Google Search return 404.

**What it does establish** is that on six of the fourteen domains the service has publicly authorised third parties to sell inventory, in a file it wrote itself, on a date now on record. I offer that as a complement to the information requests rather than a substitute, but I think it sits uncomfortably beside the expectation at paragraph 2.8 that the intermediaries measure will be needed "only in limited circumstances". On the published evidence an open-display pathway is present on more of the register than it is absent.

**The offer stands and is unconditional.** The full table, the method, the target list with its provenance, and the two parsing bugs I found and fixed while doing it, are available to Ofcom or to anyone who wants to reproduce or contradict the result, at no charge. It should be re-run before it is relied on, because the verdicts are a function of files as published on a given day.

**One further piece of evidence Ofcom already has and may wish to weight more heavily.** Volume 2 cites Beruku and Which?, *Fraud in the open-display advertising market* (2022), and the ISBA *Programmatic Supply Chain Transparency Study* (2020), at footnote 4. Both appear in support of the observation that the open-display market lacks standardisation and transparency, and then the proposed measure is expected to apply only rarely. If the open-display market is where the transparency problem lives, the measure aimed at it deserves an empirical basis for how often it will be needed.

---

**Volume 2: Advertising intermediaries**

**Do you agree with our proposal?**

Yes, with one recommendation about its evidential basis and one about record-keeping.

**The measure itself is right in principle.** Paragraph 2.4's position, that the pathway a provider uses "should not result in different safety outcomes for users", is the correct regulatory instinct, and paragraph 2.13's statement that steps "are likely to be reasonable even if they result in a reduction in a provider's revenue" is the sentence that gives it teeth. Without that sentence "all reasonable endeavours" would be negotiable against commercial convenience, which is exactly how supply-chain safety obligations usually fail. I would resist any pressure to soften it.

**Recommendation 1: test the "limited circumstances" expectation before relying on it.** Set out in the answer above. The expectation at paragraph 2.8 is load-bearing and externally checkable, and I have checked it.

**Recommendation 2: the record under 2.6(ii) should be published, not only kept.** The proposed measure requires a provider to record which measures it could not implement, why, and what it did instead. That record is, so far as I can see, the only place in the entire regime where the gap between what a categorised service does on its owned-and-operated inventory and what it achieves on open-display inventory becomes visible to anyone at all. Kept privately, it is available to Ofcom on request. Published, even in summary and annually, it becomes something researchers, journalists and the intermediaries themselves can act on, and it creates a reason for a provider to close the gap rather than to document it. I appreciate this is a heavier obligation than proposed and I would rather argue for it plainly than imply it.

**Do you have any additional examples of how providers could work with or require intermediaries to implement safety measures in circumstances where they have insufficient control?**

One, which is already standard practice in the industry and therefore hard to argue is unreasonable.

**Require, by contract, that intermediaries in the path are declared and verifiable in the public supply-path files, and that the provider periodically checks that they are.** The mechanism exists: sellers.json and the OpenRTB SupplyChain Object were built to let a buyer establish every party in a path. A provider that cannot apply an account-integrity measure to an open-display advertiser can still require that the intermediaries it deals with declare themselves correctly, and can verify that requirement automatically, from the outside, at low cost and without anyone's cooperation. It is a version of the same accountability the account measures seek, applied at the layer the provider can actually reach.

Its limits should be stated honestly. It establishes who is authorised to be in a path. It does not establish that any of them are honest, and my third answer is about precisely that gap.

---

**Volume 3: Account checks and actions**

**Do you agree with our proposal?** My comments relate to check (a), verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising.

I agree with the check and I want to record what it does not catch, because I think the framing invites more confidence than the mechanism can carry.

**The check is framed as anti-impersonation.** Volume 3 describes it as verification "to help prevent impersonation". Against impersonation it is a good control and it should be recommended.

**The documented case it does not reach.** In December 2025 Google's Threat Intelligence Group reported that, working with partners, it had "identified the companies Intellexa created to infiltrate the advertising ecosystem, and those partners subsequently shut down the accounts from their platforms". Amnesty International's Security Lab, working from Intellexa's own leaked documentation, described the associated infection vector and stated that "simply viewing the advertisement is enough to trigger the infection on the target's device, without any need to click on the advertisement itself". Intellexa is subject to US sanctions.

The relevant feature of that case for this measure is this. Those companies were not impersonating anybody. They were incorporated companies, advertising as themselves, and an account holder working for them genuinely did work for the organisation being advertised. Check (a), applied correctly and in good faith, returns a pass. The accounts were closed afterwards, on the strength of published threat research, not by any check in the path at the time.

I am not arguing the check should be dropped or that a different check would have caught this. I am arguing that the regime should be explicit that verifying *who* an advertiser is establishes corporate existence and good standing, and not intent, and that an adversary willing to incorporate a company clears that bar deliberately. Where the assessment reads as though identity verification substantially addresses the risk, I think it overstates what identity verification can do.

**A structural observation about scope.** Volume 3 runs to 101 pages on advertising account integrity and does not mention the open-display supply chain once. I have checked. That appears to be deliberate and defensible, since the account measures are naturally about accounts held with the service. But it means the account-integrity regime assumes the advertiser holds an account with the categorised service, and in an open-display path the buyer generally does not. The advertisement arrives through intermediaries and the buyer may have no relationship with the service at all.

The consequence is that Volume 3's protections and Volume 2's intermediaries measure do not meet in the middle. An advertiser who cannot pass check (a) has an obvious route that avoids ever being asked: buy through the open-display market instead, where the applicable obligation becomes the provider's "all reasonable endeavours". I do not think that is an argument against either measure. I think it is an argument for the fraud indicator assessment in Volume 2 to require providers to consider, explicitly, whether their open-display pathway is materially easier to place a fraudulent advertisement through than their owned-and-operated one, and to record the answer.

---

**Sources cited in this response**

1. Google Threat Intelligence Group, "Intellexa's Prolific Zero-Day Exploits Continue", December 2025. https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue
2. Amnesty International Security Lab, "To Catch a Predator: Leak exposes the internal operations of Intellexa's mercenary spyware", December 2025. https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/
3. IAB Tech Lab, ads.txt, app-ads.txt and sellers.json specifications. https://iabtechlab.com/ads-txt/
4. IAB Tech Lab, OpenRTB 2.6, including the SupplyChain Object. https://iabtechlab.com/wp-content/uploads/2022/04/OpenRTB-2-6_FINAL.pdf
5. Beruku and Which?, *Fraud in the open-display advertising market*, 2022, as cited at Ofcom's Volume 2 footnote 4.
6. Incorporated Society of British Advertisers, *Programmatic Supply Chain Transparency Study*, 2020, as cited at Ofcom's Volume 2 footnote 4.