BCLP. Client Intelligent

Insights

FROM FRAUDULENT ADVERTS TO CORPORATE OFFENCES: NAVIGATING POCA, ECCTA AND THE OSA

DIGITAL SPEAKS

Mar 31, 2026

Paid advertising continues to underpin the commercial model of major search and social media platforms. Yet the scale of fraud and unlawful financial promotions within this ecosystem has become increasingly difficult for regulators—and financial institutions—to ignore. As regulatory frameworks tighten and algorithmic systems become central to content governance, platforms now face complex legal risks, including the potential for corporate criminal liability for money laundering offences under the Proceeds of Crime Act (**POCA**). Taken together, these developments mark a shift in how fraudulent advertising is understood: not merely as a consumer-protection issue, but as a potential source of financial-crime exposure for the platforms themselves.

The dominant revenue stream of major search and social media platforms remains paid-for advertising. A material proportion of the adverts that feature on these platforms are believed to be fraudulent. A recent research paper commissioned by Revolut found that UK users of social media were shown 95 billion scam adverts during 2025, estimated to be roughly one-tenth of the total adverts displayed through such sites. Unsurprisingly, the amount of revenue generated from these adverts is substantial, estimated in the research paper to be £430 million. The prevalence of these adverts is of significant interest to financial institutions, who may be liable for losses suffered by victims of push payment fraud, who respond to offers made in the adverts. Beyond outright scams, another large proportion of the adverts that consumers are exposed to constitute criminal offences under the Financial Services Markets Act 2000, either because they represent a breach of the regulatory perimeter or they constitute unauthorised financial promotions. The FCA has already bared its teeth in respect of this offending, by prosecuting finfluencers who have disseminated unlawful promotions to their followers on social media. Against this backdrop, understanding how fraudulent adverts arise—and how platforms' systems interact with evolving regulatory and criminal-liability frameworks—forms the focus of this article.

ALGORITHMIC SUSPICION AND POCA OFFENDING

To manage this risk, social media and search platforms employ algorithmic systems to identify and remove potentially fraudulent adverts (as well as to detect other types of illegal content). Indeed, as developed below, the Online Safety Act (**OSA**) now requires certain platforms to implement effective systems to perform that role. However, FT reporting has shone a light on how these systems are calibrated and managed. In particular, concerns have focused on the confidence thresholds used to classify an advert as fraudulent and trigger its automatic removal, especially where no human review is applied to validate or override the system's decisions. FT articles have noted that adverts have not been identified for removal where the algorithmic system has ascribed a 90% confidence to it constituting a scam.

The output of these systems may create criminal legal risk for employees under POCA. Where an individual, in engaging with the system, approves an advert that the system has flagged as potentially fraudulent, they may have **reasonable grounds to suspect** that the revenue generated represents the proceeds of crime. In approving the advert, or otherwise deciding to continue the commercial relationship with that advertising partner, a person may commit a money laundering offence, for example by being concerned in an arrangement for the acquisition, retention or use of criminal property. Separately, a person who designs or implements a system, knowing that it has been calibrated to accept revenue from advertising partners suspected of committing fraud (or which can be easily overridden to permit a fraudulent advert to be displayed), could also be criminally liable.

The threshold for "suspicion" is famously low. In *R v Da Silva [2006] EWCA Crim 1654*, the Court of Appeal defined suspicion as "*a possibility, which is more than fanciful, that the relevant facts exist*." In practice, this creates an uncomfortable tension for digital platforms. If an internal system identifies categories of paid advertising as potentially fraudulent, then—absent a considered basis for rejecting that determination—an employee may be taken to have reasonable grounds to suspect that the associated revenue constitutes criminal property.

CORPORATE CRIMINAL LIABILITY UNDER ECONOMIC CRIME AND CORPORATE TRANSPARENCY ACT (ECCTA)

It may prove unlikely that a UK agency would prosecute an individual in a major tech firm for applying their employer's procedures and standards, in connection with an algorithmic system. However, there is a distinct criminal litigation risk to the company itself. ECCTA has significantly extended the reach of corporate criminal liability in the UK. Companies are now criminally liable for economic crimes — including money-laundering offences under POCA — committed by their 'Senior Managers' (see below) acting within in the scope of their authority. Importantly, companies can still be prosecuted even where the individual Senior Manager who committed the offence is not. 'Senior Manager' is defined under the Act to include a person who plays a significant role in the "*making of decisions about how the whole or a substantial part of the activities of the [company] are to be managed or organised*". The test is functional, focusing on the role and responsibilities of the person, as well as the level of managerial influence they can exert, rather than their job title itself, as set out in the March 2024 Policy Paper on ECCTA. The “activities” do not need to be customer facing, but can relate to non-revenue generating functions, like compliance.

In the present context, the focal question on which liability *may* hinge is whether the design and implementation of algorithmic content moderation systems, coupled with the wider control framework that sits around them, represents a “substantial part” of a platform’s activities. However, given how central paid advertising is to platforms’ business models, coupled with how important content moderation has become, it seems highly likely that decision-making about the design and operation of such systems reaches persons who qualify as Senior Managers under the ECCTA.

THE OVERLAY OF THE OSA REGIME

A central purpose of the OSA is to identify, mitigate and manage the risks of harm from illegal content and activity. It places a suite of requirements on social media and search platforms, dependent on their size and scope. In doing so, the systems and controls needed to meet the OSA’s requirements create, if not build upon, the elements through which a theory of corporate criminal liability (as explained above) could be founded.

First, the OSA requires companies to put in place the systems to detect fraudulent, or otherwise unlawful content.

The OSA places a specific duty on Category 1 platforms (section 38) to put in place proportionate systems and processes to prevent individuals from encountering fraudulent, paid for adverts. The duty applies in respect of adverts that constitute one of the specified offences under section 40, including those under the Fraud Act and certain FSMA offences (carrying out regulated activity when not authorised and contravening the restriction on financial promotions[1]). Whilst these provisions are in force, Ofcom, tasked with enforcing the OSA, has not yet prepared a corresponding Code of Practice, as required under the Act.

However, more general duties apply to all priority illegal content (PIC), of which the above listed offences (Fraud Act, FSMA) form part. For instance, section 10 imposes a duty to take proportionate measures, relating to the design and operation of the service, to prevent individuals encountering PIC, and to effectively mitigate and manage risks of the service being used for the commission of priority offending. The corresponding Codes of Practice for these more general duties have been published. They require content moderation systems and processes designed to identify, review and assess suspected illegal content, and to subsequently remove it where it is found to be illegal. The output of those systems will produce a suspicion, if not knowledge, that certain paid-for adverts may be fraudulent, and thereby create the conditions for potential liability under POCA.

Second, the regime puts in place governance requirements that increase the risk that persons who would fall within the definition of a Senior Manager under ECCTA may have visibility of, or approve, the kind of decision making that may be at risk of affixing criminal liability under POCA.

The Codes of Practice for the general duties set out Ofcom's expectations for governance, accountability, and oversight require the company to name an individual accountable to its most senior governance body tasked to explain and justify the actions and decisions taken regarding compliance with the relevant duties. They also require, the company to prepare "*written statements of responsibilities for* ***senior managers*** *who make decisions about the management of risks having to do with illegal harm in relation to individuals in the UK".*

The Codes do not adopt ECCTA's statutory definition of a Senior Manager. Even so, the governance model they require will concentrate decision-making about illegal-content risk—including the design, calibration, and operation of fraud-detection/ad-screening systems—in identifiable senior roles. Those individuals will often satisfy ECCTA's functional test (significant decision-making over "the whole or a substantial part" of activities), particularly for large platforms. That alignment raises the likelihood that decisions and rules embedded into automated systems concerning the acceptance or removal of revenue-generating adverts flagged as suspect will be developed by persons classed as a Senior Managers for ECCTA purposes.

CONCLUSION

The combined effect of POCA, ECCTA and the OSA creates a materially heightened risk environment for digital platforms whose revenue depends on paid advertising. Algorithmic systems designed to filter unlawful adverts may themselves generate the suspicion necessary to ground money-laundering offences, while new corporate attribution rules significantly broaden the circumstances in which a company may be held criminally liable. With governance obligations under the OSA drawing senior decision-makers directly into the oversight of these systems, the legal stakes are only set to increase. Platforms will need to reassess their controls, calibration thresholds and governance structures to safely navigate this evolving landscape.

---

[1] Sections 23 and 25 FSMA respectively. Also included are various market manipulation offences, under sections 89 and 90 of the Financial Services Act 2012.

EMERGING THEMES

We anticipate a pivotal year for investigations and enforcement

Stay up to date with our latest Financial Regulation and Disputes insights

RELATED CAPABILITIES

- Financial Regulation Compliance & Investigations

MEET THE TEAM

David Rundle

Partner, London

david.rundle@bclplaw.com
+44 (0) 20 3400 4027

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.