



REPORT JUNE 2022

Fraud in the open display advertising market

Contents

1. About this research	3
2. Background & scope	3
3. Methodology	4
4. Principles	4
5. Glossary of terms	5
6. Landscape	6
6.1 Overview of open display advertising ecosystem & supply chain	6
6.2 Fraud management solutions & harm	7
7. State of the problem	9
7.1 Fraud management in the open display advertising ecosystem: findings	9
8. Threat actor personas, motivations & tactics	10
8.1 Known threat actors and tactics	10
8.2 Harm to users	13
9. Pervasiveness of fraudulent adverts	15
10. Journey mapping	18
10.1 Organising phase	19
10.2 Planning phase	19
Zirconium threat actor group planning phase example	20
Nephos7 threat actor group; fake agencies, legal entities & impacted DSP's example	20
10.3 Execution phase & harm	21
Fizzcore threat actor group execution and harm phase example	22
10.4 Exit & monetisation phase	23
Monetising with material purchases example	23
Monetising using escrow services on the dark web	24
10.5 An ongoing threat: money mules	24
10.6 Components of fraud	25
11. Preliminary regulatory considerations	26
12. Recommendations & opportunities for additional research	28
About Beruku	28

1. About this research

This research was undertaken in partnership with Which?, to inform the UK government's Online Advertising Programme consultation. This programme seeks to review the regulatory framework of paid-for online advertising to investigate apparent accountability and transparency issues across the value chain. This research contributes, in tandem, to the measures being introduced through the Online Safety Bill. It builds on rather than reinforces existing measures covered by the Online Safety Bill (OSB) [as of this publication date], this research will not include an exploration, analysis or validation of existing measures already covered in the OSB as it stands.

“Rapid technological developments have transformed the scale and complexity of online advertising leading to an increase in consumer harm”

Department for Culture Media & Sport, UK Government¹

2. Background & scope

The introduction of programmatic advertising and inflated ad budgets dedicated to digital inventory have resulted in an ecosystem with many different actors who have limited accountability and transparency.

This research excludes measures already included in the current version of OSB. Meaning the following are out of scope;

- fraudulent advertising appearing directly on search engines
- fraudulent advertising/scam ads delivered or promoted by users on a platform (user-generated content)

The objectives of this report are:

- to understand the nature of digital advertising fraud **causing harm to consumers**
- to understand the fraudsters' motivations and tactics
- to identify points of weakness within the digital advertising ecosystem that facilitate a fraudster's access, with the ultimate aim to recommend processes, policies and procedures to prevent publishing of a fraudulent ad

1 <https://techcrunch.com/2022/03/09/online-safety-bill-scam-ads/>

3. Methodology

To conduct this research, a mixed-methods approach was used. A comprehensive literature review of relevant research papers, industry reports, marketing collateral, and product documentation was followed by an exploration of dark web content by our in-house dark web and threat intelligence experts.

A set of 7 semi-structured interviews were held with fraud experts, law enforcement, and ad industry subject matter experts, each having held different roles across the advertising supply chain (for example advertiser, fraud solutions provider, etc). Each interview lasted between 45 min – 1 hour & 15 min. These conversations were guided by the following, overarching research questions:

1. How are fraudsters entering into the open ad display market?
2. What fraud controls are in place along the open display advertising value chain?
How effective are they at preventing harm to the consumer?
3. What key areas of the open display advertising ecosystem are highly responsible in preventing and detecting fraud?
4. What tactics do threat actors use to carry out their crimes?
5. What are the threat actors motivations?
6. To what extent does this harm consumers?

4. Principles

The core of this initial research seeks to answer a single question; is there widespread fraud causing harm to consumers on the open display advertising market? Given the limited timescales allotted for this research by the consultation timeline, a widespread, robust analysis and evaluation of fraud within the entirety of the open display advertising ecosystem was not possible. As such, the recommendations also include a call for additional research into the matter. The majority of literature-derived insights are sourced from publicly available material and views expressed in interviews may be indicative of individuals within an organisation rather than the organisation itself. Lastly, interviews were conducted on the basis that sources will be kept anonymous.

5. Glossary of terms

Term	Definition
Ad Injection	Visible or hidden insertion of ads into an app, web page, or other online resources without the consent of the publisher or operator
Advertiser	A company, brand, or individual who pays a third party to display ads
Cloaking	A tactic where Malvertisers implement specific fingerprints and techniques that helps them define whether or not to cloak a landing page, which is the rendering/reveal of the final landing page
DMP	Data Management Platform
DSP	Demand Service Platform
Execution	A tactic used by Malvertisers to execute malicious code typically via forceful redirects
Industry fraud	Ad fraud resulting in harm that directly or disproportionately affects the advertiser typically by manipulating viewability and impression measurements with little harm experienced by the consumer. Tactics include click farms, cookie stuffing etc.
Initial access	Initial access is the first step where the Malvertiser enters the Advertising ecosystem. Usually Malvertisers access the ad ecosystem by creating fake agencies for the purpose of establishing relationships with ad buying platforms (DSPs) or by creating fake ad creatives
Landing page	The landing page is the Malvertisers final “payload” and comes in different forms and purposes ranging from drive-by downloads, exploit kits, or investment scams, etc
Malvertising	A cyber enabled attack which relies on the ad networks and digital ads
Persistence	the step where Malvertisers persist within the ad ecosystem, ensuring their campaigns can last the longest time possible while evading detection mechanisms
PII	Personally Identifiable Information
Scam advertisements	Fake or misleading advertisements where consumers’ financial or personal information is compromised through means of social-engineering (for example eg. the consumer believes they are making a legitimate financial investment because Martin Lewis appears to promote the ad). Further examples of this are where products or services are offered which either do not exist or not at all fit for purpose
SSP	Supply Side Platform
Threat actor / malicious actor	A threat actor in the context of this work refers typically to a group of people that take part in an action that is intended to cause harm across the advertising network: Often these are referred to as Organised Crime Groups (OCGs)

6. Landscape

6.1 Overview of open display advertising ecosystem & supply chain



Figure 1: Common actors and organisation examples* within programmatic open display ecosystem (Source: Plum report)²

**Note: The logos used are examples of those types of organisations. They do not imply any indication that these specific firms are knowingly involved in fraudulent or criminal activity*

Figure 1. illustrates the most common actors within the programmatic³ open display advertising ecosystem. The role of each actor broadly falls into five categories; targeting (DMPs, DSPs), advertising advisory (media agencies, DSPs), publisher sales (publisher ad server, SSPs), verification / attribution / evaluation (measurement and verification providers, advertiser ad server), and delivery (advertiser ad server, publisher ad server).

Enabled by programmatic buying, the breadth and depth of data and cash flow throughout the digital advertising supply chain makes the ecosystem increasingly complex and opaque. The industry research validated in interviews with subject matter experts, shows this complexity drives a lack of standardisation and transparency creating a fertile ecosystem for threat actors to exploit.⁴

“The ad industry is designed to be opaque... it is designed to hide who is selling what at what price.”

An executive at leading ad fraud solutions firm

2 2019, Plum consulting, Online advertising in the UK

3 Programmatic advertising comprises 88.9% of the display advertising market in the UK and the research conducted suggests most fraud is committed within the programmatic ecosystem, therefore, the analysis is based solely on the programmatic value chain (Statista, 2020)

4 <https://www.isba.org.uk/article/time-change-and-transparency-programmatic-advertising>

The complexity of this supply chain is illustrated below in a sample lumascape:



Figure 2: Display Advertising lumascape (Source: LUMA partners⁵)

6.2 Fraud management solutions & harm

There are many different types of harm that can be caused through fraudulent advertising. They can largely be categorised into consumer harm and advertiser harm.

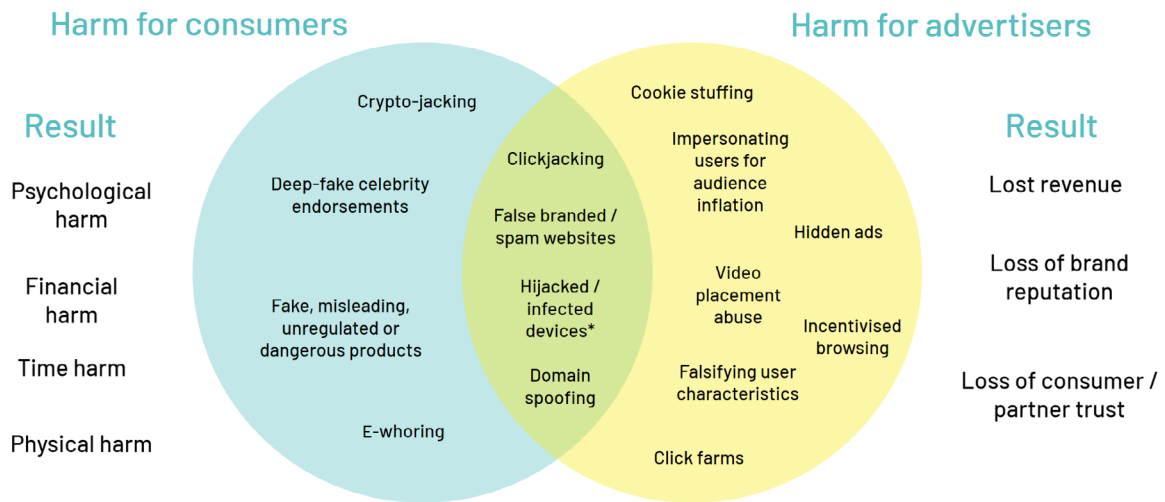


Figure 3: Breakdown of types of fraud and the allocation of harm done

* Including malware & malvertising (i.e. ads laced w/malicious code)

Within the many actors in the open display advertising market, there are fraud management solutions (eg. Confiant, Shield, DoubleVerify, IAS, Human, MOAT) and industry groups (eg. IAB, TAG) working to combat advertising fraud.

5 <https://lumapartners.com/content/lumascape/display-ad-tech-lumascape/>

The research conducted indicates that for both types of actors, their customers are the advertisers, and the type of fraud they largely seek to combat are ones that affects their customers’ bottom-line (referred to as industry fraud). Because of this, these actors primarily focus on preventing harm to the advertiser. However, some solutions do profess to focus more closely on harm to the consumer (although this appears to be a minority). One fraud management solution provider interviewed, who focuses more on consumer harm, stated their competitors’ solutions are designed to concentrate more on impression flow than creative flow, and are centred around protecting the advertiser rather than the consumer. Figure 4 outlines providers of fraud management solutions and industry groups illustrating the fraud management solutions landscape.

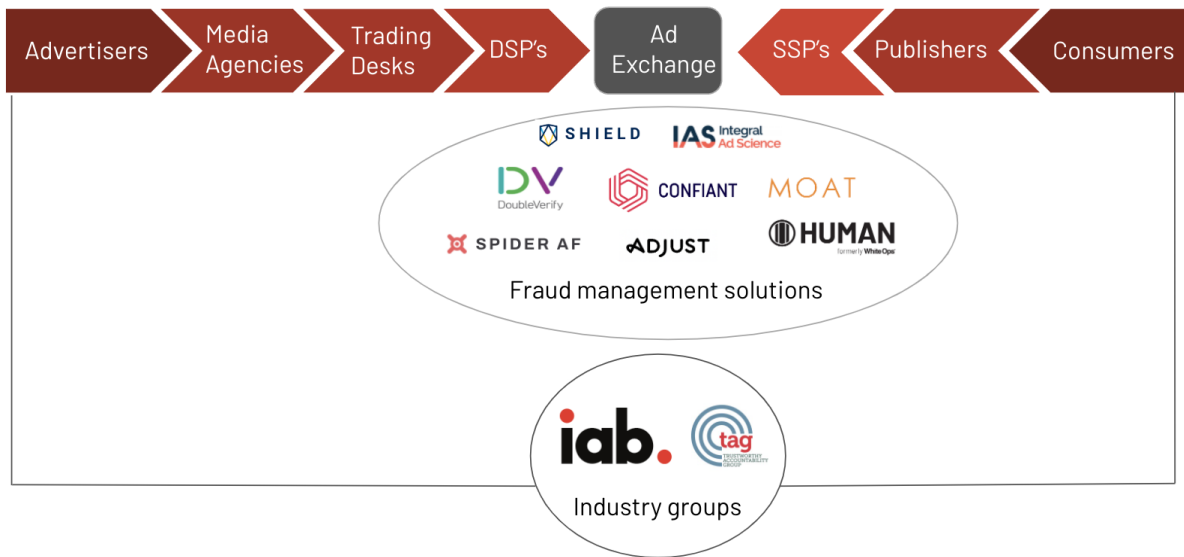


Figure 4: Fraud Management Solutions Landscape & example actors*

**Note: This is not a list of the organisations that were interviewed for this report*

“Only 1% of the digital advertising supply chain is fortified against fraud”

Industry group

7. State of the problem

The open display advertising market is a highly lucrative corner of the advertising market with approximately £88bn spent globally in 2021.⁶ Given the opaque nature of the ecosystem, limited regulation, and vast amount of capital flowing between actors, the current risk versus reward ratio of ad fraud appears to make it a highly attractive fraud vector.

As such, ad fraud that results in harm to the end consumer is rife within the professional channels of the open display advertising ecosystem. As of Q4 of 2021, an analysis conducted by Confiant revealed the number of ads considered definitively harmful to consumers had doubled compared to the same period in 2020. This was in part due to the increased popularity of cryptocurrency-related financial scams; an investigation by Confiant exposed such a scam netting over £810,000 per day from victims. The prevalence of this threat is evidenced in cryptocurrency being the second most frequently blocked category by publishers.⁷

7.1 Fraud management in the open display advertising ecosystem: findings

Collectively, a mapping of the ad fraud management landscape and an assessment of the problems as they stand draw these findings:

1. Most industry fraud management solutions focus on viewability and authenticity of measurement metrics (i.e. combatting industry fraud)
2. There are few select advertising fraud solutions that explicitly focus on the harm caused to consumers as a result of fraudulent ads, the majority focus on harm to the advertiser
3. There appears to be no mandated reporting mechanisms in place to actively gauge the scale of ad fraud harming consumers
4. The industry is bi-directional, not linear. There is demand from both advertiser and publisher ends of the marketplace to place ads in a way that generates impressions and to fill inventory in a way that generates the maximum amount of revenue, respectively. However, because advertisers remain as the sole client, all processes are optimised around creating impressions leading to a distinct lack of protection for the end consumer. This asymmetrical, decoupled marketplace creates power imbalances and a lack of transparency creating loopholes and opportunities for exploitation.
5. There is no accountability or incentive to prevent or consequence for actors in the middle of the chain to prevent malicious content being published. They still get paid even when fraudulent ads have made it to the publishing stage.

Collectively, it could be considered that current self-regulation in the form of fraud management solutions on the open display advertising ecosystem is ineffective at preventing harm to the consumer caused by fraudulent advertisements and therefore remains insufficient to continue in its current form.

6 <https://www.statista.com/statistics/276671/global-internet-advertising-expenditure-by-type/>

7 <https://www.confiant.com/maq-index>

8. Threat actor personas, motivations & tactics

Our research focused on the following threat actor types with the following objectives:^{8 9 10 11}

Type	Objective
Organised crime group	Monetisation
Hacktivist	Political influence, espionage, monetisation, disruption
Malicious insider	Disruption, monetisation
Nation state	Political influence, espionage

The research conducted shows that the majority of fraudulent advertising resulting in direct harm to the consumer, **is carried out primarily by organised criminal groups who are financially motivated.**¹² These are malicious entities responsible for organising and executing attacks that compromise the security of individuals and organisations.¹³

While the highly technical and capable opportunist or individual could potentially carry out some level of attacks, they are still reliant on infrastructure and resources established by other parties in the criminal chain¹⁴.

8.1 Known threat actors and tactics

In the research conducted, a variety of fraudulent threat actors were identified. Amongst the best articulated were from a cyber security and counter fraud service provider, Confiant. Seven prominent organised cyber-criminal operations inflicting large scale ad fraud campaigns using a variety of tactics.¹⁵ These were identified as:

Zirconium

A threat actor group responsible for large scale malvertising campaigns using tactics such as forced redirects, fake ad agencies and fingerprinting. In 2017, it was estimated that this group served in the order of 1 billion ad impressions, reaching 62% of ad-monetized websites on a weekly basis. This was largely made possible through the establishment of fraudulent ad agencies who successfully established direct business relationships with as many as 16 ad platforms.¹⁶ The user harm from this model was resource hijacking as well as financial loss.

eGobbler

A threat actor group responsible for large scale malvertising campaigns perpetrated using a variety of tactics including web exploit kits. In 2019, between August 1st and September 23rd, eGobbler

8 <https://www.redlegg.com/blog/cyber-threat-actor-types>

9 <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-5-counteracting-threats>

10 <https://home.sophos.com/en-us/security-news/2021/what-is-a-threat-actor>

11 <https://www.nicybersecuritycentre.gov.uk/cyber-threats>

12 Interviews: Law enforcement, industry group, leading fraud management solutions provider

13 <https://www.confiant.com/resources/blog/fizzcore-threat-actors>

14 Interviews: Law enforcement, industry group, leading fraud management solutions provider

15 <https://matrix.confiant.com/#matrix>

16 <https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85>

hijacked roughly 1.16 billion ad impressions to redirect potential victims to malicious payloads (re. malware).¹⁷

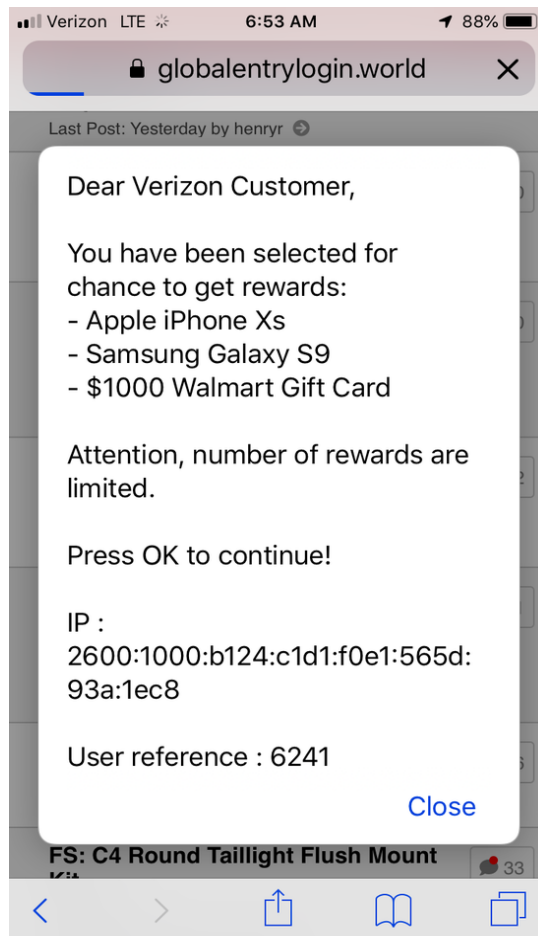


Figure 5: Example of eGobbler delivery tactic using coercive clicking strategy¹⁸

Scamclub

A threat actor group responsible for large scale malvertising campaigns mainly using tactics such as forced redirections, to scams that offer “prizes” to the victim such as gift cards or iPhones with the ultimate goal of stealing personal data from the victim. ScamClub typically deploys a strategy of bombardment, flooding the ad tech ecosystem with malicious demand knowing that while the majority of the demand will be blocked, a small percentage is likely to slip through. Between December 2020 and February 2021, it was estimated that ScamClub delivered over 50 million malicious impressions,¹⁹ resulting in financial losses to users.

17 <https://www.confiant.com/resources/news/egobbler-malvertiser-uses-webkit-exploit-to-infect-over-1-billion-ads>

18 <https://blog.confiant.com/massive-egobbler-malvertising-campaign-leverages-chrome-vulnerability-to-target-ios-users-a534b95a037f>

19 <https://blog.confiant.com/malvertiser-scramclub-bypasses-iframe-sandboxing-with-postmessage-shenanigans-cve-2021-1801-1c998378bfba>

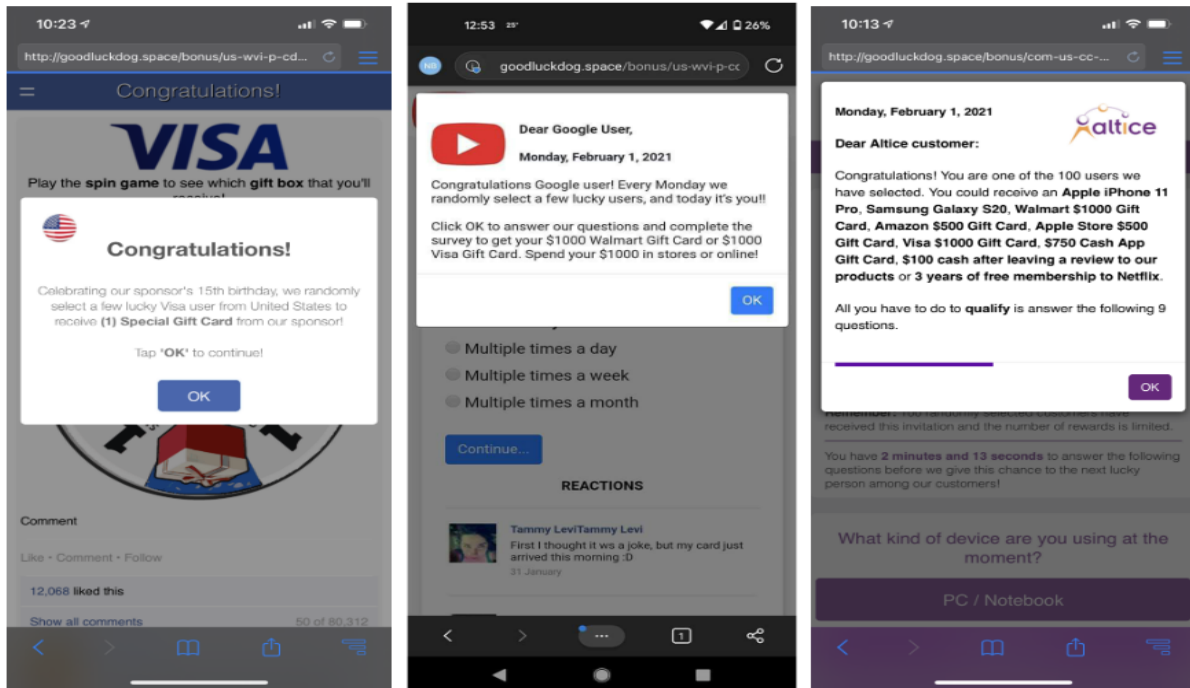


Figure 6: Example of Scamclub malvertising campaigns²⁰

DCCBoost

A threat actor group responsible for large scale malvertising campaigns mainly using tactics such as fake ad creatives for scam lottery sites, forced redirects to said sites, fingerprinting, all underpinned by JavaScript exploitation. Between December 2020 and January 2021, it is estimated that DCCBoost served over 25 million malicious ads using such tactics.²¹

TAG Barnakle

A threat actor group responsible for large scale malvertising campaigns perpetrated via a mass compromise of Revive Adservers. This allows the group access to publisher inventory without spending any money or going through QA checks before running ad campaigns. Typically, the ad creative is clickbait which redirects the user to install malicious software under the guise of a flash or operating software update, resulting in the user losing resources and a financial loss. It is estimated that TAG Barnakle have compromised 60 ad servers in total.²²

Yosec

A threat actor group responsible for large scale malvertising campaigns primarily using tactics such as fake creatives, fake ad agencies, and forced redirects. Yosec is a threat actor group that relies heavily on forced redirects at a moment when many other threat actor groups turn in favour of heavily cloaked clickbait.²³ These threat actor's tactics seek to get users to install malware which hijacks the users resource and also can result in direct financial loss to the user.

²⁰ <https://blog.confiant.com/malvertiser-scamclub-bypasses-iframe-sandboxing-with-postmessage-shenanigans-cve-2021-1801-1c998378bfba>

²¹ <https://blog.confiant.com/persistent-malvertising-attacker-dccboost-raged-as-the-year-faded-4d09340cd3f5>

²² <https://blog.confiant.com/tag-barnakle-the-malvertiser-that-hacks-revive-ad-servers-redirects-victims-to-malware-50cdc57435b1>

²³ <https://blog.confiant.com/malvertising-threat-actor-yosec-exploits-browser-bugs-to-push-malware-cve-2021-1765-3040dd3c4af1>

Fizzcore

A threat actor group responsible for large scale malvertising campaigns recently focusing on publishing fake celebrity-endorsed bitcoin scam ads on popular European new sites. Techniques used to spread these ads include fake ad creative, website targeting, a variety of cloaking techniques, and use of reputable ad servers. In 2020, a Fizzcore perpetrated bitcoin scam netted approximately \$1 million (approx. £810,000) in one day.²⁴

These threat actors typically follow a linear process of initial access, execution, persistence, browser exploitation, credential access, cloaking, defence evasion, landing page, and impact.²⁵



Figure 7: Malvertising kill chain

Within each of these steps, threat actors use a variety of tactics aptly categorised and mapped in fraud solutions provider Confiant’s Malvertising Attack Matrix

8.2 Harm to users

The most common ad fraud tactics used that result in harm to the end consumer broadly fall within five categories:

High level category	Tactic	Result
Malicious clickbait	Malware infection	Monetisation
Hacktivist	Malware infection Redirection to scam products or services	Political influence, espionage, monetisation, disruption
Malicious insider	False/misleading information advertised	Direct financial loss & compromised data
Nation state	False/misleading information advertised, malware infection	Compromised device & data Direct Financial loss
Fake software updates	Malware infection	Compromised device & data

24 <https://blog.confiant.com/fake-celebrity-endorsed-scams-abuses-ad-tech-to-net-1m-in-one-day-ffe330258e3c>

25 <https://blog.confiant.com/profiling-hackers-using-the-malvertising-attack-matrix-by-confiant-9341838887b7>

In cases where the result is a compromised device or data, victims are often faced with varying degrees of both psychological and financial harm. Disinfecting the current device or purchasing an entirely new device is often costly and time consuming, and even once the device has been fixed or replaced, threat actors oftentimes still have hold of personal information including contacts and login details held on browser keychains. In cases where individuals have fallen victim to criminal scams, whether they purchased a fake product or invested in a scam investment opportunity, the result is also both financial harm and psychological harm. Financial harm is an obvious result as victims have handed over their banking details to criminals and are largely dependent on their banks’ fraud refund policies for any recourse.

Psychological harm may stem from large amounts of capital lost to threat actors or simply from embarrassment which may also contribute to a hesitancy to report the incident. Furthermore, research conducted by Which? into the wellbeing of scam victims found that being a victim of a scam is associated with lower levels of life satisfaction, lower levels of happiness, and higher levels of anxiety- emphasising that oftentimes the psychological harm outlasts the financial.²⁶

The term ‘malvertising’ encompasses 4 of the 5 categories outlined above; malicious clickbait, forced redirects, fake ad servers, and fake software updates. Outside of the US, the UK and Canada saw the highest rate of malvertising victims by country.²⁷ This, in part, is driven by a shared language between the most affected countries as threat actors can repurpose creative copy between nations with a shared language.

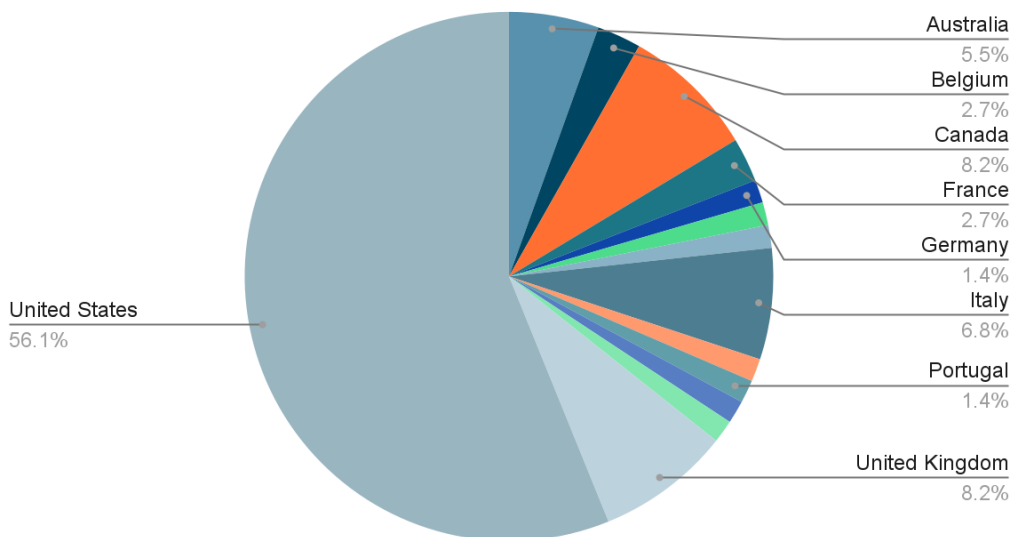


Figure 8: Malvertising Victims by country as observed by Malwarebytes LABs’ Threat Intelligence Team in 2021 via tracking of threat actor group activity²⁸

Source: *MalwareBytes LABS*

26 <https://www.which.co.uk/policy/digital/8403/scams-and-subjective-wellbeing>

27 *MalwareBytes LABS, Malvertising campaigns come back in full swing (2021)*

28 *MalwareBytes LABS, Malvertising campaigns come back in full swing (2021)*

9. Pervasiveness of fraudulent adverts

The prevalence of fraudulent advertisements is widespread. For example, the research conducted uncovered the same fraudulent ads across highly-trafficked, mainstream publishing sites such as Reuters, Fox News, and The Daily Mail.

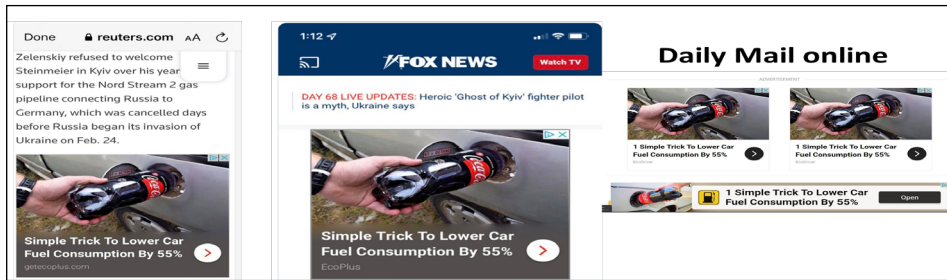


Figure 9: Examples of fraudulent ads across mainstream sites promoting a fake product causing harm to the consumer

Trends in advertising fraud identified by a leading fraud management solutions provider note the rising popularity of heavily cloaked clickbait as a means for committing malvertising (as pictured above) and a decline in forced redirects and pop ups resulting from the maturation of ad tech security over the last four years.²⁹

Tracing the origins of these fraudulent advertisements revealed an advertiser based in Lithuania (UAB Commerce Core) that had previously been the subject of a complaint to the ASA for false and misleading advertising exactly one year prior. This exemplifies the questionable efficacy of self-regulation occurring within the open display advertising supply chain. It could be hypothesised that the ruling had limited to no impact to the advertiser, which could potentially be in part because of the extraterritoriality challenges faced.

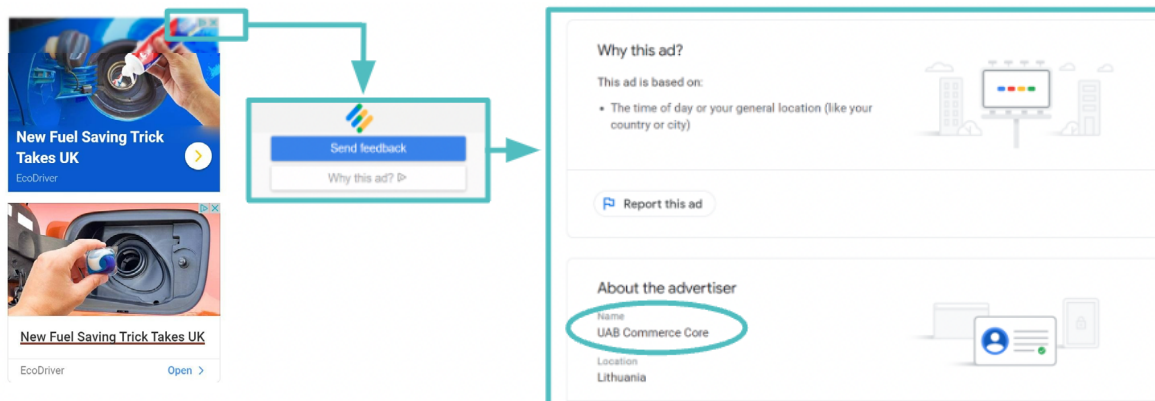


Figure 10: UAB Commerce Core fraudulent ad

²⁹ <https://blog.confiant.com/malvertising-threat-actor-yosec-exploits-browser-bugs-to-push-malware-cve-2021-1765-3040dd3c4af1>

UAB Commerce core identified as the advertiser, based in Lithuania adding further to the challenge of extraterritoriality. This was traced to a previous ruling on a different advertisement by the same advertiser by the ASA as seen in Figure 11.

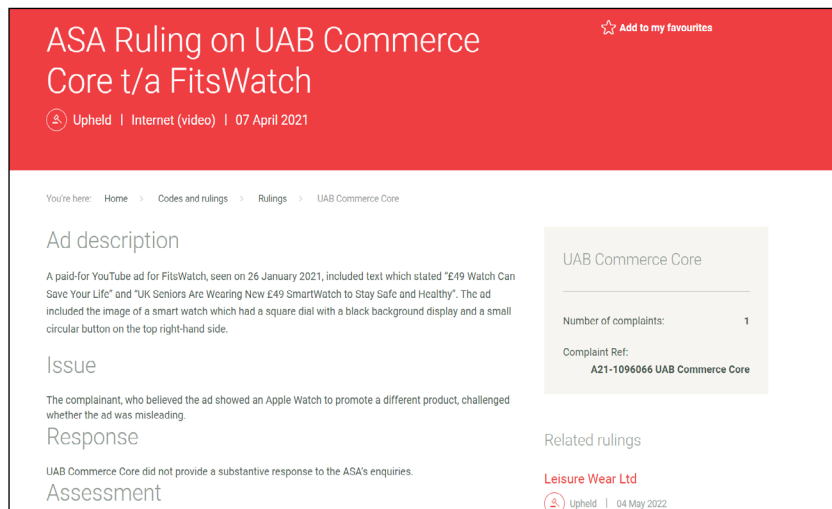


Figure 11: UAB Commerce Core published ruling by the ASA³⁰

Ultimately, an investigation conducted by media outlet, Snopes, professes to have contacted EcoPlus (the brand in the product pictured) only to be told that these ads did not belong to them. This chain of events demonstrates the nefarious nature of a widely-publicised ad that reaches far beyond simple clickbait and peddling of a fake product to exploit the sensitivities of consumers attempting to navigate a cost of living crisis only to be faced with malvertising threats.³¹

EcoPlus Ad Shows Coke Poured into Car’s Gas Tank

We reached out to a company spokesperson to ask about this very bad idea that was advertised as a "simple trick to lower car fuel consumption by 55%."

By Jordan Liles
Published 4 May 2022

Figure 12: Investigation by Snopes³² into the fraudulent ads in question

30 <https://www.asa.org.uk/rulings/uab-commerce-core-a21-1096066-uab-commerce-core.html>

31 <https://www.independent.co.uk/money/scam-fraud-tricks-what-how-help-b2086012.html>

32 <https://www.snopes.com/news/2022/05/04/ecoplus-coke-gas-tank/>

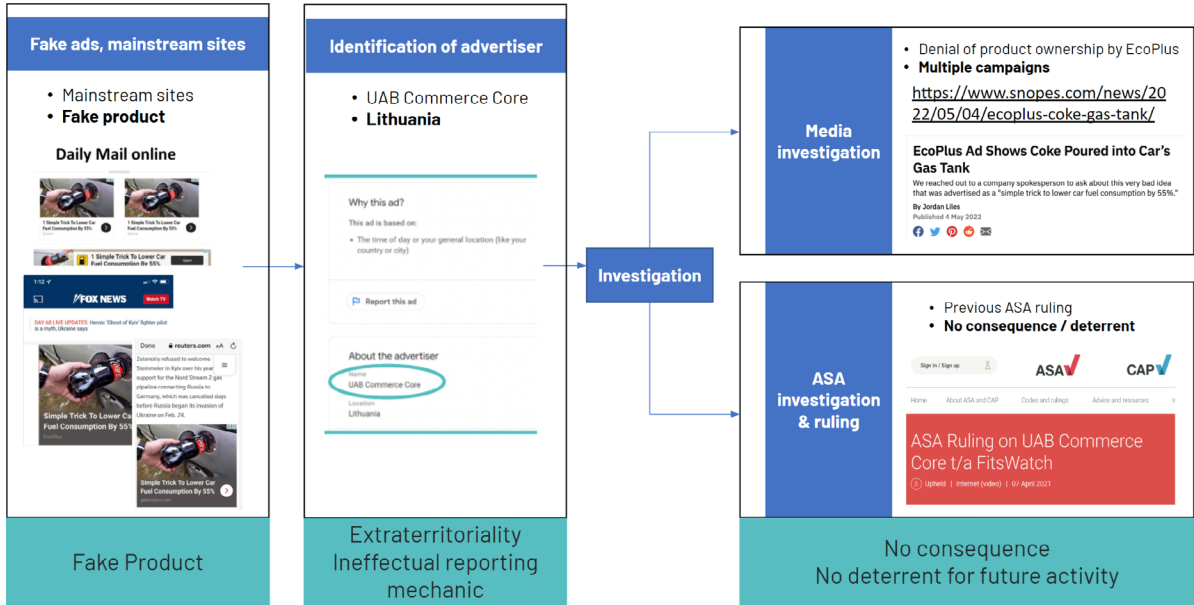


Figure 13: Summary flow of the UAB Commerce Core example

10. Journey mapping

In order to better understand the fraud journey, a process using criminal journey mapping was undertaken. This mapping was informed by the interviews conducted for this report, open source research, the “Malvertising Attack Chain”³³ and internal subject matter expertise on digitally enabled and digitally dependent crime and fraud. By visually mapping these criminal journeys, it is possible to better identify the entry and exit points within the criminal process. In turn, this exercise serves to contextualise considerations and recommendations for ongoing and future policy initiatives as well as to inform the development of awareness campaigns and measures to detect and deter such criminality.

Organising phase

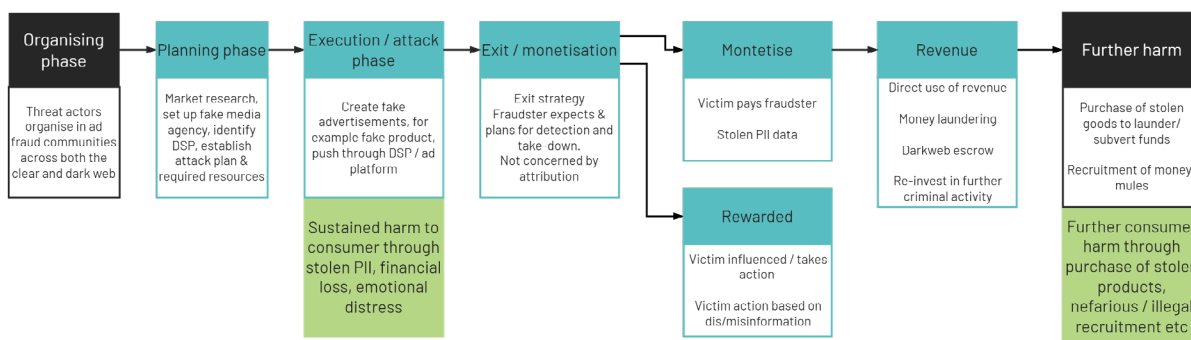


Figure 14: Summary flow of threat actor journey

33 The Malvertising Attack Matrix has been created by Confiant and is built following the [MITRE ATT&CK Framework](#) which is widely recognised and utilised across the cyber security domain. Confiant states that “it is a way to communicate actionable threat intelligence to entities that are outside of the ad tech world and give them real, credible information on threats to their digital security.” (maxtrix.confiant.com)

10.1 Organising phase

Threat actors organise in ad fraud communities across both the clear and dark web. A mapping of these communities conducted by Richet revealed four categories of communities (see Figure 15).³⁴

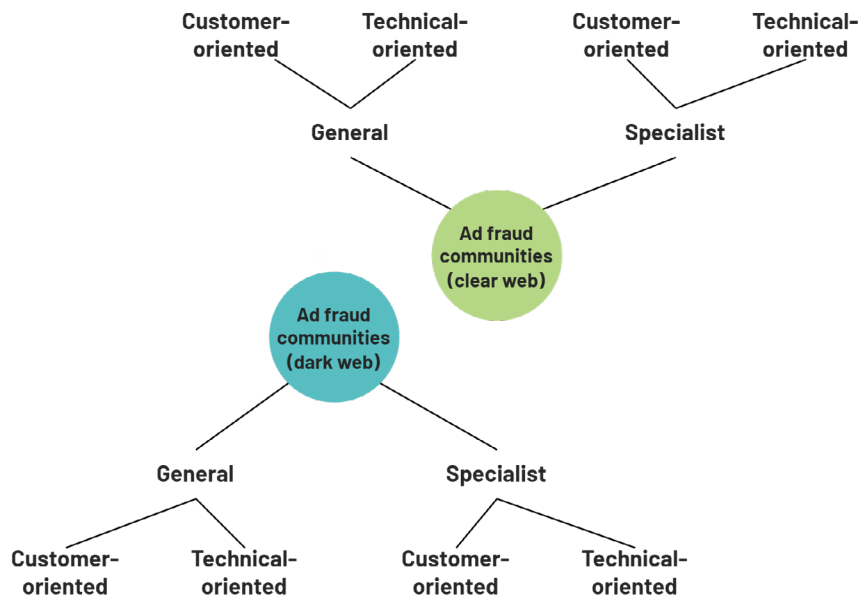


Figure 15 : Ad fraud community categories

Communities that often foster established threat actors interested in money-laundering, malware writers, and bot masters tend to be more generalist, while specialist communities focus on a certain type of ad fraud and aim to attract a very specific, expert ad-fraud service provider. Richet's research suggests that the majority of fraudulent advertising attacks that result in harm to the end consumer such as fake pharmaceuticals, gambling and investment scams, originate in general, customer-oriented communities. It is important to understand that these communities are sophisticated marketplaces with structured, formal sales cycles. Reminiscent of open-source software communities of the past two decades, these communities operate according to an ethos that innovation is existential and customer-service is paramount to keeping threat actor clients returning.

10.2 Planning phase

In this preparatory planning phase the fraudsters make a conscious decision to undertake a crime, in this instance advertising fraud. At the start of this stage they have not always decided which type of approach they will use, therefore they gather intel and undertake market research (which can also happen in peer to peer channels in criminal forums). Armed with this data they start reconnaissance to determine weak or opportunistic points of entry. In this stage of the journey fraudsters identify the appropriate vector to exploit and gain entry. They establish an attack plan and it is often at this stage they consider what resources they may need, ie. do they have them in house or do they need to outsource or partner with other fraudsters. Once these decisions have been made they commence their attacks.

³⁴ Richet, Jean-Loup. *How Cybercriminal Communities Grow & Change: An investigation of ad-fraud communities* (2021)

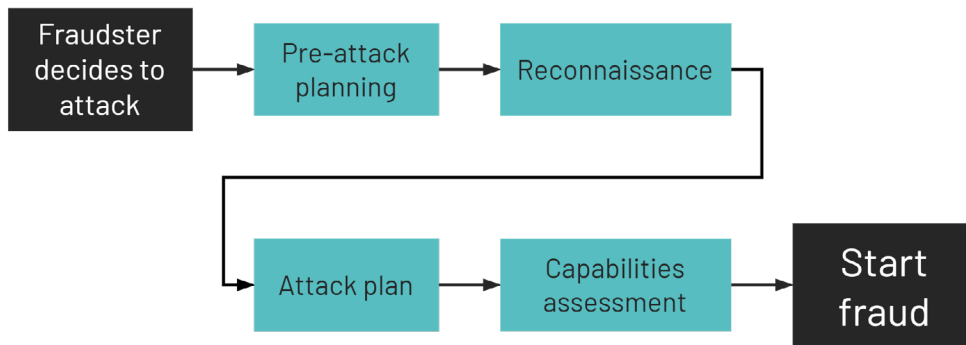


Figure 16: Fraudulent ad planning phase

Zirconium threat actor group planning phase example

In 2017, the threat actor group Zirconium deployed a strategy of establishing several fake ad agencies, replicating the ‘small business’ ad agency style in order to be embraced by the industry. Of the 28 fake agencies established, 20 successfully entered the digital advertising ecosystem. The other eight agencies remained dormant so as to amass reputation by means of accruing a social media following and company history. Once an agency was exposed as fraudulent and consequently banned, 1–3 more agencies would pop up to replace it.³⁵

Agency	Site / Ad serving domain	First seen	Last seen	Lifespan (days)
SionicMedia	sionicmedia.com	12/12/2016	12/20/2017	373
Clickopon	clickopon.com	1/27/2017	3/25/2017	57
Alliance4Media	alliance4media.com	2/20/2017	6/29/2017	129
PlaiMedia	plaiimedia.com	2/22/2017	3/10/2017	16
ChacoMedia	chacomedia.com	3/15/2017	6/9/2017	82
IndiaOnClick	indiaonclick.com	3/15/2017	10/3/2017	202
BeginAds	beginads.com	3/22/2017	12/21/2017	274
TradersBrokers	tradersbrokers.com	4/19/2017	12/21/2017	245
PowerTradeProfit	powertradeprofit.com	5/23/2017	5/23/2017	0
AxiaTraders	axiatraders.com	6/9/2017	6/23/2017	14
MediaParade	mediaparade.net	6/26/2017	12/19/2017	176
HoffmanBroker	hoffmanbroker.com	6/29/2017	7/3/2017	4
BuzzClicks	buzzclicks.com	8/7/2017	12/20/2017	135
Face2Trade	face2trade.com	8/9/2017	9/21/2017	43
MediaBarterExchange	mediabarterexchange.com	9/5/2017	12/21/2017	107
KSMarlet	ksmarlet.com	9/21/2017	11/23/2017	63
DeshMedia	deshmedia.com	10/3/2017	12/20/2017	78
ElixMedia	elixmedia.com	10/11/2017	12/21/2017	71
KobeNetwork	kobenetwork.com	11/5/2017	12/19/2017	43
AdTekMedia	adtekmedia.com	12/14/2017	12/20/2017	5
MinistryOfAds	ministryofads.com	n/a	n/a	n/a
BigSharkMedia	bigsharkmedia.com	n/a	n/a	n/a
GrandonMedia	grandonmedia.com	n/a	n/a	n/a
AdsFlame	adsflame.com	n/a	n/a	n/a

Figure 17: Example of Zirconium’s fake ad agencies³⁶

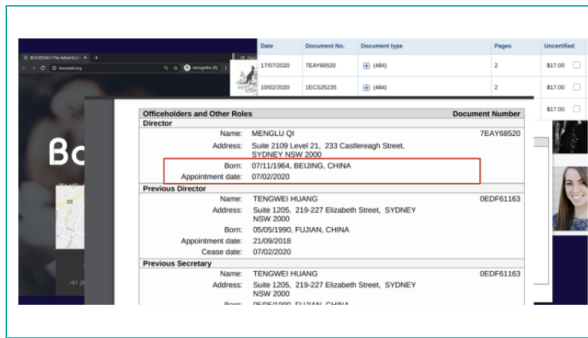
Nephos7 threat actor group; fake agencies, legal entities & impacted DSP’s example

In 2021, an investigation by Confiant uncovered a network of fake ad agencies established as legal entities by prominent threat actor Nephos7. These entities were incorporated across the US and Europe, allowing for access and connection to prominent DSP’s that would ultimately serve fraudulent ads to US and European-based users. However, this investigation later revealed the directors of these entities to be predominantly based in China. These entities were set up strategically en masse so once their fraudulent activity was exposed and they were permanently banned from the impacted DSP, they could re-enter the ecosystem as a new entity.³⁷

35 <https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85>

36 <https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85>

37 <https://blog.confiant.com/malvertising-made-in-china-f5081521b3f0>



Company name	Incorporated in	Company site	Date first seen	Date last seen
Wooden Ads	Australia	https://www.woodenads[.]com/	January 2020	November 2020
Signal Ads	USA (Colorado)	https://signal-ads[.]com/	June 2020	June 2020
Adside	USA (Colorado)	http://adsige[.]com/	June 2020	June 2020
Boostad	Australia	https://boostad[.]org/	August 2020	October 2020
WithinPlus	Canada	https://withinplus[.]com	August 2020	November 2020
Ideads	United Kingdom	https://ideads[.]org/	August 2020	September 2020
AdsCompanion	United Kingdom	http://adscompanion[.]com	August 2020	September 2020
Lindause	Hong Kong	http://lindause[.]net/	October 2020	October 2020
Link Ads LTD	United Kingdom	http://linkads[.]org/	November 2020	November 2020
AdSuccess	United Kingdom	http://www.adsuccess[.]org/	N/A	N/A
AdNic	United Kingdom	http://adnic[.]net/	N/A	N/A
AdBooming	United Kingdom	http://www.adbooming[.]com/	N/A	N/A
Betenshads	United Kingdom	http://www.betenshads[.]com/	N/A	N/A
Invechads	United Kingdom	http://www.invechads[.]com/	N/A	N/A
Reyouads	United Kingdom	http://www.reyouads[.]com/	N/A	N/A
DizzyFew	United Kingdom	http://dizzyfew[.]net/	N/A	N/A
Addigitization	United Kingdom	https://addigitization[.]com/	N/A	N/A
BuffetAds	United Kingdom	https://www.buffetads[.]com	N/A	N/A

Figure 18: List of nefarious agency entities incorporated in western nations with China-based Director's³⁸

10.3 Execution phase & harm

In this phase, the criminal moves forward with their attack. Creating in this instance their fake advertisements, these are then weaponised via “clickbait” type offers. These may proffer high rewards and/or “quick fix solutions” to typical real life problems, often illegitimately presented as being endorsed by a known or respected source. In some instances and platforms, dependent upon the nature of the expected audience, the material is sometimes more salacious in nature. In the earlier planning phase the attacker will have decided the type of attack based in part on their capabilities, risk appetite and monetisation targets.

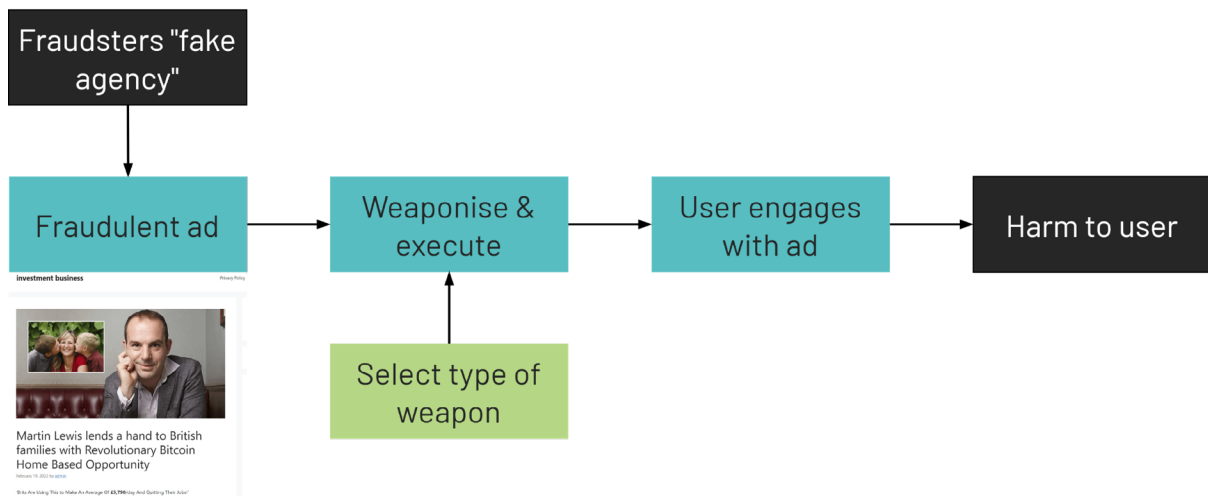


Figure 19: Attack phase

Fizzcore threat actor group execution and harm phase example

In 2021, Confiant uncovered a large-scale attack targeting European nations operated by the Fizzcore threat actor group. This scam involved photoshopped celebrities touting the profitability of a bitcoin investment scam. Patterns in campaign properties led Confiant to identify the scam as perpetrated by Fizzcore. The attack targeted both a DSP and SSP and affected 5 European nations all to varying degrees:³⁹

- Great Britain: 31%
- Netherlands: 27%
- Switzerland: 19%
- Germany: 19%
- Austria: 2%

Confiant outlined Fizzcore's strategy in three steps:

- 1. FizzCore distributes ad creatives containing shocking imagery to popular news sites in Europe, showcasing a fake photo of an injured celebrity. Because the image plays on human emotion, these creatives drive a very high click-through rate.**
- 2. After clicking the ad, the user is taken to a fake news article that acts as a pre-sale landing page for the scam. This page details how the celebrity recommends a bitcoin investment, encouraging the user to click once more into the bitcoin landing page.**
- 3. Users submit their contact information on the bitcoin landing page and receive a phone call from a salesperson. They falsely explain how the investment will provide returns to the user. The user is often a retired person who loses their pension by sending wire transfers for hundreds of thousands of dollars and receiving nothing in return.⁴⁰**

39 <https://www.confiant.com/blogs/security-research/fizzcore-style-fake-celebrity-endorsed-bitcoin-scam-targeting-europe>

40 <https://www.confiant.com/resources/blog/fizzcore-threat-actors>

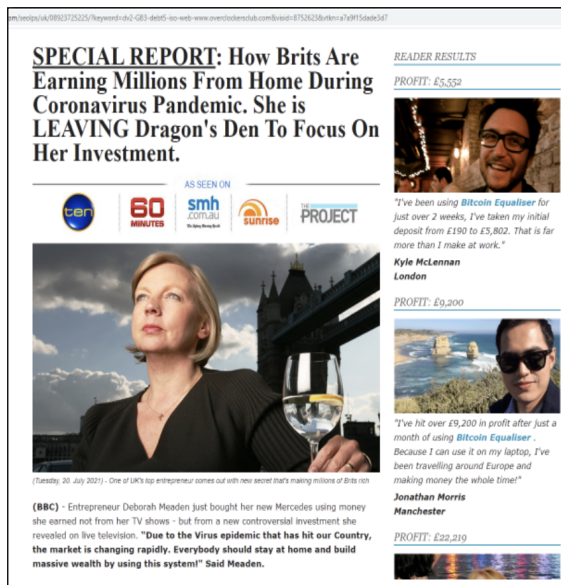


Figure 20: Scam ad creative used by Fizzcore⁴¹

10.4 Exit & monetisation phase

At this point the attacker seeks to implement their exit strategy. Hiding tracks is a part of their strategy and they deploy a range of countermeasures online through to offline routes which they use to obtain tangible assets including, but not limited to cash.

They then go on to monetise their attacks and find ways to turn virtual or fiat currencies into a range of laundered assets.⁴² It was also learned that in this type of fraud, the victim can incur harm beyond the first fraudulent event. Continued misuse of stolen PII and identity attributes occur as they are often re-sold on the darkweb and underground forums for reuse.

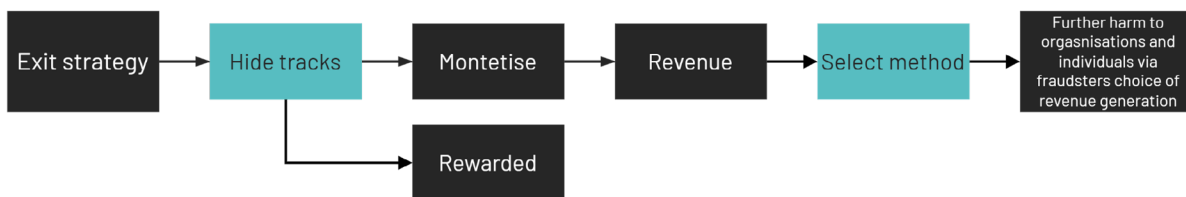


Figure 21: Fraudulent ad exit/monetisation phase

Monetising with material purchases example

In instances where threat actors monetise using cryptocurrency, a common tactic to extract capital from this (oftentimes highly-volatile) ecosystem, is to purchase tangible products using the cryptocurrency. Such products are typically popular technology products with holding a consistent and easily verifiable value. Oftentimes the purchased products are stolen and resold on the dark web or on the street for further profit.

41 <https://www.confiant.com/blogs/security-research/fizzcore-style-fake-celebrity-endorsed-bitcoin-scam-targeting-europe>

42 <https://www.nationalcrimeagency.gov.uk/news/east-london-dj-ordered-to-give-up-nightclub-equipment-with-suspected-links-to-cyber-fraud>

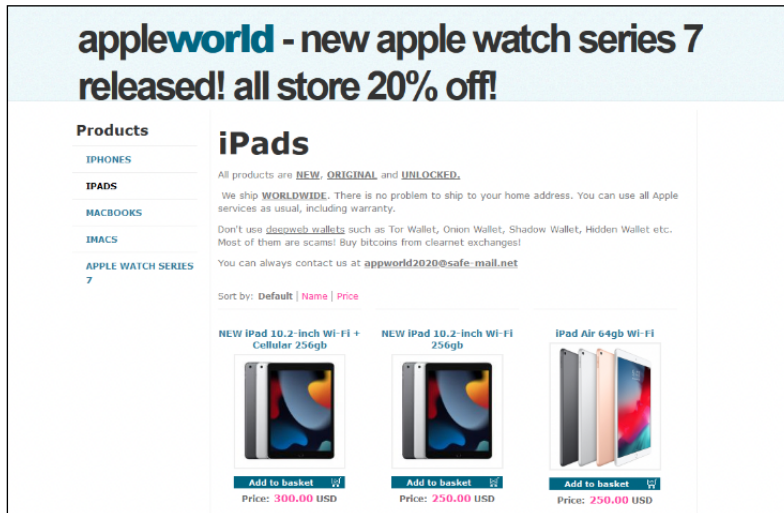


Figure 22: Example of monetising with apple watch/iPads*
**this is just one example of many*

Monetising using escrow services on the dark web

In order to monetise, threat actor groups may also utilise an escrow service offered on the dark web to help manage and obfuscate funds.

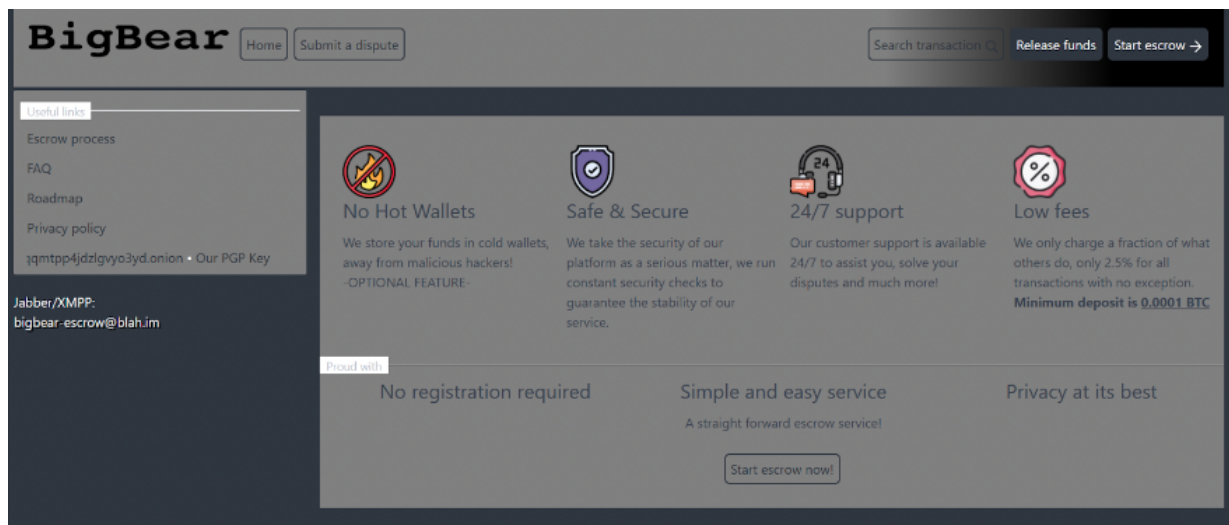


Figure 23: Example of an escrow service available on the dark web*
** this is just one example of many*

10.5 An ongoing threat: money mules

The recruitment and employment of money mules is a process both facilitated by malicious adverts and a monetisation tactic which allows threat actors to launder and withdraw their money from legitimate accounts. Money mules are often recruited by way of pop-up advertisements for seemingly legitimate job offers often published through nefarious means.⁴³

43 <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>

10.6 Components of fraud

The dark web contains a variety of different offerings by and for organised criminal groups to commit advertising fraud. Botnets are a common offer providing the threat actor access to a group of internet connected devices that have been compromised previously by an attacker. Each compromised device will have a bot installed on it in addition to other possible malware.⁴⁴ Recent techniques uncovered on ad fraud communities include tips on how to dynamically rotate IP addresses using machine learning as part of an “intelligent botnet” that is capable of committing more sophisticated ad fraud.⁴⁵

44 <https://www.cloudflare.com/en-gb/learning/bots/what-is-ad-fraud/>

45 Richet, Jean-Loup. *How Cybercriminal Communities Grow & Change: An investigation of ad-fraud communities* (2021)

11. Preliminary regulatory considerations

There is an option to regulate but at the outset, appointed regulator(s) must incentivise and work alongside the industry. It should be considered that regulators will need to learn about a rapidly dynamic environment subject to evolving sophisticated criminal tactics and techniques. Therefore, cross supply chain collaboration will be essential to the efficacy of regulation.

Adopting fraud management practices across the totality of the open display advertising value chain is a central element underpinning all regulatory recommendations. This is predicated on the research evidencing the innovative, sophisticated, and persistent nature of threat actors. As criminals will shift their tactics to exploit gaps across the digital advertising supply chain, counter fraud controls, which can be a combination of tools and processes, should be deployed across all actors in the supply chain ensuring that the focus is not on a single actor.

Suggested initiatives:

- Added transparency throughout the chain will be critical to deter malicious activity with the ability to track data throughout the pipeline to identify the buyer, DSP, SSP etc. and hold the industry and individuals to account with consequences.
 - Transparency initiatives may take the form of a reporting mechanism adopted by DSP's as a prerequisite to accessing large ad exchanges. Reports may detail agency clientele, location of agency (i.e. country of entity incorporation), length of partnership, and a high-level overview of common campaign parameters (perhaps to act as a 'trend indicator' and inform future QA practices)
 - These reports could potentially function on a grading 'scale' indicating the quality of a DSP based on their agency-relations
- Counter fraud controls, which can be a combination of tools and processes, should be deployed across all actors in the supply chain rather than focus on a single actor
- Threat intelligence sharing and fraud alerting as well as sharing of "detection and mitigation playbooks" should be implemented throughout the chain
- Identify/create/appoint regulator(s) to incentivise, cascade and hold accountability for new initiatives across the chain
- Regulatory initiatives should seek to support *legitimate* actors across the digital advertising supply chain rather than alienate or punish them in order to generate an appetite for proactive participation
- A firm regulatory stance incentivising actors throughout the chain to implement fraud management processes that protect consumers will be required. This may take the form of accreditation or certification and an accompanying kite mark/trust list which will validate and publicise legitimate actors
 - Accreditation will mandate robust information-sharing requirements (for example evidence of established data sharing practices, fortifying the integrity of data flows, and required reporting practices)
 - Suggest accreditation function as a prerequisite for accessing the ecosystems largest DSP's, ad exchanges, and highly-trafficked publisher sites; thus, responsabilisation and securing both ends of the value chain

- The appointed regulator must act in a mediating capacity so as to establish joint standards across all actors in the supply chain
- The regulator(s) should seek to ensure there are the appropriate reporting and data sharing channels and that they are being used consistently and legitimately
- The regulator(s) should support the establishment of an ombudsman function
- The regulator(s) should support threat intelligence and information sharing across ad network participants
- The regulator(s) should create a clear pathway to reporting crimes, which must be appropriately resourced to support the consumer, ad network stakeholders and whistleblowers

12. Recommendations & opportunities for additional research

A core challenge in addressing the research question(s) was understanding the scale and the impact of the problem of advertising fraud harming consumers. This challenge stems from an absence of reporting on fraud levels by actors throughout the open display advertising supply chain. Without an expectation to report or mechanism by which to report, actors within the supply chain appear to have little accountability and harm thereby falling on the consumer. This appears to be a clear gap in the ecosystem, and should legislation or regulation be implemented, it must be supported by reporting structures and mechanisms and upheld by regulatory bodies. There must also be the requisite scale of law enforcement and prosecution support alongside any legislation and regulation to be able to deal with the reported fraud.

An important next step in this research will entail a thorough investigation of both the scale and scope of this issue.

The following recommendations are suggested for future research and next steps:

- Additional interviews with actors across the supply chain such as DSP's, SSP's, and Ad Exchanges to understand their perception of consumer-harming ad fraud and the processes they have in place to combat it
- Interviews with the victims of this specific type of fraud
- A review of current legislation and frameworks from other countries in order to understand their legislative, regulatory frameworks and general landscape of consumer harming ad fraud
- An assessment of UK prosecutory options for such offences and a review to assess the volumes and outcomes of historic prosecutions for said offences
- Undertaking a mapping exercise and impact assessment to identify the geographic regions where organised crime group infrastructure and resources are most established and influential

About Beruku

Beruku operates at the cutting-edge of the digital market-place, supporting investors, policymakers, providers and consumers with digital trust, identity and personal data challenges.

Beruku are experts in digital identity, biometrics, cyber security, digital forensics and digital fraud.

www.beruku.com

Which?

Which?, 2 Marylebone Road,
London NW1 4DF
Phone +44 (0)20 7770 7000
Fax +44 (0)20 7770 7600