World of Scams

The Fraud Problem at the Heart of Online Advertising

CANADIAN ANTI-MONOPOLY PROJECT

www.antimonopoly.ca

About CAMP

The Canadian Anti-Monopoly Project (CAMP) is a think tank dedicated to addressing the issue of monopoly power in Canada and around the world. CAMP produces research and advocates for policy to make the Canadian economy more fair, free, and democratic.

Cover page image: Clark Van Der Beken

January 2026

Table of Contents

Executive Summary **4**

Introduction **6**

Advertising Technologies and Scams **8**

Ad Fraud **9**

Impersonation scams **11**

Malvertising **13**

Search Engine Optimization Poisoning 13

Fingerprinting and target acquisition 14

Chameleon Ads 15

Generative AI and The Future of Scams **15**

Uninterested Stewards, Dominant Players and the Proliferation of Scams **17**

Who Pays for Scams? **21**

Existing and Potential Regulatory Interventions **22**

Assigning Responsibility **23**

Creating a Duty of Care 23

Attribution of Liability 24

Information and Transparency **26**

Intelligence Sharing 26

Ad Libraries and API Access 27

Advertiser Verification and Know-Your-Customer Laws 28

Content Moderation **30**

Notice and Takedown and Trusted Flaggers 30

Data Restrictions **31**

Addressing the Monopoly Problem at the Core of Online Advertising **32**

What a Canadian Solution Can Look Like **34**

Protecting personal information and curbing surveillance advertising **35**

Transparency for effective enforcement and fairer markets **36**

Changing incentives with accountability and liability **37**

Executive Summary

It's been said there's a sucker born every minute, but the phrase is due for an update in the internet age.

Online fraud is a truly global problem, whose explosive growth has overwhelmed authorities around the world. Scams come in a variety of flavours, both familiar and new. From pyramid schemes and scam crypto investments to long haul confidence games like romance or pig butchering scams, a range of methods are available to separate individuals from their savings and reputations. Ad fraud, where legitimate businesses are cheated out of their advertising dollars with misrepresented low quality advertising space, also proliferates. Fraud and scams are often cross-border operations, conducted systematically by organized crime groups, and connected to public corruption, money laundering and human trafficking. As authorities once talked about narco-states, they now talk about scam states; in four years online scams have gone from one problem among many to the second biggest black market in the world, after illicit drugs.[1]

But scams, fraud, and cybercrime are not a problem beyond our borders for others to worry about. In Canada alone they are estimated to cost consumers nearly $650 million annually, alongside damages to Canadian's reputations, credit, and sanity.

Recent reporting shows that Meta's own analysis estimates 10% of their global online advertising business can be tracked to scams, frauds and ads for illegal goods, about $22 billion annually in Canadian dollars. That's a bigger figure than Canada's entire online advertising industry, estimated to be north of $16 billion a year, of which two firms, Meta and Alphabet, control 74%.[2]

Online advertising is a key vector for scams, and the distribution of scam ads is as concentrated as the online advertising industry itself. Meta's own research suggests they share up to fifteen billion scam ads per day, and anti-fraud authorities around the world report that Meta platforms like Facebook, Instagram and WhatsApp are involved in 80% of scams in Australia and 65% of scams in the UK, with Google and

[1] Tess McClure. "Age of the 'Scam State': How an Illicit, Multibillion-Dollar Industry Has Taken Root in South-East Asia." Technology. *The Guardian*, December 2, 2025. https://www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia.

[2] Dwayne Winseck. *Canada's Network Media Economy: Growth, Concentration and Upheaval, 1984-2023*. Global Media and Internet Concentration Project, Carleton University, 2024. https://doi.org/10.22215/gmicp/2024.12.124.

Amazon's platforms serving as a significant source as well.[3] In the UK, banks reported that Meta platforms were the origin of 80% of impersonation, purchase and investment fraud.[4]

Scams also represent an unnecessary tax on advertisers that depend on these platforms to reach their customers. Ad fraud, where fake users and websites extract money from real firms, cheats businesses, distorts markets, drives down revenues for legitimate publishers, and can be used to fund fraudulent activity. Because online advertising monopolies often represent both sides of the market, they can control the flow of information to both buyers and sellers of advertising. As a result, advertisers are given opaque information on audience quality and forced to compete with fraudsters who flood the market and hijack brand identities.

The biggest players at the heart of the online advertising industry, those who control how and where ads are placed, have a vested interest in a light touch approach. Because scam ads still generate real revenue for AdTech platforms, voluntary measures by AdTech monopolies will always be insufficient. When fraudulent ads are detected and removed by the platforms, those platforms keep the money that was spent to place those ads. To combat this epidemic of scams, anti-scam legislation must focus on the platforms and institutions where fraud happens and shift the incentives that keep the world of scams turning.

Well-crafted rules can reduce the volume of scams by making them a cost rather than a profit center for platforms and incentivizing them to be proactive rather than reactive in their efforts. Legislation can create more effective paths to restitution for victims of scams, ensuring institutions do their part or risk liability for losses. For advertisers, regulation can offer greater transparency from online advertising platforms, who benefit from the opacity of the marketplaces that Canadian businesses depend on to reach their customers.

To begin unraveling the world of scams, Canadian policymakers should:

- Clarify and strengthen data protection laws by defining classes of sensitive personal information and restricting their creation, collection, use, and sale for advertising purposes

[3] Jacquelin Magnay. "'Not above the Law': Facebook Warned of Liability for Scams." *The Australian*, March 13, 2024. https://www.theaustralian.com.au/business/technology/not-above-the-law-facebook-warned-of-liability-for-scams/news-story/221a619a020900f2c949f5a5dcdee1b4.
[4] Rupert Jones. "Social Media Sites Are Wild West for Shopping Fraud, Says UK Bank." Money. *The Guardian*, May 28, 2023. https://www.theguardian.com/money/2023/may/28/social-media-sites-wild-west-shopping-uk-bank-facebook-instagram.

- Require know-your-customer and both publisher and advertiser verification in advertising marketplaces, giving researchers and companies the tools to understand the market and keep competition fair
- Develop an anti-scam regulatory framework that outlines the responsibilities of large advertising platforms, including transparency and intelligence sharing requirements, and obligations to prevent, detect, disrupt and remove fraudulent content
- Empower regulators like the Office of the Privacy Commissioner to investigate and enforce data protection laws and law enforcement agencies like the Competition Bureau to ensure compliance with anti-scam laws

Introduction

The internet has been appropriately lauded for seamlessly connecting us across geography, culture, and demographics. While the once open communities of the web are increasingly put behind monopolized walled gardens, connections of all kinds continue to blossom, whether social, professional, or commercial. But one kind of undesirable connection has flourished in recent years: the connection between scammer and victim. Instances of online scams and fraud are surging in Canada, with over $648 million in losses in 2024 just from the scams that were reported.[5] This phenomenon is global, with authorities across the world grappling with a surfeit of scams originating within the advertising-based business models of major tech companies. Consumers are not the only victims of illegitimate activity perpetuated through AdTech systems; businesses have their reputations tarnished while being nearly powerless to address abuse of their names, and advertisers can be misled and defrauded by complicated systems that distort information about where their ads are placed.

The business models, technologies and systems that enable the online advertising industry (AdTech) have also enabled techniques for scams, fraud and cybercrime that exploit open-web display, social media and in-app advertising to target and reach their victims and made it easy and profitable to game the system.

[5] Melissa Tait. "Top OSC Officials Say They Are Witnessing a Surge in Online Scams and Fraud." Business. *The Globe and Mail*, April 25, 2025. https://www.theglobeandmail.com/business/economy/article-top-osc-officials-say-they-are-witnessing-a-surge-in-online-scams-and/.

Online scams have exploded since 2021, going from a cottage industry to an industrial enterprise making by some estimates up to $70 billion USD per year. These are sophisticated operations often run by organized crime groups, and connected to money laundering, illegal gambling, and human trafficking.[6]

The modern online advertising system plays an essential role in multiple stages of these criminal operations. Advertisements for fake employment opportunities are used to lure victims who are then trafficked and put to work against their will. Working from remote industrial parks, they work under to threat of violence to bait marks around the globe into romance scams[7]. Advertisements are used to attract victims into fake investment schemes, to impersonate businesses and rip-off clients, and to sign victims up for recurring credit card payments.[8] Even advertising professionals fall victim to websites launched with the sole intent of extracting revenue for ads that no human eyes will ever see, or to bankroll disinformation and hate speech.[9]

The losses from these scams are staggering and growing year over year. The Canadian Anti-Fraud Centre recorded 36 000 victims of scams fraud in 2024, with losses of $647 million CAD. Given that most frauds and scams go unreported, the real numbers are certainly much higher. The ongoing spread of AI agents will make it even easier to conduct scams at scale and give perpetrators access to more powerful tools they can use to dupe their victims. Already, a "fraud-as-a-service" sector is developing.[10] Authorities around the world are moving to alert consumers and break up scamming operations, a cat and mouse game that will be ineffective without addressing the roots of the problem.

Between the scammers and their victims sit the monopolies of the online advertising industry, whose advertising exchanges and networks function as scam distribution

---

[6] McClure. *Age of the 'Scam State*

[7] Hannah Beech and Min Let Pat. "At This Office Park, Scamming the World Was the Business." World. *The New York Times*, January 13, 2026. https://www.nytimes.com/2026/01/13/world/asia/myanmar-scam-center.html.

[8] McClure. *Age of the 'Scam State'*; Confiant. "[Profile] ScamClub." Malvertising Attack Matrix, Confiant. 2023. https://matrix.confiant.com/profile/scamclub.html.
Organized Crime and Corruption Reporting Project. "Everything You Need to Know About 'Scam Empire.'" OCCRP, March 5, 2025. https://www.occrp.org/en/project/scam-empire/scam-empire-everything-you-need-to-know-about-these-massive-investment-scams.

[9] Megan Graham. "'Made for Advertising' Websites Are the Marketing Industry's Latest Messy Situation." C Suite. *Wall Street Journal*, April 11, 2024. https://www.wsj.com/articles/made-for-advertising-websites-are-the-marketing-industrys-latest-messy-situation-560c79de.

[10] Kennedy Meda. "Fraud-as-a-Service: Creating a New Breed of Fraudsters." *Thomson Reuters Institute*, February 21, 2025. https://www.thomsonreuters.com/en-us/posts/corporates/faas-new-fraudsters/.

systems, controlling what and how advertisements are displayed. Only these actors have systematic visibility over the advertisers and their copy, and publishers and their holdings; only these actors can effectively track ad placements and intervene to ban the accounts of scammers.

The dominance that these companies have in the online advertising market distorts the incentives to take steps necessary to protect their users. This has meant limiting information sharing, looking the other way on scam behaviour, and taking action only after external pressure. Scam accounts are big spenders, and revenues are revenues, regardless of the source. In 2024, Meta itself guessed that about 10% of its revenue, about $16 billion USD came from ads for scams or illegal goods.[11] Securing the proactive cooperation and involvement of these companies requires changing their incentives and loosening their grip on the global online advertising market.

International examples of effective regulatory solutions to curb the epidemic of scams compel these companies to adopt changes to their behavior. As the example of Meta shows, bringing an end to scams on their platforms carries a multi-billion-dollar price tag, limiting their enthusiasm for bold action. Without tackling the concentrated economic power at the heart of these markets, the grip of these corporations will remain an impediment to regulation and frustrate attempts to intervene in the interests of individuals and businesses. Canada is currently without effective legal regimes that could combat the deluge of scams.

Advertising Technologies and Scams

The world of online scams is diverse and complex, with all manner of strategies on display to separate a target from their valuables, whether in the form of their money or their identities.

Some are new takes on familiar schemes, like pyramid selling or scam investments that convince users to buy worthless cryptocurrencies or transfer their wealth to fraudulent exchanges. Some are long haul confidence games operating on an industrial scale, like the evocatively named pig butchering and romance scams. There is ad fraud, which cheats businesses out of their advertising dollars by showing ads to bots instead of humans. There is purchase fraud, where people pay for goods that don't exist, taking money for vehicles, puppies, and other products

[11] Horwitz, Jeff. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show". *Reuters*, November 20, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

from fake vendors, sometimes disguised as real businesses. There are even recovery scams, which retarget individuals who have already been the victims of fraud, offering a service to help them recover stolen accounts and cryptocurrency. These advertisements adopt the imagery of white hat hackers, financial gurus and even the livery of state agencies to exploit internet users at their most vulnerable.

Whatever their form, these scams are parasitic on the advertising and social networking behemoths that increasingly structure the modern internet. These platforms offer choice hunting grounds for scammers, and opportunities for the companies themselves to deceive their own customers. Narrowing the field of view, we focus on three overlapping trends in online illegitimate activities:

1. **Ad fraud**, which distorts the outcomes of campaigns to advertisers and can be used as a tool to consolidate market power.
2. Scams, such as the **impersonation** of individuals and brands, and the reluctance of advertising monopolists to address systemic problems.
3. **Malvertising**, and the suite of tools and techniques which exploits an AdTech system based on surveillance to compromise devices and networks and spread malicious software.

Ad Fraud

In short, ad fraud abuses the online advertising system to extract money from advertisers. This includes the use of automated tools to generate fake impressions such as clicks and views, retargeting users already close to conversion, and misrepresenting the value of advertising spaces so advertisers pay inflated prices for low quality ad space. Ad fraud is typically associated with scammers who systematically inflate the value of their advertising space with fake clicks, called "click fraud", or publishers that operate “made for advertising” sites that use clickbait to draw users to websites with mediocre content and the absolute maximum amount of advertising inventory. The proliferation of illegitimate activities come about in part due to the opacity of the AdTech ecosystem, where the sheer speed and scale of programmatic advertising allow scammers, fraudsters and cybercriminals to find and exploit niches without risk of a coordinated response.

But other kinds of ad fraud can arise from the concentration of ownership across the AdTech stack. Platforms like Facebook, Instagram and YouTube are “walled gardens” where the owners of these systems have total control over how advertising is purchased and placed for users to see, and over what information and analytics they provide to advertisers. Beyond the topic of scams, for AdTech monopolists like Google, this control over the AdTech stack allows them to distort the marketplace

and punish competitors, limiting choices for advertisers and effecting costs for both advertisers and publishers.[12]

This monopoly creates a severe power imbalance in their dealings with publishers and advertisers, giving them opportunities to manipulate and mislead customers to suit their own ends. In 2023 advertising research group Adalytics reported that Google was potentially misleading advertisers who were enrolled in their TrueView advertising program.[13] On its face, TrueView offered value to advertisers, promising high value placements on YouTube and on the sites of other vetted partners. Later research revealed, however, that the majority of TrueView ad placements on partner ad space did not meet the buyer's expectations; their ads were automatically played, muted, placed in slots not visible to users, and were frequently placed alongside low quality content undesirable as an advertising placement. These included applications used by toddlers, alongside websites with persistent strikes for copyright violations, on websites used to spread disinformation and propaganda, and on websites whose primary viewers are bots. Restrictions on how advertisers can track user activity across Google's ecosystem mean they have less ability to verify suitability of placement of their ads, and limit how third-party auditors can independently assess and report on the quality of Google's ad placements.[14]

This behaviour is not unique to Google. In August 2025, a former Meta employee turned whistleblower brought a complaint about systematic ad fraud to competition authorities in the UK. The complainant alleges that Meta used deceptive tactics to promote its Shop Ads program, including counting shipping and taxes as advertiser revenue, inflating auction bids, and applying undisclosed discounts. These choices inflated a given advertiser's perceived return on ad spending by nearly 20%, giving advertisers false narratives on the performance of these ads.[15] While traditional ads served on Facebook could link out to external websites, Shop Ads keep users on

---

[12] Rebecca Bellan. "Judge Rules Google Illegally Monopolized Adtech, Opening Door to Potential Breakup." *TechCrunch*, April 17, 2025. https://techcrunch.com/2025/04/17/judge-rules-google-illegally-monopolized-ad-tech-opening-door-to-potential-breakup/.
Ryan Whitwam. "DOJ Confirms It Wants to Break up Google's Ad Business." Ars Technica, May 2, 2025. https://arstechnica.com/tech-policy/2025/05/doj-confirms-it-wants-to-break-up-googles-ad-business/.

[13] Adalytics. "Did Google Mislead Advertisers about TrueView Skippable In-Stream Ads for the Past Three Years?" May 8, 2023. https://adalytics.io/blog/invalid-google-video-partner-trueview-ads.

[14] Suzanne Vranica. "YouTube Spars With Auditor Over Transparency of Advertising Risks - W…." Archive. Is, April 20, 2020. https://www.wsj.com/articles/youtube-spars-with-auditor-over-transparency-of-advertising-risks-11587340250.
Adalytics. "Did Google Mislead Advertisers?"

[15] Trishla Ostwal. "Whistleblower Alleges Meta Artificially Boosted Shops Ads Performance." *AdWeek*, August 20, 2025. https://www.adweek.com/media/whistleblower-alleges-meta-artificially-boosted-shops-ads-performance/.

Meta's platforms to complete purchases. For Meta, the benefit would be to push more commercial and user activity into its own ecosystem, giving it access to more data and creating further economic dependencies for vendors using its platform. It also provides Meta additional opportunities for monetization of its feed, and to further sell advertising space to advertisers – be they scammers or legitimate.

The root of this problem is the centralized control over the AdTech stack, and the leverage of massive networks that corral the audiences that advertisers need to access. When these systems are subject to strategic goals of consolidating and tracking activity within walled gardens, collusion between the buy- and sell-sides of these systems becomes a self-preferencing tactic to promote certain behaviours and punish others.

Impersonation scams

Spending any time on X, YouTube or Instagram will inundate a user with scam content, whether they know it or not. Users will come across familiar faces – celebrities, elected officials, creators - promoting incredible offers or opportunities for investment. Scammers and fraudsters piggyback on the reputation of businesses and public figures to push fake websites to users and lure them into fraudulent transactions.[16] For these operations, scammers create a slew of fake accounts, steal the identities of older account holders, or generate convincingly fake websites and ads, sometimes spending months building the veneer of legitimacy.

Scammers can hijack the brands of businesses to funnel potential customers to fake websites designed specifically for purchase fraud. Reporting by the Wall Street Journal found one man was out-advertised nearly 300:1 by scammers, with over 4,400 fake ads to his 15.[17] Scammers can also steal the identities of regular users to use their accounts for marketplace scams, impersonating neighbours looking to sell used goods. Other scam advertisers take it a step further with the use of malvertising, where they use the likenesses of public figures, journalists, creators and

[16] Nova Scotia Securities Commission. "Impersonation Scams Part 1 – The Rich and Famous." March 6, 2024. https://nssc.novascotia.ca/before-you-invest/impersonation-scams-part-1-%E2%80%93-rich-and-famous.
Nova Scotia Securities Commission. "Impersonation Scams Part 2 – Registered Advisers and Regulators." March 13, 2024. https://nssc.novascotia.ca/before-you-invest/impersonation-scams-part-2-%E2%80%93-registered-advisers-and-regulators.

[17] Jeff Horwitz and Angel Au-Yeung. "Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook." Wall Street Journal. Accessed July 28, 2025. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.

celebrities to bait unsuspecting viewers into downloading software that steals their cryptocurrency or account credentials.[18]

In Canada, where Meta has banned news from its platform to avoid compliance with domestic regulation, you can still find plenty of impersonated news. While some of this may be the product of foreign interference and disinformation campaigns, many are simply scams playing on the authority of the national broadcasters and news industry figures to exploit their reputations and the trust of users. Claiming to be the CBC, the Liberal Party, or flouting the likenesses of politicians or other authority figures, these ads lead users to convincing fake sites, where they are vulnerable to being defrauded.[19] The improvement and proliferation of image and sound generating technologies is exacerbating this problem, making such scam ads easier to produce at scale, and creating more convincing impersonations, often referred to as deepfakes. This is particularly true in the case of romance and pig butchering scams but works with other advertising-based scams as well.[20]Although ads using impersonation to mislead users are against Meta's terms of service and representatives of the company claim they're working on the problem, this offers little hope to businesses and creatives fighting off armies of scammers stealing their likeness. Their reputations and livelihoods are at risk as their relationships with customers and communities are eroded, with limited recourse to force companies to

---

[18] Retire This Way with $500k, dir. *Scammers Stole My Face for Fake Ads (It Gets Worse)*. 2025. 5:40. https://www.youtube.com/watch?v=jPCjs01-AvQ.
The Wall Street Journal. "Billionaire Challenges Meta Over AI-Powered Scams – Tech News Briefing – WSJ Podcasts." Accessed August 25, 2025. https://www.wsj.com/podcasts/tech-news-briefing/billionaire-challenges-meta-over-ai-powered-scams/06067b24-46cc-430e-8fc0-457611ad4e3b.
Canadian Digital Media Research Network. "Social Media Platforms Host and Profit from Scams Using AI and Fake News Websites during Canada's 2025 Federal Election." Accessed July 30, 2025. https://www.cdmrn.ca/publications/scam-ai-fake-news.
Lyon, Jacob. "43% of Meta Ads Based on UK Prime Minister Are Crypto Scams." *Protos*, August 13, 2024. https://protos.com/43-of-meta-ads-based-on-uk-prime-minister-are-crypto-scams/.
Ponsford, Dominic. "Facebook Allows Scam Ads Stealing Journalists' Identities to Proliferate." *Press Gazette*, April 28, 2025. https://pressgazette.co.uk/platforms/facebook-allows-scam-ads-stealing-journalists-identities-to-proliferate/.
[19] Thomas Seal. "Meta Blocked News in Canada. Ads for Scams Are Taking Its Place." *The Financial Post*, January 31, 2025. https://financialpost.com/pmn/business-pmn/meta-blocked-news-in-canada-ads-for-scams-are-taking-its-place.
Canadian Digital Media Research Network. "Social Media Platforms Host and Profit from Scams Using AI and Fake News Websites during Canada's 2025 Federal Election." Accessed July 30, 2025. https://www.cdmrn.ca/publications/scam-ai-fake-news.
[20] Kevin Ozebek. "Woman Conned out of Life Savings by Scammers Using AI to Pose as 'General Hospital' Star." ABC7 Los Angeles, August 26, 2025. https://abc7.com/post/los-angeles-woman-conned-life-savings-scammers-using-ai-pose-general-hospital-star-steve-burton/17655567/.
Timothy Beck Werth. "AI Actors and Deepfakes Aren't Coming to YouTube Ads. They're Already Here." Mashable, June 21, 2025. https://mashable.com/article/youtube-ai-video-ads.

stop the spread of this content. With business models aligned with profiting from online advertising, whatever its provenance, the balance will continue to tilt towards turning a blind eye rather than taking decisive action.

Malvertising

The infrastructure that allows customized, targeted ads to be tailored and delivered to users creates unique opportunities for scammers. Malvertising, malicious or hijacked online ads embedded within online advertising networks, is a viable vector for exploitation by scammers and other malicious actors.[21]

Groups running malvertising campaigns are sophisticated, adopting the techniques and technologies of the advertising industry and combining them with exploits and malware to compromise infrastructure and target devices. The reach of scamming groups is impressive, with one malvertising group becoming for a short time "the largest digital marketer in Europe," responsible for a whopping 5% of all display ads on the continent. The same research estimates that two actors were responsible for over 6 billion malicious ads in 2020.[22] The capacities of these organizations are advanced, with some scamming groups attributed to attacks that use zero-day exploits, previously undiscovered or undocumented hacking techniques. Scamming groups have also been known to run malvertising campaigns by compromising AdTech servers and injecting their own malicious code into legitimate advertising copy.[23] Malvertising groups use a variety of techniques to serve malicious advertising to users and exploit programmatic advertising systems, including Search Engine Optimization Poisoning, Browser Fingerprinting and Chameleon Ads.

Search Engine Optimization Poisoning

Some malvertising campaigns exploit search advertising to trick web users into downloading and installing malware on their machines. The basis of this scam is that paid or "sponsored" content is pushed to the top of search results in monetized search engines like Google. This ranking is exploited by scammers who create a fake

---

[21] Canadian Anti-Monopoly Project, Electric Eyes: Advertising Monopolies and Canada's National Security (2025)
https://antimonopoly.ca/wp-content/uploads/2025/09/CAMP-Electric-Eyes-Advertising-Monopolies-and-Canadas-National-Security.pdf
[22] Dangu, Jerome. "Malvertising: Made in China." Medium, September 29, 2021.
https://blog.confiant.com/malvertising-made-in-china-f5081521b3f0.
[23] Jerome Dangu, "Malvertising"
Confiant. "[Profile] ScamClub." Malvertising Attack Matrix.
https://matrix.confiant.com/profile/scamclub.html.
Moriya, Pedael. "Decoding ScamClub's Malicious VAST Attack." *GeoEdge*, February 28, 2024.
https://www.geoedge.com/decoding-scamclubs-malicious-vast-attack/.

version of a website and use a variety of "SEO poisoning" or "typosquatting" techniques, including using subtly different URLs, as well as inflated click-through rates and backlinks that make the site seem legitimate to the search engine algorithm.[24]

Ironically, the prevalence of SEO poisoning as a malvertising technique may increase legitimate companies' ad spend with search engines like Google, as they "compete" with fake websites for placement in search results. In an interview with WIRED magazine, a senior director at cybersecurity firm Malwarebytes said the company needed to buy more search engine ads to outcompete pretenders and "defend [their] brand."[25]

Fingerprinting and target acquisition

Scammers can use surveillance and tracking techniques from the advertising world to more effectively target their victims. "Fingerprinting" is a technique for collecting information about devices based on the configuration of their browser and machine, their IP address, and time zone. This information allows programmatic advertising systems to ensure ads are properly displayed on user devices, but it is also used to track users around the web, subverting privacy preserving interventions like restrictions on cookies.

Fingerprinting is becoming more common in online advertising as regulation has given users more control over their privacy and made it easier for them to refuse tracking cookies that collect information about their online behaviour. For AdTech giants like Google, enhanced consent frameworks and built in privacy protection like Apple's ATT posed a threat to their surveillance-based business model, and they have identified and promoted fingerprinting as a workaround, a move that has worried privacy advocates and cybersecurity experts.[26]

Fingerprinting can also be used by scammers to track potential victims around the web, to ensnare vulnerable users, and even to bypass security features and steal people's identities. Fingerprinting reveals details about a user's machine, including

---

[24] Communications Security Establishment. "Search Engine Optimization Poisoning (ITSAP.00.013)." Canadian Centre for Cyber Security, March 25, 2025. https://www.cyber.gc.ca/en/guidance/search-engine-optimization-poisoning-itsap00013.

[25] Lily Hay Newman. "Malicious Ads in Search Results Are Driving New Generations of Scams." Tags. *Wired*, December 2, 2024. https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams/.

[26] "Fingerprinting: Critics Say Google Rules Put Profits over Privacy." February 16, 2025. https://www.bbc.com/news/articles/cm21g0052dno.
Suzanne Smalley. "New Google Ad Tracking Policy a 'Pandora's Box' for Privacy, Experts Warn." *The Record*, February 20, 2025. https://therecord.media/new-google-tracking-pandoras-box.

details about their operating system and browsers. Cybercriminals can identify users running outdated software and redirect them to websites that will download malware onto their machines- sometimes without them needing to click anything at all.[27]

Chameleon Ads

Scammers and other bad actors exploit programmatic advertising marketplaces to serve their advertisements while avoiding detection. For example, research by the Social Media Lab at Toronto Metropolitan University details a technique for serving scam ads, misinformation ads, or other such content called "chameleon ads". In this approach, threat actors spend time cultivating the appearance of legitimate advertisers, running benign (though fake) advertisements for weeks, or even months.

Later, and sometimes only for very small amounts of time, this copy is changed out for advertisements for scam copy or disinformation content. The short run time for these bad advertisements makes it difficult for platform administrators to track and poses major challenges for researchers seeking to systematically study these campaigns. In part this is due to the structure of the limited window that these companies have given the outside world. Users would have to comb through Meta's creative ad library to find the scam copy; since advertisers often run tens of variations of ads at a time, this would be tediously akin to finding a needle in a haystack.[28]

Malvertising campaigns are effective and difficult to prevent because they leverage the same technologies as advertisers and other actors to track users. Indeed, the entire programmatic advertising system operates on the ability for internet browsers to retrieve code from remote servers and execute it on a users' machine, generally without their knowledge or permission. The same techniques advertisers use to identify the characteristics of a user's device can be used to compromise that device.

Generative AI and The Future of Scams

Novel technologies are continually adapted to facilitate scams, frauds, and all manner of illicit activities. So far, generative AI has been no different. The use of

---

[27] Vijay Kumar Gupta. "How Do Cybercriminals Exploit Browser Fingerprinting Techniques?" *Linkedin*, September 9, 2024. https://www.linkedin.com/pulse/how-do-cybercriminals-exploit-browser-fingerprinting-vijay-gupta--4ytfc.

[28] Social Media Lab. "The Hidden Game: How Scammers Use 'Chameleon Ads' to Bypass Meta's Moderation." *Social Media Lab*, April 21, 2025. https://socialmedialab.ca/2025/04/21/the-hidden-game-how-scammers-use-chameleon-ads-to-bypass-metas-moderation/.

generative AI models by scammers is not a potential future scenario; it's already an important tool enabling the ballooning incidence of online scams, enabling new types of scams, and driving an emerging "fraud-as-a-service" industry.[29]

Generative AI models lower the barrier to entry and act as force multiplier for scammers and cybercriminals and can be applied to all stages of a scam's lifecycle. Scammers can use models to profile and target victims using publicly available information, overcome linguistic barriers by using AI to create more convincing fake websites, forged documents, ad copy and phishing emails without the usual telltale typos, and even to write malware and scan systems for cyberattacks. They can be used to conduct romance scams cheaply and at scale with chatbots specialized for catfishing, and when a human touch is desired, models can even be used to map a generated face on top of a user's face, enabling real time deepfakes for video calls.[30]

Within the range of attacks delivered specifically through programmatic advertising, AI generated "deepfake" content is fueling a surge in advertisements leading users into crypto and investment scams, as well as purchase fraud.[31] Whereas impersonation scams used to be limited to text formats, models can now generate convincing and synced audiovisual content of public figures or manufactured identities.

AI models are already contributing to an increase in both the quantity and quality of online scams. Advances will make generated content more convincing and harder for even savvy users to detect. Automated agents that can independently generate content will help scammers increase the scale and reduce the cost of their operations. This means more campaigns, more victims, and more losses, and makes a strong policy response all the more necessary.

---

[29] Corwin Perdomo. "AI Scams Exposed: 13 Tools Driving Scaled Fraud Now." Sardine, August 5, 2025. https://www.sardine.ai/blog/ai-scams.
Swartz, Lana, Alice E Marwick, and Kate Larson. *ScamGPT: GenAI and the Automation of Fraud*. Data & Society, 2025. https://datasociety.net/library/scam-gpt/.
[30] Deni Ellis Béchard. "So You Fell for a Robot—'Chatfishing' Is Taking Over the Dating Apps." Scientific American, October 23, 2025. https://www.scientificamerican.com/article/the-rise-of-ai-chatfishing-in-online-dating-poses-a-modern-turing-test/.
[31] Tech Transparency Project. *Meta Awash in Deepfake Scam Ads*. Tech Transparency Project, n.d. Accessed October 1, 2025. https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads.
Mathieu Lavigne, Alexei Abrahams, Mahnan Omar, and Aengus Bridgman. *Social Media Platforms Host and Profit from Scams Using AI and Fake News Websites during Canada's 2025 Federal Election*. Canadian Digital Media Research Institute, n.d. Accessed January 20, 2026. https://www.cdmrn.ca/publications/scam-ai-fake-news.

Uninterested Stewards, Dominant Players and the Proliferation of Scams

Online advertising is based on the collection of personal information, tracking users across the internet, and serving those users targeted content. But much like its application to intelligence services, the information and reach available to marketers is also useful for scammers. In some respects, it is used for the same purposes: to understand a target's habits, beliefs, and interests, and to create a context where their behaviour is influenced at a critical moment. A 2023 study by the National Bureau of Economic Research makes tangible the connection between surveillance and the proliferation of scams. Their study revolves around an important change in the surveillance and advertising ecosystem: changes to Apple's iOS operating system that would disable cross-site tracking of users by default. Biang et al. examine whether reported instances of scams in specific geographical areas drop after the rollout of Apple's App Tracking Transparency (ATT) policy, paying specific attention to companies known to share data with data brokers or transfer user data without adequate encryption. After ATT implementation, reducing the scope of user surveillance, they observed a 16% drop in reported complaints of fraud from iOS users and a significant increase in the price of consumer data available to would-be identity thieves on the dark web.[32]

Online advertising generates profits from the creation, processing and exchange of personal data collected from trillions of online interactions from billions of people around the world every day. The enclosure of online activities by large firms allows them to extract data about their users for a variety of profitable purposes but it also allows them to control the marketplaces deciding the placement of advertising on those platforms. Major tech companies in the online advertising ecosystem have a vested interest in maintaining the system of surveillance advertising, financially benefit from the use of programmatic advertising by scammers and legitimate businesses alike. Reporting in late 2025 showed that Meta's internal analysis suggested that up to 10% of the company's online advertising revenue, approximately $15 billion USD, could be attributed to scams and banned goods.[33] Advertisers and users looking for a less scam-ridden environment are largely out of

[32] Bo Bian, Michaela Pagel, Huan Tang, and Devesh Raval. *Consumer Surveillance and Financial Fraud*. Working Paper No. 31692. National Bureau of Economic Research, 2023. https://doi.org/10.3386/w31692.

[33] Horwitz. *Special Report: Meta is earning a fortune on a deluge of fraudulent ads, documents show.* Reuters, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

luck. Because of the monopolization of the online advertising and adjacent markets, there are few alternatives for users and advertisers. Control of online advertising ecosystems by Big Tech allows them to obscure these systemic issues by limiting the data available to advertisers, auditors, and researchers. Without access to data, systematic and independent study of the prevalence and scale of advertising scams is impeded.

Authorities around the world are struggling with the large and growing number of scams littering social media and other platforms. But understanding the true scale of online scams is difficult. Most go unreported, and those that are reported can go to a variety of institutional actors, including credit card companies, technology companies, the police, and consumer protection authorities.[34] Still, available data paints a convincing picture- online scams are flourishing, especially on platforms owned by companies like Meta, Google and Amazon.

Between 2021 and 2023, social networking sites, especially Facebook marketplace, surpassed all other vectors for classified scams in Australia, increasing 78% according to competition and consumer protection authorities, with scams on Meta products accounting for "about 80 percent of the losses." [35] In summer 2023-2024, Meta platforms were the source of almost half of scams reported to U.S. bank JP Morgan from the Zelle payment processing application.[36] Research from UK consumer watchdog Which? is even more stark, with users reporting 63% of reported scams originating from social media, followed by 42% for search engines.[37]

The scale of advertising on these platforms makes addressing scams difficult without concerted efforts from the companies themselves. Because scammers can continue to make new accounts, from anywhere in the world, even Google's claims of removing one billion scam ads is performative, referred to as "reactive moderation…

---

[34] Samuel Perreault. "Self-Reported Fraud in Canada, 2019." Statistics Canada, July 24, 2023. https://www150.statcan.gc.ca/n1/pub/89-652-x/89-652-x2023001-eng.htm.
[35] James Purtill. "Facebook Marketplace Was Built on Trust, but It Has Become Overrun with Scams." Science. *ABC News*, February 29, 2024. https://www.abc.net.au/news/science/2024-03-01/facebook-marketplace-has-become-the-home-of-scammers/103521536.; *'Not above the Law': Facebook Warned of Liability for Scams*. March 13, 2024. https://www.theaustralian.com.au/business/technology/not-above-the-law-facebook-warned-of-liability-for-scams/news-story/221a619a020900f2c949f5a5dcdee1b4.
[36] Jeff Horwitz and Angel Au-Yeung. "Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook." Wall Street Journal. Accessed July 28, 2025. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.
[37] Ash Strange. "A Year On from the Online Fraud Charter." Which?, December 18, 2024. https://www.which.co.uk/policy-and-insight/article/a-year-on-from-the-online-fraud-charter-aefBu4h2Pre8.

a game of whack-a-mole."[38] The pattern is familiar; when pressure is applied, action is taken, but the systemic problem remains. Scammers are cleared from the marketplace one afternoon, and by the next morning they have retaken their spots. Even brief windows of activity allow scammers to pump out hundreds or thousands of scam advertisements.

The proliferation of online scams is deeply intertwined with the business model of companies like Meta and Google. 98% of Meta's 2023 revenue was tied to advertising.[39] How much of that profit comes from this proliferation of scams? Recent reporting suggests the figure could be as high as 10% or $15 billion USD annually.[40] Scam advertisements are flooding into Meta's marketplaces, with internal company documents from 2022 finding "that 70% of newly active advertisers on the platform are promoting scams, illicit goods or 'low quality products.'" This inundation of scams nonetheless helps drive Meta's advertising-based revenue stream, "[driving] a 22% increase in its advertising business last year to over $160 billion."[41] Similarly, advertisements though Google Search, YouTube and Google's ad network were the majority contributors to its $305 billion USD revenue in 2023.[42] That same year, they removed 5.5 billion ads, and suspended 12.7 million advertising accounts.[43] Presumably, these scammers were not refunded for their advertising spend, and there remains no system for preventing them from making new accounts and developing new strategies to push scams.

Despite being the biggest continents in the world of scams, companies like Meta and Google are slow to act, if they act at all.[44] Scammers already understand how to

---

[38] Chris Fox. "Facebook and Google 'Failed to Remove Scam Adverts.'" Future. *BBC News*, April 26, 2021. https://www.bbc.com/news/technology-56888693.
[39] Investopedia. "How Does Facebook (Meta) Make Money?" Accessed August 28, 2025. https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp.
[40] Horwitz. *Special Report: Meta is earning a fortune on a deluge of fraudulent ads, documents show.* Reuters, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/
[41] Jeff Horwitz and Angel Au-Yeung. "Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook." Wall Street Journal. May 15, 2025. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.
[42] Statista. "Google: Advertising Revenue 2024." Accessed August 28, 2025. https://www.statista.com/statistics/266249/advertising-revenue-of-google/.
[43] Lily Hay Newman. "Malicious Ads in Search Results Are Driving New Generations of Scams." Tags. *Wired*, December 2, 2024. https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams/.
[44] Chris Fox. "Facebook and Google 'Failed to Remove Scam Adverts.'" Future. *BBC News*, April 26, 2021. https://www.bbc.com/news/technology-56888693.
Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU – EDMO. n.d. Accessed August 6, 2025. https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

game automated content moderation systems to place their scams, and a company like Meta is hesitant to act, allowing advertisers to rack up numerous reports of behaviour that breeches their standards. Groups in the EU found that Meta's actions on reported scams were inconsistent, brushing off user reports while being responsive to those coming from enforcers of the Digital Services Act (DSA). This suggests victims of impersonation fraud and users actively exposed to scams will have little ability to intervene to protect their reputations or make the platform safer. On a more positive note, the efforts in reaction to the implementation of the DSA suggests that the threat of regulatory enforcement is the starting point for effective removal of scam content.[45]

Resourcing decisions for content removal and moderation play a significant role in the problem as well. Meta's recent shift away from content moderation and corporate goals of trust and safety on its platforms may only fuel the growth of scams.[46] Insiders have reported that staff and resources to combat scams have been scaled down.[47] Meta's control over access to information by independent parties, including anti-fraud authorities and researchers also obscures not only the true scale of its scam problem, but the ability to develop productive interventions to combat it. As previously mentioned, Meta's Ad Library, which catalogues the advertising copy active on its platforms, does not keep an archive of all content. For the most part, only content that is labelled as "political" is archived, an action taken in response to regulation. Chameleon ads that pretend to be innocuous only to later push disinformation and scams are not archived, and scam ads can easily be removed, making it harder to track and study them.[48]

The story of Big Tech inaction on scams and frauds is not just a story of the outsized power of a handful of corporations, but also the results of expecting companies to independently solve the externalities of their own business models. If addressing a serious problem runs counter to the growth and profitability of a company, even

---

Ponsford, Dominic. "Facebook Allows Scam Ads Stealing Journalists' Identities to Proliferate." *Press Gazette*, April 28, 2025. https://pressgazette.co.uk/platforms/facebook-allows-scam-ads-stealing-journalists-identities-to-proliferate/.

[45] *Thanos Sitistas and Lecua Bertoldini. Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU. European Digital Media Observatory, 2025. https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.*

[46] Platformer. "Is Anyone Left to Defend Trust and Safety?" July 25, 2025. https://www.platformer.news/trustcon-trust-safety-leadership-decline-2025/.

[47] Horowitz and Ad-Yeung, 30

[48] Social Media Lab. "The Hidden Game: How Scammers Use 'Chameleon Ads' to Bypass Meta's Moderation." *Social Media Lab*, April 21, 2025. https://socialmedialab.ca/2025/04/21/the-hidden-game-how-scammers-use-chameleon-ads-to-bypass-metas-moderation/.

well-intentioned internal efforts will eventually be frustrated by the gravitational pull of the guiding goal of maximizing returns.

Who Pays for Scams?

Responsibility and effort dedicated to protecting people from online scams is tied to an entities' liability for scams that occur in systems they control. In Canada, the legal frameworks for the liability of online scams are not comprehensive, and there is limited recourse available for individuals. In some cases, financial institutions may be liable in cases where scammers gain access to victim's accounts and transfer funds, known as unauthorized fraud.[49] Banks have developed more sophisticated techniques for preventing unauthorized fraud, but in turn, scammers have adapted. Pig butchery and other romance scams, for example, are confidence games, where the victim comes to trust the scammer, and transfers them money voluntarily, representing what is referred to as authorized fraud. In cases of authorized fraud, the victim of a scam is likely out of luck. In cases where cryptocurrency is the medium of choice there may be even less recourse for victims, as cryptocurrency transactions are irreversible, and are often done without involvement of any regulated financial institution.[50]

The liability of social media and internet search companies is less clearcut. In the United States, companies like Meta typically rely on Section 230 of the Communications Decency Act to argue that they are not liable for any of the content posted on their platforms, regardless of its potential harm to users, because they have been found to be neither the "publisher [nor] speaker." Though that defense has worked to shield them from liability for things like hate speech and defamatory statements, scams may be a different story. In 2024, for example, US courts found that Section 230 did not shield Meta from liability for fraudulent advertisements and scams, because the claim to liability arose from Meta's failure to act on promises they make in their terms of service to prevent fraud. Plaintiffs in the case are arguing that Meta's failure to live up to its promises provides the basis for a lawsuit, but

[49] Alexandra Pozadzki. "You Were Targeted in a Scam. Is Your Bank Liable for the Losses?" *The Globe and Mail*, July 24, 2025. https://www.theglobeandmail.com/business/economy/article-you-were-targeted-in-a-scam-is-your-bank-liable-for-the-losses/.

[50] Canada, Competition Bureau. "Quick Easy Money? Sometimes It's a Quick Easy LIE." News releases. March 1, 2023. https://www.canada.ca/en/competition-bureau/news/2023/03/quick-easy-money-sometimes-its-a-quick-easy-lie.html.
Canada, Financial Consumer Agency of. "Crypto Assets." Education and awareness. June 17, 2016. https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html.

whether the case is successful will be another matter.[51] In the EU, courts have already set the stage for wider platform liability, establishing responsibility for scanning advertising content and verifying advertiser identity to ensure that ad copy complies with GDPR requirements for sensitive data.[52]

While Canada lacks protections for social media companies like section 230 in the United States, the liability of social media platforms is currently a legal gray area. Financial institutions may be liable for repayment in cases of unauthorized access fraud. Most of interventions to combat frauds and scams are informational, focussed on raising awareness and collecting information about documented scams. After the fact, there is also little in the way recourse for victims, beyond reporting the crime to relevant authorities. The Online Harms act, which proposed some responsibilities for transparency and content moderation on social media companies, did not explicitly address frauds and scams. Overall, given their prevalence and damage, scams and fraud should be considered in any future legislation around online harms, if not in their own legislation. This legislation should clarify the role and responsibilities of social media platforms in promoting or publishing scams and frauds through the variety of systems they control. Importantly, this includes the marketplaces for advertisements and classifieds where scams proliferate.

Existing and Potential Regulatory Interventions

Online scams flourish in a complex environment, owing to the sophistication and adaptability of scammers, the involvement of diverse institutions and platforms, and the sheer scale of online advertising systems. Owing to this complexity, legislation intended to tackle online scams must take a holistic approach if it hopes to be successful in combating scams. Prominent examples of this approach include Singapore's combination Online Criminal Harms Act (OCHA) and Shared Responsibility Framework (SRF) and Australia's Scams Prevention Framework (SPF). Holistic approaches to online scams create roles and responsibilities for all involved

[51] Nancy S. Kim. "Beyond Section 230 Liability for Facebook." *St. John's Law Review* 96, no. 2 (2023). https://scholarship.law.stjohns.edu/lawreview/vol96/iss2/5.
Patton, Elizabeth A. "Breaching Social Media Platforms' Section 230 Shield." *Above the Fold*, August 1, 2024. https://advertisinglaw.foxrothschild.com/2024/07/breaching-social-media-platforms-section-230-shield/.
"Section 230 Immunity for Publishing Scam Ads." Accessed August 28, 2025. https://www.thowardlaw.com/2023/06/section-230-immunity-for-publishing-scam-ads.

[52] Ruth Boardman, Benjamin Docquir, Willy Mikalef, Oriane Zubcevic, and Lisa Gius. "CJEUs Russmedia Decision How Online Marketplace Platforms Could Be Held Liable under the GDPR." Bird & Bord, December 3, 2025. https://www.twobirds.com/en/insights/2025/cjeus-russmedia-decision-how-online-marketplace-platforms-could-be-held-liable-under-the-gdpr.

parties, especially institutions and large organisations, and set the terms for their cooperation through information sharing. Anti-scam legislation must also recognize that online platforms, who create revenue through advertising, are the vectors for most online scams, and must play an active and accountable role in their suppression, for which a variety of methods have been devised.

Anti-Scam Legislation		Online Criminal Harms Act and Shared Responsibility Framework (Singapore)	Digital Services Act (EU)	Scams Prevention Framework (AUS)
Assigning Responsibility	Obligations and Duties of Care	X	X	X
	Attribution of Liability	X	X	X
Information and Transparency	Intelligence Sharing and Reporting	X		X
	Ad Library Retention		X	
	Identity Verification and Know-Your-Customer	X	X **(Partial)**	X **(Partial)**
Content Moderation	Notice and Takedown	X	X	X
	Trusted Flaggers		X	
Data Restrictions	Restrictions on Collection and Sale			
	Restrictions on Targeting		X	

Assigning Responsibility

Creating a Duty of Care

Content moderation is the examination and removal of advertisements and user generated posts that breach local laws or platforms terms of service. Anti-scam and other related legislation impose specific obligations on online platforms to remove illegal or fraudulent content, either proactively or in response to requests from public authorities. Despite a push in the last decade to increased content moderation and "trust and safety", online platforms like Meta and X are pulling back from these commitments.

Automated content moderation systems are already employed and will continue to evolve, with image recognition technologies improving their effectiveness in some cases. Meta has already proposed to use facial recognition technology to attempt to

remove impersonation scams and is likely to have other automated systems to flag content as well. This could include continuous scanning of advertising copy, including videos, to detect potential presence of malicious code. Nonetheless, automated systems for content moderation should not be considered as standalone solutions, which are reactive in nature. Scammers are already accustomed to avoiding automated systems and will continue to refine their tactics; and the systems themselves will require monitoring, as well as processes for appeal when content is mistakenly removed. Without rigorous transparency requirements, platforms themselves can also dilute the effectiveness of automated moderation; reporting on internal Meta documents found that accounts were only banned if automated systems are 95% certain of scamming, a metric which can easily be gamed. In these cases, Meta simply charged the suspected scam advertiser a higher advertising fee, which they did not disclose to the scammer, increasing Meta's profits while still allowing scams to be served.[53]

Attribution of Liability

Online scams often require the use of one, or several, institutional systems, from the online platforms where scams originate, the telecommunications networks delivering scam calls, and the payment processors. Distribution of liability and obligation across institutional stakeholders, including telecoms, financial institutions and the operators of advertising marketplaces lessen ambiguity for these institutional stakeholders, providing guidance for the role they play in protecting users.

Singapore has moved toward adopting a comprehensive liability framework to combat scams. In 2023 it adopted a Shared Responsibility Framework (SRF) that imposed duties on both telecommunications providers and financial institutions to protect against certain types of scams. This framework does not, however, cover digital platform providers; they are covered by the 2023 Online Criminal Harms Act (OCHA). The OCHA gives authorities the ability to compel online platforms to implement policies to detect and disrupt scam activities, and to report on the actions it takes and their effectiveness. This allows Singaporean authorities to track both the implementation and results of these measures.[54] The first such order under

[53] Horwitz, Jeff. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Sh…." Reuters, November 20, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

[54] CNA. "Banks, Telcos and Scam Victims to Share Liability for Losses under New Framework to Kick in on Dec 16." Accessed August 28, 2025. https://www.channelnewsasia.com/singapore/phishing-scams-banks-telcos-shared-responsibility-framework-dec-16-responsibilities-duties-4699236. "Online Criminal Harms Act 2023 - Singapore Statutes Online." Accessed August 28, 2025. https://sso.agc.gov.sg/Act/OCHA2023.

the OCHA was given to Meta into impersonation scams using the likeness of Singaporean government officials. Authorities are now reviewing Meta's efforts, with noncompliance potentially resulting in fines of S$1,000,000 plus another S$100,000 daily.[55]

Australia's Scams Prevention Framework (SPF), a part of an updated *Competition and Consumer Act*, imposes obligations on telecoms, banks and digital platforms, with penalties for noncompliance. Specifically, the SPF obliges regulated entities to detect, disrupt, prevent, and report scams, as well as creating documentation on how these obligations are governed and executed in their organization. This holistic approach is intended to ensure entities implicated in scam and fraud activity are taking "reasonable steps" to tackling fraud and scams within their domains. The SPF involves different regulatory agencies in the verification of SPF obligations, the Australian Securities and Investment Commission oversees financial institutions, the Australian Communications Media Authority telecoms, and the Australia Competition and Consumer Commission for digital platforms.

The SPF also provides vehicles for victims of scams to seek compensation, obliging each actor to establish an internal dispute resolution system, as well as allowing redress through the Australian Financial Complaints Authority.[56] This does not mean that redress for scams is mandatory, but sets up a "no wrong door" system for scam victims. Redress can be decided through these mechanisms or a private right of action, where liability for losses will be weighed against the party's adherence to their responsibilities under the SPF.

Rensburg, de van. "Meta Singapore Ad Rules: New OCHA Compliance Requirements." *Fixfb.Co.Uk*, March 7, 2025. https://fixfb.co.uk/meta-singapore-ad-rules-ocha-compliance/.

[55] Christine Tan. "Authorities to Assess Meta's Compliance with Directive to Curb Govt Official Impersonation Scams: MHA." *The Straits Times* (Singapore), November 2, 2025. https://www.straitstimes.com/singapore/courts-crime/authorities-to-assess-metas-compliance-with-directive-to-curb-govt-official-impersonation-scams-mha.

Christine Tan. "Police to Issue Meta First Online Harms Order in S'pore to Fight Scams; Possible Fines of up to $1m." *The Straits Times* (Singapore), September 3, 2025. https://www.straitstimes.com/singapore/police-to-issue-meta-first-online-harms-order-in-spore-to-fight-scams-possible-fines-of-up-to-1m.

[56] Commission, Australian Competition and Consumer Commission. "ACCC Welcomes Passage of World-First Scams Prevention Laws." Text. February 13, 2025. Australia. https://www.accc.gov.au/media-release/accc-welcomes-passage-of-world-first-scams-prevention-laws.

Chakravarti, Jayant. "New Australian Law Makes Banks, Telecoms Liable for Scams." BankInfo Security, February 13, 2025. https://www.bankinfosecurity.com/new-australian-law-makes-banks-telecoms-liable-for-scams-a-27516.

The Treasury, Australian Government. "Scams Prevention Framework – Protecting Australians from Scams." Gov.Au, 2025. https://treasury.gov.au/publication/p2025-623966.

The EU's Digital Services Act requires social media platforms of sufficient size (i.e. Facebook, Instagram, TikTok, etc.) to remove illegal content when reported, and to regularly report on the measures they take to combat illegal content on their platforms. Recently, the EU parliament has also approved laws that create liability related to this duty. In particular, the EU has proposed to make social media platforms liable to payment processors like banks. This liability is limited, since it only applies when the content has previously been reported and had not been removed, and transitive; it moves the liability for damages from payment processors to social media platforms.[57]

Information and Transparency

Intelligence Sharing

Addressing online scams requires the cooperation of institutional actors, including relevant consumer protection authorities. Intelligence sharing helps each actor identify and prepare its systems to identify and respond to new tactics and campaigns. From a policy perspective, this can mean requiring social media platforms to provide data on advertisements they have removed from their platforms, as well as user reports for scams.

The Australian SPF requires businesses to share intelligence on scams with the Australian Competition and Consumer Commission (ACCC) and gives it power to monitor efforts to proactively prevent and disrupt scam activity. In cases where these obligations are not met, the framework allows for the imposition of fines up to $50 million AUD. The same is true in Singapore's OCHA, which obliges designated providers to inform relevant authorities of detected trends in scam and malicious cyber activities and their response, and to retain data about accounts used in criminal activities for a minimum of 90 days.

Intelligence sharing, as well as other transparency features like Ad Libraries, allow researchers and authorities to track emerging trends and tactics and formulate

[57] European Union. "Digital Services Act." EUR-Lex, February 17, 2024. https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html.
Giovanna Faggionato and Eliza Gkritsi. "Social Media Giants Liable for Financial Scams under New EU Law." POLITICO, November 27, 2025. https://www.politico.eu/article/social-media-giants-meta-tiktok-liable-for-financial-scams-under-new-eu-law/.
"Payment Services Deal: More Protection from Online Fraud and Hidden Fees | News | European Parliament." November 27, 2025. https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees.

effective response, create information to protect consumers, and disrupt criminal networks.

Ad Libraries and API Access

Retention and access to information about online ads is important to understand and stem the spread of scams on advertising platforms. To comply with retention and access legislation, advertising platforms can maintain "ad libraries" which keep a record of advertisements and campaigns run through their platforms. For researchers, regulators and authorities, ad libraries are an important resource and can be used to monitor and detect campaigns, threat actors, and tactics employed by scammers. Access to information is most effective when it supports systematic, historic access to advertising copy, tailored to the needs of the requesting party.[58] However, programmatic demand-side platforms that facilitate ads on the open web, like Google's DV360 , Amazon DSP, or The Trade Desk, DSP are not currently required to maintain creative ad libraries.

Many advertising marketplaces maintain ad libraries, but they are not all created equal.[59] Meta, for example, maintains an ad library for all ads currently running on its platforms, although with important limitations. Meta's Ad Library only shows currently running versions of ads, except in the EU, where the DSA requires ad copy to be retained for at least one year.[60] If ad copy is changed, previous versions are no longer available in the ad library. If campaigns are withdrawn, no trace is left behind. The exception is advertisements self-identified as "political," which are archived. Given the tactics of scammers to avoid detection, retention of advertisements and ad copy, and details of advertisements and advertisers who have been removed from the platform for fraudulent and other illegal activities should be a goal for any proposed regulatory response.

For advertisers, regulatory interventions promoting transparency can also improve their position when advertising on major AdTech platforms. The EU Digital Markets Act, for example, obliges "gatekeepers" like Meta, Google and Amazon to provide

---

[58] Spark Ninety. *Online Advertising Programme Market Insights: Final Report*. Department of Digital, Culture, Media and Sport, 2022. https://www.gov.uk/government/consultations/online-advertising-programme-consultation.
Social Media Lab. "The Hidden Game: How Scammers Use 'Chameleon Ads' to Bypass Meta's Moderation." *Social Media Lab*, April 21, 2025. https://socialmedialab.ca/2025/04/21/the-hidden-game-how-scammers-use-chameleon-ads-to-bypass-metas-moderation/.
[59] Craig Silverman. "A Guide to Investigating Digital Ad Libraries." Indicator, October 3, 2024. https://indicator.media/p/a-guide-to-investigating-digital.
[60] Meta Business Help Center. "About the Meta Ad Library." 2025. https://www.facebook.com/business/help/2405092116183307.

free and comprehensive data on campaign results. This gives advertisers more information about the performance of their campaigns, and can help them to detect potential ad fraud, and give them more control over what kinds of content their ads are served with.[61]

Regulatory intervention should go further in recognizing the importance of specifying what information must be included in advertising libraries, and how long data should be retained. This serves two complementary purposes: for researchers and regulators, ad libraries are important resources for detecting and tracking fraud campaigns. For advertisers, library access provides an important resource for keeping the marketplace for online advertising fair and transparent.

Advertiser Verification and Know-Your-Customer Laws

"Know your customer" (KYC) rules create requirements for entities to verify the identities of entities they work with and may even validate that they meet advertisers that qualifies them as legitimate.[62] In the context of online scams, KYC requirements are typically applied to digital platforms. KYC would mark a shift to proactive authentication of participants in the digital advertising market, a change from the current reactive whack-a-mole report-and-takedown cycle. Verification of at least some advertisers is required in Australia, Singapore, and the European Union. In Australia, the SPF creates requirements for digital platforms to verify the legitimacy of advertisers of financial products, requiring them to provide a financial services valid license. Compliance with the OCHA has led Meta to adopt verification requirements for all advertisers running campaigns in Singapore, with verification including declaration of the advertisement's beneficial owners and funding source. In the EU, the Digital Services Act also requires Meta Ads that can be served to EU residents to include information about beneficial ownership and funding [63]

---

[61] Spark Ninety. *Online Advertising Programme Market Insights: Final Report*. Department of Digital, Culture, Media and Sport, 2022. https://www.gov.uk/government/consultations/online-advertising-programme-consultation.

[62] Spark Ninety. *Online Advertising Programme Market Insights, p.42*

[63] CNA. "Facebook to Verify Identities of All Advertisers amid Rise in Scams." Accessed August 28, 2025. https://www.channelnewsasia.com/singapore/meta-facebook-advertisements-verify-identities-advertisers-rise-scams-mha-carousell-ocha-4989486.
Taylor, Josh. "Meta to Force Financial Advertisers to Be Verified in Bid to Prevent Celebrity Scam Ads Targeting Australians." Australia News. *The Guardian*, December 1, 2024. https://www.theguardian.com/technology/2024/dec/02/meta-to-force-financial-advertisers-to-be-verified-in-bid-to-prevent-celebrity-scam-ads-targeting-australians.
European Commission. "The Impact of the Digital Services Act on Digital Platforms | Shaping Europe's Digital Future." European Commission, 2025. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms.

Although Meta has also offered an optional paid verification for businesses since 2023, it has generally tried to avoid required verification for advertisers. Meta argues that mandatory verification would present a significant burden on advertisers and drive them away from the platform.[64] Nonetheless, they have complied in the EU, Singapore and Australia. Microsoft and Google also have advertiser verification requirements, with Google required to give political advertisements additional scrutiny.[65] While the effects on advertiser verification on the proliferation of scams, as well as legitimate vendors (domestic and international) is worth study, data from Singapore and Australia provides some indication that verification is effective at reducing the volume of scams.[66]

Industry-led, voluntary approaches similar to advertiser verification also exist, primarily addressing malvertising risks on more open display advertising marketplaces. Buyers.json and DemandChain, both part of the Interactive Advertising Bureau's OpenRTB standards, allow publishers and their partners to see and verify the reputations of the advertisers that bidding DSPs represent. Recommended by the UK's National Cybersecurity Centre, adoption of buyers.json may help thwart malicious advertisers from serving their ads on mainstream publishing platforms but must be accompanied by intelligence sharing for maximum effectiveness.[67]

KYC policies can also help to build transparency for advertisers and publishers alike to help prevent ad fraud. Robust KYC data could be used, in conjunction with ad library access, to provide necessary checks on the advertising market's plethora of advertisers. In turn, advertisers can use information about publishers to verify their

---

[64] Horowitz and Ad-Yeung, 30

[65] Google for Developers. "Advertiser Identity Verification | Google Ads API." Accessed August 28, 2025. https://developers.google.com/google-ads/api/docs/account-management/advertiser-identity-verification.
sling-distribution-importer. "Making Microsoft Advertising Safer with Advertiser Identity Verification." Accessed August 28, 2025. https://about.ads.microsoft.com/en/blog/post/june-2023/making-microsoft-advertising-safer-with-advertiser-identity-verification.

[66] Ministry of Home Affairs. "Assessment of Carousell's and Meta's Enhanced Verification Measures Under the E-Commerce Code of the Online Criminal Harms Act." 2025. https://www.mha.gov.sg/mediaroom/press-releases/assessment-of-carousell-and-meta-enhanced-verification-measures-under-the-e-commerce-code-of-the-online-criminal-harms-act/.
National Anti-Scam Centre. "Australians Better Protected as Reported Scam Losses Fell by Almost 26 per Cent." Text. March 11, 2025. Australia. https://www.nasc.gov.au/news/australians-better-protected-as-reported-scam-losses-fell-by-almost-26-per-cent.

[67] buyers.json. "Buyers.Json." https://www.buyersdotjson.org.
National Cyber Security Centre. "Guidance for Brands to Help Advertising Partners Counter Malvertising." National Cyber Security Centre, November 6, 2024. https://www.ncsc.gov.uk/guidance/guidance-brands-advertising-partners-counter-malvertising.

ads are served on legitimate websites, instead of on Made for Advertising sites, disinformation outlets, or other low-quality locations.

Content Moderation

Notice and Takedown and Trusted Flaggers

When authorities detect and report fraud or malvertising campaigns, anti-scam legislation gives them the power to force platforms to remove these ads. Without enforcement, removal of illegal content by platforms can become inconsistent and slow. Because of the scale at which ads can be shown to users however, ads can be shown to large numbers of users even if they run for a very short time. In Singapore and Australia, as well as in Taiwan, anti-fraud laws now mean failure to remove identified scam ads can invite monetary penalties. Insofar as platforms are underinvested in proactive measures to remove fraudulent activity, notice and takedown duties are required to intervene quickly and effectively to protect users. Even if platforms become more invested in removing fraudulent content, participation in detection by third parties will still be necessary to deal with campaigns that go initially undetected, as in the case of chameleon ads. It is also important to recognize that scammers often can spin up new accounts once old ones are compromised, which keeps the scams going under new names – meaning that a narrow focus on removing ads doesn't attack the root of the problem.

Here, non-governmental and research organizations can also play a role. The EU DSA creates a special classification for "trusted flaggers," organizations like financial institutions, NGOs and companies with a validated expertise in media ecosystem observation that includes systematic monitoring illegal content, like scams and scam networks operating under multiple identities. Under the DSA, reports submitted from trusted flaggers must be given priority consideration by platform operators. The responsiveness of online platforms in dealing with reports can be inconsistent, but observers in the EU note responses are significantly faster when reports come from trusted flaggers, but only in some cases. Trusted flaggers are limited to reporting only 20 URLs at a time. In cases where bulk reports are made, Meta's moderation can take up to a month to remove the content. These trusted flaggers face a major uphill battle, with less than fifty operating across the whole EU and facing down millions of scam posts on Meta platforms.[68] Notice and takedown obligations are an important

[68] European Commission. "Trusted Flaggers under the Digital Services Act (DSA)." December 1, 2025. https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa.
Mei-Ling McNamara, Nico Schmidt, Pascal Hansens, Lorenzo Buzzoni, and Paula Zwolenski. "Investment Scammers Slip through Cracks in EU Big Tech Law." Investigate Europe, October 15,

part of a holistic anti-fraud strategy but are not enough on their own. They rely on transparency and intelligence sharing arrangements, as well as liability and enforcement.

Data Restrictions

Restrictions on the creation, sale, and transfer of data can also be used to protect users from online scams. Baking in privacy protections like Apple's ATT did address one of the root causes of scam proliferation, personal data aftermarkets that help scammers to track and target victims. Since then, new workarounds like fingerprinting have been developed to circumvent these measures, with support from AdTech giants like Google to further cement their dominance in the advertising market. No matter how much focus companies like Apple puts on privacy, this will do little to protect users that interact with other online surveillance platforms. The clearest example, users of the Google-controlled Android platform are using an operating system practically built for surveillance advertising.[69]

The EU Digital Services Act introduces prohibitions on targeting minors and targeting based on sensitive data such as a person's ethnicity, religion, or politics.[70] While not as categorical as proposals such as the Banning Surveillance Advertising Act in the US, the DSA begins to address the underlying connection between pervasive collection of sensitive information and vulnerability to scams.[71]

While the OPC has provided guidance on the use of sensitive personal information, there is little real constraint on the collection and creation of information that can be

---

2025. https://www.investigate-europe.eu/posts/investment-scammers-slip-through-cracks-in-eu-big-tech-law.
Thanos Sitistas and Lecua Bertoldini. *Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU*. European Digital Media Observatory, 2025. https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[69] Pieter Arntz. "Android Devices Track You before You Even Sign In." *Malwarebytes*, March 12, 2025. https://www.malwarebytes.com/blog/news/2025/03/android-devices-track-you-before-you-even-sign-in.

[70] European Commission. "The EU's Digital Services Act." European Comission, October 27, 2022. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
European Commission. "The Impact of the Digital Services Act on Digital Platforms | Shaping Europe's Digital Future." European Comission, 2025. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms.

[71] Rep. Eshoo, Anna G. [D-CA-18. "H.R.6416 - 117th Congress (2021-2022): Banning Surveillance Advertising Act of 2022." Legislation. January 19, 2022. 2022-01-18. https://www.congress.gov/bill/117th-congress/house-bill/6416.

used to extort and harm individuals.[72] The continued proliferation of sensitive data will only accelerate the proliferation of scams as generative AI technologies advance. Combined with personal information, the commercial availability biometric information is a major risk. If biometric information about people's voices and faces become available to scammers, it is only a matter of time before deepfakes not only of public figures, but of family and friends are used to target and defraud victims. Much stricter controls on the creation, collection, use and sale of sensitive personal information, are urgently needed.

Addressing the Monopoly Problem at the Core of Online Advertising

There is growing evidence of the effectiveness of legislative interventions on the proliferation of scams. Preliminary results of the SPF and other policies are promising in Australia, with the ACCC reporting a 24% year-over-year decrease in reported scams in the first half of 2025. The Australia New Zealand banking group also reported improvements coinciding with the introduction of the framework, with a 15% decrease in customer losses and improved prevention and recovery results, owing to an increased resource investment.[73] But regulatory approaches that stress compliance and transparency only address the symptoms of the underlying problems that have led to the proliferation of scams on online advertising systems. Halting the proliferation of scams online means addressing the root cause of this problem: the unwillingness of democratic governments to proactively address questions of internet governance. Over time, this has led to a concentration of power in the hands of a few companies whose business models revolve around continual

[72] Office of the Privacy Commissioner of Canada. "Interpretation Bulletin: Sensitive Information." May 16, 2022. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/.

[73] "ANZ Reports Drop in Scam Losses as Customers Embrace New Protections." Accessed August 28, 2025. https://www.anz.com.au/newsroom/media/2025/august/anz-reports-drop-in-scam-losses-as-customers-embrace-new-protections/.
National Anti-Scam Centre. "Australians Better Protected as Reported Scam Losses Fell by Almost 26 per Cent." Text. March 11, 2025. Australia. https://www.nasc.gov.au/news/australians-better-protected-as-reported-scam-losses-fell-by-almost-26-per-cent.
SBS News. "'New Weapon of Choice': Australians Are Reporting Fewer Scams — but Losing More." August 25, 2025. https://www.sbs.com.au/news/article/australians-are-reporting-fewer-scams-but-losing-more/dl26g4ebn.

engagement and pervasive surveillance, where user behaviour is tracked to sell advertisements.[74]

A lack of transparency and accountability facilitates this behaviour and allows Meta to set the rules in way that favour its profit, at the expense of users and legitimate advertisers. Rather than a problem to be tackled, scams are a risk to be managed, with the possible costs of regulatory penalties far lower than the profit they made from running scam ads. Other documentation reveals how Meta created systems to give the appearance of policing scams but were careful to maintain their revenue. Small scale scam accounts could sometimes receive up to 8 strikes against their accounts for breaking Meta's policies before action was taken. "High value accounts" could have up to 500 strikes before Meta acted. In cases where accounts were likely to be running scams, but that did not meet Meta's own 95% certainty threshold, Meta simply raised the prices for those accounts. If fees had increased enough that it eliminated the profit margins of scammers, they may have stopped running ads, but this is obviously not the case. Instead, all but the most obvious scammers paid a premium to run their campaigns, with Meta simply taking an increased cut.[75]

It is this concentration of power that allows companies to resist and dilute legislative and regulatory responses, and in some cases even flaunt compliance with the law. Any international regulatory effort in the coming years will meet the pushback of the partnership between Big Tech and the current U.S. administration. Today, compliance with existing efforts should be understood as strategic and provisional. Meta's implementation of advertiser verification, for example, functions on the assumption that Meta would verify legitimate advertisers and uniformly enforce its obligations to remove malicious advertisers. But scam advertisers continue to flourish on Facebook and Instagram, and Meta continues to profit from their presence. Recent research from the Tech Transparency Project found numerous prolific scam advertisers consistently in the top spenders for Facebook ads, spending millions of dollars to pump scams, often targeting seniors.[76]

The concentration of power in the hands of companies like Google and Meta creates a necessary focus on their platforms as the sites for policy interventions. For these

---

[74] Aleksandre Zardiashvili. "Internet Ozone Layer: A Vision for Reclaiming Human Freedom in Information Civilization." November 10, 2025. https://ssrn.com/abstract=5735624 or http://dx.doi.org/10.2139/ssrn.5735624

[75] Jeff Horwitz. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show." Investigations. *Reuters*, November 6, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

[76] Tech Transparency Project, Meta Awash in Deepfake Scam Ads (2025) https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads

interventions to be successful, Canada and other states must work to unwind the power that has been allowed to accrue in the market that fuels much of the internet. An anti-monopoly approach is a key ingredient to online spaces that are safe for users of all kinds. Canada needs to keep pace with its international peers in developing and passing holistic anti-scam legislation and invigorating existing authorities to target scammers and hold the platforms that enable them to account. But without working in concert with allies to break up the economic power that has been allowed to centralize, these efforts will always face an uphill battle.

What a Canadian Solution Can Look Like

With the uphill nature of the battle in mind, there are still concrete steps that Canada can take to begin reining in the world of scams facing everyday citizens. After the fact interventions, like trusted tagging programs and tribunals for victims are important interventions, but they are unable to address the true scale of online scams and their harms. Effective interventions must involve platform operators; they are the only actors who have sufficient information about activities in their networks and the power to intervene. Scams continue to wreak havoc on Canadians while the country's legal and regulatory frameworks remain underdeveloped in comparison to its peers.

The key ingredients to building an effective response to scams must address the systems that lead to their proliferation, namely, business models based on surveillance advertising at scale that make serving scams to users profitable, but essentially free of consequences. Currently, Australia has the most comprehensive and holistic approach to dealing with online scams, and it could serve as a model for Canada's approach. Australia's Scams Prevention Framework includes many of the key features identified in this research, including the assignment of responsibility and liability to large platforms, intelligence sharing and transparency requirements, and empowered enforcement. The SPF is also implemented within a similar legal and regulatory environment. Canada should seek to build a similar framework for addressing the epidemic of scams, while also targeting the surveillance advertising business models through restrictions on the commercial creation and use of sensitive data. This requires a Canadian commitment to capable and empowered regulatory bodies performing the roles of data protection and anti-fraud enforcement to accomplish three complementary objectives: protecting Canadians by regulating the use of personal data; creating an effective regulatory and enforcement environment through greater transparency and information sharing;

and incentivizing advertising platforms through the assignment of obligations and liability.

Protecting personal information and curbing surveillance advertising

Whether originating from privacy or specific scam-focused legislation, restrictions on the generation and collection of highly personalized data is a key step in cutting off the data flows that enable highly sophisticated scams and fraud online. States can and should exercise control over how private companies create and transact about their citizens. The availability of personal data, including sensitive information about individuals through data brokers, provides fuel for scammers to target vulnerable individuals and exploit the online advertising ecosystem.

Canada must adopt public and private sector regulations that define sensitive personal information and prohibit the use of these classes of information from being used in online advertising. This means revising and strengthening regulations around publicly available information and when profiles containing information sensitive enough to cause harm to individuals can be created, stored and sold. Once created, controlling the proliferation of these datasets is impossible. Legislation must go beyond weighing privacy against commercial interest and take seriously the potential and real damage caused by surveillance advertising.

Targeted advertising should be limited to specific classes of information and exclude protected classes. Health data, precise geolocation data and biometric information, like facial structure and vocal signature are strong candidates. These classes of data should be removed from the data structures and standards used for advertisement targeting. The use of other sensitive classes of information such as financial history, should have their uses constrained to limit the ability of data brokers to circulate information that fuels scams.

The CPPA, which updated Canada's data protection regime, proposed to expand the Office of the Privacy Commissioner of Canada's (OPCC's) investigatory powers and given them the authority to impose administrative monetary penalties. These penalties would have been levied by the Data Protection Tribunal, which would also have seen private claims relating to violation of data protection laws.[77] By

[77] Kirsten Thompson. "CPPA: An in-Depth Look at the Enforcement and Penalty Provisions in Canada's Proposed New Privacy Law." *Dentons Data*, November 30, 2020. https://www.dentonsdata.com/cppa-an-in-depth-look-at-the-enforcement-and-penalty-provisions-in-canadas-proposed-new-privacy-law/.

strengthening the OPCC's resources and mandate, and creating a Data Protection Tribunal, Canada would take a step towards a data protection authority with capabilities matching current realities.

Transparency for effective enforcement and fairer markets

Fighting scams, fraud, and other illegitimate activities online means entering an arms race where criminal capacity adapts and improves as defensive systems respond and technology evolves. But you can't stop what you can't track. The giants of online advertising have the greatest scope and depth of information in the ecosystem and maintain tight control over what information is provided to clients, researchers and regulators. Beyond this asymmetry between the platforms and external observers, the platforms themselves can use a strategic lack of information to obscure scams and fraudulent activity.

There are three categories of information that could address existing information asymmetries and equip businesses, researchers, and regulators with the tools needed for effective action: verification of advertisers and know-your-customer rules, systematic access to advertising libraries, and reporting and intelligence sharing on activities undertaken by platforms to address illicit activity. By mandating the collection and production of these sources of information, Canadian policymakers could supercharge existing responses to online scams and fraud.

For law enforcement, this information fuels existing intelligence sharing centres that disparate agencies use to track criminal operations and intervene. The National Anti-Fraud Centre, managed by the Royal Canadian Mounted Police, Ontario Provincial Police and the Competition Bureau, would be an ideal recipient of this information.[78] By creating a more direct link between online ads and the individuals and companies purchasing them and making that information available to law enforcement, Canada's national capacity to track and disrupt online scams and fraud would be augmented.

But the value of greater platform transparency extends beyond law enforcement. Researchers and other regulators must be able the assess effectiveness of platform responses if they are to compete with advances in scam and fraud practises. This means solidifying archiving and retention requirements for advertising copy libraries,

---

Tamara Nielsen, Ryan Black, and Tyson Gratton. "And Then It Grew Teeth: Canada's Privacy Law Gets enforcement-Laden Overhaul." DLA Piper, November 17, 2020. https://www.dlapiper.com/en-ca/insights/publications/2020/11/new-canadian-federal-privacy-statute.

[78] Government of Canada. "About the Canadian Anti-Fraud Centre." Government of Canada, January 31, 2020. https://antifraudcentre-centreantifraude.ca/about-ausujet/index-eng.htm.

focussed especially on content flagged as potentially fraudulent or otherwise illegal. Know-your-customer requirements give businesses whose brand identities and trademarks are infringed through impersonation leverage to have content removed and raise the hurdle for future misrepresentation. Finally, advertisers benefit from this increased transparency in the form of greater capacity to track where their ads are placed and who advertising platforms allow to offer and resell ad space.

Changing incentives with accountability and liability

Technical solutions and industry led standards already exist that address many of the features of the online advertising space that lead to scams and ad frauds. The goal for policymakers should be to solidify the use of these by clearly assigning responsibility and liability. Reporting of internal documents from Meta paint a picture of engineers willing and able to aggressively attack illicit activity on their platforms only to be stymied by management seeking to protect revenue.[79] If the inability to act decisively is the result of a cost benefit analysis, then increasing the cost of inaction is the way forward.

To do so, Canadian policymakers must follow the example of peers like Australia and develop a comprehensive piece of anti-scam legislation that lays out the obligations of key actors in the scam ecosystem, including online advertising platforms, telecommunications company, and financial institutions to proactively prevent, detect, and address scams. A range of technical and organizational solutions, such as improving automated checks when ad copy is uploaded and changed, and more comprehensive and timely content moderation complement restrictions on personal data and greater visibility and transparency in stemming the flow of scams. Requiring platforms to take proactive measures to prevent, detect, and address scammers is one thing; validating those efforts is another. Many of these processes are already in place, but their application is limited and inconsistent. Actions in support of these obligations must be supported by credible reporting and threat of sanction, fines and other forms of civil and criminal liability.

While legislation tailored to the contours of the modern scam economy is warranted, Canadian policymakers can also look to the expansion of the application of existing laws focused on preventing deception in the Canadian economy. The Competition Act's deceptive marketing provisions that provide both civil and criminal liability for

[79] Jeff Horwitz and Engen Tham. "Meta Tolerates Rampant Ad Fraud from China to Safeguard Billions in Revenue." Investigations. *Reuters*, December 15, 2025. https://www.reuters.com/investigations/meta-tolerates-rampant-ad-fraud-china-safeguard-billions-revenue-2025-12-15/.

false representations to the public are just one example of this potential.[80] The Competition Bureau's existing mandate to address false and misleading advertising is a promising mechanism against practices such as ad fraud and impersonation schemes where the quality or origin of advertising is being misrepresented. Echoing the 2020 settlement against Facebook for misrepresentations regarding privacy protections on the platform, with appropriate expansion this existing mandate could be trained on the adequacy of platform efforts to address scams on their platform.[81]

Taken together, these elements build on international regulatory efforts to create a promising Canadian response to an epidemic of scams affecting everyday citizens as they struggle under an ongoing cost of living crisis and businesses as they navigate unprecedented uncertainty. Today's online advertising system is a conduit to a tidal wave of scams and fraud that generate clear harms to people around the world. To begin stem that tide, Canada must do its part to rein in the world of scams.

[80] Sharon E. Groom, Joshua Chad, and Andrea Kroetch. *Misleading Advertising and Deceptive Marketing*. LexisNexis, 2025. https://www.lexisnexis.ca/pdf/2025/legal-brief/Misleading_Advertising_and_Deceptive_Marketing.PDF.
[81] Competition Bureau, *Facebook to pay $9 million penalty to settle Competition Bureau concerns about misleading privacy claims*. 2020. https://www.canada.ca/en/competition-bureau/news/2020/05/facebook-to-pay-9-million-penalty-to-settle-competition-bureau-concerns-about-misleading-privacy-claims.html

CANADIAN
ANTI-MONOPOLY PROJECT

www.antimonopoly.ca