TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

FRAUDULENT ADVERTISING ONLINE

EMERGING RISKS AND CONSUMER FRAUD

Key Messages

Summary

- A new report from Transnational Alliance to Combat Illicit Trade (TRACIT) and the American Apparel and Footwear Association (AAFA) shows that 70 major international brands were targeted by fraudulent advertisements on Instagram and Facebook since 2017, some of which received up to a quarter of a million views before they were detected.
- Fraudulent advertising is rapidly emerging as a new risk to consumers shopping online – presenting a new gateway to an old problem – the massive world of counterfeiting and piracy available throughout the Internet.
- Millions of consumers are exposed to thousands of fraudulent advertisements all over social media networks like Facebook and Instagram, or other popular websites like YouTube or Google, where people are not expecting fraud, taking them to thousands of illegitimate e-commerce websites that defraud and/or sell counterfeit products and deceitful services.
- Fraudulent advertising is of such professional quality that they easily deceive consumers, and when they are directed to a site from an advert on well-known and familiar website or app, they are more likely to regard the destination site as legitimate and trustworthy than if they had found it via a search engine or accidentally. This places extra responsibility on sites that host and provide optimization for advertising or receive payment for doing so.
- The TRACIT/AAFA report is intended help rid the Internet of widespread consumer fraud and counterfeiting. This means strengthening the ability of Internet platforms to defend against fraudulent advertising that lures consumers to illegal websites.

What is the problem?

- The international business community has aggressively fought trademark counterfeiting and other forms of consumer fraud for decades. One key learning is that criminals exploit weaknesses in supply chains and then amplify their efforts when they have landed upon a successful scheme.
- Internet-based platforms for social networking or shopping from home have inherent systemic weaknesses that enable criminals to exploit these gaps to sell any variety of counterfeit—or any illegal product or substance—with little risk of apprehension.
- The lack of sufficient policies and procedures to verify users’ true identity and to conduct the necessary vetting and due diligence during the onboarding process is a system weakness

across multiple Internet-based platforms for social networking and shopping. Deterrence can only be achieved when fraudulent advertisers are identified and punished.

What are the dangers?

- Consumer risks - Fraudulent adverts give innocent consumers a false impression of authenticity. Counterfeit goods are generally of poor quality, will not last, are not guaranteed, and may be dangerous.
- Business and brand owners - IP theft in the form of trademark counterfeiting and copyright piracy, stifles economic growth and job creation by discouraging innovation, reducing incentives for companies to invest in R&D and inhibiting creative industries from realizing their full potential.
- Data privacy - Most fraudulent websites show a disregard for data privacy of any type, including customer data, security, and financial information. Since these websites rarely use any form of security, consumers are often also exposed to credit card fraud, identify theft, and other cybercrimes.
- Organized crime - The fraudulent and infringing adverts discovered on Facebook often share similar characteristics and suggest that organized crime groups or organized illicit networks are operating these fraudulent ad campaigns.

What are the causes?

The root cause of the problem is that most social media platforms and e-Commerce websites accept advertising without proper controls over the source of the advertiser.

- Limited verification – Without robust due diligence checks that verify the identity of who is advertising on the platform, fraudulent advertisers are free to exploit the system with little risk of exposure and virtually no risk of punishment or penalty. The placement of a fraudulent advert can be done in just a couple hours at very little cost.
- System weaknesses – Fraudsters exploit system weaknesses, such as lacking controls on accounts sponsoring the fraudulent advertisements, such as account history or relevance between advertising accounts and the advertisement.
- No controls on destination websites - When Instagram or Facebook users click on fraudulent sponsored adverts, an in-app browser typically directs them to an external websites designed specifically to sell counterfeit or fraudulent products. In the absence of rogue destination websites, fraudulent adverts would have nowhere to redirect consumers. For these reasons, efforts have been directed at domain name registrars and Internet Service Providers to prevent or take down such infringing sites.
- Little protection from repeat infringers - It is not difficult to repeat a fraudulent advert, even after being reported.
- Deceptive practices - A fraudulent advert typically appearing on Instagram or Facebook targeting a well-known brand can be of very high design quality, showcasing hundreds of products images, often feature very high discounts and bogus logos for payment to entice consumers into a quick purchase.
- Online advertising supply chain – Demonstrated by the repeated similarities identified throughout this report, there is a systemic problem with the online advertising supply chain.

What needs to be done?

Advertising has long been regulated by governments to ensure that messages are truthful and do not mislead reasonable consumers about aspects of a product or service. In some countries, there is also consideration of fairness, which focusses on whether an advertisement causes substantial consumer injury. The same controls should be applied to online advertising. Fraudulent online advertising can be considerably reduced by the following measures:

1. *Enhanced "Know Your Business Customer" protocols*

Websites and social media platforms should know who they are working with when accepting paid advertising, by gathering and verifying individual/business name and street address (proven with recognised ID), phone number, email, and a proof of business registration.

2. *Rigorous review of advertisement prior to publication*

To ensure that their terms of service are being adhered to, and that no innocent consumers are being defrauded by fraudulent, scam advertising, all adverts published on a site or platform should be reviewed for infringing content, both algorithmically and where high risk has been flagged, manually. In addition, the external sites to which such adverts link should also be reviewed to determine their legality and authenticity.

3. *Effective reactive measures against fraudulent advertisers*

To act as an effective deterrent to illegal advertising activities, sites and platforms must establish strong, effective, and enforced measures against advertisers who have been found to infringe their terms of service. This should go beyond termination of the advertising agreement and include removal of the infringer's account and blocking the advertiser from the website or platform.

4. *Ensure consumers and rights holders can report and share information about fraudulent advertisers*

Until such time that advertising on websites and social media platforms have a robust system to prevent bad actors, there needs to be avenues for consumers and rights holders to share information that can be used to dismantle criminal networks currently operating on their platforms. Currently, while adverts can be reported and removed, platforms appear unreceptive to receiving trends and data-sharing initiatives that could assist them in blocking bad actors accessing advertising.

5. *Establish requirements for an e-business license for advertisers*

Such a license would require verification of (i) financial disclosures that can be corroborated by third parties (e.g., bank statements), and (ii) physical location information that can be supported by government records or trusted third parties. Such a system could be accompanied by a central registry ideally managed by a highly secure, disinterested party or industry group to maintain the licenses.

# # #

For more information, to arrange an interview, please contact:
Cindy Braddon
Head of Communications and Public Policy, TRACIT
Tel: +1 571-365-6885 / cindy.braddon@TRACIT.org / Twitter: @TRACIT_org
TRACIT and AAFA's report is available at: www.tracit.org/publications.