



**FRAUDULENT
ADVERTISING ONLINE
EMERGING RISKS AND
CONSUMER FRAUD**

EXECUTIVE SUMMARY

ABOUT TRACIT

The Transnational Alliance to Combat Illicit Trade (TRACIT) is an independent, private sector initiative to drive change to mitigate the economic and social damages of illicit trade by strengthening government enforcement mechanisms and mobilizing businesses across industry sectors most impacted by illicit trade.

ABOUT AAFA

The American Apparel & Footwear Association (AAFA) is the national trade association representing apparel, footwear and other sewn products companies, and their suppliers, which compete in the global market. Representing more than 1,000 world famous name brands. AAFA is the trusted public policy and political voice of the apparel and footwear industry. www.aafaglobal.org

FOR MORE INFORMATION

This document is an Executive Summary of the full report, Fraudulent Advertising Online, Emerging Risks and Consumer Fraud. To reference the full report and the more extensive analysis and case studies contained therein, please visit: www.tracit.org/featured-report-fraudulent-advertising-online.html

MEDIA

All media enquires should be directed to Cindy Braddon, Head of Communications and Public Policy, cindy.braddon@TRACIT.org

SOCIAL MEDIA

Twitter: @TRACIT_org

LinkedIn: www.linkedin.com/company/tracitorg

ACKNOWLEDGMENTS

We express our appreciation to Toe Su Aung and Sam Irving of Elipe, Ltd., for their diligent research and insightful guidance (www.elipe-global.com). We also appreciate the contributions of the many corporations who have identified and shared examples of fraudulent advertising of their products.

The objective of this report is to help rid the Internet of widespread fraud in advertising. The first step in this process is to shed light on the prevalence of fraudulent advertising appearing on shopping and social media platforms. Better educated consumers are in a better position to defend themselves against fraud. Whenever fraudulent advertisements are found, we suggest in the first instance that these are reported to the relevant platform on which they appear, and where appropriate to law enforcement or government regulators.

EXECUTIVE SUMMARY

What's the fuss about fraudulent advertising?

Fraudulent advertising is rapidly emerging as a new risk to consumers shopping online, where millions of consumers are exposed to thousands of fraudulent advertisements taking them to thousands of illegitimate e-commerce websites that defraud and/or sell counterfeit products and deceitful services.

In keeping pace with consumer trends—and to stay one step ahead of controls—illicit traders now post fraudulent adverts that divert unsuspecting consumers to websites featuring counterfeits, fake services, and other fraud. Of concern is that the adverts are all over social media networks like Facebook and Instagram, or other popular websites like YouTube or Google, where people are not expecting fraud.

This report shows that many popular international brands were targeted by fraudulent adverts on Instagram and Facebook since 2017, some of which received up to a quarter of a million views before they were detected. And just like legal adverts that seem to magically know what you are looking for, even before you started searching for it, fraudulent adverts are also often hyper-targeted at consumers based on specific interests, location, demographics or browsing history.

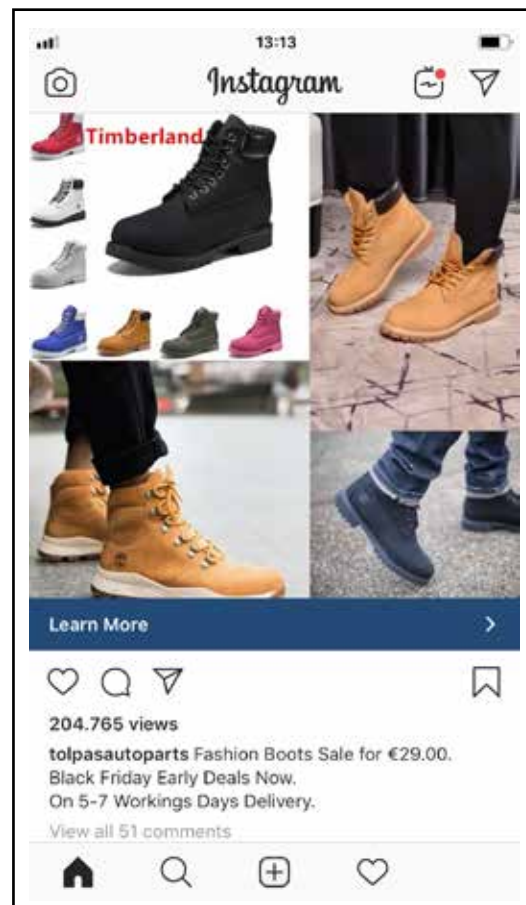
In addition to advertising fake and substandard products, there is a growing trend of deceptive advertising for fraudulent commercial and financial services, where names and images of popular personalities are used without authorization.

For consumers, their exposure to counterfeit goods and fraudulent services presents direct and indirect health and safety risks. Most fraudulent

websites also show a disregard for data privacy and expose consumers to credit card fraud, identify theft, and other cybercrimes. Even more alarming is evidence that a coordinated criminal network (or networks) are often behind the adverts.

Fraudulent advertising is everywhere online

- Since May 2017, more than 70 consumer and apparel companies confirmed to have been targeted by fraudulent and infringing sponsored adverts on **Instagram** and **Facebook**. (Figure 1).¹ The actual number is likely to be significantly higher, as these advertisers target brands indiscriminately



across multiple sectors. Given a common modus operandi, it appears there may also be a coordinated criminal network or networks behind the adverts, using hacked Facebook or bot-generated profiles together with stolen credit card data to post adverts that mislead consumers and direct them to e-commerce websites that defraud and/or sell counterfeit products.

- Fraudsters have used **Google's** video platform **YouTube** to exploit the popularity of certain popular video games to create videos that trick consumers to download risky apps or purchase bogus services. In worst cases, users are being tricked out of significant sums of money. One scam automatically charged a subscription fee of \$99.99. Within days, it generated over 118,000 views.² Also on YouTube, scammers are using COVID-19 to profit through easy-to-find videos touting overpriced face masks and bogus vaccines, costing consumers more than \$5 million.³
- In April 2019, an advert for fake Tommy Hilfiger apparel was identified on **LinkedIn**.

The advert was directing people to the rogue website www.tommy-top.com, that was identical to other fraudulent and counterfeit websites identified via **Instagram** adverts.

Fake adverts are intended to deceive

Just like legal adverts that seem to magically know everyone's online shopping wish list, fraudulent adverts are also often hyper-targeted at consumers based on specific interests, location, demographics or browsing history.

Moreover, tactics used by counterfeiters to confuse shoppers on Amazon or other e-Commerce platforms are similarly being used by criminals posting fraudulent advertisements. These deceptive tactics include the use of well-known trademarks, unauthorized images protected by copyright and fake offers to create extremely professional looking fake adverts that would be indistinguishable from legitimate adverts—except the hyperlinks divert consumers to criminal websites selling counterfeit items or fraudulent services.

Figure 1⁴

1. Adidas	21. Dewalt	41. Moncler	58. Stone Island
2. Apple	22. Dr. Martens	42. Montblanc	59. Superdry
3. Arc'teryx	23. Emporio Armani	43. Monsoon and Accessorize	60. Supreme
4. Ariat	24. Fila	44. Muck Boots (Honeywell)	61. The North Face
5. Balenciaga	25. Fjällräven	45. National Football League (US NFL)	62. Timberland
6. Berluti	26. Geox	46. National Hockey League (US NHL)	63. Tommy Hilfiger
7. Bose	27. Gymshark	47. New Balance	64. Tony Bianco
8. Braun	28. HP (laptops)	48. Nike	65. Trek (bikes)
9. Breville	29. Hugo Boss	49. Nintendo	66. TUMI
10. Brooks Sports	30. Husqvarna	50. Off-White	67. UEFA Football Club jerseys (including Juventus F.C., Liverpool F.C., Real Madrid C.F. and Tottenham Hotspur F.C.)
11. Calvin Klein	31. JBL	51. Patagonia	68. Ugg/Deckers
12. Camper	32. Keen	52. PlayStation (Sony)	69. Van Cleef
13. Canada Goose	33. Kenzo	53. Ralph Lauren	70. Vans
14. Canon	34. Kipling	54. Ray-Ban	71. Vasque
15. Carhaart	35. Lacoste	55. Salomon	72. Weber
16. Cartier	36. Lego	56. Saucony	73. Xbox (Microsoft)
17. Chanel	37. Levi's	57. SKECHERS	
18. Clarks (Shoes)	38. Louis Vuitton		
19. Converse	39. Makita		
20. Delonghi	40. Michael Kors		

For example, there was a significant spike in the number of fraudulent adverts posted by generic new accounts (e.g. “Fashion jacket store” and “Backpack discount”) in the two-week run-up to “Black Friday” in 2019. The adverts and the associated rogue websites offered huge unrealistic discounts targeting popular toys, handbags, winter jackets and boots, guitars, and fitness trackers, as well as many popular fashion clothing brands. Underpinning the scam is the consumer knowledge that discounts from legitimate brands may be higher than normal around Black Friday.

Hand in hand with the fraudulent advertising is the deployment of falsely displayed destination URLs within the adverts, multiple URL redirects, URL cloaking techniques and URL shorteners (bit.ly) to deceive consumers and prevent detection from investigators. These sophisticated URL redirects will often change the website destinations when a user clicks on an advert depending on whether the user is viewing the advert on a desktop browser or via the social network’s own app.

Economic impact

The emerging gateway to illicit sales online is a link from a fraudulent advert to a rogue website offering illicit products. Collected research provides evidence over time indicating there are hundreds of thousands of fraudulent adverts available, backed by large networks of scam and rogue websites ready to receive and defraud unsuspecting consumers. As highlighted in this report, the trend is to increasingly feature the realistic, but nonetheless fraudulent, adverts on social media platforms that can instantly reach millions of unsuspecting online users.

Although this report is not a quantitative study on the size and value of counterfeiting, important conclusions on the impact of fraudulent advertising can be drawn from current trends. According to a 2017 report by Frontier Economics, the global economic value of counterfeiting (not including digital piracy) in 2020 is approximately \$1.8 trillion.⁵ Online sales now represent between 14-16 percent of total global retail sales during the 2019-2020 time frame.⁶ Consequently, as a share of global counterfeiting, the value of counterfeits purchased through online outlets would equal \$252-288 Billion. This estimate compares reasonably to the 2018 Global Brand Counterfeiting Report, which estimates that the losses suffered due to online counterfeiting globally amounted to \$323 Billion in 2017.⁷

Sometimes the campaigns are fiercely aligned to global shopping events, where criminal networks are orchestrating the creation of hundreds of ad accounts, websites, hosting and payment infrastructures in order to maximize their return on investment whilst competing against the legitimate brands in the same space. Some of the fraudulent adverts for well-known brands can attract a quarter of a million views in a single day. In another example, one fraudulent advert Instagram for counterfeit goods used a domain linked to 3,200 other rogue domains, all featuring ‘high discounts’ for branded items and no contact information.

Given that counterfeiting increased by 154 percent over the last decade and that online shopping is increasing by 10-20 percent per year, if left unchecked, this problem will continue to grow.⁸

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, identity 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 website operating a web shop. These are typically rogue 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. The fact that so many international brands have been targeted by fraudulent adverts using the same modus operandi over a three year period suggests social media platforms must take more robust measures on stopping recidivist activities relating to advertising or seek assistance from law enforcement.
- **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. They feature very high discounts and bogus logos for payment to entice consumers into a quick purchase.
- **Online advertising supply chain** – Given the repeated similarities identified throughout this report, it is evident that there is a systemic problem with the online advertising supply chain. In particular, the current absence of any substantive verification of an advertiser's commercial and/or personal identity and the review process for submitted ads themselves appears to be insufficient in tackling the scale of the deception and fraud occurring on social media platforms.

CONCLUSIONS

Given the findings of this report, there is a systemic problem with the online advertising supply chain and an urgent need to improve controls over it. For starters, governments must begin the process of establishing guidelines and standards. Several examples already exist and could be modified or expanded to include the challenge of eliminating fraudulent advertising:

- In the UK, new powers have been given to the communication watchdog Ofcom to force social media firms to act over harmful content, including violence, terrorism, cyber-bullying and child abuse. Ofcom will have the power to make tech firms responsible for protecting people from such content, including ensuring that the content is removed quickly and to minimizing the risks of it appearing at all.
- Germany introduced the NetzDG Law in 2018, which states that social media platforms with more than two million registered German users have to review and remove illegal content within 24 hours of being posted or face fines of up to €50 million.
- Australia passed the Sharing of Abhorrent Violent Material Act in April 2019, introducing criminal penalties for social media companies, possible jail sentences for tech executives for up to three years and financial penalties worth up to 10% of a company's global turnover.⁹

Some groups have been formed on Facebook to help raise consumer awareness about fraudulent adverts:

- Facebook *Ad Scambusters!* was created to raise awareness of the many fraudulent ads on Facebook. The group states that many of these ads look legitimate and have professional videos, images etc. It also explains that Facebook, Shopify, and PayPal profit from fraudulent ads, and make it very complicated to lodge complaints or get refunds. The group offers to help people learn how to research a site and make sure that it is legit before buying products online.¹⁰

- Facebook (*ProtectOthers*) *Ad Scams* group was created to alert people of the vast amount of scam ads that Facebook is allowing to circulate. The group encourages people to report fraudulent ads and warn others by sharing the advert's link to their page.¹¹

In the meantime, however, it is imperative that the websites and platforms which are making revenue from the provision of advertising services to criminal networks take action to identify and block them—for good. By immediately adopting best practices in “know your business customer” checks, platforms can mitigate against the risks right away. This problem is already at least five years in the making, so it is imperative to address the root causes that enable such profitable opportunities.

Consumers are entitled to an online browsing and shopping experience that is safe and secure from fraud. Online platforms connecting people and those that profit on commerce over their sites should be responsible, comply with the law and recognize the ethical/moral responsibility to assure consumers a safe and trusted environment. This paper suggests that the fraudulent online advertising can be considerably reduced by the following measures:

1. Enhanced “Know Your Business Customer” protocols

It is imperative that websites and social media platforms know who they are working with when accepting paid advertising. By gathering and verifying an appropriate amount of data on who is utilizing their advertising services, they will be better able to

- assess risk levels and proactively identify bad actors
- avoid recidivist infringing activity from previously removed accounts
- provide data on infringers to affected consumers, rights holders, and law enforcement

Data collected could include individual/business name and street address (proven with recognized ID), phone number, email, and a proof of business registration.

For example, Facebook (and Instagram) could make it mandatory to participate in two-factor authentication for any profile or page. For online shopping, and in particular sponsored advertising, transparency and being able to definitively attribute an advertiser is essential for consumer trust and safety. This means being able to have confidence that whoever is selling a particular product or service can be identified, contacted, and held to account if things go wrong. Being proactive and socially responsible to ensure market integrity and that shoppers are safe should be standard to companies worth billions.¹²

Ultimately, when jointly targeted by sustained criminal activity, there should be a determined willingness to work together and hold those ultimately responsible to account, and make it as difficult as possible for counterfeiters to continue to operate and infiltrate genuine buyer experiences.

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.

For its part, Facebook is aware of the issue and recently pointed to its anti-counterfeiting tools and efforts. In a recent post, Facebook recognized that the issue of fake goods is especially top-of-mind for advertisers in the lead up to the holiday season, and pledged that the company has “strict policies against counterfeit goods and other kinds of IP violations.”¹³ To prove that point, it revealed that in the first half of 2019, it removed 359,000 pieces of content on Instagram in response to 39,200 counterfeit reports submitted by brand owners. Furthermore, it claimed to be investing in machine learning and artificial intelligence “to help block or reduce the distribution of potentially counterfeit content on both Facebook and Instagram.”¹⁴

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 unresponsive 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.¹⁵ 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.¹⁶

NOTES

¹ Primary research conducted by TRACIT and AAFA member brands, Elipe Limited and unassociated brands (i.e., those that supplied examples).

² Lince, T. (2020). Kasper VPN scam: YouTube urged to combat fraudulent ads featuring third-party brands. *World Trademark Review*, 23 January 2020. Retrieved from: <https://www.worldtrademarkreview.com/kasper-vpn-scam-youtube-urged-combat-fraudulent-ads-featuring-third-party-brands>

³ Leskin, P. (2020, April 2). Scammers and grifters are hawking face masks and fake coronavirus vaccines on YouTube as the platform fails to moderate its content yet again. *Business Insider*. Available at: <https://www.businessinsider.com/youtube-videos-ads-face-masks-coronavirus-vaccines-misinformation-content-moderation-2020-4>

⁴ Screenshot captures of the identified fraudulent ads and the destination websites are available upon request.

⁵ International Chamber of Commerce. (2016) Available at: <https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/>

⁶ Statista. (2020). *E-commerce share of total global retail sales from 2015 to 2023*. n.p.: Statista. Available at: <https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/>

⁷ Global Brand Counterfeiting Report 2018-2020. See <https://apnews.com/ef15478fa38649b5ba29b434c8e87c94>

⁸ US Department of Homeland Security. (2019). Combating Trafficking in Counterfeit and Pirated Goods, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

⁹ BBC. (2020, February 12). Regulator Ofcom to have more powers over UK social media. *BBC*. Available at: <https://www.bbc.com/news/technology-51446665>

¹⁰ See <https://www.facebook.com/groups/stopfraudads/>

¹¹ See <https://www.facebook.com/protectothers/>

¹² Bradford, D. S. (2019, December 6). Facebook Ad Scams Are Hitting Users Hard, What Can We Do? *Buzzfeed*. <https://www.buzzfeed.com/davidsbradford/facebook-ad-scams-are-hitting-users-hard-what-can-cbr58l7wiq?fbclid=IwAR1mRgZntRfZmqQqvhhmV4-9X3rwMnQqer79bGohiP3MVOMrxBS4jxEEnng>

¹³ Facebook Business. (2019). *Good Questions, Real Answers: Protecting Brands Against Counterfeits*. Available at: <https://www.facebook.com/business/news/good-questions-real-answers-how-facebook-helps-brands-protect-against-counterfeits/>

¹⁴ Facebook for Business, at <https://www.facebook.com/business/news/good-questions-real-answers-how-facebook-helps-brands-protect-against-counterfeits>

¹⁵ This recommended by the American Apparel and Footwear Association (AAFA) in response to the US Memorandum on Combating Trafficking in Counterfeit and Pirated Goods.

¹⁶ FINRA's Central Registration Depository could be a model for this.

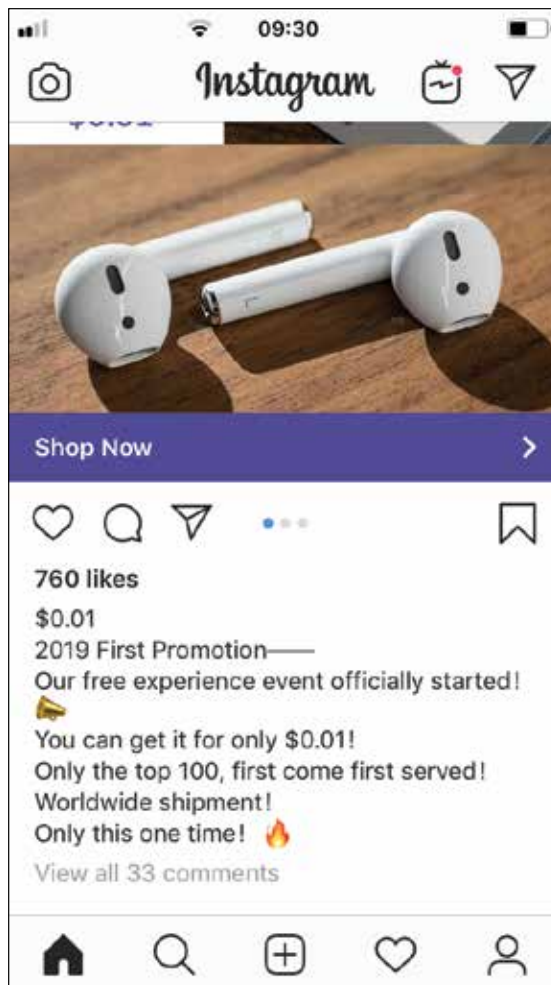
APPENDIX 1: EXAMPLES OF BRANDS

These examples have been either provided by brands or found through online research. Where the brands have provided these examples, permission has been given to include them in this appendix.

Apple

Ad Source: Fraudulent advertisements found on Instagram and via Facebook's Commerce and Ads IP Tool

Ad Image 1:



Ad Image 2:



Factory direct sales!

donottag.co

Big sales! 🏠🔥 Recently, my factory closed down and only these AirPods are left.

✅ Close to the cost price, ✅ a discount lower than the employee price, ✅ the cheapest AirPods you have encountered in your life! 🔥🔥🔥 Don't miss it >>> bit.ly/2Jz2C50 See Less




Ad ID: 23844633453950416

[f Donottaga1](#)
[@ donottaga14](#)

HP

Ad Source: Fraudulent advertisement found via Facebook's Commerce and Ads IP Tool

Ad Image:

	<p>HOT!! CLEARANCE~HP OfficeJet 5255 Wireless All-in... elcheer.com HOT!! https://bit.ly/2V5DtVL HOT!! https://bit.ly/2V5DtVL Limited time deal! ! Super deals that should not be missed! Free delivery. In order to get this discount, please buy as soon as possible! See Less Ad ID: 23844946626830106</p>	<p>Unelcheer unelcheer54</p>
	<p>HOT!! CLEARANCE~HP OfficeJet 5255 Wireless All-in... elcheer.com HOT!! https://bit.ly/2V5DtVL HOT!! https://bit.ly/2V5DtVL Limited time deal! ! Super deals that should not be missed! Free delivery. In order to get this discount, please buy as soon as possible! See Less Ad ID: 23844946626850106</p>	<p>Unelcheer unelcheer54</p>
	<p>HOT!! CLEARANCE~HP OfficeJet 5255 Wireless All-in... elcheer.com HOT!! https://bit.ly/2V5DtVL HOT!! https://bit.ly/2V5DtVL Limited time deal! ! Super deals that should not be missed! Free delivery. In order to get this discount, please buy as soon as possible! See Less Ad ID: 23844946624690106</p>	<p>Unelcheer unelcheer54</p>

Ad Notes: The destination URL from these adverts uses Facebook's own visitor tracking and analytics tool called Facebook Pixel highlighted in bold below:
[https://elcheer.com/shopping/uncategorized.html/hot%**F0%9F%94%A5%EF%BC%81**clearance%EF%BD%9Ehp-officejet-5255-wireless-all-in-one-printer/?fbclid=IwAR0ualOZp57uDDmoVkSqvBGScetIM_-vUBDNkmUQk16bXK7gjJEYT1S_q4](https://elcheer.com/shopping/uncategorized.html/hot%F0%9F%94%A5%EF%BC%81clearance%EF%BD%9Ehp-officejet-5255-wireless-all-in-one-printer/?fbclid=IwAR0ualOZp57uDDmoVkSqvBGScetIM_-vUBDNkmUQk16bXK7gjJEYT1S_q4)

Lacoste

Ad Source: Fraudulent Adverts identified on Facebook and Instagram

Ad image 1:

Active
Started running on Feb 17, 2020
ID: 640703013389384

Swetstore Shop
Sponsored

LACOSTE 🇵🇪 😊 envíos a todo el Perú PE



Ad image 2:

Instagram

Search

Log In Sign Up


trend_gomlek • Follow

trend_gomlek
1 Adet Gömlek 60 tl
✓ 2 Adet Gömlek 99 tl
✓ %100 cotton A+++ kalite
✓ Kapıda ödeme
✓ Şeffaf kargo
✓ Değişim var
✓ KAMPANYAMIZ KISA BİR SÜRE İÇİN GEÇERLİDİR ✓ SİPARİŞ İÇİN DM
#lacoste #moda #shirt #toplan #parekendesatış #istanbul #kalite

mehmet.karayil Toplan satışınız varmı fiyatları nedir
1d 1like Reply

49 likes
2 DAYS AGO

Log in to like or comment.



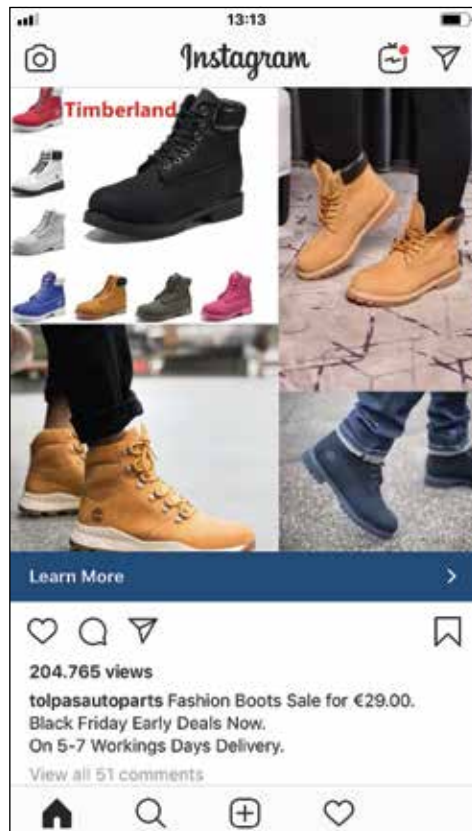
Timberland

Ad Source: Fraudulent advertisements found on Instagram

Ad Image 1:



Ad Image 2:



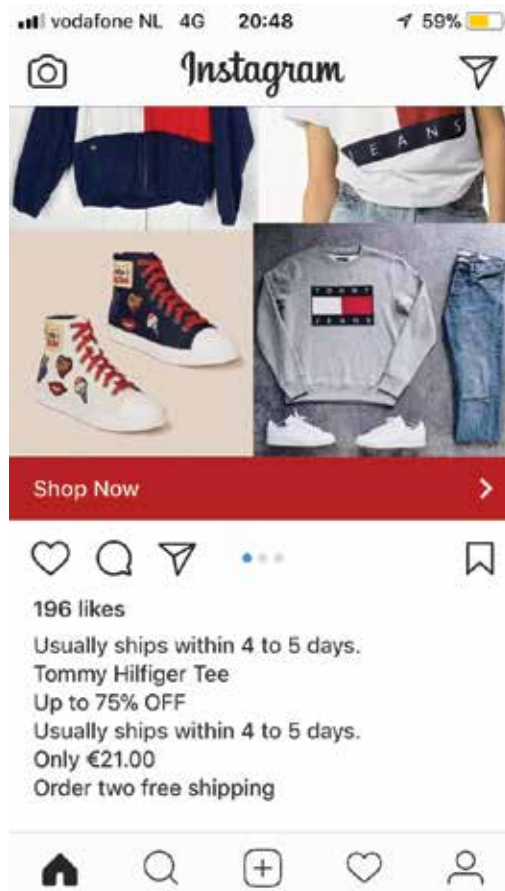
Tommy Hilfiger

Ad Source: Fraudulent advertisements found on Instagram and via Facebook's Commerce and Ads IP Tool

Ad Image 1:



Ad Image 2:





**TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE**

TRACIT.ORG

Transnational Alliance to Combat Illicit Trade
One Penn Plaza, New York, NY | +1.917.815.2824
email: info@TRACIT.org | TRACIT.org