TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

AMERICAN
APPAREL & FOOTWEAR
ASSOCIATION

FRAUDULENT ADVERTISING ONLINE

EMERGING RISKS AND CONSUMER FRAUD

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, its management and shareholders, its nearly four million U.S. workers, and its contribution of more than $400 billion in annual U.S. retail sales. www.aafaglobal.org

FOR MORE INFORMATION

This report is available online in PDF format, along with an Executive Summary and ancillary documentation. Visit www.tracit.org/publications.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 identifed 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 more than 70 major 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.

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 focuses on whether an advert causes substantial consumer injury.[1]

However, similar controls are not sufficiently applied to advertising on the Internet. While there are several new initiatives to address certain aspects of online advertising, more controls on fraudulent advertising appearing on legitimate websites including social media are needed.

Solutions could be driven by government leadership, through the application of offline advertising standards to today's online marketplaces. Such steps could ensure multi-factor verification systems or other mechanisms to support a "trusted" user program are applied to the act of fraudulent online advertising.

Leadership could also be taken by the major Internet platforms that are currently enabling the fraudulent practices. Notably Facebook and Instagram are not implementing sufficient verification of an advertiser's identity as they enter a commercial advertising relationship with these platforms.

Hand in hand with fraudulent advertising is the persisting presence of rogue websites specifically built to sell counterfeit or other illicit products.

In the absence of rogue destination websites, fraudulent adverts would have nowhere to redirect consumers. For these reasons, efforts taken concurrently with domain name registrars and Internet Service Providers can improve the prevention, blocking and removal of these infringing sites and, consequently, reduce the effectiveness of the fraudulent advertising schemes. Notably, the converse is also true that these websites would gain little to no traffic without advertising to divert consumers to them. Clearly, a holistic, across-the-board, approach is needed to address the misuse of Internet platforms for illicit trade.

Is there a reasonable solution?

The lack of sufficient policies and procedures to verify an advertising intermediary's true identity and conduct the necessary vetting and due diligence during the onboarding process[2] is a system weakness across multiple Internet-based social media and shopping platforms.

Therefore, requiring these intermediaries to provide sufficient and accurate information is a solution of the highest priority, especially when considering that those abusing the platforms will not be sufficiently deterred unless they can be identified and punished. A parallel example is the priority included in the January 2020 U.S. Department of Homeland Security (DHS) Report on Combating Trafficking in Counterfeit and Pirated Goods to significantly enhance vetting of third-party sellers by encouraging platforms to put in place a uniform and articulable vetting regime.

Similar verifications should be required for online advertisers, including the disclosure of certain verified information regarding sellers, such as identity, principal place of business, contact information, verified bank account information, government-issued photo identification, and a business tax identification number.

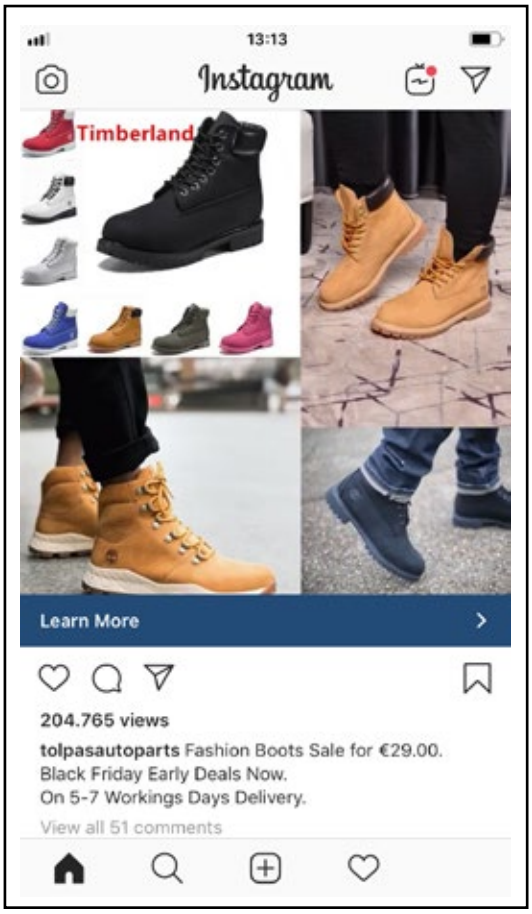
The objective of this report is to help rid the Internet of widespread fraud in advertising. Consumers should have a safe and secure shopping experience like that available offline. This means defending against the sale of fraudulent products consumers may find on their own as well as defending against the fraudulent advertising that lures consumers to illegal websites.

HOW BIG IS THE PROBLEM?

Fraudulent advertising is everywhere online

Fraudulent advertising has emerged as the latest online threat to consumers. In keeping pace with consumer trends—and to stay one step ahead of controls—illicit traders now post fraudulent ads that divert unsuspecting consumers to websites featuring counterfeits, fake services, and other fraud. Alarmingly, the adverts are all over social media platforms like Facebook and Instagram, or other popular websites like YouTube or Google, where people are not expecting fraud.

- 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.*** 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.[3] 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.[4]



- An advert on ***Facebook*** told a gloomy story of a Los Angeles family that died from COVID-19 as a trick to divert customers to a website selling protective face masks. Turns out the story is not true; the family is alive and well and the face masks for sale are unapproved.[5]
- 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.

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. In addition, many of these links are *only* accessible when viewed within the Instagram app (and not on the desktop browser). This means that counterfeiters have figured out precisely how to hide their activities from investigation by brands and possibly even the platforms themselves. Consequently, it can be extremely difficult to determine the actual destination website where potentially deceived consumers end up. And even if an originating fraudulent advert itself may be reported and removed from the platform, the website it once directed to will continue to operate and probably be used again in another advert. Moreover, some scammers use an innocuous website address when configuring an advert (such as a legitimate website from a department store) only to swap to a counterfeit website as soon as the advert has been approved and gone live.

By conducting reverse IP address investigations on these websites, it was also discovered that it was possible to find multiple other rogue websites selling counterfeit of many well-known brands. For example, the website http://oite.poitemall.com was identified from a Facebook advertisement targeting Japanese consumers. The website shares its IP address with 232 other domains/websites, including http://www.denlweshop.com which targeted the luxury brand Coach. Similar to the other counterfeit sites sharing the same IP address, this one likewise offered "80% off", displayed false company and address information about the website's operator and included a Russian email address (24service@bag-ok.ru) that did not match the domain name. This suggests there is a larger cybercriminal network utilizing these domains to exploit consumers across different search engines and social media platforms.

Product fraud and counterfeiting

Scams can spread like wildfire on social media, the very nature of which encourages us to share and like posts so that they are seen by as many people as possible. 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.

Some potential scams may seem innocent at first. For example, a simple quiz that ultimately gets you to reveal the answers to common banking security questions. There are also cases where scammers pose as your Facebook friends and reach out, claiming they are in urgent need of money.

This report is underpinned by data collected on more than 70 consumer and apparel brands confirmed to have been targeted by fraudulent and infringing sponsored adverts on Instagram and Facebook since 2017 (Figure 1).[7] The actual number is likely to be significantly higher, as these advertisers target brands indiscriminately across multiple sectors. Furthermore, the adverts are optimized to attract attention and can receive large numbers of views even if only active for a short period of time. It has been observed that some of these adverts have received over 240,000 views within just a couple of days. Given the size, scope and number of brands affected, the scale of the deception and fraud occurring on social media platforms cannot be underestimated.

Services fraud

In addition to fraudulent adverts of fake or substandard products, there is a growing trend of fraudulent advertising of commercial and financial services. Public figures such as UK financial journalist Martin Lewis[8] and Dutch businessman John de Mol[9] have spoken out about how their names and images have been used without authorization in adverts to promote fraudulent services and fake products. Both have taken legal measures to compel action against these scams.

Martin Lewis initially sued Facebook for defamation after a year in which over 1,000 scam adverts abusing his name or image had appeared on the platform, likely seen by millions of people in the UK. In response, Facebook acknowledged the scale of the problem, its impact on real people, and agreed to commit to making a difference both on its own platform and across the wider sector.

Dutch billionaire John de Mol filed a lawsuit against Facebook for allowing fake adverts on its platform, which used his name and image to perpetrate Bitcoin-related fraud. Lawyers for De Mol said that consumers had been swindled out of €1.7 million ($1.9 million) by the fraudulent

Figure 1[6]

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

adverts, and that he was only one of several Dutch celebrities targeted. In this case, the Amsterdam District Court found that while it may not be "technically easy" for a platform to take measures against these serious advertising scams, it is still the platform's responsibility to protect consumers.[10]

Certainly, Facebook's response to the Lewis case acknowledges at least a degree of responsibility and the Amsterdam Court's view calls for greater responsibility. However, while many popular websites and social media platforms provide tools for de-listing fake adverts based on IP infringements, these measures do not address the root problem. Unfortunately, even after being reported and removed adverts often reappear within 24 hours, with slightly different content. Fraudulent Ads have even been found appearing in "Instagram Stories" which only last 24 hours. That makes it impossible for brand owners to keep track of the threats and take effective action. One brand owner reported taking down an average 30 adverts every day on just one popular social media site.

Taken together, the question remains whether the platforms can and will improve preemptive measures to identify and block fraudulent adverts.

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.[11] Online sales now represent between 14-16 percent of total global retail sales during the 2019-2020 time frame.[12] 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.[13]

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.[14]

WHAT ARE THE DANGERS?

1. Consumer risks

Fraudulent adverts give innocent consumers a false impression of authenticity by using fake trademarks of popular brands and other infringements such as misrepresented images of genuine products, slogans, and corporate style. They often use words such as “discount”, “100% genuine”, “Official store”, ”90% off” or other wording designed to attract attention.

For brands and consumers, the threat posed by fraudulent adverts can be severe and their exposure to counterfeit goods poses direct and indirect health and safety risks.

Legal manufacturers abide by regulations and invest heavily in innovation and product development, with brands serving as guarantees of quality and safety. In contrast, counterfeiters make their money by sidestepping product safety regulations, environmental controls, and labor laws. Consequently, counterfeit goods are often of sub-standard quality or of unknown and sometimes dubious chemical/material composition.[15] Even relatively innocuous goods, such as watches, apparel and handbags can pose health risks for consumers when counterfeiters use potentially harmful materials (allergenic and/or toxic).[16] Examples include the use of prohibited carcinogenic dyes to color fabrics and children’s clothing made from highly flammable fabrics that burn quickly and intensively.[17] Counterfeit cosmetics and personal care products containing dangerous levels of lead, mercury, cyanide and other carcinogens can cause severe allergic reactions and pose a particular threat to pregnant women and their unborn babies.[18]

2. Business and brand owners

Today’s increasingly knowledge-based economy is driven and dependent on continuous innovation. In contrast, 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.

Fraud, especially involving the acquisition of counterfeits, severely damages the reputation of legitimate brands, as well as taking away potential customers. Counterfeit goods are generally of poor quality, will not last, are not guaranteed, and may be dangerous. When consumers are disappointed with the purchasing experience, it diminishes legitimate sales, which has consequences for investment, employment, revenue, and tax collection. Meanwhile, it also places additional demands on law enforcement agencies.

3. Data privacy

Most fraudulent websites show a disregard for data privacy of any type, including customer data, security, and financial information. (Figure 2.) Since these websites rarely use any form of security, consumers are often also exposed to credit card fraud, identify theft, and other cybercrimes.[20]

Another risk is linked to scam adverts concerning consumer goods. Adverts purporting to be from legitimate fast-moving consumer goods (FMCG) companies will offer free products, such as toothbrushes, toothpaste, or laundry detergent, in exchange for completing a survey or otherwise

Figure 2 [19]

inputting personal data. The data gathered through these means may then be used to further defraud the consumer through other phishing and cold-calling scams.

4. Organized crime

As noted by EUROPOL, "Trading in counterfeit products is a relatively low risk activity, involving minimal penalties whilst providing high profits, and will increasingly attract [organized crime groups] previously involved in other crime areas."[21] The fraudulent and infringing adverts discovered on Facebook often share similar characteristics, suggesting that organized crime groups or organized illicit networks are operating these fraudulent ad campaigns.

Further evidence of a sophisticated, coordinated criminal approach is found in the common application of the deceptive/misleading technological features and techniques. For example, fraudulent advertisements provide a visible URL of well-known online retailers (e.g., amazon.de, jdsports.co.uk and Zalando.co.uk) that also use Instagram to advertise. In some cases, the scams use the official URLs of the brands being counterfeited only to redirect consumers to a fraudulent website that mirrors the official one.

- In some examples, the adverts actually directed users to these retailers' websites, possibly indicating that they were initially configured to appear legitimate in order to pass Facebook's ad review stage – and then once approved they were edited to direct consumers to the fraudulent websites.
- The adverts use a series of URL redirects and utilize Facebook's own website analytics visitor and tracking tool, Facebook Pixel, to analyze the success of the adverts and improve the reach of new adverts in the next fraudulent campaign.
- The ad destination URLs sometimes did not direct to an active website, but the destination URL would have a .cn, .tw or .pw extension. In many cases, the websites are created using Chinese registrant details; however, these appear to be false or incomplete.

WHAT ARE THE CAUSES?

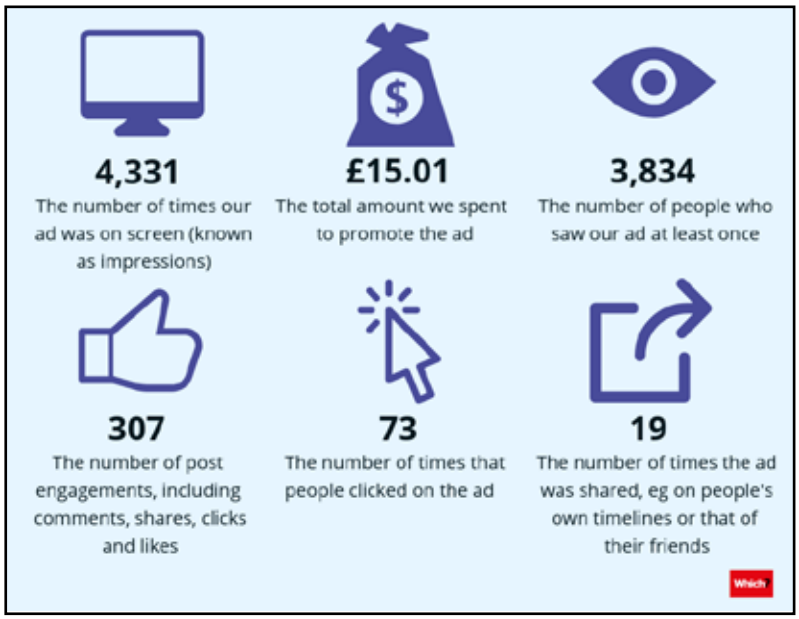
The root cause of the problem is that most social media platforms and e-Commerce websites accept advertising without proper controls over the source of the advertiser. In addition, weaknesses in the system that enable advanced technologies to generate and place the adverts are also a big part of the problem. There is also little protection from repeat offenders and the fraudulent adverts would have no purpose if it were not for larger failures which allow fraudulent, infringing and otherwise rogue websites and domains to exist.

1. 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. In fact a UK-based consumer interest journal recently demonstrated the ease of posting a fake scam ad on a popular social media site.[22] They reported 3,834 views, 73 clicks and 19 forwards all within 24 hours and for the small price of £ 15. (Figure 3.)

Figure 3



It appears that social media platforms, notably Facebook and Instagram, are not implementing sufficient substantive verification of an advertiser's identity as they enter into a commercial advertising relationship with such platforms; often as little as a credit card and an email address is enough to create an advertising account, both of which could be stolen from other unwitting customers. This is placing consumers at significant risk by exposing them to adverts by unknown parties intending the sale of counterfeit goods or other fraudulent practices. By adopting best practices in "know your business customer" checks, platforms can mitigate against this risk.

2. System weaknesses

Research has shown that a fundamental gateway to fraudulent advertising is the creation of an illegitimate hosting page. In order to be able to advertise on Instagram or Facebook, a Facebook account and page is required. However, there are no apparent controls on such accounts, such as account history, relevance to the advert, or level of activity.

What has been observed in the accounts posting the fraudulent adverts is that they are often (i) compromised (hacked) Facebook profiles/pages or (ii) a newly created bot-generated Facebook "Community" page.

- Many of the fraudulent sponsored ads are from compromised Facebook accounts of businesses or small organizations that have been "hacked" and have no connection to the advert that is being sponsored. For instance, a fraudulent advert for a (fake) Tommy Hilfiger shirt, might be artificially sponsored by some completely unrelated Facebook host, such as *"Business Insurances", "Medisch Pedicure"* or *"Georgian College Benefit Concert"*. With multiple high-profile personal data breaches in recent years, millions of email and password records have been exposed thus making compromised Facebook profiles and pages by cyber criminals more likely.
- A bot-generated account is a sophisticated operation, where a computer sets up a Facebook account or page which is then used to post the fraudulent adverts. These pages often contain unrelated, little or no information and no content. They are typically generated within a 6-month window of the advert going live, which gives the bot-generated pages a "legitimate" Facebook "footprint", which may be strengthened by bot-generated "likes" that build up a history on the platform.

3. 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.

For these reasons, domain name registrars and Internet Service Providers have been encouraged to prevent or take down such infringing sites. However, the converse is also true that these websites would gain little to no traffic without advertising that diverts consumers to them. While some consumers may discover these fraudulent websites through organic search results, a significant number will be diverted to them by the fraudulent adverts.

Efforts to clean up fraud online, must go hand in hand, so that social media platforms are kept aware of any websites being taken down which are linked to an advertising account on their platforms, so that they might check for other potentially infringing websites connected to the same account; where an advert is successfully taken down, the platform should also notify the relevant ISP and registrar so that they can take appropriate action against the registrant.

4. Little protection from repeat infringers

It is not difficult to repeat a fraudulent advert, even after being reported. This is partly because some adverts may avoid using IP-infringing brand names and keywords and partly because adverts often reappear in slightly different forms after being delisted—even after hundreds of similar adverts have been reported. The fact that so many international brands have been targeted by fraudulent adverts using the same *modus operandi* over a three year period suggest social media platforms must take more robust measures on stopping recidivist activities relating to advertising or seek assistance from law enforcement.

5. Deceptive practices

A fraudulent advert typically appearing on Instagram or Facebook targeting a well-known brand can be of very high design quality, showcasing the most popular product's images (typically taken from the original brand's website). They feature very high discounts,

usually 50% and above, and bogus logos for payment (e.g., Visa, Mastercard, Paypal) to entice consumers into a quick purchase. Domain name typically uses generic TLDs or ccTLDs (.top, .VIP, .tw, .pw, .online, .store, .club). Websites are not typically SSL secured (https); however, this appears to be changing.

Figure 4

Examples of deceptive marketing

"100% authentic"
"Free & fast delivery available"
"Official store online"
"No reason refund in 7 days"
"Secure payment"
'Factory direct price"
"Satisfied or refunded"
"Summer sales – only 3 day"
"Black Friday"
"Stock Clearance Sale"
"Warehouse Clearance Sale"
"90% discount"

In October 2017, an advert was identified with Facebook's *Commerce & Ads IP Tool*, which used images of counterfeit products. The URL displayed to consumers was "ebay.com" and the advertisement was sponsored by a "Community" page that appeared to be compromised with no affiliation or connection to the subject brand. The actual destination was www.saletommy.com, a fraudulent website, which made unauthorized use of Tommy Hilfiger copyright protected imagery and logos. The website did not have a "contact us" page or contact form, or any information to identify the entity responsible for its operation. On 10 November 2017, an advert by a Facebook page called *XZ Fancy Bread* was identified with over 18,000 "Likes". This ad directed users to the website www.clotheshe.com which was identical to www.saletommy.com. Six months later, on 18 April 2018, another fraudulent advert appeared, displaying to consumers the website address Love.sjut1i.cn, but was actually directing consumers to the destination website www.vote2018.site. The website www.vote2018.site was identical to both www.saletommy.com and www.clotheshe.com websites shown above. It is of note that when registering domain names with a .cn extension, registrants are required to verify their personal or business identity.

6. Online advertising supply chain

Given the repeated similarities of fraudulent adverts 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.

This is a problem that has been identified by many brand owners, operating in various sectors, and with numerous websites. It therefore requires a concerted, industry-wide solution. At present, brand owners are carrying the bulk of responsibility by taking down fraudulent websites and the adverts that link to them. But this is not going to solve the problem, as it is too big and fast-moving.

While it is appreciated that there is a need for a degree of anonymity for social media users in many situations, when use of a platform changes from personal use (social interaction and connection) to a commercial use (advertising of goods/services), there should be enhanced checks and transparency for potential customers into the identity of those commercial actors.

Platforms need to confirm that any data provided to an advertiser is complete, correct and not bot-generated and enhanced verification needs to be made of the external websites that adverts direct to in order to achieve this.

WHAT IS BEING DONE?

Despite its prevalence and harm, very little is being done to rid the Internet of fraudulent advertisements. Nonetheless, very little is being done to rid the Internet of fraudulent advertisements. In particular, the current absence of any substantive verification of an advertiser's commercial and/or personal identity along with a weak review process for submitted adverts are major vulnerabilities illicit traders exploit to deceive and defraud consumers online and particularly on social media platforms.

In response to mounting evidence—such as that contained in this report—along with pressure from brand owners and consumer groups and complaints from social media users, the platforms have recently promised improvements.

For example, Google has announced that it will require advertisers to verify their identity to prevent them from misrepresenting themselves.[23] Key elements of the program (as indicated) will be the requirement of personal legal information (like a W9 or IRS document showing the organization's name, address and employer identification number). There will also be a 30-day verification process, after which Google said it will suspend the account and the advertiser's ability to serve ads until verification is provided. Google also stated that advertising agencies will need to complete verification on behalf of each of their advertiser clients. And where businesses like pharmacies already must go through certification processes, they will still need to take the new, additional verification steps.

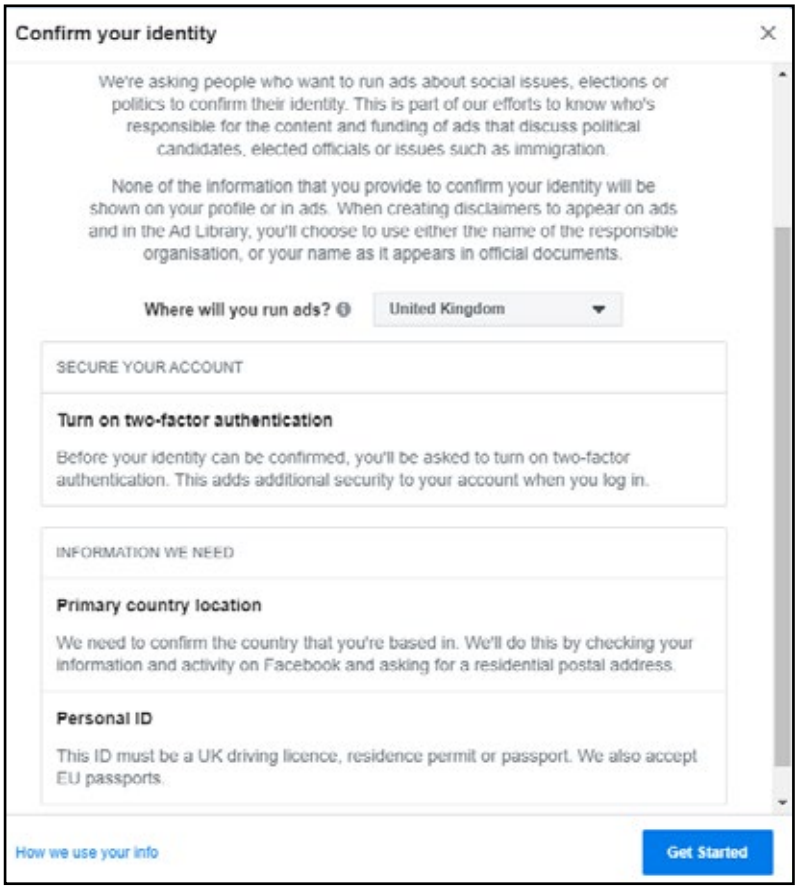
While the elements of this program are in the right direction, it will be important to evaluate its effectiveness to ensure that Google puts in place pre-emptive measures to block fraudulent adverts, such that burdens are not placed on consumers who do not have skills to police fraudulent adverts. It will also be essential that the program move swiftly. As presented the program will give feedback or provide approval within three to five business days, using a combination of human and tech reviews. Currently, Google policy is to make every effort to ensure that adverts which may violate their policies do not run prior to review, but that some may run on Google before the Google Ads Specialists check them.[24]

With regard to its popular YouTube platform, Google has ad policies that address misrepresentation and misleading content, copyright infringement, and trademark infringement. However, IP owners report that enforcement largely falls to them and the ability to monitor for such activity is limited by deceptive techniques employed by the infringers. Consequently, Google must consider taking proactive actions against fraudulent ad campaigns.[25]

In the case of Facebook, in the aftermath of a fraudulent Facebook ad for a company selling face masks, which claimed all but one member of a Los Angeles family died from COVID-19, Facebook pulled all versions of the advert. Furthermore, the company says in order to crack down on businesses taking advantage of fear during the coronavirus pandemic, it has banned all ads having to do with hand sanitizer, face masks, wipes, and COVID-19 tests.[26]

In some countries, Facebook also requires proof of identification for any user wishing to post advertisements relating to politics, elections, or social issues.[27] This is not, however, a global policy, nor does it extend to forms fraudulent advertising delineated in this report. (Figure 5.)

Figure 5



While some progress is being made, platforms, notably Facebook and Instagram, are not implementing sufficient verification of an advertiser's identify when they enter a commercial advertising relationship with such platforms.

At the minimum, all platforms should be implementing measures at least equal to the system Google is putting in place.

It should be incumbent on websites and social media platforms that offer and host advertising to make simple checks such as these before accepting advertising. Doing so could be done manually or, with appropriate software, automatically. Further to this, proactive checks should be made into the behavior of the advertisers at the point of registering ads; for example, since many of these adverts are registered using stolen credit card details, scammers may attempt to use multiple different stolen cards before finding one which allows a payment transaction. This behavior should be an immediate red flag to any website or platform which hosts advertising to manually review the legitimacy of the advert and advertiser profile.

In addition to these voluntary efforts by platforms to put in place more effective "know-your-business-customer" measures, there are some useful programs that could be applied to better defend platforms against fraudulent advertising. These programs draw on experience from programs that address the placement of "good" adverts on "bad" websites, where a legitimate company pays advertising revenues to operators of rogue sites.

Two examples are:

- TAG (the Trustworthy Accountability Group) has a "Certified Against Fraud" certification program, by which actors in the advertising supply chain can show they are taking action against fraudulent, invalid ad traffic. The primary focus of this programs is to tackle issues such as "click-fraud", where automated computer programs mimic legitimate web users to generate pay-per-click on an advert. Measures that could be applied to fraudulent advertising include Payment ID system to ensure payments track where payments are going, lists identifying of common IP addresses from which it is unlikely to expect legitimate ad traffic, disclosure requirements

for publishers to show how much traffic is from paid sources, and a public record of authorized digital sellers.

- The EU MOU on Online Advertising and Intellectual Property Rights aims to minimize the placement of legitimate adverts by IP owners or other advertisers on websites which sell counterfeit goods or provide access to pirated content. While the MOU is non-binding, it suggests that signatories involved in both the buying and selling of ad space adopt IPR policies and use (or require the use of) tools to prevent their advertising being placed on IPR infringing sites.[28] This MOU could be extended to include measures to defend platforms from fraudulent advertising.

Generally, consumers are becoming more aware and experienced at avoiding rogue websites that sell counterfeits and other fraudulent, substandard, or unsafe products. EUROPOL, for example, promotes Red Flags to help consumers detect fraudulent websites.

However, the problem with fraudulent advertising is that the advertisements are 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 and/or receive payment for doing so.

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.[29]

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.[30]
- 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.[31]

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.[32]

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."[33] 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."[34]

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.[35] 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.[36]

NOTES

[1] Azcuenaga, M. L. (1997). *The Role of Advertising and Advertising Regulation in the Free Market*. Washington, DC: Federal Trade Commission. Available at: https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market

[2] 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, p24

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

[4] 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

[5] 13abc. (2020, April 15). Mother finds fake Facebook ad claiming her family died from coronavirus. *13abc*. https://www.13abc.com/content/news/Mother-finds-fake-Facebook-ad-claiming-her-family-died-from-coronavirus-569652591.html

[6] Screenshot captures of the identified fraudulent ads and the destination websites are available upon request.

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

[8] Mason, C. (2019, January 23). Martin Lewis settles lawsuit as Facebook agrees to donate £3m to anti-scam charity and launch new scam ads reporting button. *Money Savings Expert*. Available at: https://www.moneysavingexpert.com/news/2019/01/martin-lewis-drops-lawsuit-as-facebook-agreed-to-donate-p3m-to-a/

[9] Sterling, T. (2019, June 5). Dutch 'Big Brother' creator sues Facebook over fake Bitcoin ads. *Reuters*. Available at: https://www.reuters.com/article/us-facebook-ads-netherlands/dutch-big-brother-creator-sues-facebook-over-fake-bitcoin-ads-idUSKCN1T61N5

[10] In both of these cases, the affected parties took legal action against Facebook as the platform they were seeing the most adverts on. For Lewis, a settlement was reached in which Facebook agreed to launch a new scam reporting tool for consumers in the UK and donate £3m to a project which would tackle these adverts. In De Mol's case on the other hand, Amsterdam district court ruled that Facebook must pay 10,000 euros each time fraudulent ads using the image of John de Mol appear, up to a maximum of 1 million euros. Sources: Klaassen, N. (2019, November 11). De Mol wint van Facebook: bitcoin-vonnis zet platform voor het blok. AD. Available at: https://www.ad.nl/tech/de-mol-wint-van-facebook-bitcoin-vonnis-zet-platform-voor-het-blok~a72ebabb/ ; Proper, E. (2019, November 11). Facebook Ordered to Ban Scam Ads Using Big Brother Founder. *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2019-11-11/facebook-ordered-to-ban-scam-ads-using-big-brother-founder

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

[12] 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/

[13] Global Brand Counterfeiting Report 2018-2020. See https://apnews.com/ef15478fa38649b5ba29b434c8e87c94

[14] 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

[15] WIPO. (2017). *The Environmentally Safe Disposal and Destruction of Intellectual Property Infringing Goods*. Geneva: WIPO. Retrieved from: http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_3_ppt.pdf

[16] Federation of the Swiss Watch Industry. (2018). *Thinking of buying a counterfeit product? Shame!* n.p.: Federation of the Swiss Watch Industry. Accessed 16 October 2018. Available at: http://www.fhs.swiss/eng/buy_counterfeit.html

[17] ITV. (2015, November 4). UK's first Fake Shop reveals danger of counterfeit goods. *ITV*. Available at: http://www.itv.com/news/westcountry/2015-11-04/rat-droppings-in-cigarettes-and-urine-in-perfume-fake-shop-reveals-danger-of-counterfeit-goods/

[18] Greenwood, C. (2015, May 17). Warning on fake make-up tainted by CYANIDE and other dangerous chemicals: Counterfeit versions of leading brands are being cooked up by criminals in squalid underground labs. *Daily Mail*. Available at: http://www.dailymail.co.uk/news/article-3085665/Warning-fake-make-tainted-cyanide-dangerous-chemicals-Counterfeit-versions-leading-brands-cooked-criminals-squalid-underground-labs.html

[19] MarkMonitor. (2019). Global Consumer Survey Social media: Insights into consumer shopping behaviour. n.p.: MarkMonitor.

[20] Muncaster, P. (2017, September 26). Police: Buying Fake Goods Online Can Lead to ID Theft. *Info Security*. Avaialble at: https://www.infosecurity-magazine.com/news/uk-police-buying-fake-goods-online/

[21] SOCTA. (2013). *EU serious and organised crime threat assessment (SOCTA 2013)*. The Hague: European Police Office. Available at: https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013

[22] Research by the consumer rights and reviews organisation which found that with just an email address, name, a few stock images and a credit card, it is possible to have an advertising account up and potentially defrauding consumers within 24 hours: Stanaway, C. (2019, June 27). How our fake 'scam' ad breezed through Facebook's approvals process. *Which?*. Avaialble at: https://www.which.co.uk/news/2019/06/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process/

[23] Graham, M. (2020, April 23). Google will make all advertisers prove their identities, so people can see who they are and which country they're in. CNBC. Available at: https://www.cnbc.com/2020/04/23/google-advertiser-verification-process-now-required.html

[24] Google. (n.d.). *Google Ads Help: Report an ad.* Accessed from: https://support.google.com/google-ads/troubleshooter/4578507?hl=en

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

[26] 13abc. (2020, April 15). Mother finds fake Facebook ad claiming her family died from coronavirus. 13abc. https://www.13abc.com/content/news/Mother-finds-fake-Facebook-ad-claiming-her-family-died-from-coronavirus-569652591.html

[27] See https://www.facebook.com/business/help/208949576550051?id=288762101909005

[28] European Commission. (2018). *Memorandum of Understanding on online advertising and IPR. Brussels: European Commission*. Retrieved from: https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en

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

[30] See https://www.facebook.com/groups/stopfraudads/

[31] See https://www.facebook.com/protectothers/

[32] 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=IwAR1mRgZntRfZmqQqvhhmV4-9X3rwMnQqqer79bGohiP3MVOMrxbS4jxEnng

[33] 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/

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

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

[36] FINRA's Central Registration Depository could be a model for this.

APPENDIX

TABLE OF CONTENTS

Appendix 1: Examples of Brands 21

Apple 21
Bose 23
Braun 24
Canon 26
Fujifilm 27
HP 28
Keen 29
Lacoste 31
LEGO 32
Levi's 33
National Hockey League (NHL) 34
Ray-Ban 35
Richemont (Montblanc) 36
SKECHERS 36
Star Wars (Disney) 37
Timberland 38
Tommy Hilfiger 39
Under Armour 40

Appendix 2: Customer complaints 42

Bose 42
Fjällräven 43
Dewalt and Milwaukee Power Tools 44
LEGO 45
Tommy Hilfiger 46
Weber 47

Appendix 3: Fraudulent Financial Services 49

Appendix 4: Japan Case Study 50

1. Brands Impacted by fraudulent Japanese Ads 50
2. Keywords in Ads 51
3. Brand infringing Facebook Pages used to advertise 51
4. Examples of Ads 53
5. Example destination websites 56

Appendix 5: COVID-19 related fraud 58

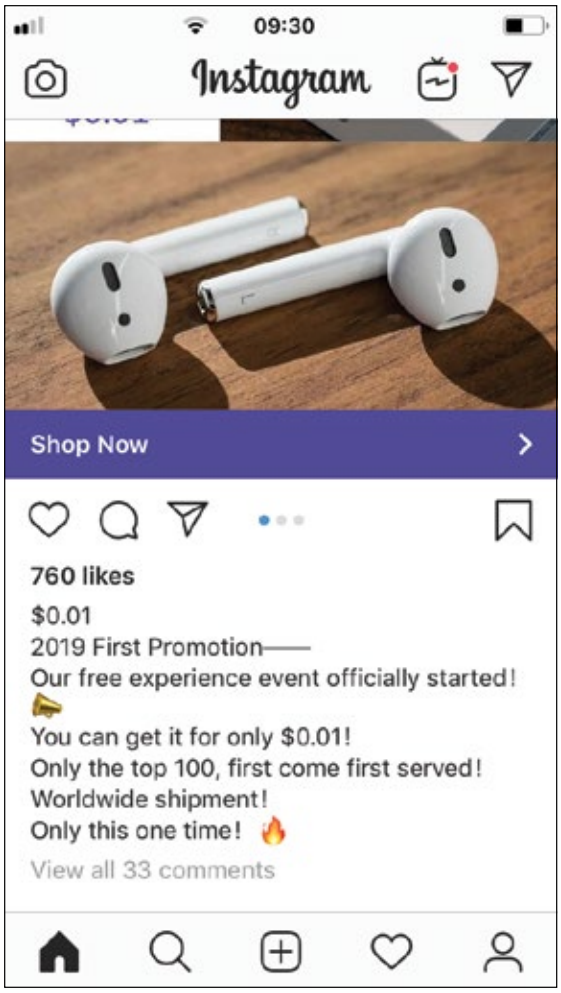
APPENDIX 1: EXAMPLES OF BRANDS

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

Donottaga1
donottaga14

Ad Notes: In the second example the Facebook advertiser's page was created in October 2019 shortly before the advertisement was identified and provided no contact or business information about the operator. The advertisement's destination website URL https://donottag.co/products/airpods-pro.

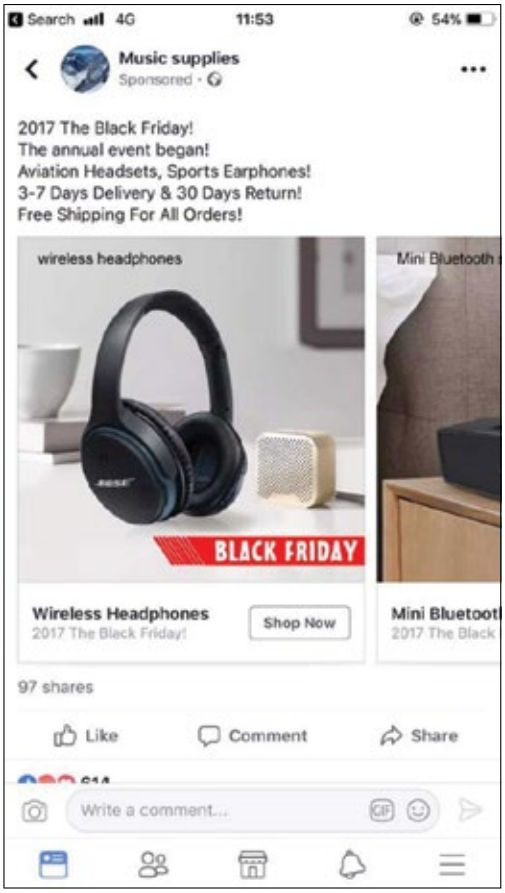
Ad 2 Destination Website Image:

On the destination website, the published contact email address (Destiny20190610@koko-erp.com) was different from the domain name and no company information was available. The website's Privacy Notice page provides shoppers with a Gmail email address: "*If you would like to: access, correct, amend or delete any personal information we have about you, register a complaint, or simply want more information contact our Privacy Compliance Officer at "eustaciaboyd3510@gmail.com".*

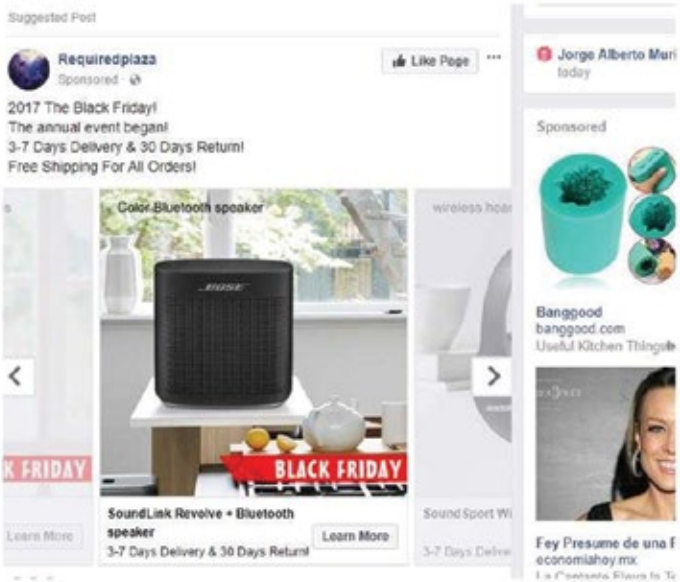
Bose

Ad Source: Frauduent advertisements found on Facebook

Ad Image 1:



Ad Image 2:

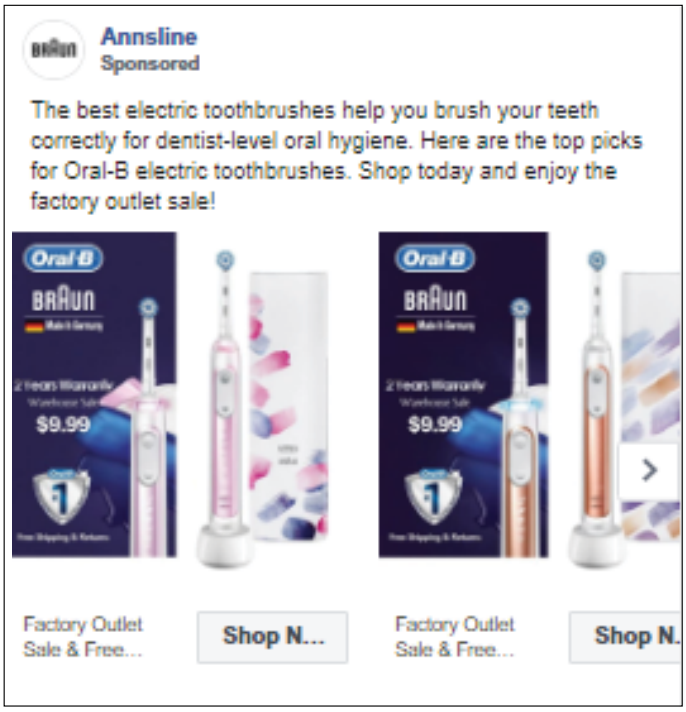


Braun

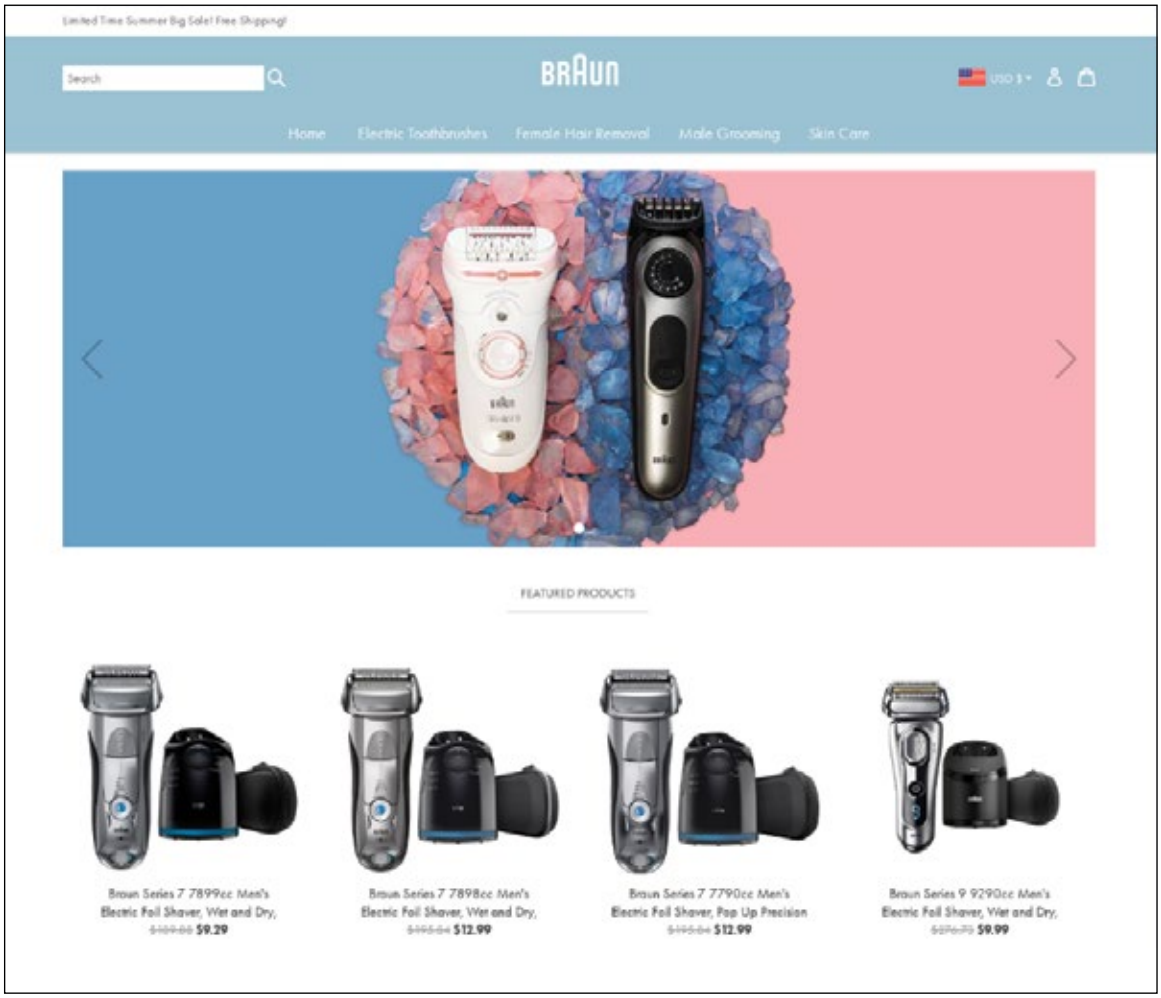
Ad Source: Fraudulent advertisement identified via Facebook's Commerce and Ads IP Tool

Ad Image 1:

Ad Image 2:



Ad Notes: The advertiser's page was created on 26 May 2020, four days before the adverts were identified. At the time of identification, the advertiser was running 120 different adverts for Braun shavers, toothbrushes and epilators. The ads destination website (https://www.annsline.com) is designed to appear like an official Braun website, but with unrealistic discounts:



Canon

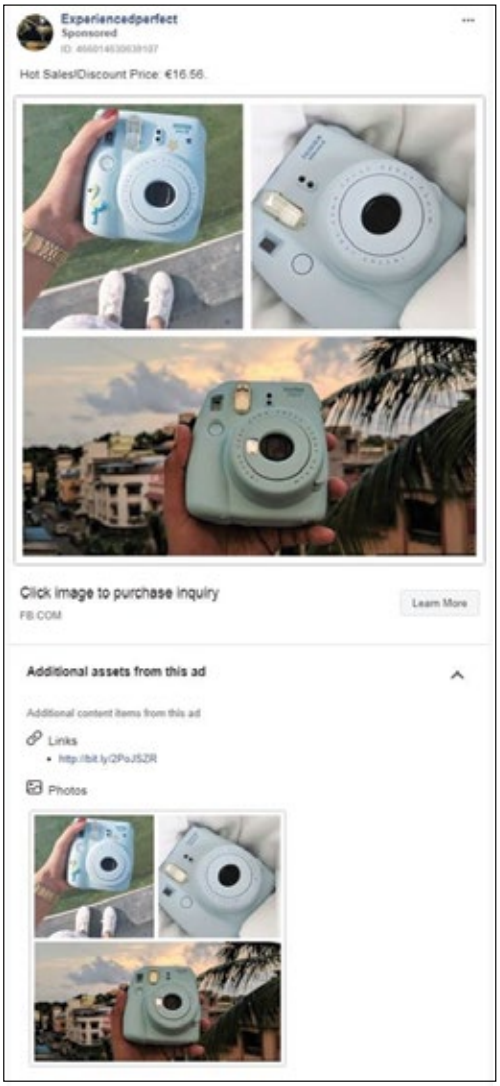
Ad Source: Fraudulent advertisement found on Instagram

Ad Image 1:

Fujifilm

Ad Source: Fraudulent advertisement found on Instagram

Ad 2 Destination Website Image:



Ad Notes: The above advert was using a Bitly URL shortener leading to: http://love.902399.xyz/zc546.php; however when accessing via a desktop browser the destination was for an irrelevant garden landscaping website demonstrating the Bitly URL was using URL Redirection and Cloaking techniques to avoid detection.

On the official Instax Fujifilm website the company has placed a warning notice about fraudulent websites to warn consumers about the dangers of scam websites: https://instax.com/camera/

Caution

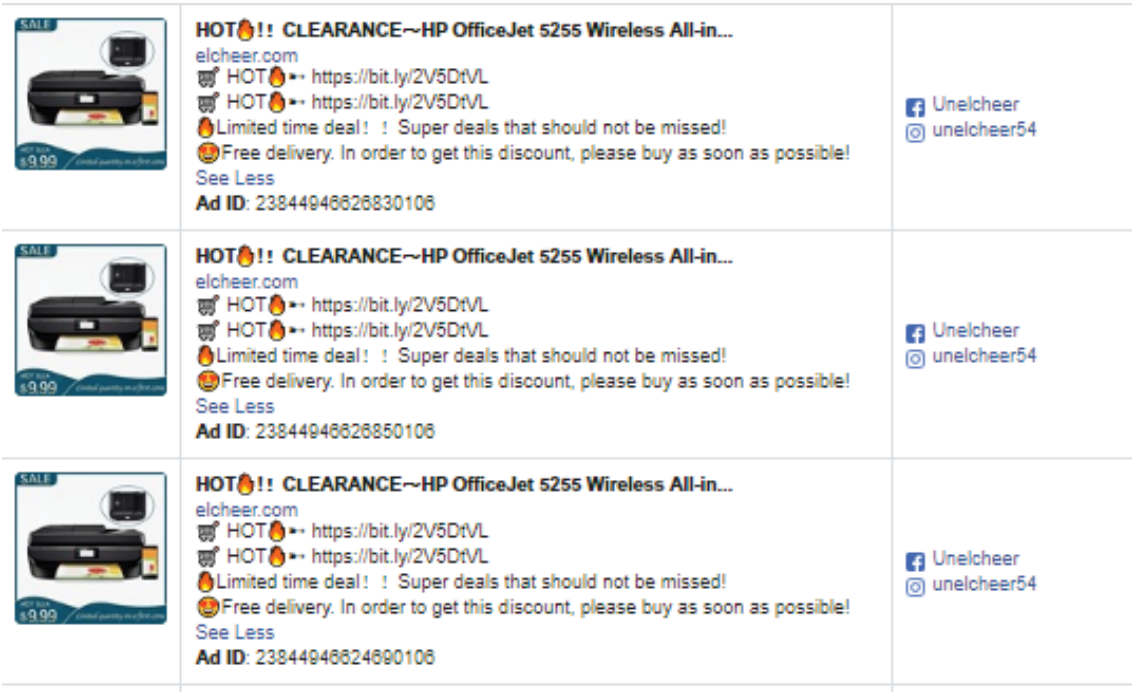
Fraudulent Website Alert

Please be advised that there may be fraudulent websites making unauthorized use of Fujifilm logos and images in an attempt to sell product and possibly obtain sensitive information such as user names, passwords, and credit card details.
Please note that these sites are not sanctioned by Fujifilm, and that all authorized Fujifilm websites carry the appropriate Terms and Conditions and Privacy Policy.
You can find the official Fujifilm websites in your country from the link on the top right corner of this page.

HP

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

Ad Image:

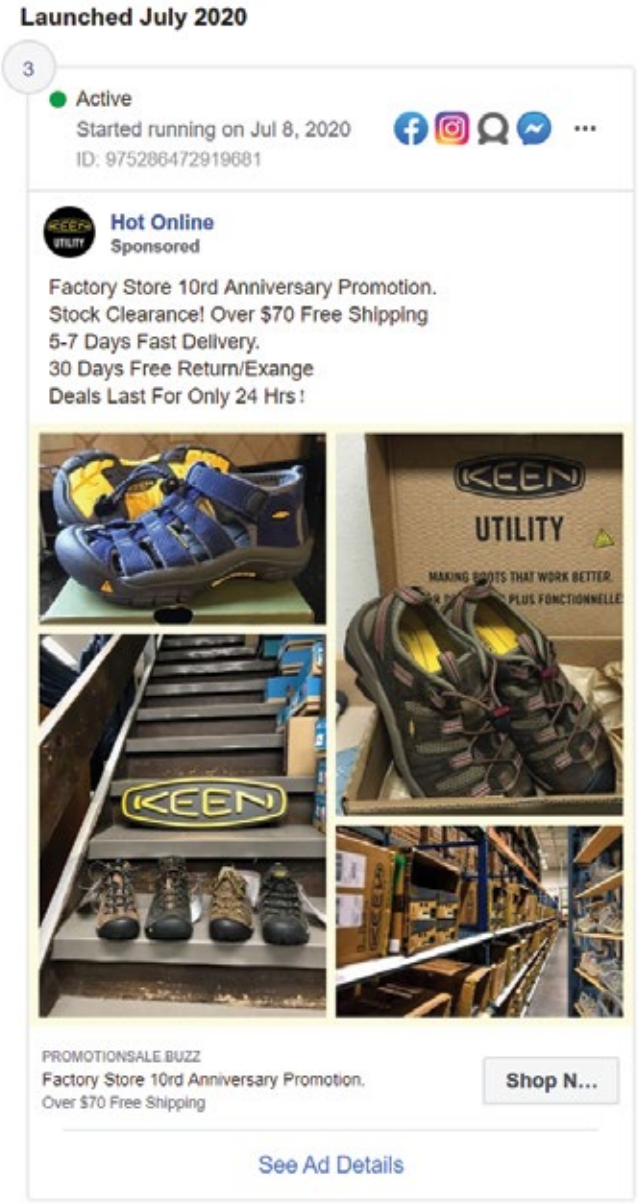


Ad Notes: The destination URL from these adverts uses Facebook's own visitor tracking and analytics tool called Facebook Pixel highlighted in bold below: https://elcheer.com/shopping/uncategorized.html/hot%f0%9f%94%a5%ef%bc%81clearance%ef%bd%9ehp-officejet-5255-wireless-all-in-one-printer/?fbclid=IwAR0uaIOZp57uDDDmoVkSqvBGSctelM_-vUBDNKmUQk16bXK7gjJEYT1S_q4

Keen

Ad Source: Fraudulent advertisements identified via Facebook's Commerce and Ads IP Tool

Ad Image:

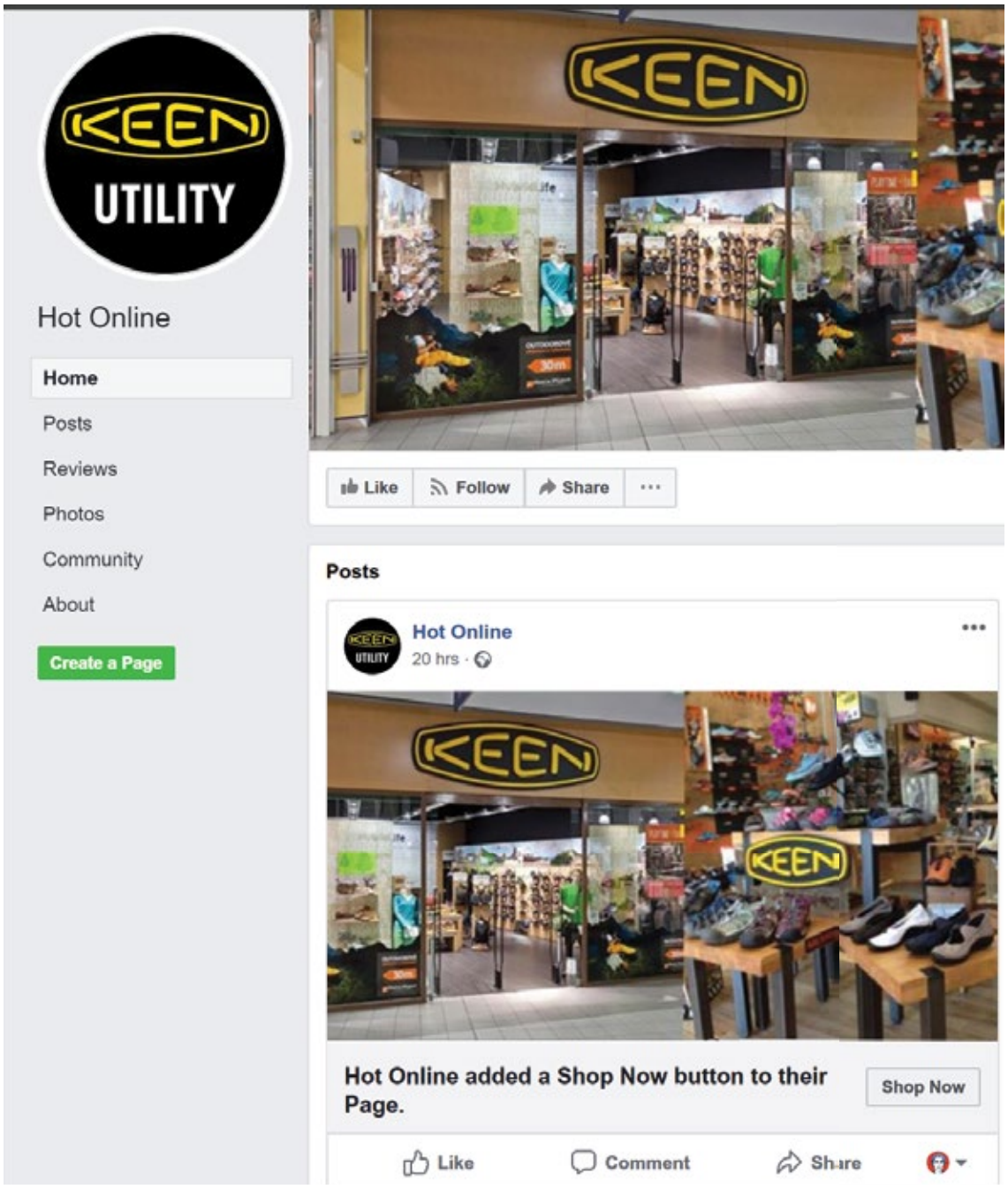


Ad Notes: The destination websites identified used Facebook's own visitor tracking and analytics tool called Facebook Pixel highlighted in bold below:

1. https://www.outdoorsstore.buzz/shop/?fbclid=IwAR3ypWn68LJyhC-GNt3u4-phjmb3zQT6Gluii2DRKIEh35KkT9pcGvisC-BA

2. https://www.hotdisountsvps.com/shop/?fbclid=IwAR3Ys2c4dedI-SA-n1a04YTHB_eRo2LECeR5HUf0H-Op4Hps4H8uHs-UUQwE

The fraudulent advertiser's Page was branded with the Keen logo, but the page was named "Hot Online":

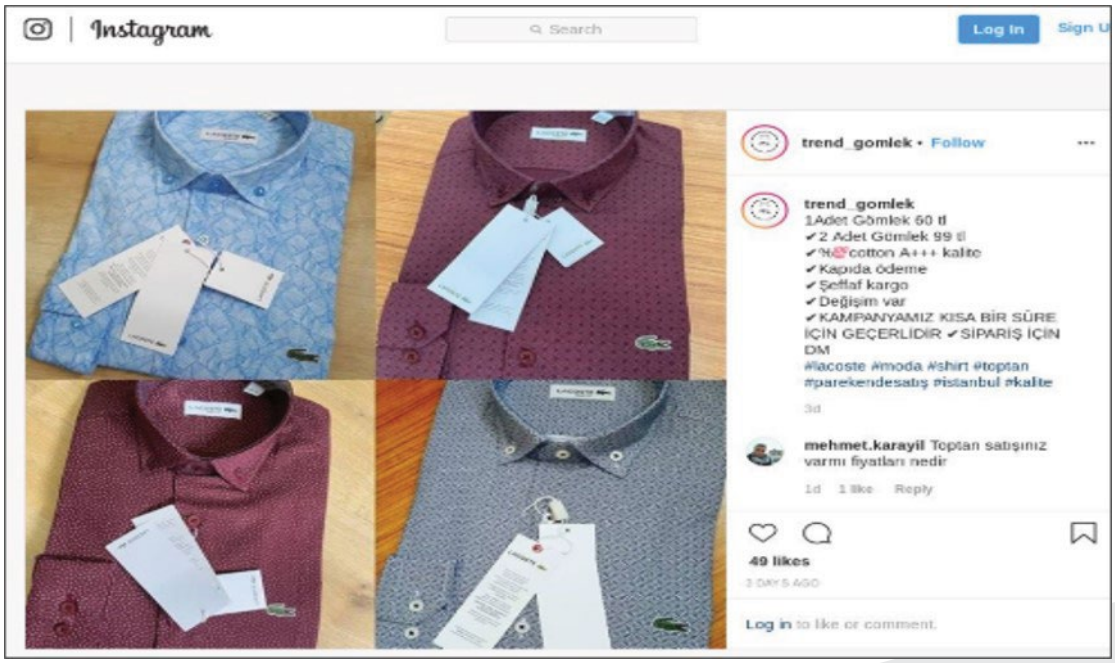


Lacoste

Ad Source: Fraudulent Adverts identified on Facebook and Instagram

Ad image 1:

Ad image 2:

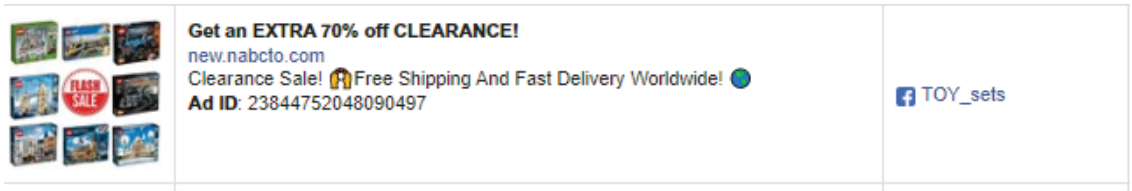


LEGO

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

Ad Image 1:

Ad Image 2:



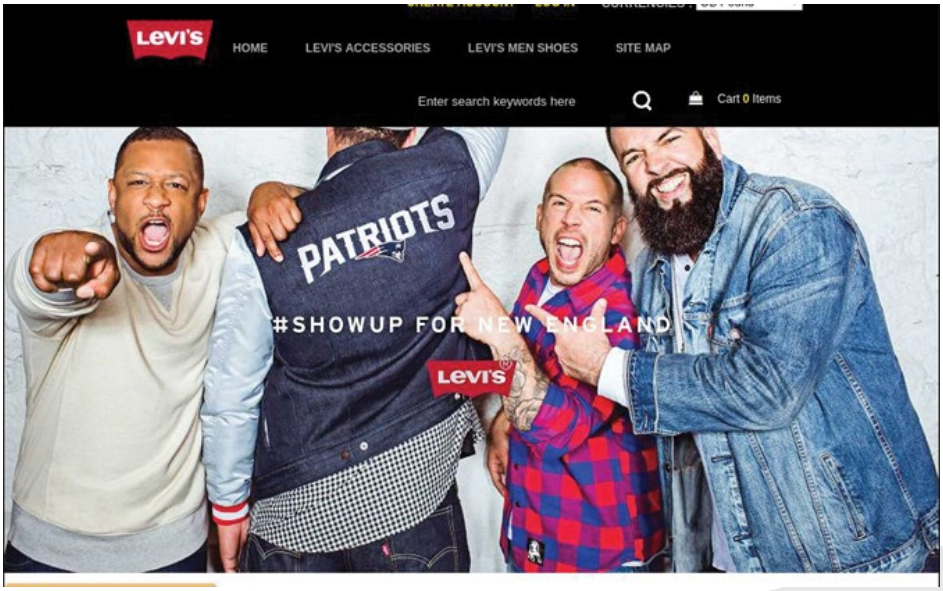
Ad Notes: The fraudulent advertiser's page was called "TOY sets" (https://business.facebook.com/TOY_sets-109322840753140/) and featured Lego marketing materials and branding.

Levi's

Ad Source: Fraudulent websites identified through Instagram Stories

Website Image 1:

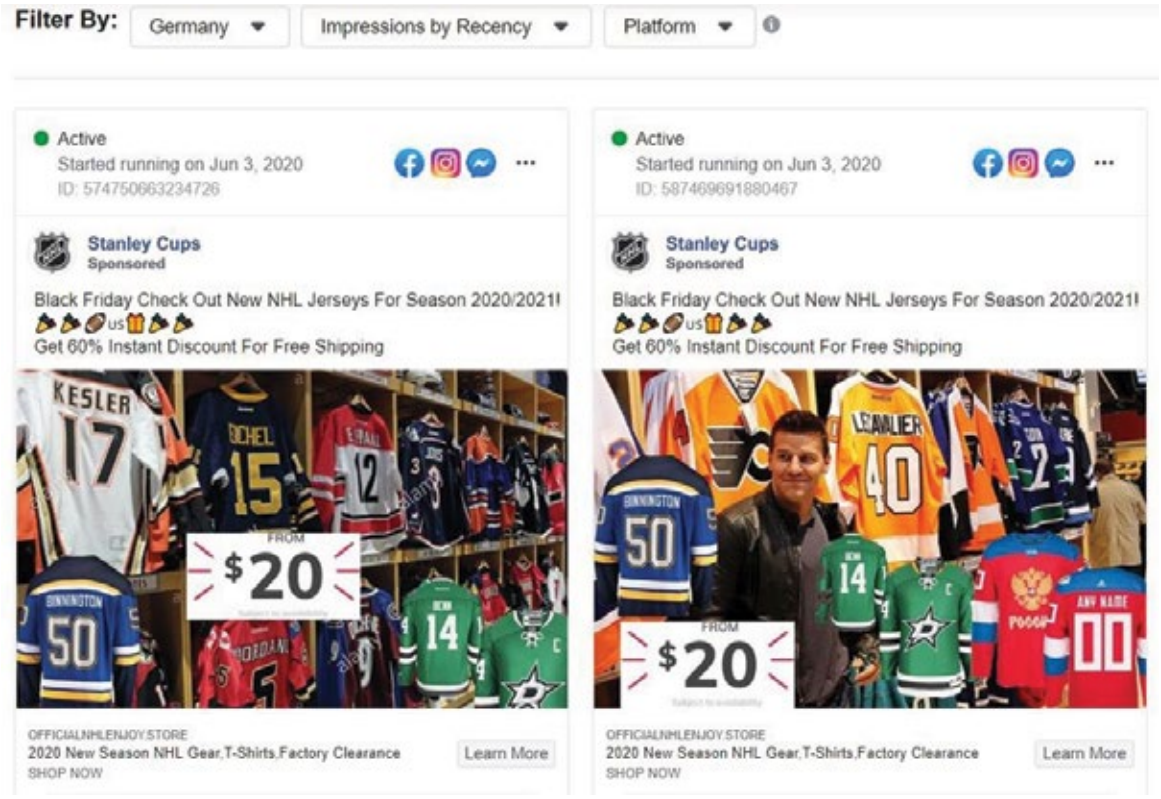
Website Image 2:



National Hockey League (NHL)

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

Website Image 1:

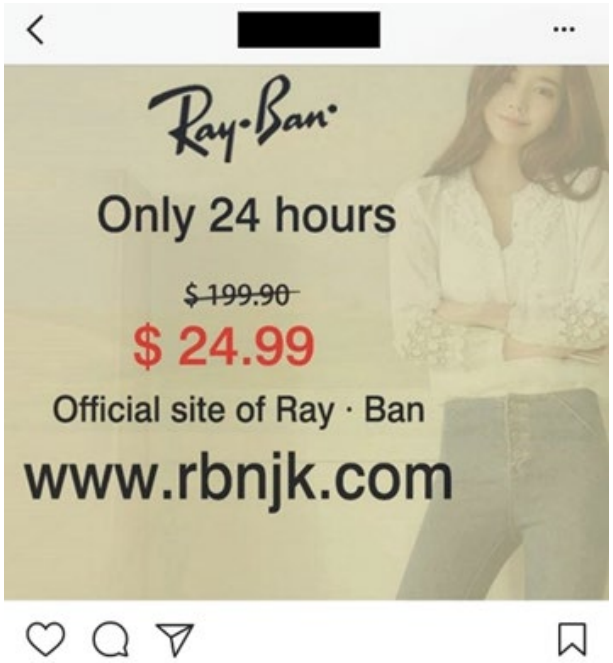


Ad Notes: The destination website https://www.officialnhlenjoy.store contains the word official in the URL in order to deliberately mislead online shoppers.

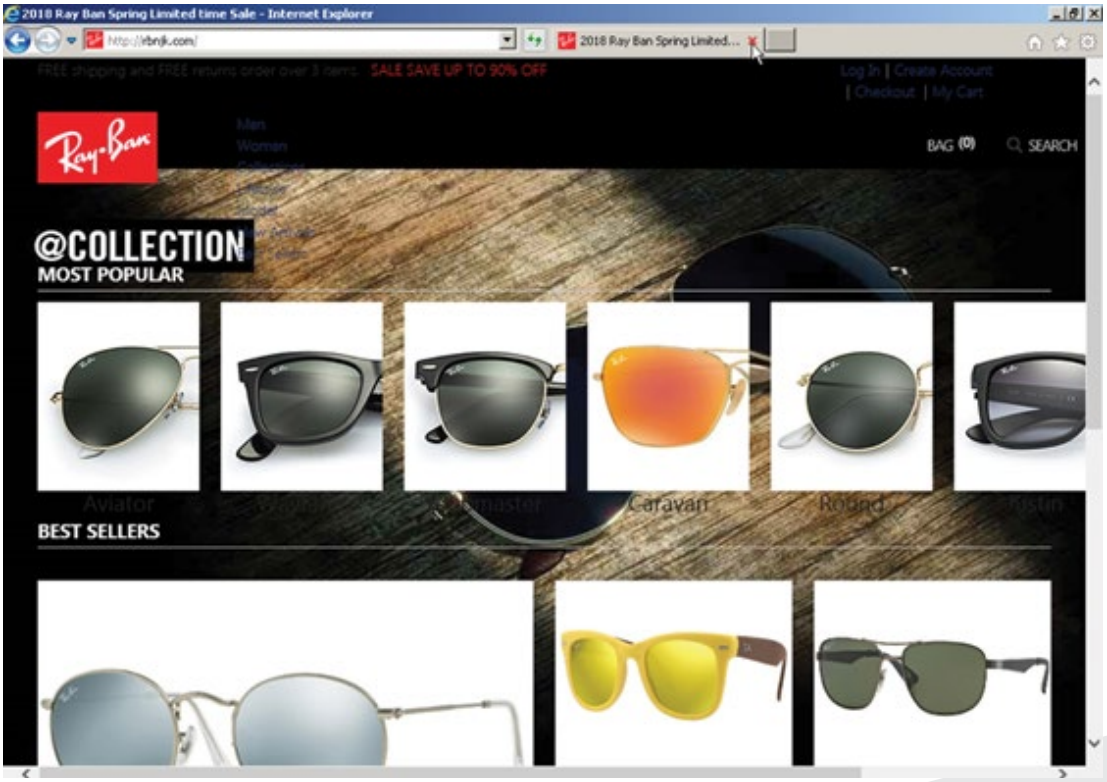
Ray-Ban

Ad Source: Fraudulent advertisements for Ray-Ban were featured in the 2018 article "Rolling Back the Curtains on a Retail Phishing Campaign "(https://medium.com/@wesleyraptor/rolling-back-the-curtains-on-a-retail-phishing-campaign-23cab178d558)

Ad Image 1:



Website Image 1:



Richemont (Montblanc)

Ad Source: Fraudulent advertisement found on Instagram

Ad Image:

SKECHERS

Ad Source: Fraudulent advertisements identified via Facebook's Commerce and Ads IP Tool

Ad Image:

Ad Notes: The fraudulent advertiser's page was called "Skechers Factory Outlet" https://www.-facebook.com/Skechers-Factory-Outlet-112147220522303 and was branded to deliberately mislead online shoppers. Likewise the ddestination website https://www.dealersale.club used the keywords "dealer" and "sale" suggesting the source of the products may be legitimate.

Star Wars (Disney)

Ad Source: Fraudulent advertisement for a Star Wars The Mandalorian licensed collectable offered for £32.42 (RRP £250+) was identified via the Facebook's Commerce and Ads IP Tool

Ad Image:

Ad Notes: The destination website uses Facebook's own visitor tracking and analytics tool called Facebook Pixel highlighted in bold: https://cowris.com/products/manda?fbclid=IwAR2oqwwbcfM-rCvvC_ERxVzO51m9b5sDOy9XwtRoA9ugY34ZI3mXgHfHJ98 and uses inducements including free shipping and "selling out fast".

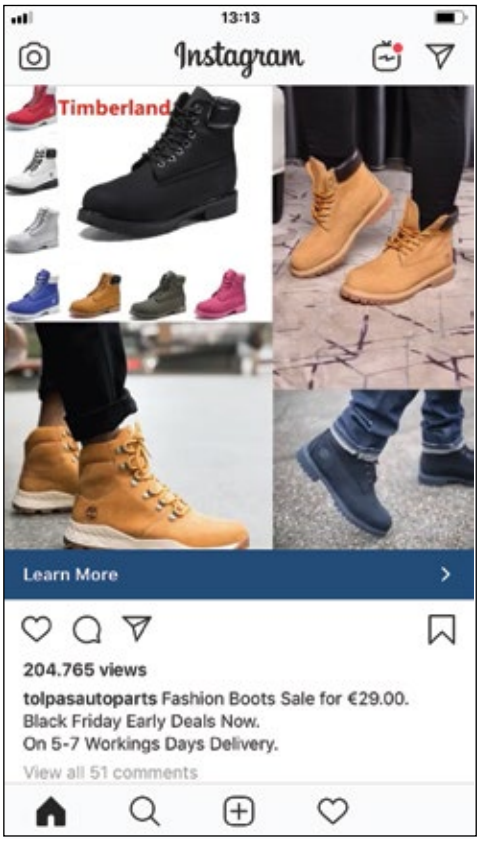
Website Image 1:

Timberland

Ad Source: Fraudulent advertisements found on Instagram

Ad Image 1:

Ad Image 2:

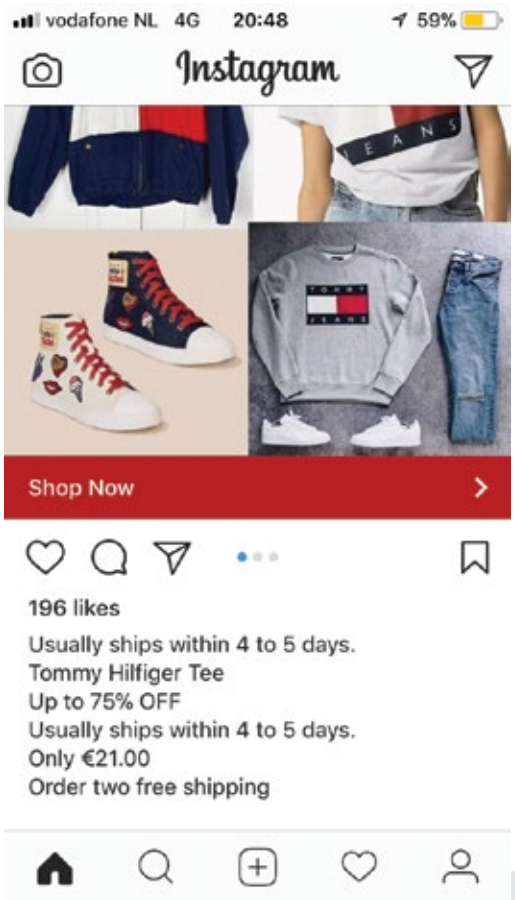


Tommy Hilfiger

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

Ad Image 1:

Ad Image 2:

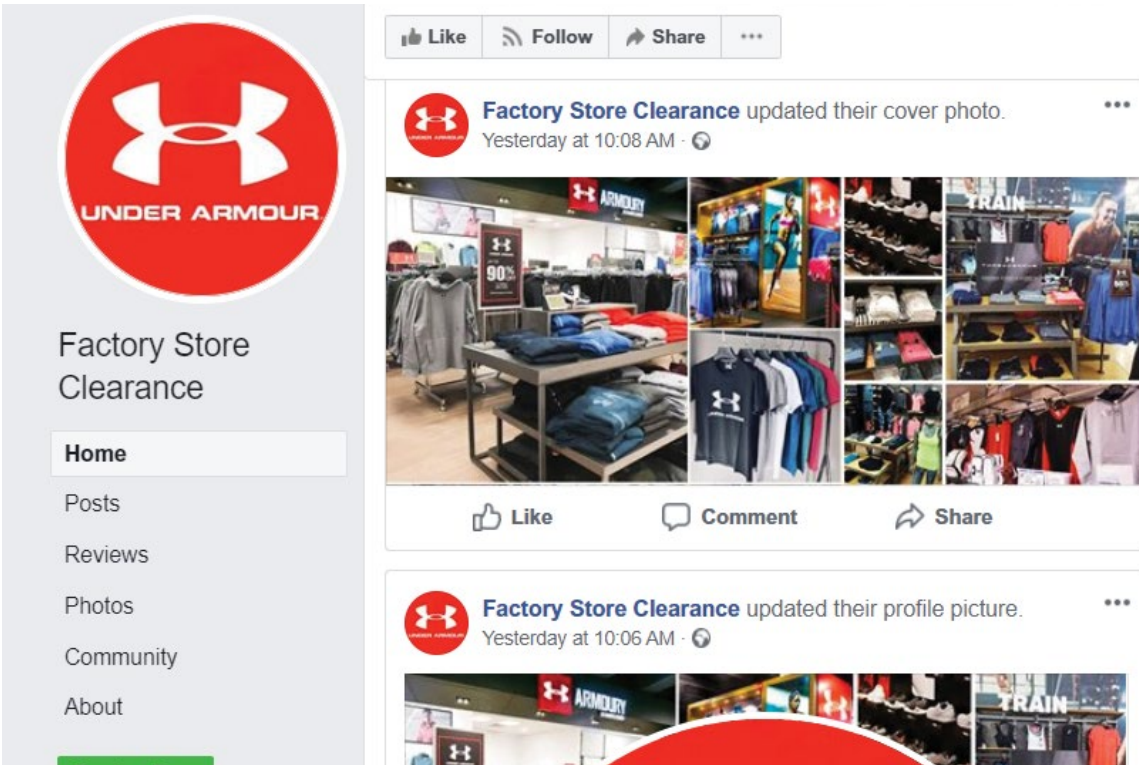


Under Armour

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

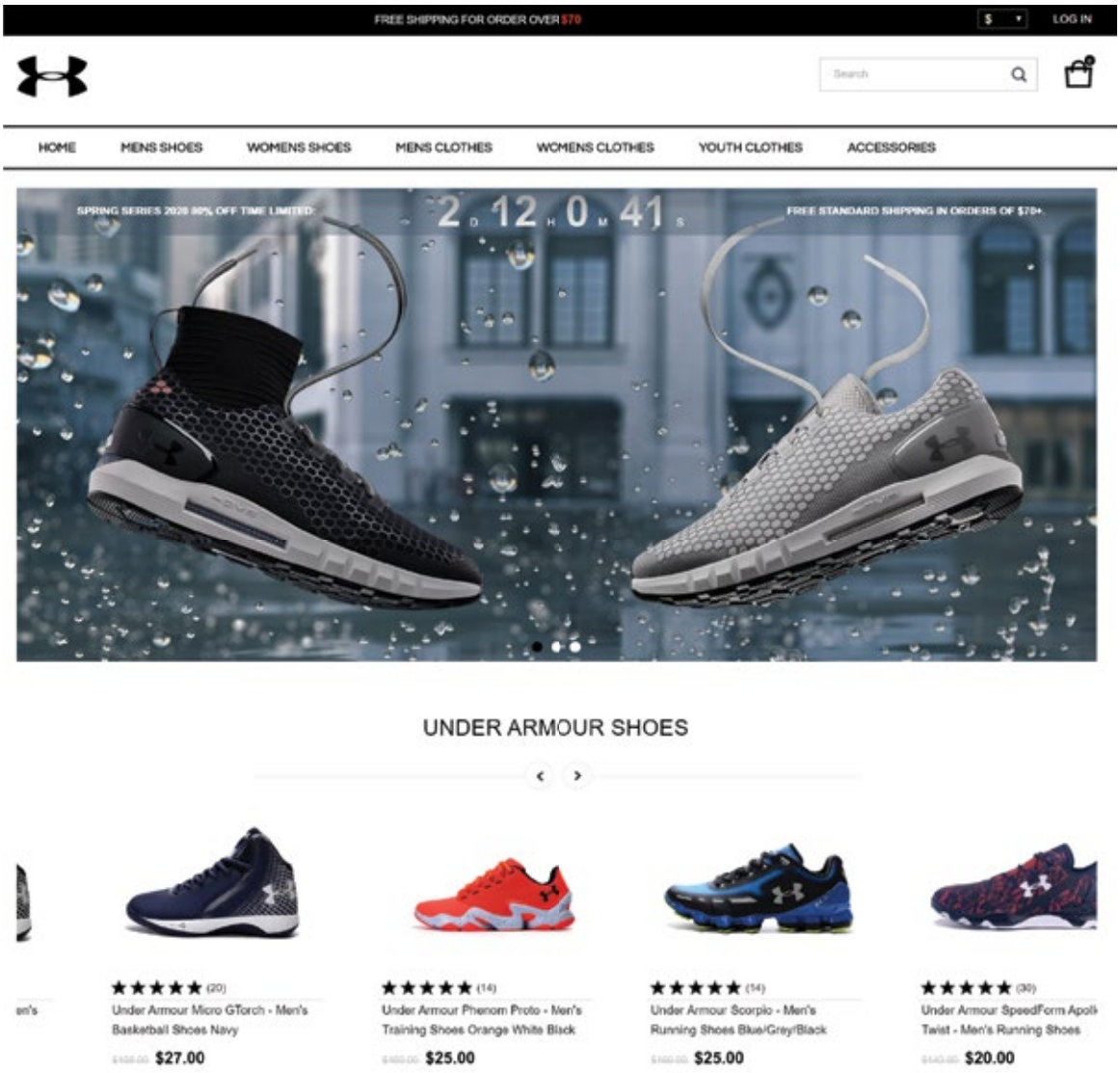
Ad Image 1:

Ad Notes: The fraudulent advertiser's Facebook page was created on the 29 June 2020 and the advertisement started running on the same day. The page is designed to mislead shoppers into believing it's an official Under Armor page:



Ad Notes: The destination website http://www.strawberrys.xyz/ uses the original brand's logos and marketing imagery alongside unrealistic discounts.

Website Image 1:

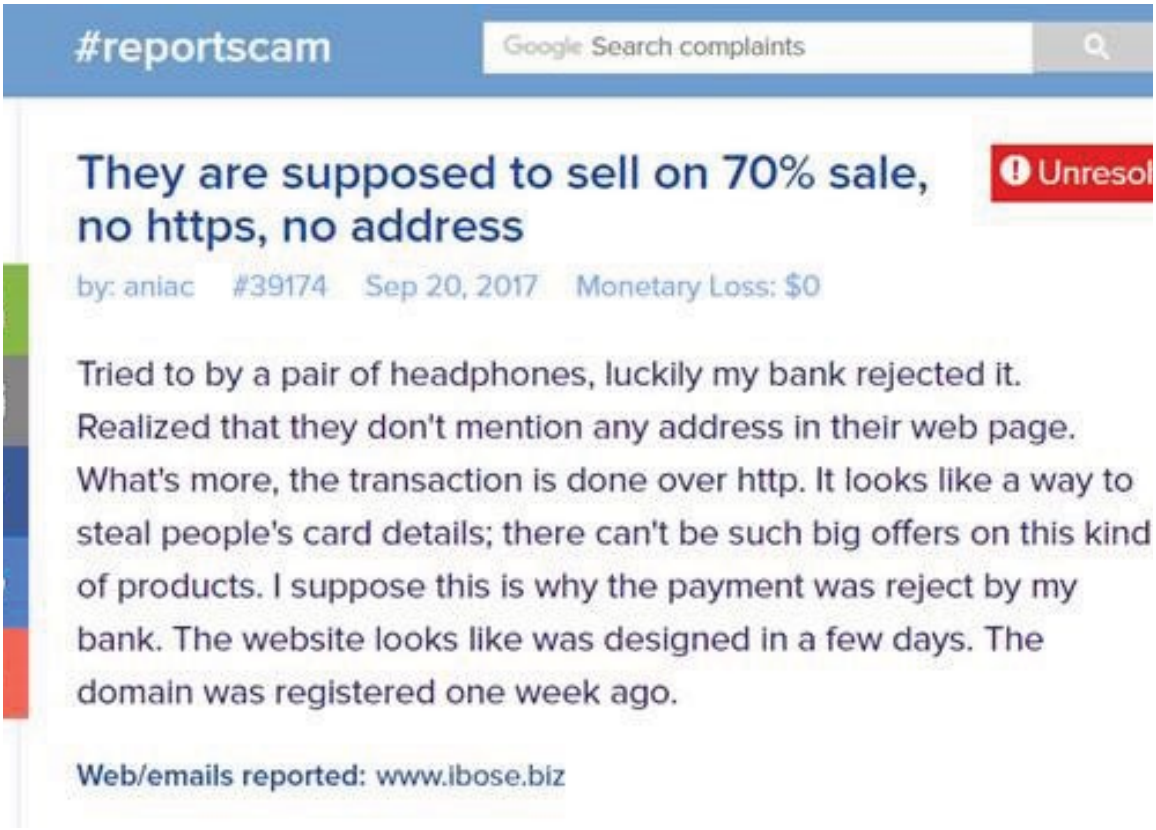


APPENDIX 2: CUSTOMER COMPLAINTS

Research online has identified numerous complaints by consumers who have fallen victim to fraudulent advertising scams found on social media.

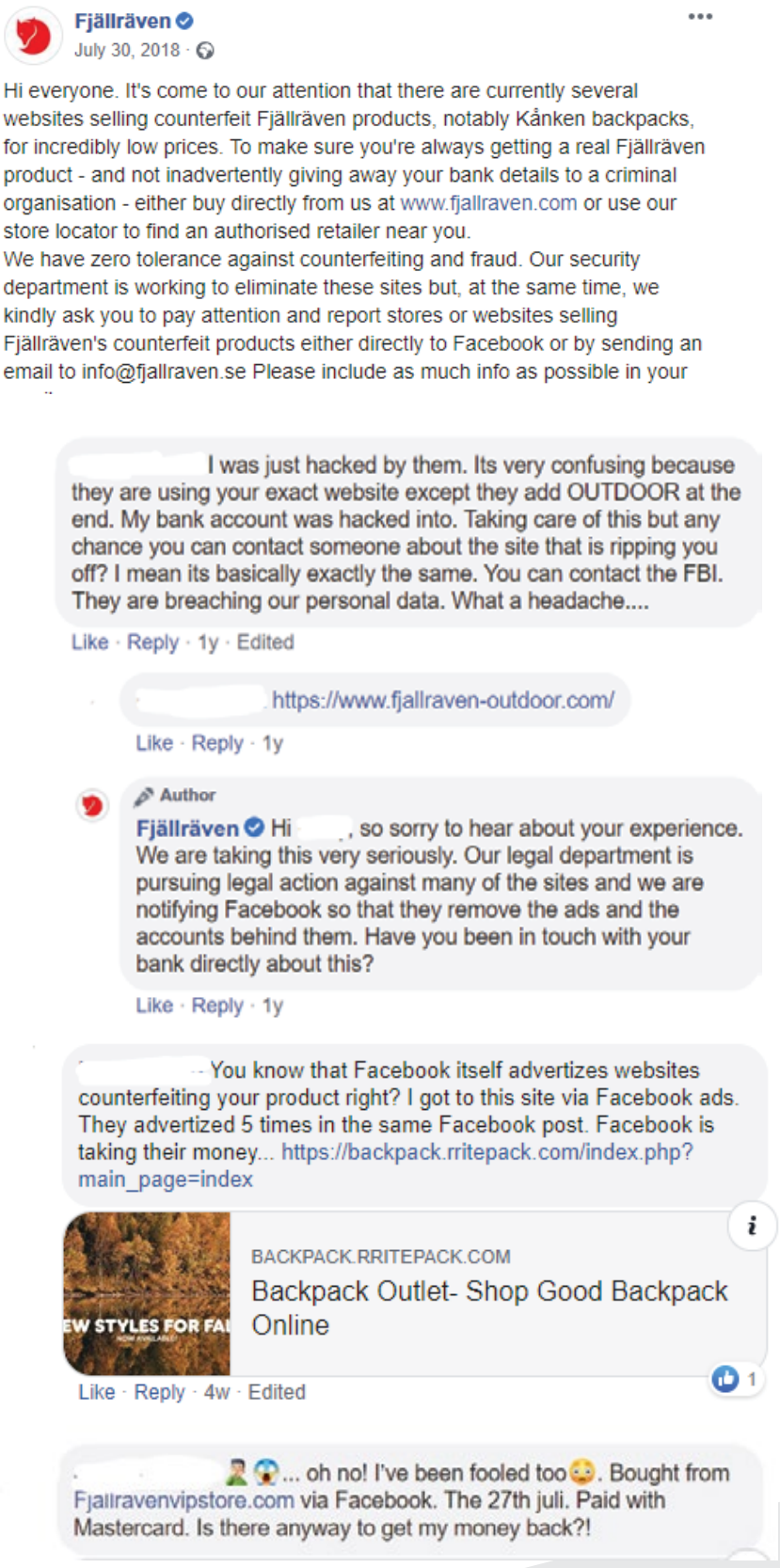
Bose

Complaint Source: Consumer complaint regarding fraudulent website on a Scam reporting site (https://reportscam.com/ibosebiz)



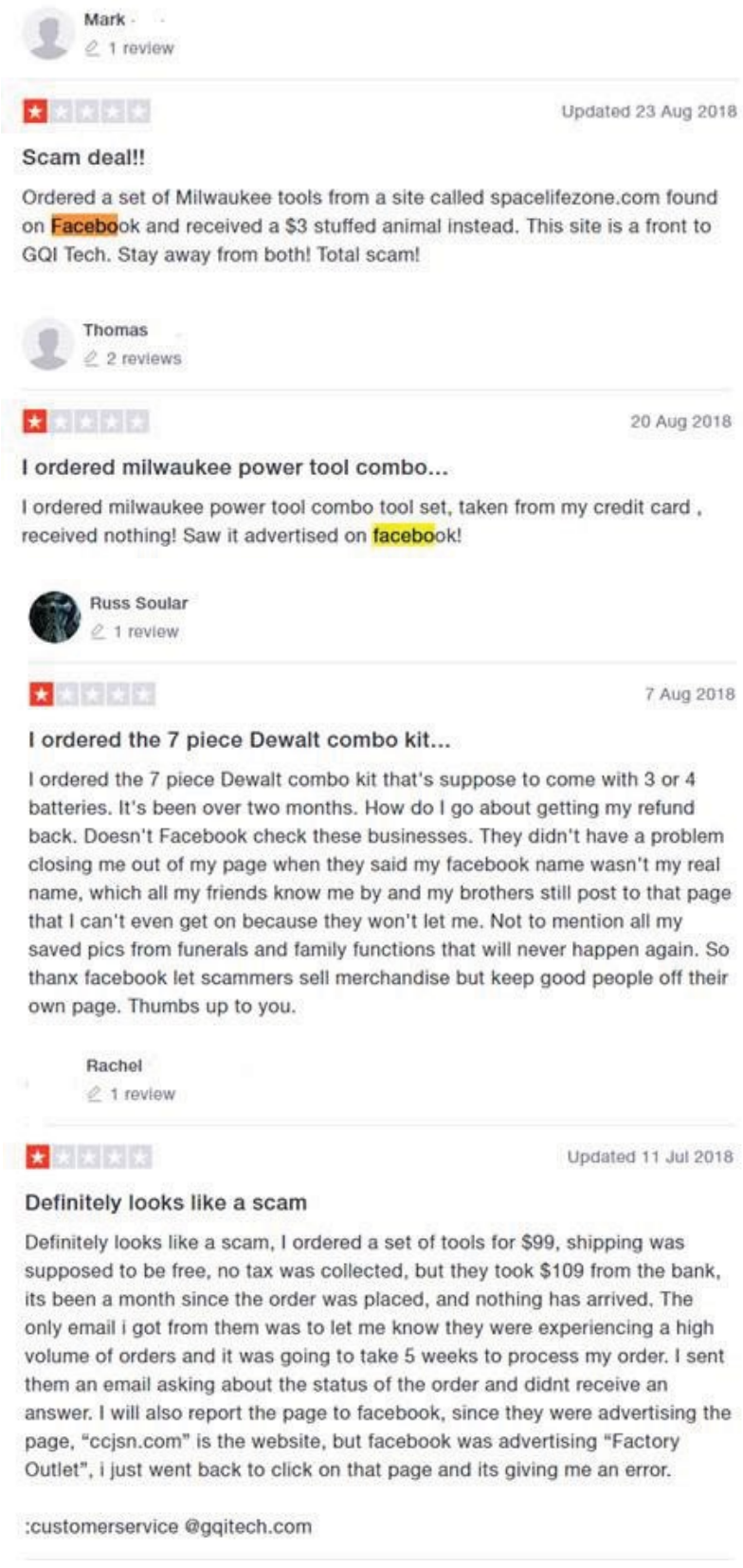
Fjällräven

Complaint Source: Fjällräven official Facebook page (https://www.facebook.com/Fjallraven/posts/hi-everyone-its-come-to-our-attention-that-there-are-currently-several-websites-/10156792217819208/)



Dewalt and Milwaukee Power Tools

Complaint Source: Online research of complaints relating to advertisements on Facebook identified a TrustPilot page for a business called gqitech.com (https://ie.trustpilot.com/review/gqitech.com) that had defrauded multiple purchasers.



Mark
1 review

Updated 23 Aug 2018

Scam deal!!

Ordered a set of Milwaukee tools from a site called spacelifezone.com found on Facebook and received a $3 stuffed animal instead. This site is a front to GQI Tech. Stay away from both! Total scam!

Thomas
2 reviews

20 Aug 2018

I ordered milwaukee power tool combo...

I ordered milwaukee power tool combo tool set, taken from my credit card , received nothing! Saw it advertised on facebook!

Russ Soular
1 review

7 Aug 2018

I ordered the 7 piece Dewalt combo kit...

I ordered the 7 piece Dewalt combo kit that's suppose to come with 3 or 4 batteries. It's been over two months. How do I go about getting my refund back. Doesn't Facebook check these businesses. They didn't have a problem closing me out of my page when they said my facebook name wasn't my real name, which all my friends know me by and my brothers still post to that page that I can't even get on because they won't let me. Not to mention all my saved pics from funerals and family functions that will never happen again. So thanx facebook let scammers sell merchandise but keep good people off their own page. Thumbs up to you.

Rachel
1 review

Updated 11 Jul 2018

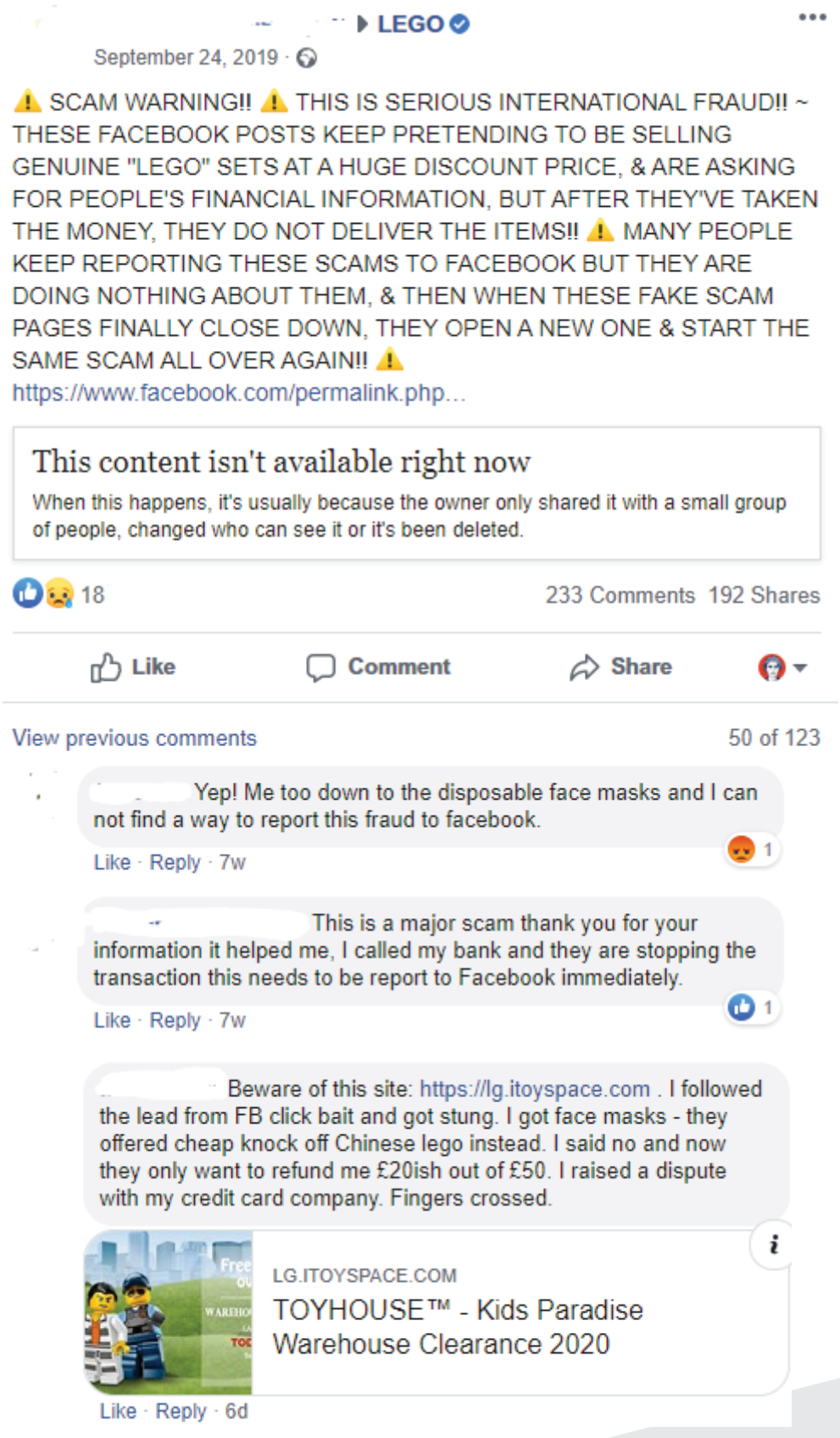
Definitely looks like a scam

Definitely looks like a scam, I ordered a set of tools for $99, shipping was supposed to be free, no tax was collected, but they took $109 from the bank, its been a month since the order was placed, and nothing has arrived. The only email i got from them was to let me know they were experiencing a high volume of orders and it was going to take 5 weeks to process my order. I sent them an email asking about the status of the order and didnt receive an answer. I will also report the page to facebook, since they were advertising the page, "ccjsn.com" is the website, but facebook was advertising "Factory Outlet", i just went back to click on that page and its giving me an error.

:customerservice @gqitech.com

LEGO

Complaint Source: Official Lego page on Facebook (https://www.facebook.com/LEGO/posts/10156844122453403/)



Tommy Hilfiger

From a US Customer:
I was browsing in Instagram and found a website from Tommy Hilfiger and it looks official. It says copyright 2017 Tommy Hilfiger outlet on the bottom, it has all the photos from Tommy, and the logos, etc so, I made a purchase, but after was charged more than I authorized. I called the bank and its a Chinese company. I couldn't even cancel the transaction. The website is fake. What can I do? I trusted the brand and I may not be the only one being deceived! Can you do something about this?

From a Danish Customer:
My name is [.....] and I have been a victim of fraud. I was trying to buy Tommy Hilfiger t-shirts on a webpage called VIPDK.TOP through facebook. I was on the webpage to buy t-shirts with your brand and I was not aware that the webpage was fake. I entered my Credit Card informations, sadly as it is, and now the people behind this webpage (which is located in China), has withdrawn a big amount of money from my accounts.

In order to get my insurance to cover the damage, I need you from Tommy Hilfiger to confirm that you are not cooperating or funding the webpage VIPDK.TOP and that the items on this particular webpage is copied items, abusing your brand.

Will you please do that for me?

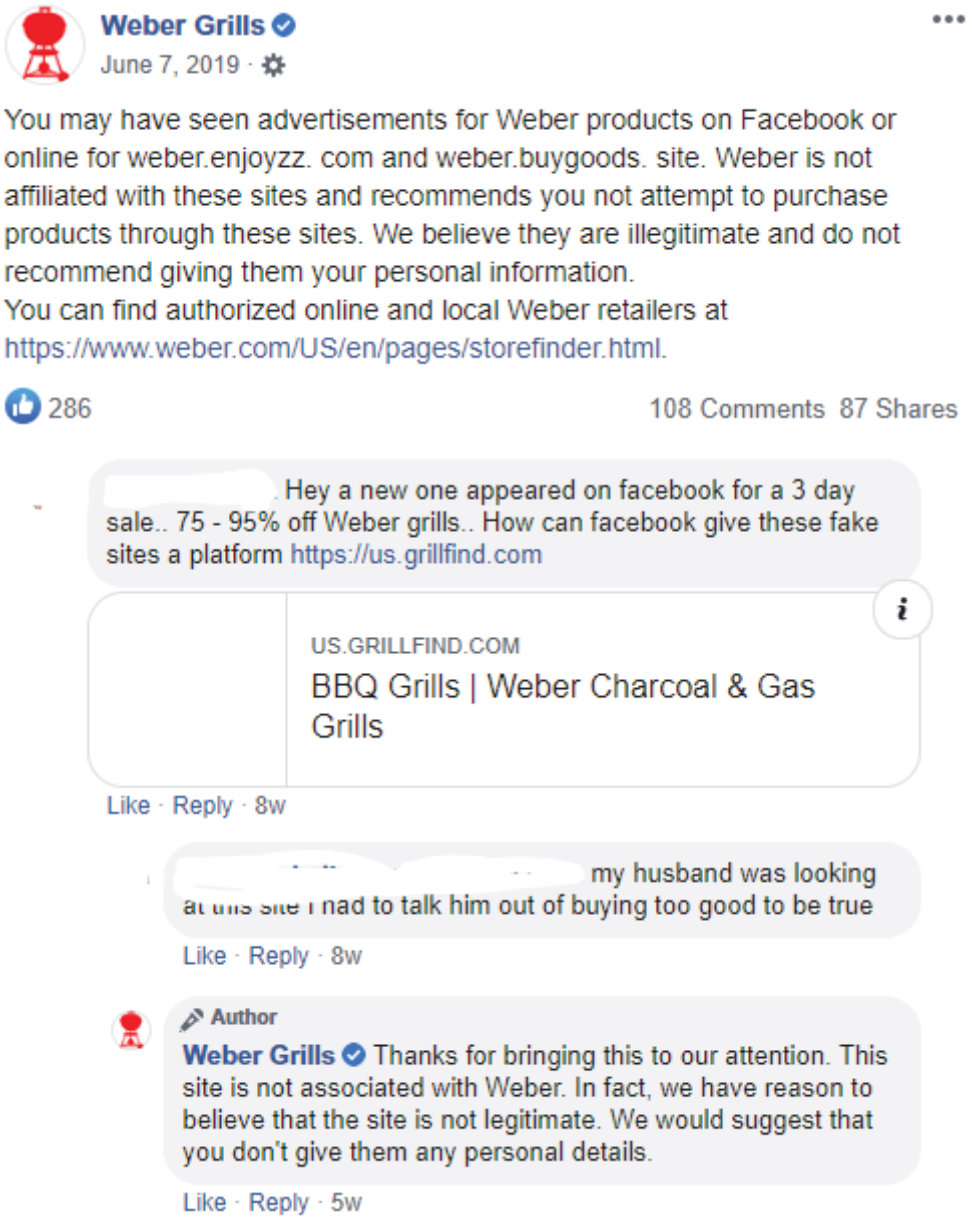
From the Tommy Hilfiger customer service team in Poland:
A few days ago we got the first customer information that came up with a fake website with our online store. The website looks very reliable with all the graphics and logos, however, the prices are very low. Yesterday, three more cheated customers came to the Stores.

The case is very serious, because customer accounts are charged more than double the amount of the purchase fee...the payment for shopping was 232,00PLN. The money (531,00PLN) went to a Chinese bank account.

This lady came to the online store through Instagram, but you can directly enter through the link: www.tmmypl.com. Of course, any clients that our employees talked, didn't receive the goods so far.

Weber

Complaint Source: Official Weber BBW Facebook page (https://www.facebook.com/weberbbq/posts/you-may-have-seen-advertisements-for-weber-products-on-facebook-or-online-for-we/10156606512903422/)



Complaint Source: Post on the Reddit.com forum r/grilling (https://www.reddit.com/r/grilling/comments/gg04b2/if_youre_looking_for_a_grill_beware_facebook_ad/)

8

r/grilling · Posted by [redacted] 1 month ago

If you're looking for a grill BEWARE FACEBOOK AD SCAMS

It's no secret that if you search for certain terms on the internet or especially using Facebook Marketplace, Google and Facebook tailor ads to you based on your common search terms. Over the past week or so I've been looking at Weber charcoal grills. It was no surprise then that last night I saw an ad on my Facebook feed that looked like it was from Weber and they were advertising a flash sale on grills. "Fantastic!" I thought. I clicked on the link and it took me to a website that looks exactly like the Weber website, has their logo and the url had weber in the name.

The deals were too good to be true, which should have been my first warning that something was wrong. After signing up and trying to add a grill to my cart, it took me to some weird 3rd party payment website that said the payment was going to Malaysia. I noped the f ck out of there and messaged Weber directly on their website and flagged the Facebook ad as a scam. Upon closer inspection the Facebook ad was from a page called "Weber_US" and the page was only created 3 or 4 days ago. Today while perusing facebook I got ANOTHER IDENTICAL ad that popped up with a slightly different name. The scammers must have dozens and dozens of these ready to go as one gets shut down another pops up.

The Facebook ad looks like this:

APPENDIX 3: FRAUDULENT FINANCIAL SERVICES

It is not just consumer product and fashion companies that are targeted by fraudulent advertising on social media. There have been a number of high profile legal cases involving fraudulent Bitcoin and Investment scams and the celebrities who appeared (unauthorised) in them.

John de Mol fraudulent advert. Source: cdn.adformatie.nl

Martin Lewis fraudulent adverts. Source: moneysavingexpert.com

APPENDIX 4: JAPAN CASE STUDY

Since April 2020 at least seventeen fashion and luxury brands have been targeted by fraudulent sponsored (paid) advertising on Facebook and Instagram targeting Japanese consumers.

The advertisements use images of counterfeit products while the Facebook advertiser's pages used to post the ads are either compromised (hacked) or newly created (within approximately 6 months).

Some of the pages identified even use the name of the brand owner for example (Versace Japan, Ralph Lauren Japan, Nike Jackets, Adidas and ToMMY) and use the logos of the brand in the profile avatars.

The destination websites of the adverts often contain the keywords shop, store or mall and typically use the .com extension.

The websites identified have shopping cart functionality, and all generally follow the same build template. Some claim to be the "official flagship store". Unlike other scam websites, those identified often display a Japanese company name, address and email address (differing from the website).

Given these indicators these adverts and websites must be coordinated by a common bad actor or network that is able to bypass Facebook's advertising monitoring systems and deploy ads at scale across multiple pages.

1. Brands Impacted by fraudulent Japanese Ads:

Burberry
Fendi (LVMH)
Givenchy (LVMH)
Balenciaga (LVMH)
Louis Vuitton (LVMH)
Gucci (Kering)
Moncler
Ralph Lauren
Coach (Tapestry)
Nike
The North Face (VF Corp)
Tommy Hilfiger
Dior
Adidas
Versace (Capri Holdings)
Stüssy
Supreme

2. *Keywords in Ads:*

Many of the ads share the same keywords pointing to a common actor. Translations of the Japanese text show the ads offer unrealistic free products with purchases and make false claims such as “Official genuine”:

今日注文なら、もう一つ無料サービス	*Another free service if you order today*
Tommy hilfiger 2020 年夏の新作シャツ 今日注文なら、もう一つ無料サービス	*Tommy hilfiger 2020 Summer New Shirts Get one more free order if you order today*
夏の新作 今日注文なら、もう一つ無料サービス 数量限定、早い者勝ち	*Summer new work* *Another free service if you order today* *Limited quantity, first come first served*
公式正品 今日注文なら、もう一つ無料サービス 数量限定、早い者勝ち	*Official genuine* *Another free service if you order today* *Limited quantity, first come first served*
【大感謝　祭】 今日注文なら、もう一つ無料サービス 【男女兼用】	*[Great Thanksgiving] Another free service if you order today [Unisex]*
『ラルフ ローレン』今日注文なら、もう一つ無料サービス	*"Ralph Lauren" If you order today, another free service*
バレンシアガレインボーモルトロゴ半袖 今年の最新のホットセール（男女兼用） 今日注文なら、もう一つ無料サービス 数量限定発売, 早い者勝ち	*Balenciaga Rainbow Malt Logo Short Sleeve* *The latest hot sale of the year (unisex)* *Another free service if you order today* *Limited release, first come first serve*

3. *Brand infringing Facebook Pages used to advertise:*

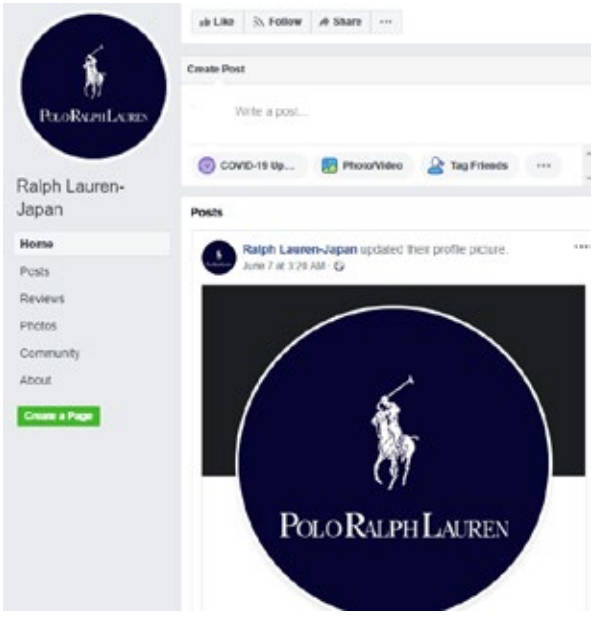
Multiple Facebook Pages used to post the ads were found to be infringing the name and logos of the brands targeting by the ads and were created just days before the ads were published and in some cases the same day.

a. *Versace*

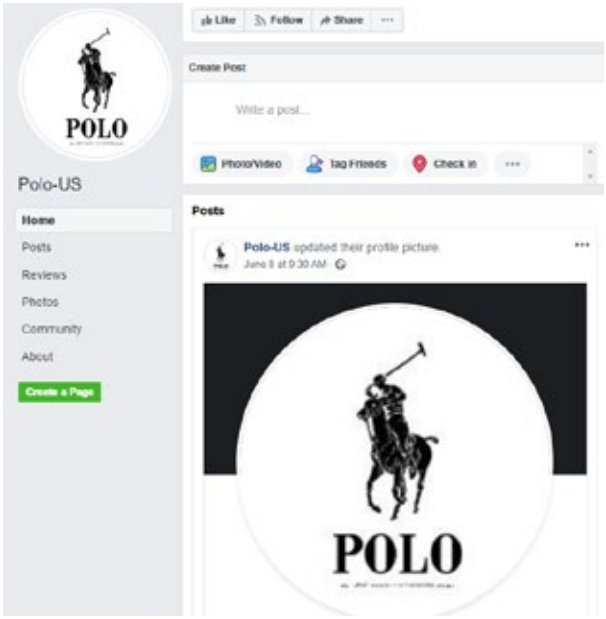
https:/www.facebook.com/VERSACE-Japan-113383623731279/ Page created - June 3, 2020

b. Ralph Lauren

https://www.facebook.com/Ralph-Lauren-Japan-114036903669545 Page created - June 7, 2020

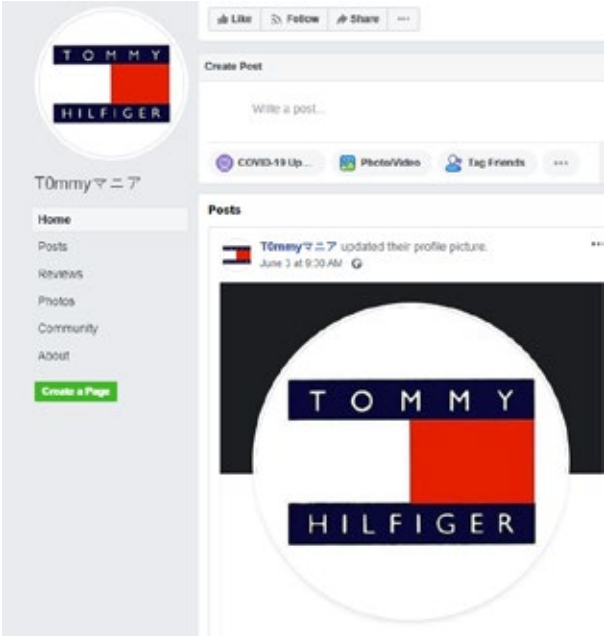


https://www.facebook.com/ADIDaS-103488224739483/?business_id=10152446361520686 Page created - June 10, 2020



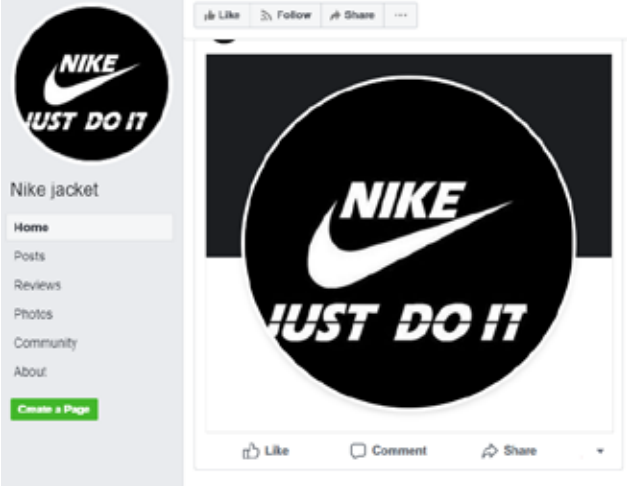
d. Tommy Hilfiger

https://www.facebook.com/Tommy%E3%83%9E%E3%83%8B%E3%82%A2-101962258219137 Page created - June 3, 2020



e. *Nike*

https://www.facebook.com/Nike-jacket-107450461002864 Page created - June 8, 2020



4. *Examples of Ads:*

Many of the ads look visually similar featuring images of branded t-shirts together with the brand logo. Often the products in the images are obviously counterfeit missing correct labelling or being products not made by the brand.

Launched June 2020

Launched June 2020

Launched June 2020

Active
Started running on Jun 4, 2020
ID: 193066071901282

laulau_doyle
Sponsored

夏の新作
今日注文なら、もう一つ無料サービス
数量限定、早い者勝ち

TWLYMALL.COM
twlymall.com
Learn More

See Ad Details

Active
Started running on Jun 2, 2020
ID: 604215963635138

laulau_doyle
Sponsored

TWLYMALL.COM
twlymall.com
Learn More

See Ad Details

Launched June 2020

Active
Started running on Jun 6, 2020
ID: 184037272981821

شباب السويس
Sponsored

パレンシアガレインボーモルトロゴ半袖
今年の最新のホットセール（男女兼用）
今日注文なら、もう一つ無料サービス
数量限定発売,早い者勝ち

HAPPYSHOPPINGCO.COM
★今年は人気No.1半袖★今日注文なら、もう一つ無料サービス（男女兼用）
パレンシアガレインボーモルトロゴ半袖# 今年の最新のホットセール（男女兼用）# 原価：26800円、今日の特価：12300円# 今日注...
Learn More

See Ad Details

Launched June 2020

Active
Started running on Jun 9, 2020
ID: 728453157907722

ADIDaS
Sponsored

今日注文なら、もう一つ無料サービス【男女兼用】

VIP.WITEYSTORE.COM
adidas
Learn More

See Ad Details

Identical advertisements were also identified from different advertisers. See below for an example of a FENDI ad using the same title keywords and imagery:

今日注文なら、もう一つ無料サービス
https://makkmap.com/iteminfojp/BHGHKTRRB/ BHGH6F05D09.html
Ad ID: 23844791890610387

Koka
kjkjhk820

今日注文なら、もう一つ無料サービス
https://sxyykk.com/iteminfojp/BHGHRB/BHGH6F05D09.html
Ad ID: 23845229031200781

Povo
inofensivo.poeticame...

Identical keywords in advertisements for different brands were also identified from different advertisers, but directed to the same destination website. Below is an example of Gucci and Moncler ads using the same keywords and destination website:

hot.aidueshop.com
hot.aidueshop.com
夏の新作
今日注文なら、もう一つ無料サービス
数量限定、早い者勝ち
Ad ID: 23844815820380126

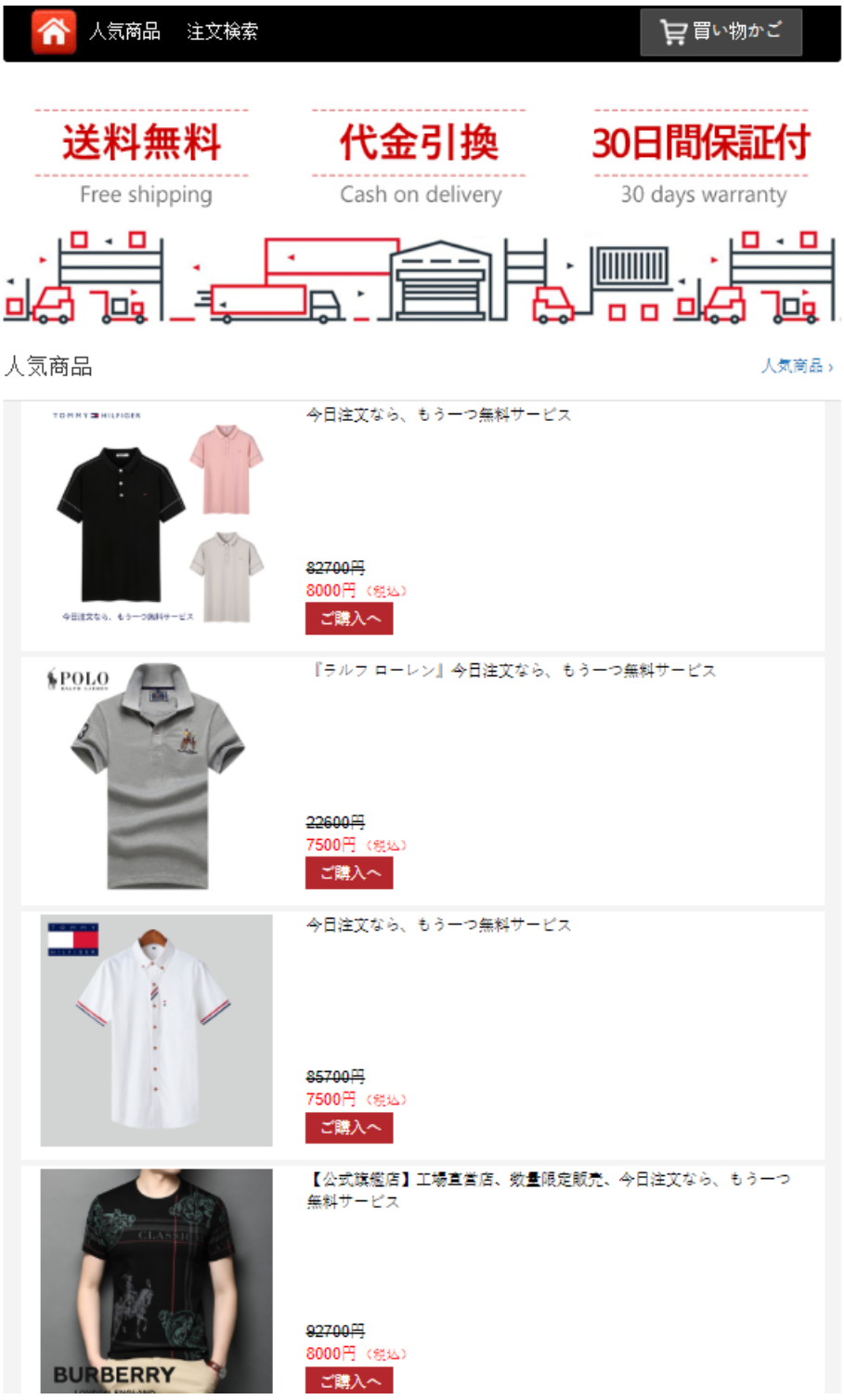
Justine
ju_stine7227

sale.aidueshop.com
sale.aidueshop.com
夏の新作
今日注文なら、もう一つ無料サービス
数量限定、早い者勝ち
Ad ID: 23844733763620363

つるのはしマルシェ@鶴橋本通商店街
pbaccount_1501077623...

5. *Example destination websites:*

a. The website http://vip.hotepstore.com is targeting Tommy Hilfiger, Ralph Lauren and Burberry and shows unrealistic price discounts with offers of free deliver, 30-day warranty and cash on delivery.



b. The website https://sxyykk.com/ is targeting Fendi (LVMH) and Tommy Hilfiger and claims to be the official flagship store. It also shows unrealistic price discounts with offers of free deliver, 30-day warranty and cash on delivery.

c. The website http://twlymall.com is targeting Moncler, Givenchy (LVMH) and Gucci (Kering) and claims to be the official flagship store. It also shows unrealistic price discounts with offers of free deliver, 30-day warranty and cash on delivery.

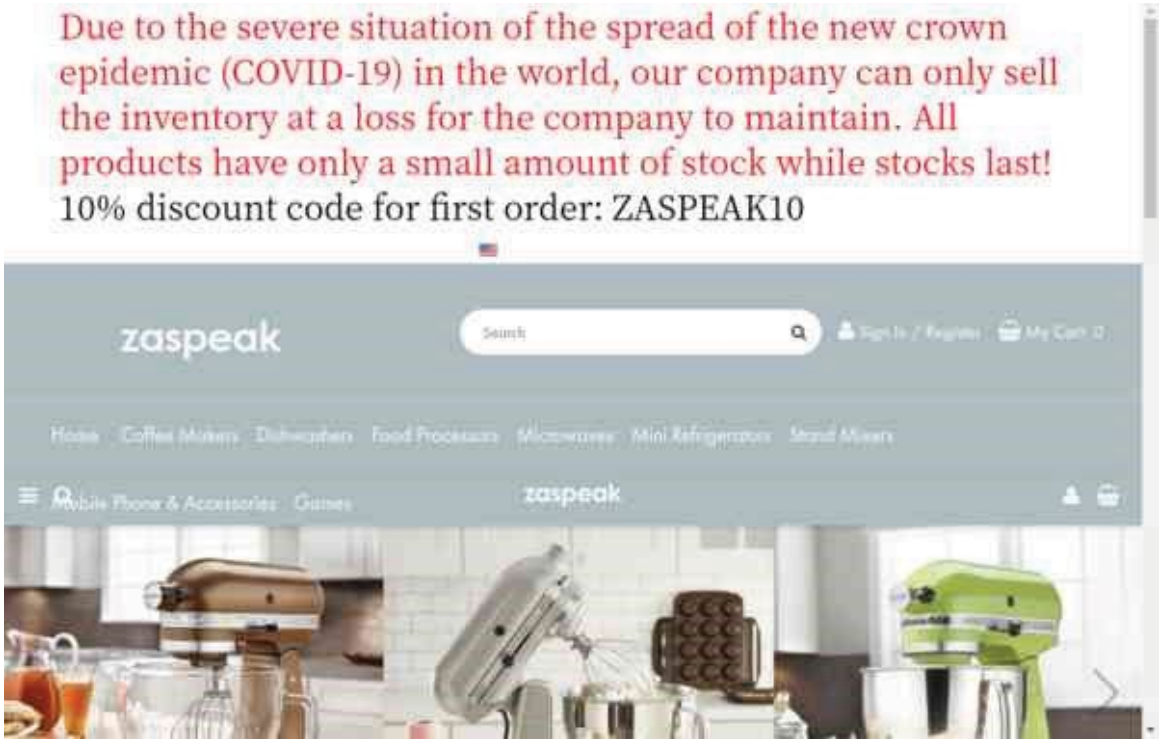
APPENDIX 5: COVID-19 RELATED FRAUD

COVID-19 Example 1: As the COVID19 pandemic spread globally, fraudulent ads for face masks and anti-bacterial hand gels were identified targeting the UK and other European countries on Facebook and Instagram, which led consumers to scam websites (e.g.) www.healthprotectionmask.com, www.handhealth.co.uk and https://muanha.myshopify.com/collections/anti-corona-virus , the latter showed only Vietnamese contact information.

COVID-19 Example 2: Scam advertisers on Facebook and Instagram have also specifically referring to COVID19 to appeal to consumers with false discounts.

Ad Notes: Facebook advertisers' page (https://www.facebook.com/Zaspeak-111164433880298/) shows the following post:

The destination website advertised (https://www.zaspeak.top) had the same COVID-19 banner at the top of the page.



COVID-19 Example 3: Fraudulent advertisements were identified that refer to business closures, bankruptcy and financial hardship as the reason behind unrealistic offers. Below are examples of scam ads for PlayStation, XBOX and Nintendo game consoles:

Launched June 2020

Active
Started running on Jun 27, 2020
ID: 1811059055702073

Ezio Udinese
Sponsored

The cheapest game console in the entire network,the boss went bankrupt,so the stock of Switch PS4 PRO XBOX ONE sold for $90 each one,Today only,opportunities aren't to be missed.Get it here;https://bit.ly/2NzPbEf

KJ81234.COM
Limited Discount.$99 Only Today !
Arrival within three days, brand new authentic, inventory clearance
Shop N...

Launched June 2020

Active
Started running on Jun 30, 2020
ID: 566489377289592

Biagio Russo
Sponsored

The boss ran away. We had to sell all game consoles at a low price to pay the store rent. Arrival within three days, no reason to return within seven days! Quality assurance! Get it here: https://bit.ly/2BoFVjH

ALPHAHYDRA.COM
Limited Discount.$99 Only Today !
Branded game consoles, Ship wi123thin 24 hours after order
Shop N...

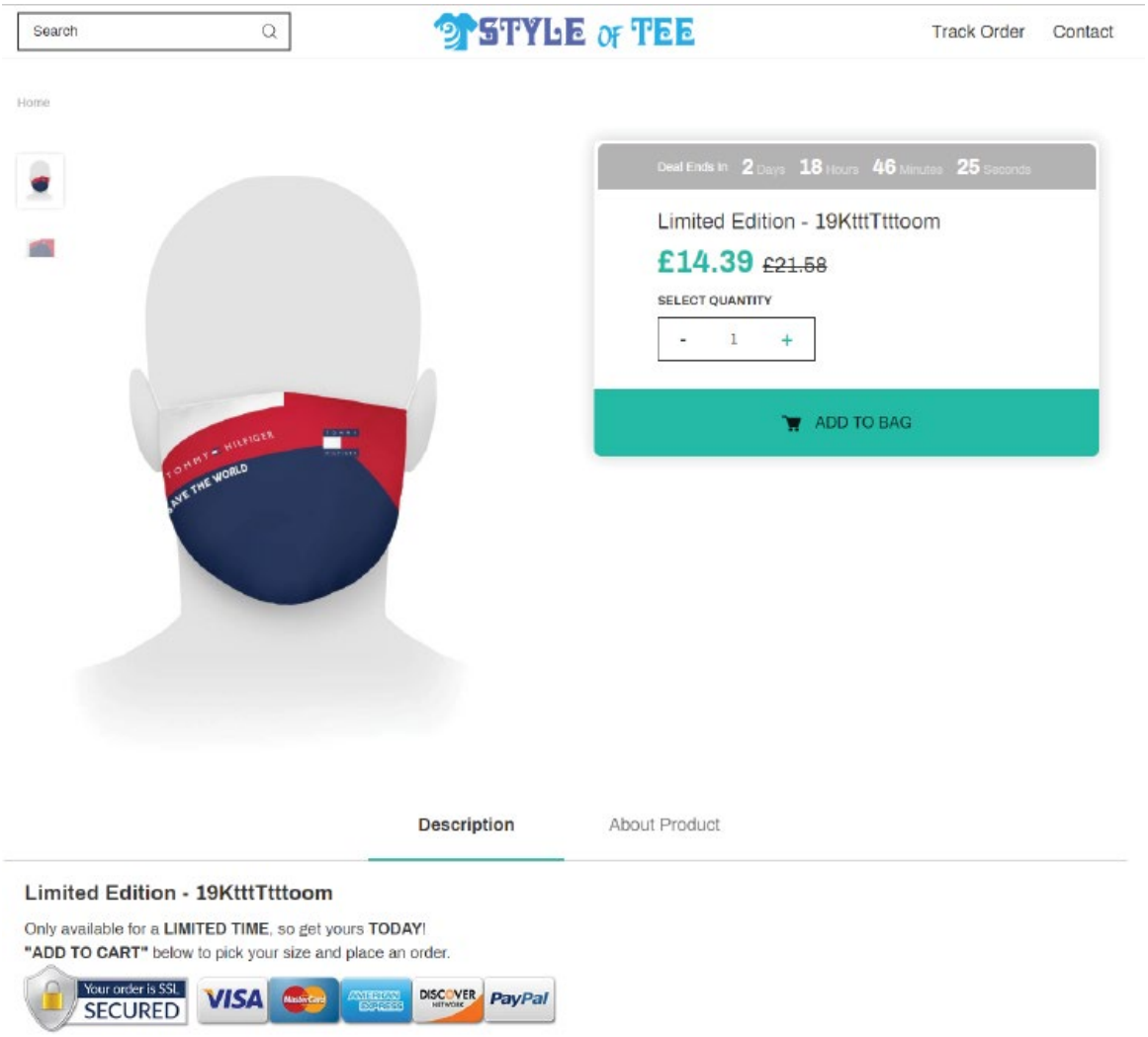
COVID-19 Example 4: Fraudulent advertisements were identified for counterfeit branded Tommy Hilfiger face masks. The advertiser was also found to be advertising face masks of UEFA football clubs.

Ad Image 1:

Ad Image 2:

The destination website advertised (https://styleoftee.com/) offered no information about the website's operator or location. Further research of the telephone number provided found a Facebook page for another company whose location map indicated it was based in Vietnam.

Website Image 1:



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 I TRACIT.org