Contents

[Appendix 1: Examples of Brands 3](#_Toc45288252)

[Apple 3](#_Toc45288253)

[Bose 5](#_Toc45288254)

[Braun 7](#_Toc45288255)

[Canon 9](#_Toc45288256)

[Fujifilm 10](#_Toc45288257)

[HP 11](#_Toc45288258)

[Keen 12](#_Toc45288259)

[Lacoste 14](#_Toc45288260)

[Lego 15](#_Toc45288261)

[Levis 16](#_Toc45288262)

[National Hockey League (NHL) 17](#_Toc45288263)

[Ray Ban 18](#_Toc45288264)

[Richemont (Mont Blanc) 19](#_Toc45288265)

[Skechers 19](#_Toc45288266)

[Star Wars (Disney) 20](#_Toc45288267)

[Timberland 21](#_Toc45288268)

[Under Armour 22](#_Toc45288269)

[Appendix 2: Customer complaints 24](#_Toc45288270)

[Bose 24](#_Toc45288271)

[FjallRaven 25](#_Toc45288272)

[Dewalt and Milwaukee Power Tools 26](#_Toc45288273)

[Lego 27](#_Toc45288274)

[Tommy Hilfiger 28](#_Toc45288275)

[Weber 29](#_Toc45288276)

[Appendix 3: Fraudulent Financial Services 31](#_Toc45288277)

[Appendix 4: Japan Case Study 33](#_Toc45288278)

[1. Brands Impacted by fraudulent Japanese ads: 33](#_Toc45288279)

[2. Keywords in Ads: 33](#_Toc45288280)

[3. Brand infringing Facebook Pages used to advertise: 34](#_Toc45288281)

[4. Examples of Ads: 36](#_Toc45288282)

[5. Example destination websites: 39](#_Toc45288283)

[Appendix 5: COVID-19 related fraud 41](#_Toc45288284)

# 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:**  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\APPLE\IMG_1994.PNG  **Ad Image 2:** |
| **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@kokoerp.com](mailto:Destiny20190610@kokoerp.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:** |
| **Ad Source:** Fraudulent advertisements found in Bing search results |
| **Ad Image:** |

## 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:**  H:\Legal\Shared\BRAND PROTECTION\ONLINE ENFORCEMENT\SOCIAL MEDIA\Facebook Inc\Project Hornpipe\Non-TH reports and adverts\iCloud Photos (15)\iCloud Photos\IMG_2053.PNG  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\CANON\Canon 2.png |

## Fujifilm

|  |
| --- |
| **Ad Source:** Fraudulent advertisement found on Instagram |
| **Ad 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/> |

## 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**](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=IwAR3ypWn68LJyhCGNt3u4-phjmb3zQT6GIuii2DRKIEh35KkT9pcGvisC-BA**  2. https://www.hotdisountsvps.com/shop/**?fbclid=IwAR3Ys2c4dedISA-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:**  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\LACOSTE\IMG_0953.PNG  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\LACOSTE\IMG_0944.PNG |

## Lego

|  |
| --- |
| **Ad Source:** Fraudulent advertisements found on Instagram and via Facebook’s Commerce and Ads IP Tool |
| **Ad Image 1:**  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\LEGO\IMG_5897.PNG |
| **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. |

## Levis

|  |
| --- |
| **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 |
| **Ad Image:** |
| **Ad Notes:** The destination website [https://www.officialnhlenjoy.store](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 (Mont Blanc)

|  |
| --- |
| **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\_ERxVzO51m9b5sDOy9XwtRoA9ugY34Zl3mXgHfHJ98**](https://cowris.com/products/manda?fbclid=IwAR2oqwwbcfM-rCvvC_ERxVzO51m9b5sDOy9XwtRoA9ugY34Zl3mXgHfHJ98) 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:**  C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\TH & Other Brands - IG Fraudulent Ads\TIMBERLAND\IMG_1557.PNG |

## 

## Under Armour

|  |
| --- |
| **Ad Source:** Fraudulent advertisement identified via Facebook’s Commerce and Ads IP Tool |
| **Ad Image:** |
| **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:    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>) |
|  |

## 

## FjallRaven

|  |
| --- |
| **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. |
| cid:image004.jpg@01D64FD1.81385480cid:image010.jpg@01D64FD1.81385480cid:image011.jpg@01D64FD1.81385480cid:image012.jpg@01D64FD1.81385480 |

## Lego

|  |
| --- |
| **Complaint Source:** Official Lego page on Facebook (<https://www.facebook.com/LEGO/posts/10156844122453403/>) |
| cid:image003.png@01D64FD0.0FC997B0 |

## 

## 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*](http://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/>) | | https://i.imgur.com/SZ7IV0x.png | |

# 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* | |
|  |  |
| On 1 March 2020 The Guardian published an article “*Fake 'traders' prey on victims in global investment scam*” (<https://www.theguardian.com/world/2020/mar/01/revealed-fake-traders-allegedly-prey-on-victims-in-global-investment-scam>). The article reported on suspected fraudsters lure investors with fake ads featuring celebrities such as Gordon Ramsay.  *An army of more more than 200 fake “traders” based in Ukraine have been persuading victims all over the world to part with their savings, according to a whistleblower from the operation who describes it as a huge investment scam.*  *British and Australian victims of a sophisticated enterprise were apparently lured by* ***fake ads posted on Facebook and mobile phone games featuring celebrities such as Gordon Ramsay, Hugh Jackman and the moneysaving expert Martin Lewis.*** *After responding to the ads, the whistleblower alleges that unsuspecting victims were contacted by call-centre workers operating in a building in the heart of Kyiv’s business district, promising lucrative investment opportunities.*  *But the investments in bitcoin, commodities and foreign currencies all appear to be fake, as do the follow-up calls from companies telling victims that they could help them recover the losses.*  *Investors in the UK and Australia are among thousands of people caught up in the apparent scam, which is allegedly being run from two floors of a respectable office building in the Ukrainian capital. Some have lost their life savings to fraudsters.*  *Details of the operation have been leaked by a whistleblower who provided the Swedish daily newspaper Dagens Nyheter with secretly filmed footage, internal company documents and testimony about its practices. The material has been seen by the Guardian and other partners in the Organized Crime and Corruption Reporting Project (OCCRP).*  *According to the whistleblower, the fraudulent investment operation made $70m (£55m) last year. The information he supplied also suggests that:*  *• Victims of the scam were persuaded to install software on their computers and phones that gave fraudsters access to their bank details.*  *• Accounts were faked showing huge returns to encourage people to trust the company and invest more.*  *• Fake traders were disparaging about their victims in internal company postings, repeatedly remarking how they had “fucked” unsuspecting investors.*  *• Members of the “retention” team at the firm, which was tasked with making 300 calls a day to extract more money from investors, were rewarded by commission-based payments according to how much money they persuaded victims to hand over.* | |

# 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 T0MMY) 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.

### Brands Impacted by fraudulent Japanese ads:

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

### 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”:

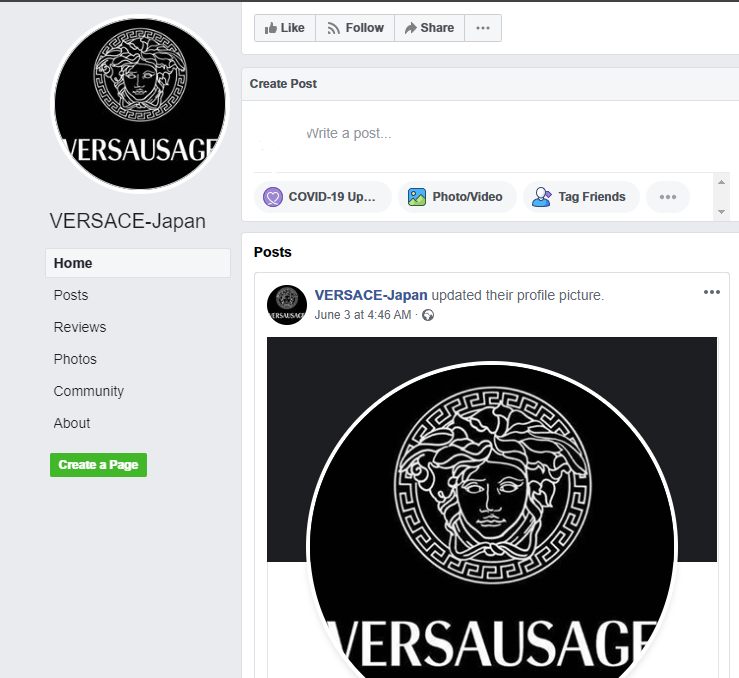
|  |  |
| --- | --- |
| 今日注文なら、もう一つ無料サービス | *Another free service if you order today* |
| Tommy hilfiger 2020年夏の新作シャツ 今日注文なら、もう一つ無料サービス | *Tommy hilfiger 2020 Summer New Shirts Get one more free order if you order today* |
| 夏の新作 今日注文なら、もう一つ無料サービス 数量限定、早い者勝ち | *Summer new work*  *Another free service 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* |

### 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.

1. **Versace**

[https:/www.facebook.com/VERSACE-Japan-113383623731279/](https://business.facebook.com/VERSACE-Japan-113383623731279/) Page created - June 3, 2020



1. **Ralph Lauren**

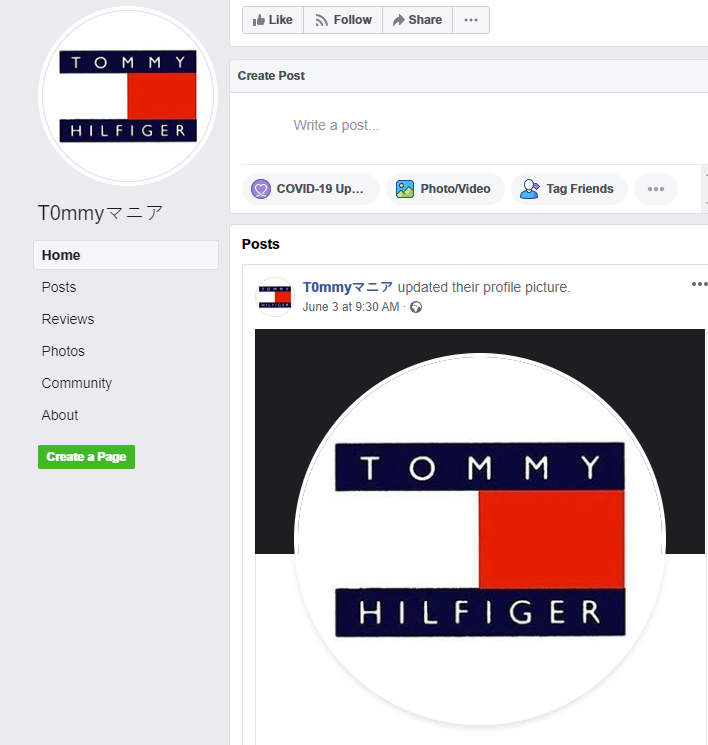
|  |  |
| --- | --- |
| <https://www.facebook.com/Ralph-Lauren-Japan-114036903669545> Page created - June 7, 2020 | <https://www.facebook.com/Polo-US-106626031086804/> Page created - June 8, 2020 |
|  |  |

1. **Adidas**

|  |  |
| --- | --- |
| <https://www.facebook.com/Adidas-clover-105720807845785> - Page created - June 9, 2020 | <https://www.facebook.com/ADIDaS-103488224739483/?business_id=10152446361520686> Page created - June 10, 2020 |
|  |  |

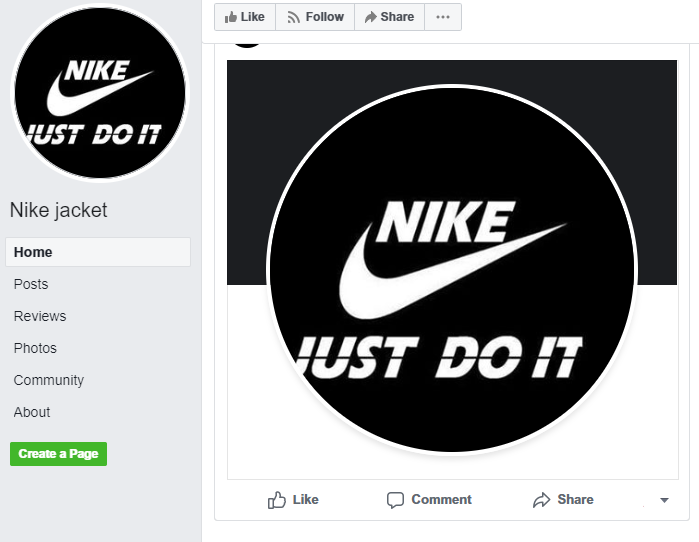
1. **Tommy Hilfiger**

<https://www.facebook.com/T0mmy%E3%83%9E%E3%83%8B%E3%82%A2-101962258219137> Page created - June 3, 2020



1. **Nike**

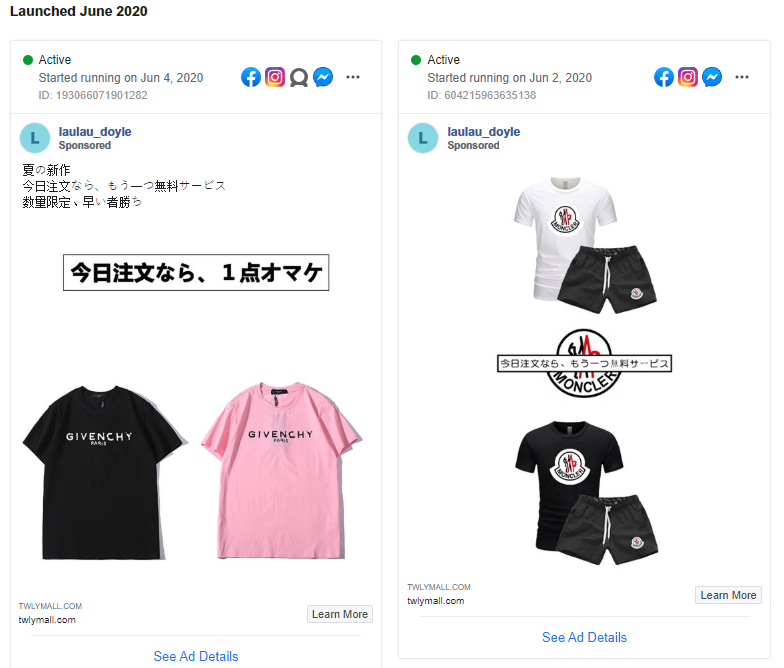
[https://www.facebook.com/Nike-jacket-107450461002864](https://business.facebook.com/Nike-jacket-107450461002864) Page created - June 8, 2020



### Examples of Ads:

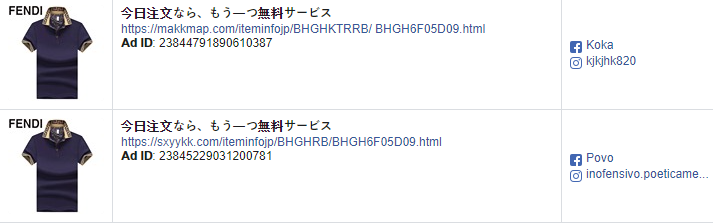
Many of the ads look visually similar featuring images of branded t-shirts together with the brand logo. Often the products in the images are obviously counterfeit missing correct labelling or being products not made by the brand.







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

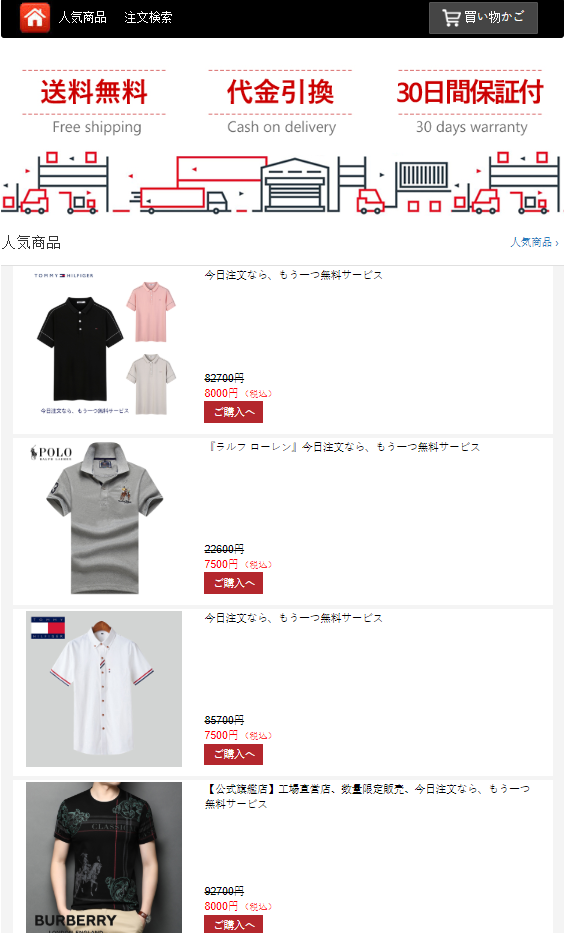


Identical keywords in advertisements for different brands were also identified from different advertisers, but directed to the same destination website. Below is an example of Gucci and Moncler ads using the same keywords and destination website:



### Example destination websites:

1. The website[http://vip.hotepstore.com](http://vip.hotepstore.com/details.php?id=61295237&fbclid=IwAR32d9Qp_YFIbnTldRtMm7HR5xt15Tq_dMHDf7tKB1eZn5dVnSfVx-W4bE0) 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.



1. 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.



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](http://www.healthprotectionmask.com), [www.handhealth.co.uk](http://www.handhealth.co.uk) and <https://muanha.myshopify.com/collections/anti-corona-virus> , the latter showed only Vietnamese contact information. |
| C:\Users\algray\OneDrive - PVH Corp\Facebook Instagram\Corona - Handhealth.co.uk ads\Handhealth.co.uk - Facebook Ads 03042020.JPG |

|  |
| --- |
| **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.  **Website Image 1:**  https://www.webpagetest.org/results/20/04/21/R2/1f51acd43f2e318049ecef48f249f548/1_screen.jpg |

|  |
| --- |
| **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:  **Ad Image 1 : Ad Image 2:** |