TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

AMERICAN
APPAREL & FOOTWEAR
ASSOCIATION

PUBLICIDAD FRAUDULENTA ONLINE

RIESGOS EMERGENTES Y FRAUDE AL CONSUMIDOR

RESUMEN EJECUTIVO

SOBRE TRACIT

La Alianza transnacional para combatir el comercio ilícito (Transnational Alliance to Combat Illicit Trade, TRACIT) es una iniciativa independiente del sector privado para impulsar el cambio a fin de mitigar los daños económicos y sociales del comercio ilícito, mediante el fortalecimiento de los mecanismos de aplicación de la ley de los gobiernos y la movilización de las empresas de los sectores industriales más afectados por el comercio ilícito.

SOBRE AAFA

La Asociación Norteamericana de Ropa y Calzado (American Apparel & Footwear Association, AAFA) es la asociación comercial nacional que representa a las empresas de ropa, calzado y otros productos de costura, y a sus proveedores, que compiten en el mercado mundial. Representa a más de 1.000 marcas de renombre mundial. La AAFA es la representante de las políticas públicas de confianza y de la política de la industria de la ropa y el calzado. www.aafaglobal.org

PARA MÁS INFORMACIÓN

Este documento es un Resumen Ejecutivo del informe completo, Publicidad Fraudulenta Online, Riesgos Emergentes y Fraude al Consumidor. Para consultar el informe completo y los análisis y estudios de casos más extensos que contiene, por favor visite: www.tracit.org/featured-report-fraudulent-advertising-online.html

MEDIOS DE COMUNICACIÓN

Todas las preguntas de los medios de comunicación deben dirigirse a Cindy Braddon, Responsable de Comunicaciones y Políticas Públicas, cindy.braddon@TRACIT.org

REDES SOCIALES

Twitter: @TRACIT_org
LinkedIn: www.linkedin.com/company/tracitorg

RECONOCIMIENTOS

Expresamos nuestro agradecimiento a Toe Su Aung y Sam Irving de Elipe, Ltd., por su investigación exhaustiva y su orientación minuciosa... (www.elipe-global.com). También apreciamos las contribuciones de las numerosas empresas que han identificado y compartido ejemplos de publicidad fraudulenta de sus productos.

El objetivo de este informe es ayudar a eliminar de Internet el fraude generalizado en la publicidad. El primer paso en este proceso es aclarar la incidencia de la publicidad fraudulenta que aparece en las plataformas de compras y de las redes sociales. Los consumidores más informados están en mejores condiciones de defenderse contra el fraude. Siempre que se encuentren anuncios fraudulentos, sugerimos, en primer lugar, que estos se comuniquen a la plataforma pertinente en la que aparezcan y, cuando proceda, a los organismos encargados de la aplicación de la ley o a los organismos reguladores gubernamentales.

RESUMEN EJECUTIVO

¿Cuál es el gran tema sobre la publicidad fraudulenta?

La publicidad fraudulenta se está convirtiendo rápidamente en un nuevo riesgo para los consumidores que compran online, donde millones de personas están expuestas a miles de anuncios fraudulentos que las llevan a miles de sitios web de comercio electrónico ilegítimos que las defraudan y/o les venden productos falsificados y servicios engañosos.

Para mantener el ritmo de las tendencias de los consumidores -y para ir un paso más allá de los controles-, los comerciantes ilícitos publican ahora anuncios fraudulentos que desvían a los consumidores desprevenidos hacia sitios web que presentan falsificaciones, servicios falsos y otros fraudes. Es preocupante que los anuncios estén en todas las redes sociales como Facebook e Instagram, u otros sitios web populares como YouTube o Google, donde la gente no espera que se cometa un fraude.

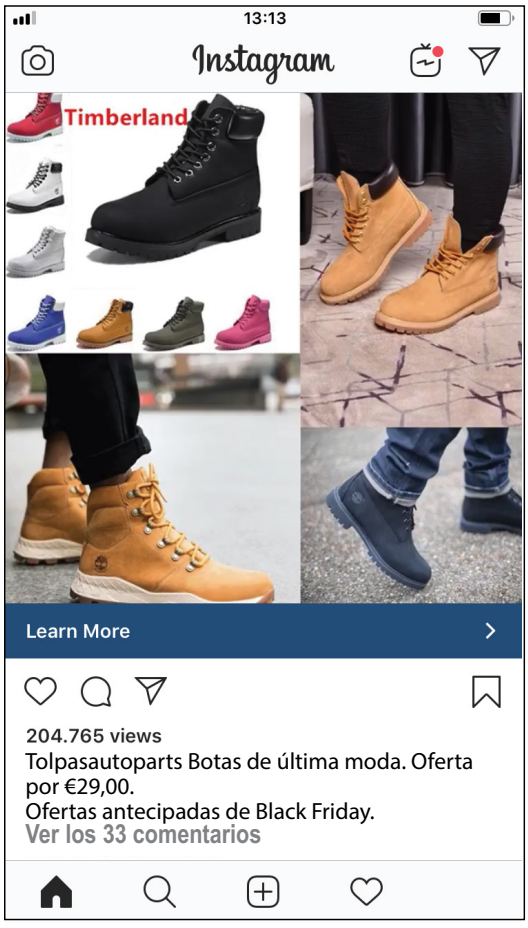
Según este informe, muchas marcas internacionales populares fueron blanco de anuncios fraudulentos en Instagram y Facebook desde 2017, algunas de las cuales recibieron hasta un cuarto de millón de visitas antes de ser detectadas. Y al igual que los anuncios legales que parecen saber por arte de magia lo que se busca, incluso antes de empezar a buscarlo, los anuncios fraudulentos también suelen estar extremadamente dirigidos a los consumidores en base a intereses específicos, ubicación, datos demográficos o historial de navegación.

Además de la publicidad de productos falsos y de calidad inferior, existe una tendencia creciente a la publicidad engañosa de servicios comerciales y financieros fraudulentos, en la que se utilizan sin autorización nombres e imágenes de personalidades populares.

Para los consumidores, su exposición a los productos falsificados y a los servicios fraudulentos presenta riesgos directos e indirectos para la salud y la seguridad. La mayoría de los sitios web fraudulentos también muestran una falta de respeto por la privacidad de los datos y exponen a los consumidores al fraude con tarjetas de crédito, al robo de identidad y a otros delitos cibernéticos. Aún más alarmantes son las pruebas de que una red o varias redes delictivas coordinadas suelen estar detrás de los anuncios.

La publicidad fraudulenta online está en todas partes

- Desde mayo de 2017, más de 70 empresas de consumo y de ropa confirmaron haber sido



blanco de anuncios patrocinados fraudulentos e infractores en ***Instagram*** y ***Facebook*** (Figura 1).[1] Es probable que el número real sea significativamente mayor, ya que estos anunciantes se dirigen a las marcas de forma indiscriminada en varios sectores. Dada la existencia de un modus operandi común, parece que también puede haber una red o varias redes delictivas coordinadas detrás de los anuncios, que utilizan perfiles pirateados de Facebook o generados por *bot* junto con datos de tarjetas de crédito robadas para publicar anuncios que engañan a los consumidores y los dirigen a sitios web de comercio electrónico que defraudan y/o venden productos falsificados.

- Los estafadores han utilizado la plataforma de vídeo de ***Google***, ***YouTube,*** para explotar la popularidad de ciertos videojuegos populares y crear vídeos que engañan a los consumidores para que descarguen aplicaciones de riesgo o compren servicios falsos. En el peor de los casos, los usuarios están siendo engañados con importantes sumas de dinero. Una estafa cobró automáticamente una cuota de suscripción de 99,99 dólares. También en YouTube, los estafadores utilizan COVID-19 para obtener beneficios mediante vídeos fáciles de encontrar que promocionan máscaras faciales y vacunas falsas a precios excesivos, que cuestan a los consumidores más de 5 millones de dólares.[2]
- En abril de 2019, se identificó un anuncio de ropa falsa de Tommy Hilfiger en ***LinkedIn***. El anuncio dirigía a la gente al sitio web fraudulento www.tommy-top.com, que era idéntico a otros sitios web fraudulentos y falsificados identificados a través de los anuncios de Instagram.

Los anuncios falsos tienen la intención de engañar

Al igual que los anuncios legales que parecen conocer por arte de magia la lista de deseos de compra online de todo el mundo, los anuncios fraudulentos también suelen estar extremadamente dirigidos a los consumidores en

Figure 1[3]

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 (que incluyen Juventus F.C., Liverpool F.C., Real Madrid C.F. y Tottenham Hotspur F.C.)
68. Ugg/Deckers
69. Van Cleef
70. Vans
71. Vasque
72. Weber
73. Xbox (Microsoft)

función de intereses específicos, ubicación, datos demográficos o historial de navegación.

Además, las tácticas utilizadas por los falsificadores para confundir a los compradores en Amazon u otras plataformas de comercio electrónico se utilizan igualmente por los delincuentes que publican anuncios fraudulentos. Estas tácticas engañosas incluyen el uso de marcas comerciales conocidas, imágenes no autorizadas protegidas por derechos de autor y ofertas falsas para crear anuncios falsos de aspecto extremadamente profesional que no se pueden distinguir de los anuncios legítimos, salvo que los hipervínculos desvían a los consumidores a sitios web delictivos que venden artículos falsificados o servicios fraudulentos.

Por ejemplo, hubo un aumento significativo del número de anuncios fraudulentos publicados por cuentas nuevas genéricas (por ejemplo, "Tienda de chaquetas de moda" y "Descuento para mochilas") en las dos semanas previas al "Black Friday" en 2019. Los anuncios y los sitios web fraudulentos asociados ofrecían enormes descuentos poco realistas dirigidos a juguetes populares, bolsos, chaquetas y botas de invierno, guitarras y rastreadores de fitness, así como a muchas marcas populares de ropa de moda. El fundamento de la estafa es el conocimiento del consumidor de que los descuentos de las marcas legítimas pueden ser más altos de lo normal cerca del Black Friday.

Junto con la publicidad fraudulenta está el despliegue de URL de destino indicados de manera falsa dentro de los anuncios, redireccionamientos múltiples de URL, técnicas de encubrimiento de URL y acortadores de URL (bit.ly) para engañar a los consumidores e impedir la detección por parte de los investigadores. Estas sofisticadas redirecciones de URL suelen cambiar los destinos del sitio web cuando un usuario hace clic en un anuncio, dependiendo de si el usuario está viendo el anuncio en un navegador de escritorio o a través de la propia aplicación de la red social.

Impacto económico

La nueva puerta de entrada a las ventas ilícitas online es un enlace de un anuncio fraudulento a un sitio web fraudulento que ofrece productos ilícitos. Las investigaciones realizadas aportan pruebas que indican que con el tiempo se dispone de cientos de miles de anuncios fraudulentos, respaldados por grandes redes de sitios web fraudulentos y de engaño listos para recibir y defraudar a consumidores desprevenidos. Como se pone de relieve en el presente informe, la tendencia es a presentar cada vez más anuncios realistas, pero no por ello menos fraudulentos, en plataformas de redes sociales que pueden llegar instantáneamente a millones de usuarios en línea desprevenidos.

Aunque el presente informe no es un estudio cuantitativo sobre la magnitud y el valor de la falsificación, de las tendencias actuales pueden extraerse importantes conclusiones sobre las repercusiones de la publicidad fraudulenta. Según un informe de 2017 de Frontier Economics, el valor económico mundial de la falsificación (sin incluir la piratería digital) en 2020 es de aproximadamente 1,8 billones de dólares.[4] Las ventas online representan ahora entre el 14 y el 16 por ciento del total de las ventas al por menor en todo el mundo durante el período 2019-2020.[5] Por consiguiente, como parte de la falsificación mundial, el valor de las falsificaciones adquiridas a través de los puntos de venta online se estima entre 252.000 y 288.000 millones de dólares. Esta estimación se compara razonablemente con el Informe sobre la falsificación de marcas a nivel mundial de 2018, en el que se estima que las pérdidas sufridas por la falsificación online a nivel mundial ascendieron a 323.000 millones de dólares en 2017.[6]

A veces las campañas se alinean ferozmente con los eventos de compras globales, donde las redes delictivas están coordinando la creación de cientos de cuentas publicitarias, sitios web, hosting e infraestructuras de pago para maximizar su retorno de inversión mientras compiten con las

marcas legítimas en el mismo espacio. Algunos de los anuncios fraudulentos de marcas conocidas pueden atraer un cuarto de millón de visitas en un solo día. En otro ejemplo, un anuncio fraudulento de productos falsificados de Instagram utilizaba un dominio vinculado a otros 3.200 dominios fraudulentos, todos ellos con "importantes descuentos" para artículos de marca y sin información de contacto.

Dado que la falsificación aumentó en un 154% en la última década y que las compras online aumentan entre un 10 y un 20% al año, este problema seguirá creciendo si no se controla.[7]

¿Qué peligros hay?

- **Riesgos para el consumidor:** Los anuncios fraudulentos dan a los consumidores inocentes una falsa impresión de autenticidad. Los productos falsificados son generalmente de mala calidad, no duran, no están garantizados y pueden ser peligrosos.

- **Los empresarios y los propietarios de marcas:** El robo de IP en forma de falsificación de marcas y piratería de derechos de autor, frena el crecimiento económico y la creación de empleo al desalentar la innovación, reducir los incentivos para que las empresas inviertan en I+D e impedir que las industrias creativas desarrollen todo su potencial.

- **Privacidad de datos:** La mayoría de los sitios web fraudulentos muestran una falta de respeto por la privacidad de los datos de cualquier tipo, incluidos los datos de los clientes, la seguridad y la información financiera. Dado que estos sitios web rara vez utilizan alguna forma de seguridad, los consumidores también suelen estar expuestos al fraude con tarjetas de crédito, al robo de identidad y a otros delitos cibernéticos.

- **Delito organizado:** Los anuncios fraudulentos e infractores descubiertos en Facebook suelen compartir características similares y sugieren que los grupos de delitos organizados o las redes ilícitas organizadas están operando estas campañas publicitarias fraudulentas

¿Cuáles son las causas?

La causa raíz del problema es que la mayoría de las plataformas de las redes sociales y los sitios web de comercio electrónico aceptan publicidad sin los controles adecuados sobre la fuente del anunciante.

- **Verificación limitada:** Sin controles rigurosos de diligencia debida que verifiquen la identidad de quien se anuncia en la plataforma, los anunciantes fraudulentos tienen libertad para explotar el sistema con poco riesgo de exposición y prácticamente sin riesgo de castigo o penalización. La colocación de un anuncio fraudulento puede hacerse en solo un par de horas a un costo muy bajo.

- **Debilidades del sistema:** Los estafadores se aprovechan de las deficiencias del sistema, como la falta de control de las cuentas que patrocinan los anuncios fraudulentos, por ejemplo, el historial de la cuenta o la relevancia entre las cuentas publicitarias y el anuncio.

- **Sin controles en los sitios web de destino:** Cuando los usuarios de Instagram o Facebook hacen clic en anuncios patrocinados fraudulentos, un navegador *in-app* normalmente los dirige a un sitio web externo que opera una tienda web. Por lo general, se trata de sitios web fraudulentos diseñados específicamente para vender productos falsificados o engañosos. Si no hubiera sitios web de destino fraudulentos, los anuncios engañosos no tendrían ningún lugar al que redirigir a los consumidores. Por estas razones, se han realizado esfuerzos dirigidos a los registradores de nombres de dominio y a los proveedores de servicios de Internet para impedir o eliminar esos sitios ilegales.

- **Poca protección contra los infractores reincidentes:** No es difícil repetir un anuncio fraudulento, incluso después de haber sido denunciado. El hecho de que tantas marcas internacionales hayan sido objeto de anuncios fraudulentos que utilizan el mismo modus operandi durante un período de tres años sugiere que las plataformas de redes sociales

deben adoptar medidas más enérgicas para poner fin a las actividades reincidentes relacionadas con la publicidad o solicitar la asistencia de los organismos responsables de la aplicación de la ley.

- Prácticas engañosas: Un anuncio fraudulento que suele aparecer en Instagram o Facebook dirigido a una marca conocida puede ser de muy alta calidad de diseño, mostrando cientos de imágenes de productos. Presentan descuentos muy altos y logotipos falsos de pago para atraer a los consumidores a una compra rápida.
- Cadena de abastecimiento de la Publicidad online: Dadas las repetidas similitudes identificadas a lo largo de este informe, es evidente que existe un problema sistémico en la cadena de suministro de la publicidad en línea. En particular, la actual ausencia de una verificación sustantiva de la identidad comercial y/o personal de un anunciante y el proceso de examen de los propios anuncios presentados parecen ser insuficientes para hacer frente a la magnitud del engaño y el fraude que se producen en las plataformas de redes sociales.

CONCLUSIONES

En vista de las conclusiones del presente informe, existe un problema sistémico en la cadena de suministro de la publicidad online y una necesidad urgente de mejorar los controles al respecto. Para empezar, los gobiernos deben iniciar el proceso de establecer directrices y normas. Ya existen varios ejemplos y se podrían modificar o ampliar para incluir el desafío de eliminar la publicidad fraudulenta:

- En el Reino Unido, se han otorgado nuevas facultades al organismo de control de las comunicaciones Ofcom para obligar a las empresas de redes sociales a actuar en relación con los contenidos perjudiciales, como la violencia, el terrorismo, el ciberacoso y el abuso infantil. Ofcom tendrá el poder de hacer a las empresas de tecnología responsables de proteger a las personas de tales contenidos, incluyendo la garantía de que el contenido se elimine rápidamente y minimizar los riesgos de que aparezca de alguna manera.
- Alemania introdujo la Ley NetzDG en 2018, que establece que las plataformas de redes sociales con más de dos millones de usuarios alemanes registrados tienen que revisar y eliminar el contenido ilegal en las 24 horas siguientes a su publicación o se enfrentarán a multas de hasta 50 millones de Euros.
- En abril de 2019, Australia aprobó la Ley sobre el intercambio de material violento aberrante, que introduce sanciones penales para las empresas de redes sociales, posibles penas de cárcel para los ejecutivos de tecnología de hasta tres años y sanciones financieras de hasta el 10% del volumen de negocios mundial de una empresa.[8]

Se han formado algunos grupos en Facebook paraayudar a generar mayor conciencia entre los consumidores sobre los anuncios fraudulentos:

- Facebook *Ad Scambusters!* se creó para concientizar sobre los muchos anuncios fraudulentos en Facebook. El grupo afirma que muchos de estos anuncios parecen legítimos y tienen videos, imágenes, etc. profesionales. También explica que Facebook, Shopify y PayPal se benefician de los anuncios fraudulentos y hacen que sea muy complicado presentar quejas o conseguir reembolsos. El grupo ofrece ayudar a la gente a aprender a investigar un sitio y asegurarse de que es legítimo antes de comprar productos online.[9]
- El grupo de Facebook *(ProtectOthers) Ad Scams* se creó para alertar a las personas de la gran cantidad de anuncios de estafa que Facebook está permitiendo que circulen. El grupo alienta a las personas a denunciar los anuncios fraudulentos y advertir a otros compartiendo el enlace del anuncio a su página.[10]

Mientras tanto, sin embargo, es indispensable que los sitios web y las plataformas que obtienen ingresos de la prestación de servicios de publicidad a las redes delictivas tomen medidas para identificarlas y bloquearlas definitivamente. Al adoptar inmediatamente las mejores prácticas en las verificaciones de "conozca a su cliente comercial", las plataformas pueden mitigar los riesgos de inmediato. Este problema lleva ya por lo menos cinco años de preparación, por lo que es indispensable abordar las causas fundamentales que hacen posible esas oportunidades rentables.

Los consumidores tienen derecho a una experiencia de navegación y compra online que sea segura y protegida contra el fraude. Las plataformas online que conectan a las personas y las que se benefician del comercio en sus sitios deben ser responsables, cumplir con la ley y reconocer la responsabilidad ética y moral de garantizar a los consumidores un entorno seguro y de confianza. En este documento se sugiere que la publicidad fraudulenta online podría reducirse considerablemente a través de las siguientes medidas:

1. Mejores protocolos de "Conozca a su cliente comercial"

Es fundamental que los sitios web y las plataformas de redes sociales sepan con quién están trabajando cuando acepten publicidad paga. Al recopilar y verificar una cantidad apropiada de datos sobre quién está utilizando sus servicios de publicidad, podrán:

- evaluar los niveles de riesgo e identificar proactivamente a los que no sean responsables,
- Evitar la actividad reincidente de las cuentas eliminadas con anterioridad,
- proporcionar datos sobre los infractores a los consumidores afectados, a los titulares de derechos y a los organismos encargados de aplicar la ley.

Los datos recogidos podrían incluir el nombre y la dirección de la persona o la empresa (con una identificación reconocida), el número de teléfono, el correo electrónico y una constancia de la inscripción de la empresa.

Por ejemplo, Facebook (e Instagram) podrían hacer obligatoria la participación en la autenticación de dos pasos para cualquier perfil o página. Para las compras en línea y, en particular, la publicidad patrocinada, la transparencia y la posibilidad de imputar definitivamente a un anunciante es esencial para la confianza y la seguridad del consumidor. Esto significa poder tener la confianza de que quienquiera que esté vendiendo un determinado producto o servicio puede ser identificado, contactado y considerado responsable si las cosas van mal. La norma de las empresas que valen miles de millones debería ser que se muestren proactivas y socialmente responsables para asegurar la integridad del mercado y que los compradores se sientan seguros.[11]

En última instancia, cuando son objeto de una actividad delictiva sostenida, debe haber una voluntad decidida de trabajar juntos y de pedir que rindan cuentas los responsables en última instancia, y dificultar al máximo que los falsificadores sigan operando e infiltrándose en las experiencias de los compradores genuinos.

2. Revisión rigurosa de la publicidad antes de su publicación

Para garantizar que se respeten sus condiciones de servicio y que los consumidores inocentes no sean objeto de fraude mediante publicidad fraudulenta y engañosa, todos los anuncios publicados en un sitio o plataforma deben revisarse manualmente para comprobar que no infrinjan el contenido, tanto de forma algorítmica como en los casos en que se haya detectado un alto riesgo. Además, los sitios externos a los que se enlazan esos anuncios también se deben revisar para determinar su legitimidad y autenticidad.

3. Medidas de reacción eficaces contra los anunciantes fraudulentos

Para actuar como un elemento disuasorio eficaz de las actividades publicitarias ilegales, los sitios y plataformas deben establecer medidas firmes, eficaces y aplicadas contra los anunciantes que se haya descubierto que infringen sus condiciones de servicio. Estas medidas deben ir más allá de la rescisión del acuerdo publicitario e incluir la eliminación de la cuenta del infractor y el bloqueo del anunciante del sitio web o la plataforma.

Por su parte, Facebook es consciente del problema y recientemente señaló sus herramientas y esfuerzos contra la falsificación. En una publicación reciente, Facebook reconoció que el tema de los productos falsificados es especialmente importante para los anunciantes en el período previo a las fiestas, y aseguró que la empresa tiene "políticas estrictas contra los productos falsificados y otros tipos de violaciones de la propiedad intelectual".[12] Para probar este punto, reveló que en la primera mitad de 2019, retiró 359.000 piezas de contenido en Instagram en respuesta a 39.200 informes de falsificación presentados por los propietarios de marcas.

Además, afirmó que estaba invirtiendo en aprendizaje automático e inteligencia artificial "para ayudar a bloquear o reducir la distribución de contenidos potencialmente falsificados tanto en Facebook como en Instagram."[13]

4. Garantizar que los consumidores y los titulares de derechos puedan informar y compartir información sobre anunciantes fraudulentos

Hasta que la publicidad en los sitios web y las plataformas de redes sociales cuenten con un sistema eficaz para prevenir la presencia de delincuentes, deben existir vías para que los consumidores y los titulares de derechos compartan información que pueda utilizarse para desmantelar las redes delictivas que operan actualmente en sus plataformas. En la actualidad, si bien es posible denunciar y eliminar los anuncios, las plataformas parecen no ser receptivas a las tendencias de recepción y las iniciativas de intercambio de datos que podrían ayudarlas a bloquear a los delincuentes que acceden a la publicidad.

5. Establecer requisitos para una licencia de e-business para los anunciantes

Esa licencia exigiría la verificación de i) las declaraciones financieras que puedan ser corroboradas por terceros (por ejemplo, los estados de cuenta bancarios), y ii) la información sobre la ubicación física que pueda ser respaldada por registros gubernamentales o por terceros de confianza.[14] Lo ideal sería que ese sistema estuviera acompañado de un registro central, administrado por una parte o un grupo industrial altamente seguro y desinteresado para mantener las licencias.[15]

NOTES

[1] Las investigaciones principales realizadas por las marcas miembros de TRACIT y AAFA, Elipe Limited y las marcas no asociadas (es decir, las que proporcionaron ejemplos).

[2] Leskin, P. (2 de abril de 2020). Estafadores y estafadores están promocionando máscaras y falsas vacunas contra el coronavirus en YouTube, ya que la plataforma no logra moderar su contenido una vez más. *Business Insider*. Disponible en:https://www.businessinsider.com/youtube-videos-ads-face-masks-coronavirus-vaccines-misinformation-content-moderation-2020-4

[3] Las capturas de pantalla de los anuncios fraudulentos identificados y de los sitios web de destino están disponibles a pedido.

[4] Cámara de Comercio Internacional. (2016) Disponible en: https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/

[5] Statista. (2020). *Participación de E-commerce en las ventas minoristas totales a nivel global de 2015 a 2023*. n.p.: Statista. Available at: https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/

[6] Informe mundial sobre la falsificación de marcas (*Global Brand Counterfeiting Report*) 2018-2020. Consultar: https://apnews.com/ef15478fa38649b5ba29b434c8e87c94

[7] Departamento de Seguridad Nacional de los Estados Unidos. (2019). Lucha contra el tráfico de productos falsificados y la piratería, https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

[8] BBC. (12 de febrero de 2020). El regulador Ofcom tendrá más poderes sobre las redes sociales del Reino Unido. *BBC*. Disponible en: https://www.bbc.com/news/technology-51446665

[9] Consultar: https://www.facebook.com/groups/stopfraudads/

[10] Consultar: https://www.facebook.com/protectothers/

[11] Bradford, D. S. (6 de diciembre de 2019). Las estafas publicitarias de Facebook están golpeando duramente a los usuarios, ¿qué podemos hacer? *Buzzfeed*. https://www.buzzfeed.com/davidsbradford/facebook-ad-scams-are-hitting-users-hard-what-can-cbr58l7wiq?fbclid=IwAR1mRgZntRfZmqQqvhhmV4-9X3rwMnQqqer79bGohiP3MVOMrxbS4jxEnng

[12] Facebook Business. (2019). *Buenas preguntas, respuestas verdaderas: Proteger las marcas contra las falsificaciones.* Disponible en: https://www.facebook.com/business/news/good-questions-real-answers-how-facebook-helps-brands-protect-against-counterfeits/

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

[14] La Asociación Americana de Ropa y Calzado (AAFA) lo recomendó en respuesta al Memorando de los EE. UU. sobre la lucha contra el tráfico de productos falsificados y la piratería.

[15] El Depósito Central de Registros de la FINRA podría funcionar como modelo para esto.

APÉNDICE 1: EJEMPLOS DE MARCAS

Estos ejemplos han sido proporcionados por marcas o encontrados a través de investigaciones en línea. En los casos en que las marcas han proporcionado estos ejemplos, se ha dado permiso para incluirlos en este apéndice.

Apple

Fuente publicitaria: Avisos fraudulentos encontrados en Instagram y por medio de la herramienta de Facebook Commerce and Ads IP.

Imagen publicitaria 1:

Imagen publicitaria 2:

¡Ventas directas de fábrica!
donottag.co
¡Grandes ventas! Hace poco mi fábrica cerró y sólo quedan estos AirPods. Casi al precio de costo. Un descuento menor que el precio de empleado. ¡Los AirPods más baratos que has encontrado en tu vida! No te lo pierdas.
bit.ly/2Jz2C50 Ver menos
Ad ID: 23844633453950416

HP

Fuente publicitaria: Publicidad fraudulenta encontrada por medio de la herramienta de Facebook Commerce and Ads IP.

Imagen publicitaria:

¡YA!! DESPACHO-HP OfficeJet 5255 Wireless All-in...
elcheer.com
¡YA! https: bit.ly/2V5DtVL
¡YA! - https: bit.ly/2V5DtVL
¡Oferta por tiempo limitado! ¡Súper ofertas que no te las puedes perder!
Entrega gratis. ¡Para obtener el descuento, compra lo antes posible! Ver menos
Ad ID 23844946626830106

¡YA!! DESPACHO -HP OfficeJet 5255 Wireless All-in...
elcheer.com
¡YA! https: bit.ly/2V5DtVL
! ¡YA! - https: bit.ly/2V5DtVL
¡Oferta por tiempo limitado! ¡Súper ofertas que no te las puedes perder!
Entrega gratis. ¡Para obtener el descuento, compra lo antes posible! Ver menos
Ad ID 23844946626830106

¡YA!! DESPACHO -HP OfficeJet 5255 Wireless All-in...
elcheer.com
¡YA! https: bit.ly/2V5DtVL
! ¡YA! - https: bit.ly/2V5DtVL
¡Oferta por tiempo limitado! ¡Súper ofertas que no te las puedes perder!
Entrega gratis. ¡Para obtener el descuento, compra lo antes posible! Ver menos
Ad ID 23844946626830106

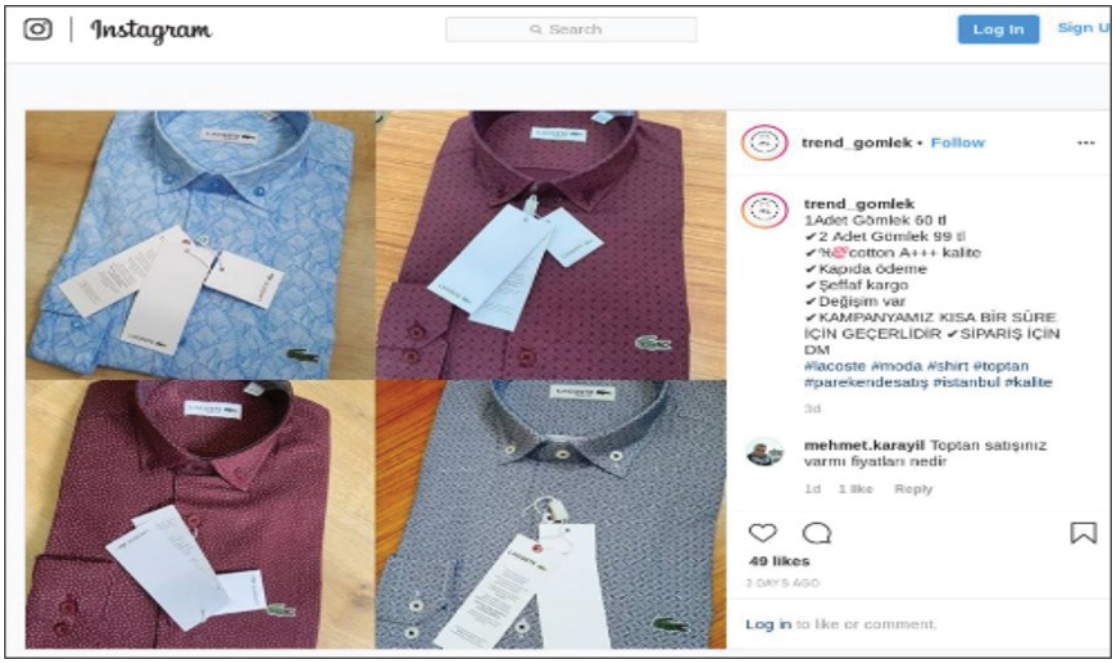
Notas publicitarias: La URL de destino de estos anuncios utiliza la propia herramienta de seguimiento y análisis de visitantes de Facebook llamada Píxel de Facebook que se destaca en negrita a continuación: https://elcheer.com/shopping/uncategorized.html/hot%f0%9f%94%a5%ef%bc%81clearance%ef%bd%9ehp-officejet-5255-wireless-all-in-one-printer/?fbclid=IwAR0ualOZp57uDDDmoVkSqvBGSctelM_-vUBDNKmUQk16bXK7gjJEYT1S_q4

Lacoste

Fuente publicitaria: Publicidades fraudulentas identificadas en Facebook e Instagram

Imagen publicitaria 1:

Imagen publicitaria 2:

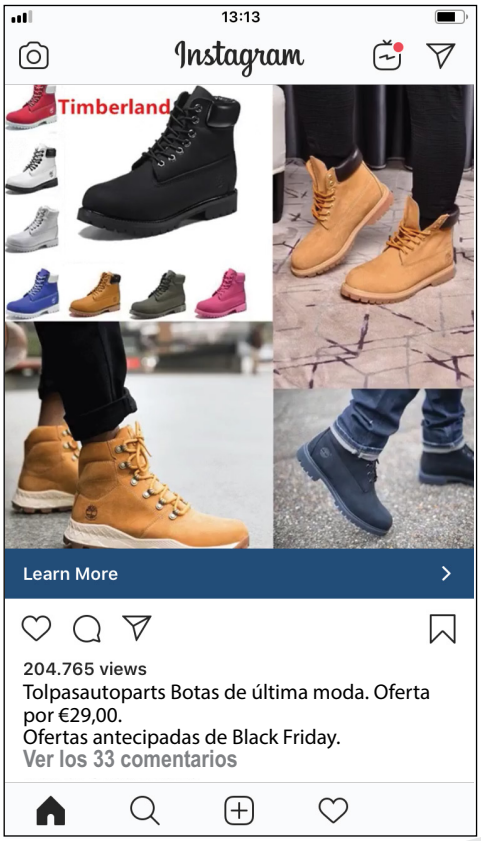


Timberland

Fuente publicitaria: Anuncios fraudulentos encontrados en Instagram.

Imagen publicitaria 1:

Imagen publicitaria 2:



Tommy Hilfiger

Fuente publicitaria: Anuncios fraudulentos encontrados en Instagram y a través de la herramienta de Facebook Commerce and Ads IP.

Imagen publicitaria 1:

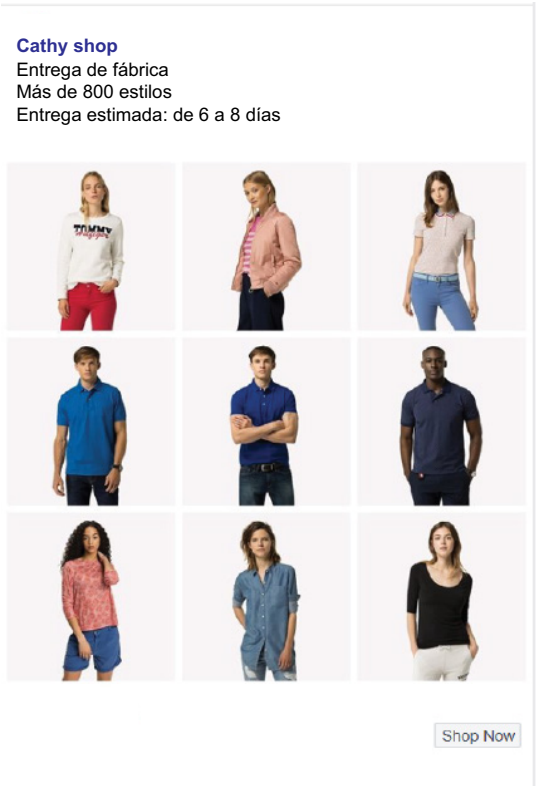
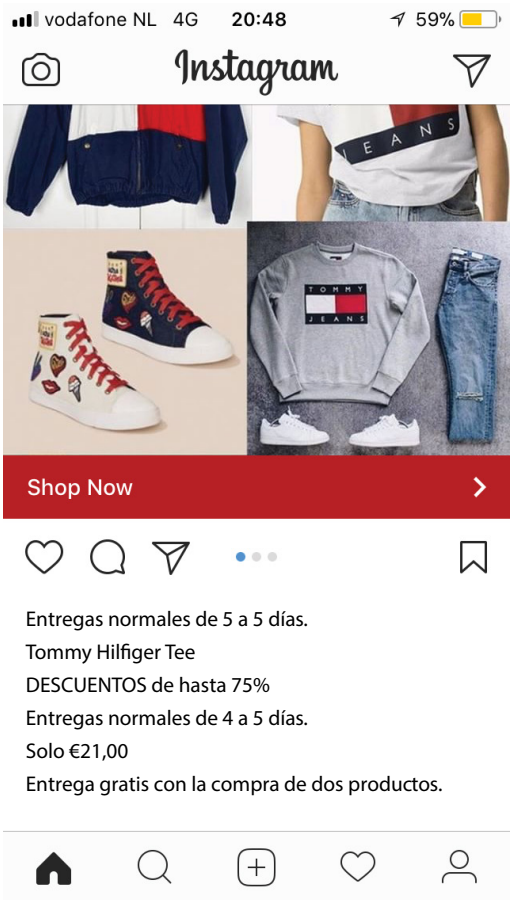


Imagen publicitaria 2:



TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

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