

VENDOR ACCOUNTS ON THIRD PARTY TRADING PLATFORMS

RESEARCH ON ONLINE BUSINESS MODELS INFRINGING
INTELLECTUAL PROPERTY RIGHTS – PHASE 4

Executive Summary



October 2021

EXECUTIVE SUMMARY

Background

In 2020, the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, commissioned a research study on intellectual property (IP) infringement through vendor accounts on third-party trading platforms. The purpose of the research was to enhance the level of understanding about the ways in which IP infringers misuse online trading platforms to market goods and services infringing IP rights, how the business models adopted by IP infringers work, and thereby provide new knowledge to tackle the challenge of this phenomenon more effectively.

The research study was commissioned to the Centre for Intellectual Property Policy and Management (CIPPM) of Bournemouth University, which set up a team of researchers in law and computer science⁽¹⁾. The research team was assisted by a group of experts including representatives of rights holders, online trading platforms, shipping and payment companies, law enforcement, judiciary, private investigation services and digital security.

This report was carried out as a study into the legal, technical and logistical aspects of the supply of IP-infringing goods and services on online trading platforms. It reviews the existing literature and policy initiatives, the legislative framework and case-law and provides a qualitative analysis of the existing business models and the available enforcement options to respond to them.

Methodology

The business models analysis was developed through a series of structured interviews with domain experts and an independent investigation leveraging cybersecurity techniques. A series of structured interviews was carried out with experts representing brand owners, rights holders, online marketplaces, customs, courier services, payment service providers, judiciary

⁽¹⁾ Bournemouth University research team was led by Professor Maurizio Borghi and Professor Vasilis Katos, and included Dr Dimitrios Koukiadis, Dr Cagatay Yucel, Mr Panagiotis Bellonias, Mr Ioannis Chalkias and Mr Dukki Hong.

and law enforcement. Independent research was carried out using cybersecurity investigation approaches and practices in the domain of digital forensics and incident response. Such an approach allowed the identification of the so-called tactics, techniques and procedures (TTPs) used by the infringers. The TTPs were then developed in the business case descriptions and formed the basis of the analysis of the business models ⁽²⁾.

The context of the study: IP infringement in a changing internet environment

In 2019, the value of counterfeit and pirated goods imported in the EU was estimated to be **up to EUR 119 billion, or 5.8 % of all EU imports** ⁽³⁾. Internet transactions account for a major share of this value. The huge market penetration of online trading platforms makes them a sought-after channel for the sale of those goods. As highlighted by the EUIPO and Europol in 2019, the misuse of these platforms has become ‘an important source of income for criminal groups engaged in the sale of counterfeit and pirated goods’ ⁽⁴⁾.

While the sale of infringing goods on online marketplaces is not new, some **emerging trends** hamper IP enforcement efforts.

- **Multiple vendor accounts.** Organised crime groups (OCG) systematically misuse trading platforms by opening multiple accounts under different names on the same platforms and across different media.
- **Online advertising.** Vendors manipulate online advertising services by associating their illicit activity with brands, and place adverts on legitimate websites or social media platforms to direct traffic to external websites or to online marketplaces’ listings offering IP-infringing goods.
- **Social media presence.** Vendors can misuse multiple functionalities of social media platforms to reach a high number of consumers ⁽⁵⁾. For example, they can advertise counterfeit goods through posts and messages via public, private or selected group

⁽²⁾ A selection of 13 case studies is presented in Appendix to this report.

⁽³⁾ OECD/EUIPO (2021) *Global Trade in Fakes: A Worrying Threat*, OECD Publishing, Paris 2021, p. 3 and 58.

⁽⁴⁾ EUIPO/Europol (2019) *Intellectual Property Crime Threat Assessment 2019*, p. 11.

⁽⁵⁾ EUIPO (2021) *Monitoring and analysing social media in relation to IP infringement*; EUIPO (2021) *Social Media – Discussion Paper. New and existing trends in using social media for IP infringement activities and good practices to address them*, June 2021.

communication, or through live-streaming sales, and then direct customers to illegal sales, either on external platforms or on the social media e-commerce facilities.

Mapping IP infringements on online trading platforms

IP-infringing activities occurring on online marketplaces involve primarily the sale of counterfeit or pirated goods. Counterfeit and pirated goods are defined in various legal instruments and national legislations. These definitions may vary significantly. For the purpose of this study, counterfeit refers to a blatant form of trade mark infringement, where goods bear a sign that is either identical or otherwise indistinguishable from a registered trade mark. Counterfeit goods range from low-quality imitations ('fakes') to copies that are closer to the appearance of branded products ('replicas'). Piracy is the sale of goods that infringe copyright or design rights, and it applies to both physical and digital goods.

Other forms of IP infringement involve the use of signs that are confusingly similar to those of the legitimate trade mark owner, or that cause harm to a trade mark's reputation. These less blatant forms of infringement encompass both simple and very complex cases, which may require ad hoc examination. Furthermore, IP infringement may involve the sale of 'grey market' products, namely authentic products that are imported and sold without the authorisation of the IP owner.

For the purposes of the present study, the descriptions as appear in the following table are used. These descriptions may differ from the purely legal definitions in some jurisdictions, but the idea is that all the activities or goods covered violate IPRs in a way or another.


INFRINGING GOODS: EXAMPLES		
	Physical	Digital
Counterfeit	<ul style="list-style-type: none"> Fakes (low-quality imitations) Replica (same-appearance copies) 	<ul style="list-style-type: none"> Computer Aided-Design (CAD) files for 3D printing
Piracy	<ul style="list-style-type: none"> Copies of copyright content on physical support (CD, DVD) Replica design objects TPM circumvention devices TV decoder smartcards Fully-loaded set-top boxes or sticks 	<ul style="list-style-type: none"> Software copies Activation keys for software, video games or databases Hacked accounts for streaming services Computer Aided-Design (CAD) files
Confusion	<ul style="list-style-type: none"> Look-alike brand name, logo or packaging on similar goods 	<ul style="list-style-type: none"> Look-alike brand name and/or logo on similar digital goods, e.g. software, video games or apps
Brand exploitation	<ul style="list-style-type: none"> Use of famous brands on unrelated goods 	<ul style="list-style-type: none"> Use of famous brands in virtual worlds or on non-fungible tokens

Grey market	<ul style="list-style-type: none"> • Parallel imports • Overruns • Rejects 	n/a
-------------	---	-----

The IP infringers’ choice of the online platform is highly dependent on the kind of good or service that is offered for sale, the target audience and whether the infringer is an ‘occasional’ or ‘systematic’ vendor. Alongside ‘general’ wholesale and auction marketplaces there are ‘specialised’ marketplaces, such as marketplaces for handcrafted goods, independent retailers, digital goods (e.g. video games and software licences) and non-fungible tokens (NFT). An increasingly important role is played by ‘social commerce’, namely C2C and B2C sales through social media. Major social media platforms have developed their own e-commerce functionalities. A growing trend is the use of social media live-streaming facilities to market and demonstrate the product to buyers.

Systematic counterfeit sellers may also use illegal marketplaces operating in the darknet, where transactions are carried out anonymously and using cryptocurrencies.

The table below illustrates indicatively the **destination marketplaces** for each category of IP-infringing goods, in terms of likelihood that a given product is detected on a certain type of marketplace.

Marketplace type	Infringing goods					 High Low
	I. Counterfeit	II. Piracy	III. Confusion	IV. Exploitation	V. Grey-market	
Wholesale	High	Low	Low	Low	Low	
Auction/2nd hand	Low	Low	Low	Low	Low	
Handcraft / art	Low	Low	Low	Low	Low	
Social media	Low	Low	Low	Low	Low	
Labour / Services	Low	Low	Low	Low	Low	
Digital goods	Low	Low	Low	High	Low	
Darknet	High	High	Low	Low	Low	

A supply-chain approach to investigation and enforcement




The process underlying IP infringements via vendor accounts on third-party trading platforms consists of a seven-stage supply chain, from the production to the delivery of the infringing





good. It is a continuous process through a flow of information, physical items and money that involves a number of intermediaries. From an enforcement perspective, the visibility of the illegal activity is expected to decrease as we travel back along the supply chain (from right to left) and to increase as we approach the customer (shipping, at the far right).



Along the supply chain, **infringers** use a number of techniques to elude enforcement actions, such as techniques to elude detection, takedown, seizure or confiscation of goods. This informs the actions that can be taken by **enforcement actors** at each stage of the chain. These actions include investigation and law enforcement, as well as self-regulatory enforcement measures.

The table below summarises the **key enforcement actions** available to law enforcers, online platforms and IP owners at each stage of the supply chain:

ENFORCEMENT ACTIONS	
 <p>1. Raw material supply</p>	<ul style="list-style-type: none"> • Monitoring of materials: identification of hotspots where the materials are produced or originate from and maintaining a database of locations. • Custom checks: leverage historical information from countries of origin and/or known hotspots and information on custom declaration forms.
 <p>2. Production</p>	<ul style="list-style-type: none"> • Blocking the bank accounts of the producers. • Following trends and seasonal events that affect the production of goods (e.g. beginning of sport events, release of popular products).
 <p>3. Storage and inventory</p>	<ul style="list-style-type: none"> • Confiscation/seizure of goods: raiding the inventory of IP infringers and taking control of the infringing items.

 <p>4. Online offer for sale</p>	<ul style="list-style-type: none"> • Detection of the vendors of the illicit items that are hosted, unknowingly, by the trading platform. • Activation of notice-and-takedown procedures: taking down listings and vendor accounts.
 <p>5. Marketing</p>	<ul style="list-style-type: none"> • Following flags: alert indicators for a marketplace, such as offers that are: ‘too good to be true’ and/or receive an inflated amount of positive feedback in a short time. • Monitor communication: follow online communications from social media platforms, peer-to-peer communication and ad applications. • Advertisement takedowns: takedowns of ad keywords, de-listing results on search engines, removal of a product or vendor account.
 <p>6. Sales</p>	<ul style="list-style-type: none"> • Liaison with banks/financial authorities to detect and identify the entities behind financial transactions and block bank accounts. • Liaison with payment service providers to block transactions in the case of identified illicit vendors. • ‘Follow-the-money’ investigations: create a full profile of the vendors by analysing the financial transactions under investigation. • Test purchases: purchasing of IP-infringing products to collect the evidence required to build a case against an illicit vendor.
 <p>7. Shipping</p>	<ul style="list-style-type: none"> • Liaison with couriers/postal services to prevent the distribution of counterfeit products and/or identify the distributors’ addresses. • Liaison with customs to activate procedures for seizure and forfeiture of infringing goods and request data after goods are destroyed. • Seizure of goods at customs or postal services. • Monitoring routes to discover the origin of the product, distributors and vendors and how the products are transferred to the buyers. • Monitoring suspects who receive unusual amounts of unexpected orders from regular routes.

Measures, policies and strategies for effective enforcement

Tackling IP infringements on third-party trading platforms involves a number of measures, policies and tactics. These include enforcement actions and voluntary measures taken as part of the collaboration between all stakeholders involved. In the EU, the MoU, signed in 2011 and revised in 2016, provides the general framework for these voluntary measures ⁽⁶⁾. Good practices under the MoU include **proactive measures** aimed at preventing infringing activities before they occur, and **reactive measures** aimed at repressing or limiting the effect of those activities once they occur.

- **Voluntary proactive and preventive measures (PPM).** The legal basis for these measures is provided by the contractual obligations deriving from the acceptance of the Terms & Conditions (T&C) of online marketplaces, which prohibit the sale of goods that infringe third parties' rights. These measures, developed in collaboration with IP owners, include the following.
 - (i) Repeat offenders policies:** users that repeatedly violate the T&C may have their accounts suspended or disabled.
 - (ii) Identity verification:** to ensure effectiveness of policies against repeat infringements, platforms require users to provide valid identification, such as proof of identity or an address, as a condition for opening an account. Trading platforms may also require proof of a business licence and may restrict the use of certain keywords in profile names.
 - (iii) Traceability of products:** major trading platforms have introduced traceability schemes in which each item is provided with a unique code to verify its authenticity before it reaches the customer.

⁽⁶⁾ European Commission (2016) *Memorandum of understanding on the sale of counterfeit goods on the internet*, https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

- (iv) **Other technological prevention measures:** trading platforms and social media apply keyword filtering, content moderation and image recognition technology to detect infringing listings before the sale can be finalised.
- **Notice-and-takedown (NTD):** NTD procedures represent the key voluntary **reactive measures** to streamline the process of notification and removal of infringing content that is made available online. According to the good practices developed in the framework of the MoU, effective NTD procedures include the following.
 - (i) **information package for rights holders**, with detailed instructions on the information that must be submitted to activate the notification.
 - (ii) tools to manage **multiple notifications**, or ‘in-bulk’ requests, enabling rights holders to include multiple infringing listings in a single takedown request.
 - (iii) **‘trusted flaggers’ programmes**, with fast-track, privileged channels for notifications and more expeditious removal for ‘trusted’ rights holders with specialised expertise and dedicated technology for the detection and identification of infringing content.
 - (iv) **search and report tools**, to facilitate the process of searching for potentially infringing content on the platform, by means of image recognition and other technologies.
 - (v) **information for users** on the reason for the removal and the potential consequences of repeated infringements, as well as easily accessible information on the right to appeal or **counter-notice procedure** to challenge the notice of the IP owner.
- **Automated detection measures.** Detection systems based on artificial intelligence and machine learning play an increasing role in both proactive and reactive measures.

Along with the voluntary measures developed in collaboration with online marketplaces, rights holders and law enforcement agencies adopt investigative and enforcement measures that are broader in scope and span across the whole supply chain.

- **Follow-the-money investigation.** A ‘follow-the-money’ approach consists in monitoring and extracting information from the financial transactions involved in an illicit activity, with the purpose of collecting evidence and/or disrupting the activity. The approach requires cooperation between the different stakeholders involved, most importantly the payment services, and has been adopted in proceedings against IP infringers.
- **Customs and border checks.** EU customs authorities adopt streamlined procedures and condensed time frames to destroy suspected IP-infringing goods in small packages, and provide data to rights holders on request.
- **Darknet enforcement.** Given the anonymity of online providers and possible affiliates, enforcement in the darknet marketplaces presents specific challenges. Global cooperation between law enforcement authorities has led to the **shutdown** of darknet marketplaces.

Vendors prosecution

Legal actions can be taken against vendors for importation, offer for sale and distribution of IP-infringing goods. Proceedings can be brought by IP owners or by operators of online marketplaces, or jointly by both. While civil liability for IP infringement is broadly harmonised at EU level, at least as far as direct infringement is concerned, criminal liability remains the competence of national legislators. In most EU Member States, the infringement of trade marks or copyright and related rights attracts criminal sanctions when the infringer acts with *mens rea* or wilful intent and on a commercial scale. However, these criteria are not construed uniformly across Member States.

There is limited evidence of legal proceedings against individual vendors in the EU-27. The available case-law suggests that **wilful intent** can be established based on objective factors, such as a lack of express authorisation from the trade mark owner or constructive knowledge that the products are counterfeit. The criterion of ‘**commercial scale**’ is less clear, and heavily dependent on the volume of transactions. Evidence of activity such as receiving orders and shipping is crucial to determine the volume required by national jurisdictions to trigger criminal sanctions.

Injunctions against intermediaries

Together with legal actions against vendors, IP owners may seek remedies from the operators of online marketplaces and other intermediaries along the supply chain. These include, in particular, warehouses, advertising platforms, payment services and shipping services. The judicial remedies available consist of **injunctive relief**, which may be granted by the judicial authority even when the intermediary is not liable for the infringement or is exempt from liability.

Injunctions against intermediaries can aim not only at terminating existing infringements but also at preventing further infringements. This requires the implementation of some proactive monitoring duties. The scope of such monitoring duties under EU law is limited by the provisions of the e-Commerce Directive⁽⁷⁾ and can be derived from the **'double identity' approach** suggested by Advocate General Jääskinen in the 'L'Oréal v eBay' case: 'the infringing third party should be the same and that the trade mark infringed should be the same in the cases concerned'⁽⁸⁾.

The issue of jurisdiction

Due to the transnational nature of IP infringements committed through vendor accounts on third-party marketplaces, the issue of jurisdiction is a crucial aspect for effective enforcement. Claimants are generally obliged to bring a case before the courts where the defendant is **domiciled**, but it is also possible to start proceedings in the place where the **damage** occurred, where the **event** that caused the damage took place, or where the infringement was **committed**.

In relation to the allocation of jurisdiction in civil proceedings, a key factor to consider is whether the infringers targeted the EU (in the case of **pan-EU IP rights**) or a specific Member State. If the target is established, IP owners may bring proceedings before the courts of the targeted jurisdiction.

⁽⁷⁾ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Article 15(1).

⁽⁸⁾ Opinion of AG Jääskinen (12/07/2011, C-324/09, L'Oréal SA-eBay, EU:C:2010:757, § 182).

IP RIGHTS	LEGAL BASIS TO ESTABLISH JURISDICTION IN INTERNATIONAL (PAN-EU) IP DISPUTES
EU trade marks	EUTM Regulation No 2017/1001 ⁽⁹⁾ , Article 125
Community designs	Community Designs Regulation No 6/2002 ⁽¹⁰⁾ , Article 82
National IP rights (national trade marks, copyright and related rights, patents, etc.)	Brussels I Regulation (recast) ⁽¹¹⁾

Recognition and enforcement of **foreign judgments** between EU Member States is uniformly provided by the Brussels I Regulation (recast), whilst enforcing judgments in jurisdictions other than EU Member States can be extremely challenging due to the discrepancies in national laws.

Jurisdiction in **criminal law matters** is generally based on the **principle of territoriality**. Currently, there are no binding instruments under EU law to resolve conflicts of jurisdiction in criminal matters. However, the Council of Europe Cybercrime Convention 2001 ⁽¹²⁾ represents an important instrument of international law that assists in determining adjudication in criminal proceedings against online copyright infringers ⁽¹³⁾.

⁽⁹⁾ Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, OJ L 154, 16.6.2017, p. 1.

⁽¹⁰⁾ Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, as amended, OJ L 386, 29.12.2006, p. 14.

⁽¹¹⁾ Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20.12.2012, p. 1.

⁽¹²⁾ Convention on Cybercrime, European Treaty Series No 185.

⁽¹³⁾ EUIPO (2021) *International judicial cooperation in intellectual property cases*, March 2021, p. 33.

Vendor accounts study – Final report

