As counterfeit goods continue spreading widely across the Internet today and put consumers and European economies at risk, it is important to have a comprehensive understanding of the current situation, what are the existing measures to counter this issue and why those should and could be improved.

In addition to providing concrete examples on the issues our members are facing today, this note also includes our proposed solutions to tackle them as part of the proposed Digital Services Act (DSA). The Together Against Counterfeiting (TAC) Alliance advocates for a proportionate and adequate regulatory framework, which is based on already available practices, technologies and tools and effectively tackle the growing threat of online counterfeiting.

More particularly, our note covers the following issues:

I. Counterfeiting: a phenomenon going beyond online marketplaces

II. Verification of sellers’ identity already exists and should be mandatory

III. Introducing stay-down measures does not go against the ban on a general monitoring obligation

IV. Individual right holders need to be eligible to the trusted flaggers status

V. Liability exemption should not incentivize intermediaries to stop acting against any illegality on their platform

VI. Annex – Examples of counterfeit products promotion through social media

More information on our recommendations for the DSA can be found in our position paper.

ABOUT US

The Together Against Counterfeiting (TAC) Alliance brings together almost 100 companies from all industrial sectors, with the support of over 20 trade associations and NGOs. Our purpose is to raise awareness about the impact of the worrying growth of counterfeiting and push for the adoption of immediate, horizontal and ambitious legislative solutions at European level.

Learn more about the Alliance: https://tacalliance.eu/
I. COUNTERFEITING: A PHENOMENON GOING BEYOND ONLINE MARKETPLACES

Online counterfeiting is not just a mere “e-commerce” issue. While illegal goods can be found on online marketplaces, it is also significantly sold through other channels, including social media, messaging apps, etc. Rogue players also use advertising on platforms or search engines to gain visibility for their standalone websites. In fact, most counterfeit sellers today are professional criminal organisations acting at commercial scale, advertising fake products on multiple platforms, through several accounts.1

It is therefore crucial that the Digital Services Act (DSA) takes the full landscape into account and provides tools to identify sellers and remove counterfeits anywhere they occur. Otherwise counterfeit products will only move to other platforms instead of being removed from the Internet. It is even more important as the lines between different business models are blurring and we know new types of platforms will develop in the years to come. Should the new framework be limited to pure online marketplaces, consumers will continue being misled into buying fake and dangerous goods, especially on platforms such as social media where sellers can easily reach individual users (e.g. through promoted content).

PROTECTING FREEDOM OF SPEECH:

It is important to highlight that tackling illegal goods online does not go against the freedom of speech. TAC members are strongly attached to safeguarding the ability for users to share messages, posts and content, and most brands use social media platforms extensively to promote their own products. But this should not come at the expense of legality and safety. Advertising illegal and dangerous goods should be prevented and severely punished, just like it is the case for physical stores. It is not about restricting freedom of expression, but rather ensuring traders only promote and sell legal goods, in a trustworthy and safe environment for consumers.

WHAT WE RECOMMEND:

We understand there may be some concerns about the fact that social media platforms are being used both as e-commerce platforms and as platforms allowing individuals to share views and opinions. While we recommend extending the KYBC provision to all intermediaries involved in the promotion or sale of products, we strongly believe a generalised identity verification for all users should not be introduced. It is indeed important to safeguard freedom of expression. To avoid this, one suggestion could be, where it is not already the case, to require individuals and companies willing to use social media platforms to promote or sell products to create a separate, seller type of account, which would be the only one to get verified. These individuals and companies could still be free to express themselves on social media in an anonymous way through their other account. This system already exists today on platforms such as Instagram, where a user needs to get a business account to sell its products and activate the ‘buy’ button.

II. VERIFICATION OF SELLERS’ IDENTITY ALREADY EXISTS AND SHOULD BE MANDATORY

As part of Article 22 of the DSA, the TAC Alliance calls on extending the obligation to verify the identity of sellers (so-called KYBC) to all online intermediaries engaged in the promotion of a product, including those such as advertising, domain registrations and webhosting services (i.e. certain B2B services), and not just to online marketplaces or consumer-facing platforms. It is not uncommon for rogue sellers to establish domain names similar to large corporate entities and seek to fraudulently secure payments from customers of those large corporate entities. By the time the fraud is identified, those illegal traders have often vanished or are relying on privacy shields to avoid disclosure of their name and address details.

This measure should be easy to implement for intermediaries, as (1) many of them are already doing it today, (2) tools and technologies are available and (3) those obligations exist in a number of other sectors.

1 TODAY, A NUMBER OF INTERMEDIARIES ALREADY VERIFY THE IDENTITY OF SOME OF THEIR USERS THROUGH DEDICATED PROGRAMS.

While these programs are very helpful in the fight against counterfeiting, there are still a majority of online services that do not implement them. Such measures should be harmonised and mandated as part of the DSA. Below are a few examples of existing systems:

1 See Annex I for examples of counterfeits promoted through social media and messaging apps.
**EXPLANATORY NOTE ON THE DIGITAL SERVICES ACT (DSA)**

### Company Type of intermediary | KYBC system
--- | ---
**eBay** | Online marketplace
Sellers can apply for a verified account on a voluntary basis. This status provides them with benefits when operating on the platform. In Belgium for example, they need to register through the eID system. More information [here](#).

**Amazon** | Online marketplace
Documents requested vary based on the country or region. Most of the time, sellers need to provide a copy of their ID to operate on the platform. More information [here](#).

**Airbnb** | Short-term rental intermediary
Verification of identity through picture of the users’ IDs. More information [here](#).

**Google Pay** | Online payment service provider
Verification of identity with information such as name, address, date of birth, pictures of the users’ ID or proof of address. More information [here](#).

2. **THE TECHNOLOGY AND TOOLS TO VERIFY THE IDENTITY OF A SELLER ALREADY EXIST AND ARE USED IN A NUMBER OF SECTORS.**

Some platforms have developed their own tools and procedures to verify the identity of their users while others rely on services provided by third-party service providers, such as Onfido, Jumio, Ubble or IDnow.

**HOW DOES IT WORK IN PRACTICE?** There are three main types of identity verification:

- **Purely automated:** this is very fast but does not always work for technical reasons (e.g. the machine does not recognize the picture);
- **Purely manual:** this solution takes more time and there is a risk of human error;
- **Mix:** automated process with human intervention in case of doubt. This is what most existing providers are using. Even in case an agent needs to perform a manual check, verification does not take more than 5 minutes.

For example, providers such as Onfido verify the identity of individuals only, checking the authenticity of identity documents and the correspondence between the picture shown on these documents and the picture of the individual – both are required to use the service. Onfido’s system can tell whether the picture is a scan, whether it has been altered, whether the hologram seems genuine, etc. and is therefore able to determine whether the identity document is legit. Today, Onfido is capable of processing 4 600 types of documents in 195 countries. Other identity verification methods are available [here](#).

From our knowledge of the market, price for existing solutions range from EUR 1 to 10 per verification, but this may vary depending on the solutions used and the volumes processed.

3. **KYBC IS ALREADY MANDATED IN REGULATIONS COVERING OTHER SECTORS.**

- **The Anti-Money Laundering Directives** (2018/843 and 2015/849, respectively AMLD 5 and AMLD 4) require obliged entities (e.g. payment service providers, online gambling sites, etc.) to verify the identity of their customers, through ‘customer due diligence measures’ (Articles 13 and 14). AMLD 5 specifies that ‘accurate identification and verification of data and natural legal persons are essential for fighting money laundering or terrorist financing’ (recital 22). This should be done ‘on the basis of documents, data or information obtained from a reliable and independent source’, including via electronic identification means as set out in the eIDAS Regulation (910/2014).

- In France, a law adopted last year to protect victims of domestic violence (n° 2020-936 from 30 July 2020) requires porn sites to verify the age of their users and ban minors from accessing content violating the law (article 23).

In a nutshell, all of the above shows that all intermediaries, and not just online marketplaces, have all the means and resources in place to verify the identity of sellers on their website and make sure they comply with the law. This is crucial to ensure a safe and trustworthy environment in the EU.
III. INTRODUCING STAY-DOWN MEASURES DOES NOT GO AGAINST THE BAN ON A GENERAL MONITORING OBLIGATION

While TAC welcomes the introduction of a harmonised notice-and-action obligation within the DSA, this will not be enough to effectively tackle counterfeits online, in particular to prevent them from reappearing. While a notice to take down illegal listings can take weeks to be processed, those goods almost instantaneously reappear after being removed, be it through similar ads leading to the same website URL or identical content reappearing under different names (‘back-up accounts’). TAC members also found that different sellers are using the same catalogue pictures to sell the same counterfeit products.

Therefore, the DSA should include a ‘best effort’ requirement for all hosting service providers to prevent the reappearance of illegal listings. This should apply only when content has already been removed by the platform and in absence of any appeal on the validity of the notice.

HOW IT WOULD WORK IN PRACTICE AND WHAT TOOLS COULD BE USED?

This would not be any different from what the platforms which have chosen to implement proactive measures and remove illegal content before it is posted online are doing today. As an example, Amazon claims to have proactively removed 6 billion of ‘suspicious’ listings in 2019. Out of these listings, it is obvious there is a substantial number which were previously removed as being illegal. Platforms can use several factors (pictures of the product, country of the seller, seller history, listings’ details such as title, description and price, blurring of some elements of the pictures, etc.) to determine whether a listing is suspicious and how suspicious it is, or even apply simpler techniques based on the factors above in the backend and frontend code of a site, which allow to block the same seller from listing the same product offer again. The listings identified by algorithms are sometimes reviewed by agents to confirm the illicit nature of the product.

Further, an adequate Know Your Business Costumer principle should help platforms to implement those stay-down measures. The more verified information they have about the seller, the better they can prevent illegal products from reappearing.

Platforms regularly warn of the risks of over removals and over suspensions, but we have never seen any figures regarding the number of abusive notices and/or the number of sellers who appeal against removal or suspension measures they deem to be unjustified. In any event, under the current DSA proposal, sellers have the right to appeal if they believe the platform removed a content or suspended their account in a wrongful way. Sellers are therefore protected in the few cases where the removal or the suspension should not have happened.

Sellers have a right to do business online, but it does not mean they do have the right to sell illegal items. It is time to put European consumers first.

A STAY-DOWN OBLIGATION DOES NOT GO AGAINST THE BAN ON GENERAL MONITORING OBLIGATION (ARTICLE 7 OF THE DSA)

The European Court of Justice found in Eva Glawischnig-Piesczek v. Facebook Ireland Limited (C- 18/18) that EU law does not preclude a hosting provider such as Facebook from being ordered by EU courts to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal. As such, platforms may be required under EU law to proactively remove from their platform content that was previously declared illegal.

Such requirement is perfectly compatible with the absence of a general monitoring obligation, as indicated by the ECJ, in those circumstances, (…) it is legitimate (…) to require that host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information. In particular, in view of the identical content of the information concerned, [it] cannot be regarded as imposing on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31.”

However, from a practical standpoint, for a right owner to go to court each time an illegal content is removed by the platform to ensure such content stays down is not a workable solution. Collectively, right owners report millions of listings every year and neither them, nor courts would have the resources to deal with that amount of individual procedures. Therefore, it is indispensable to require platforms to implement a stay down mechanism.

WHAT WE RECOMMEND:

The terms of the above ECJ decision could be used as a basis for setting the boundaries of this stay down mechanism. Where appropriate and where there is a defined distribution channel, we would suggest it applies to identical or equivalent content, which was previously removed by the platform under a final decision (i.e. the seller has not appealed or the platform has confirmed its decision after the appeal). These identical or equivalent content would be limited in scope, as defined by the ECJ: “Provided that the monitoring of and search for the information (…) are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality (…), and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content”.

EXPLANATORY NOTE ON THE
DIGITAL SERVICES ACT (DSA)
IV. INDIVIDUAL RIGHT HOLDERS NEED TO BE ELIGIBLE TO THE TRUSTED FLAGGERS STATUS

We welcome the introduction of a provision creating a trusted flaggers mechanism in Article 19. This will be an important part of the notice and action mechanism, as they bring expertise and knowledge of illegal practices, and can build a reliable partnership with intermediaries to quickly identify illegal content across a range of different areas. However, while for many other types of illegal content, collective organisations are more appropriate, it is important in the case of illegal products that individual brands are certified as trusted flaggers.

This system already exists in practice, as a number of intermediaries implement it on a voluntary basis (e.g. Alibaba’s Good Faith/IPP+ program, Amazon Brand Registry and Project Zero, eBay Vero, Allegro Right Protection Program) and it is very often praised by both brands and platforms who use it for its efficiency. Benefits include a faster processing time for takedown requests (in 48h or less), simpler requirements for takedown requests, and both platforms and brands are able to communicate more directly with each other. However, the voluntary nature of the status and the fact that not all platforms are willing to do it causes legal uncertainty and shows the need to introduce a legal, harmonized obligation. This would create a level playing field and prevent counterfeiters from using certain platforms because of a laxer enforcement.

WHY SHOULD BRAND OWNERS BE ELIGIBLE TO THE TRUSTED FLAGGER STATUS?

Individual brand owners remain the best placed to assess the validity and infringement of their rights regarding counterfeit goods. Not only do they have expertise on the nature of the illegal content, but it is also in their interest to remove infringing products swiftly. A clarification on the eligibility of brand owners will contribute to alleviating the burden on online platforms, benefiting from the reliability of brand owner notifications and allowing them to spend more time on the less clear-cut reports of illegal content.

IT IS IMPORTANT TO OUTLINE THAT THE TRUSTED FLAGGER MECHANISM WILL NOT LEAD TO OVER-REMOVALS OR WRONG NOTICES.

The status of trusted flagger is not simply claimed; it is granted by the national Digital Services Coordinators, using certain criteria and appropriate safeguards, such as the success rate of notification. Furthermore, the status can be revoked at any point in case of abuse. Given the importance of the tool in the ex-post removal of counterfeits, brands take this responsibility very seriously. The implication of public authorities and the transparency of information on entities that have been awarded the status should also help preventing abuses.

V. LIABILITY EXEMPTION SHOULD NOT INCENTIVIZE INTERMEDIARIES TO STOP ACTING AGAINST ANY ILLEGALITY ON THEIR PLATFORM

Ahead of the publication of the DSA proposal, intermediaries had expressed concerns about whether they could rely on the Hosting Defence if they had voluntarily established an activity - technological or otherwise - to root out a particular illegality on their platforms. Their concern was that in merely establishing such an activity, it could be deemed that they had actual knowledge of illegality. This would in turn require them to act expeditiously, or else risk losing the Hosting Defence and attract direct criminal or civil liability for acts of their users.

A limited clarification by the Commission was all that was needed to overcome this concern and could have involved merely stating that intermediaries shall not be deemed to have actual knowledge of an illegality (for the purpose of relying on the Hosting Defence) by:

- the mere suspicion, development and implementation per se of an activity to identify a specific illegality; or
- the failure to identify a specific illegality in a set of content, if the activity implemented was designed to identify a different specific illegality.

Instead, the European Commission created through Article 6 an additional and overlapping defence for intermediaries. This could potentially undermine the fundamental nature of accountability set forth in the DSA. Through this new defence, intermediaries could therefore argue that almost any vague unspecific activity that they implement and pursue allegedly to counter the presence of counterfeits could give them a complete defence to any liability in respect to counterfeits hosted on their platform. Further, intermediaries could argue that as long as they are engaged in some necessary measures to comply with requirements of EU law, they are excluded from any criminal or civil liability a third party wishes to assert against them.

For example, while an intermediary may be well aware that its platform is the platform of choice for counterfeiters, it would be able to avoid liability thanks to the new defence under Article 6, provided it can show it has carried out voluntary own-initiative investigations or taken some form of necessary measure to comply with EU law - irrespective of how inadequate, ineffective or hopeless these investigations or necessary measures are. This would apply up until the intermediary is notified by a rights holder of a specific infringing link when it would be deemed to then have actual knowledge, by which time many counterfeiters may have been sold through that link.

In short, Article 6 shields platforms from any liability for systemic failure. On this basis and as elaborated in its position paper, TAC recommends to limit the unintentionally broad protection offered by Article 6 by further clarifying its scope to cover specifically voluntary measures undertaken by intermediaries in response to or to mitigate the effects of illegalities or risks as already clearly identified and catered for by Articles 26 and 27, provided these articles apply to all online platforms.
EXAMPLES OF COUNTERFEIT PRODUCTS PROMOTION THROUGH SOCIAL MEDIA

The below pictures show examples of social media accounts promoting counterfeit products. These illustrate how counterfeiters use multiple online channels to sell fake products and manage to adapt very quickly to take downs and accounts suspensions, e.g. by creating ‘back-up accounts’. Buying counterfeiting is no longer a linear process and an increasing number of intermediaries are involved, including through advertising on social media redirecting to a standalone website or a private messaging apps to finalise the sale. While this variety of support makes it more and more difficult for brand owners to spot counterfeits, it creates at the same time more opportunities for them to spot illegal activities.