SUGGESTED AMENDMENTS ON THE DIGITAL SERVICES ACT (DSA)

TOGETHER AGAINST COUNTERFEITING ALLIANCE

June 2021

>> Additions are in ***bold italic***; deletions are in ~~**bold and crossed out**~~.

TRUSTED FLAGGERS

SUGGESTED AMENDMENT

Recital 46

(….) Such trusted flagger status should only be awarded to entities, not ***natural persons***, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, ~~**that they represent collective interests**~~ and that they work in a diligent and objective manner. (…)

For intellectual property rights, ***legal entities***, organisations of industry and ***organisations*** of ~~**individuals**~~ right-holders could ***also*** be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions…

Article 19: Trusted flaggers ***[This Article should be moved into Section 2 so that it applies to all hosting providers]***

2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:

(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;

~~**(b) it represents collective interests and is independent from any online platform;**~~

(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner

JUSTIFICATION

The trusted flagger mechanism should serve to reduce the unnecessary deployment of resources on all sides while ensuring that those with the relevant expertise are called upon to authenticate content. This system is already implemented on a voluntary basis by some hosting providers today, and is very often praised for its efficiency. However, it is crucial to make this mechanism mandatory as part of the Digital Services Act, to avoid legal uncertainty and ensure a level playing field between all providers.

Just as in Regulation 608/2013 on customs enforcement of intellectual property rights, in the case of counterfeits those experts are the right holders, as they remain the best placed to assess the validity and infringement of their rights. It should thus be clarified that individual brand owners are eligible to the trusted flagger status. While some right holders do operate through collective interest bodies to notify illegal content many do not, so to require them to add the extra resource and time layer of a separate (usually paid) third party would not be beneficial, and would actively damage SMEs. A clarification on the eligibility of brand owners will also contribute to alleviating the burden on online platforms, benefitting from the reliability of brand owner notifications and allowing them to spend more time on the less clear-cut reports of illegal content.

The trusted flagger mechanism is proportionate as it will be built on accreditation by the national Digital Services Coordinators, on safeguards against potential misuse (see Article 19.6) and will result in a publicly available list. To be so trusted, the flagger must be expert and competent, and act in a timely, diligent and objective manner: these are the essential criteria.

In addition, the independence criterion in Article 19.2 (b) may cause unforeseen issues: the platform may be affiliated with the right holder in some way, or the right holder itself may sell its goods there or have an official channel on the platform. It is also possible that trusted flaggers may now or in the future develop proprietary online platforms for other services. As this would not interfere with its competence and expertise in fulfilling its trusted flagger status, the independence criterion should be deleted.

KNOW-YOUR-BUSINESS-COSTUMER

SUGGESTED AMENDMENT

Recitals:

(49) In order to contribute to a safe, trustworthy and transparent online environment for ***users*** **consumers**, as well as for other interested parties such as competing traders and holders of intellectual property rights, and to deter traders from selling products or services in violation of the applicable rules, online ***providers of intermediary services, including online platforms***, ~~**allowing consumers to conclude distance contracts with traders**~~ should ensure that such traders are ***identifiable and*** traceable. The trader should therefore be required to provide certain essential information to the ***providers of intermediary services*** ~~**online platform**~~, including for purposes of promoting messages on or offering products. That requirement should also be applicable to traders that promote messages on products or services on behalf of brands, based on underlying agreements. ***Providers of intermediary services should make the information about professional traders (such as, where applicable, trade registry numbers, etc.) publicly available in traders' advertisements or profiles***. Those ***providers of intermediary services*** ~~**online platform**~~ should store all information in a secure manner for a reasonable period of time that does not exceed ~~**what is necessary**~~ ***the applicable statutes of limitation***, so that it can be accessed, in accordance with the applicable law, including on the protection of personal data, by public authorities and private parties with a legitimate interest, including through the orders to provide information referred to in this Regulation.

(50) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, ***providers of intermediary services*** ~~**online platform covered**~~ should ***take effective steps that would reasonably be taken by a diligent operator*** ~~**reasonable efforts**~~, ***including those based on existing services and technologies***, to verify the ***accuracy and*** reliability of the information provided by the traders concerned, in particular by using freely available official online databases and online interfaces, such as national trade registers and the VAT Information Exchange System, or by requesting the traders concerned to provide trustworthy supporting documents, such as copies of identity documents, certified bank statements, company certificates and trade register certificates. They may also use other sources, available for use at a distance, which offer a similar degree of accuracy and reliability for the purpose of complying with this obligation. ~~**However, the online platform covered should not be required to engage in excessive or costly online fact-finding exercises or to carry out verifications on the spot. Nor should**~~ ***However, the requirement for such providers of intermediary services*** ~~**online platform**~~, ~~**which have**~~ to take ***the effective steps that would reasonably be taken by a diligent operator in accordance with a high industry standard of professional diligence*** ~~**made the reasonable efforts required by this Regulation**~~, ***should not*** be understood as guaranteeing the reliability of the information towards consumers or other interested parties. ***Where the trader's identification information, despite vetting by the provider of intermediary services, turns out to be incorrect, the trader's profile (and all corresponding advertisements) should be taken offline until such time as the incorrect information is rectified***. Such ***providers of intermediary services*** ~~**online platform**~~ should also design and organise their online interface in a way that enables traders to comply with their obligations under Union law. (...)

Article 2:

(e)'trader' means any natural person, or any legal person irrespective of whether privately or publicly owned, who is ~~**acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession**~~ ***promoting and/or offering products and/or services; and if a natural person then acting as a professional trader having regard to the products offered to sale or sold, frequency of activities, and commercial scale.***

Article 22: Traceability of traders ***[This Article should be moved into Section 1 so that it applies to all intermediary service providers]***

~~**1. Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information:**~~

1. ***A provider of intermediary services shall ensure that it has obtained the following information from a trader prior to its use of its services:***

(...)

2. The ***provider of intermediary services*** ~~**online platform**~~ shall, upon receiving that information, ***take appropriate steps that would reasonably be taken by a diligent operator*** ~~**make reasonable efforts**~~ to assess whether the information referred to in points (a), (d) and (e) of paragraph 1 is ***accurate***, reliable and ***up to date having regard to any publicly accessible official databases or information obtained directly from the trader***. ~~**through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents from reliable sources**~~

3. Where the ***provider of intermediary services*** ~~**online platform**~~ obtains ***indications an indication at any time prior to or after providing services to a trader*** that any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate, ***unreliable*** or incomplete, ***that provider of intermediary services*** ~~**platform**~~ shall request the trader to correct the information in so far as necessary to ensure that all information is accurate ***and***, complete ***and up to date***, without delay or within the time period set by Union and national law. Where the trader fails to correct or complete that information, ***the provider of intermediary services*** ~~**online platform**~~ shall suspend the provision of its service, ***including but not limited to advertising services made available to the trader***, to the trader until the request is complied with.

4. The ***provider of intermediary services*** ~~**online platform**~~ shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of ***the applicable statutes of limitations.*** ~~**their contractual relationship with the trader concerned. They shall subsequently delete the information.**~~

5. Without prejudice to paragraph 2, the ***provider of intermediary services*** ~~**platform**~~ shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.

6. The ***provider of intermediary services*** ~~**online platform**~~ shall make the information referred to in points (a), (d), (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.

Providers of intermediary services should make the general information about professional traders publicly available in such traders' advertisements or profiles in accordance with Article 5 of Directive 2000/31/EC of the European Parliament and of the Council.

7. The ***provider of intermediary services*** ~~**online platform**~~ shall design and organise its online interface in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.

JUSTIFICATION

Applying the Know-Your-Business-Costumer (KYBC) principle to all online intermediaries engaged in the promotion of a product, including those providing B2B services (such as advertising or domain registrars), is key to ensure sellers are identified, wherever they operate. This should be the starting point in the prevention against illegal products online. Currently, 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 online intermediaries, as:

(a) The mechanism already exists today: Many platforms have put in place such programmes, on a voluntary basis. The measure should be harmonised and mandated as part of the DSA.

(b) Tools and technologies are available: These are already being used by some online intermediaries and third-party service providers.

(c) This obligation already exists in a number of other sectors and in the offline world: For example, 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).

Additionally, the identity verification obligation should not only apply to established professional sellers, but also to any direct business costumers offering or promoting products and services on a platform at a commercial scale. This is crucial to avoid sellers registering as private individuals to circumvent verification measures.

Finally, we believe this provision should also include a process to ensure the information collected and verified by the intermediary is accurate, reliable and up-to-date if and when necessary, and require the intermediary to keep the verified information for as long as necessary under applicable statutes of limitations. We have suggested amendments to the relevant paragraphs accordingly.

INCLUSION OF A STAY DOWN OBLIGATION

SUGGESTED AMENDMENT

Recital 28

Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case, ***including content that has already been removed or to which access has already been disabled, or content of which providers of intermediary services have knowledge or awareness***, and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.

Article 14: Notice and action mechanisms

Paragraph 7 (new)

7. Where the provider of hosting services has previously removed, delisted or disabled access to illegal content, it shall implement all reasonable and proportionate measures to ensure that the illegal content subject to the removal, delisting or disablement, shall not, subject to (8), be made available through its services.

8. The removal, delisting or disablement prescribed by Article 14 (7) may be overcome by the following: a successful appeal procedure; or, a court order issued by a court of competent jurisdiction in a Member State, the General Court or the Court of Justice of the European Union.

JUSTIFICATION

While harmonised notice and action procedures will be helpful in making the process more efficient, it should be complemented by a "best effort" requirement for all hosting providers to prevent the reappearance of illegal content already taken down by the platform. Currently, a takedown can take weeks to be processed. Most importantly, once taken down, illegal content including illegal goods almost instantaneously reappear, often on the same platforms, be it through similar ads leading to the same website URL or identical content reappearing under different names ("back-up accounts"). Introducing a stay down obligation would address these concerns and not go against the ban on general monitoring obligation: it would only apply when content has already been removed by the platform in absence of any appeal, and be based on a "best effort" requirement for all hosting service providers to avoid overburdening small actors. This obligation is necessary to create effective notice and action mechanisms, and it would only codify today's jurisprudence of the CJEU (Case C-18/18 (Eva Glawischnig-Piesczek v Facebook Ireland Limited)).

INTERMEDIARIES' VOLUNTARY INITIATIVES

SUGGESTED AMENDMENT

Article 6 : Voluntary own-initiative investigations and legal compliance

Delete

JUSTIFICATION

Article 6 creates an additional and overlapping defence for intermediaries further to the "hosting defence" already provided by Article 5. Through this new defence, intermediaries could argue that almost any vague unspecific activity that they implement and pursue allegedly to counter the presence of, for example, 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. We therefore suggest deleting article 6, as we have not seen any sufficient and objective justification that this new protection is needed.

CONSUMER INFORMATION

SUGGESTED AMENDMENT

Article 14: Notice and action mechanisms

Paragraph 9 (new)

9. Providers of hosting services shall without undue delay, inform consumers having purchased illegal products between the moment they have been uploaded on the provider's website and the moment the listing has been taken down by the platform following a valid notice.

JUSTIFICATION

Fighting counterfeiting is a matter of consumer protection, and the EU and national authorities should improve information to consumers on their online purchases. That is particularly true in light of the increasing percentage of consumers who are tricked into buying counterfeit products and fall prey to online scams.

The Regulation should therefore include an additional notification requirement for online platforms to inform consumers who have bought illegal products such as counterfeit products between the moment they have been uploaded on the platform's website and the moment the listing has been taken down by the platform, following a valid notice from a brand owner or enforcement authority. Such an obligation should be seen as an essential component of consumer protection and a logical follow-up to a notice and action procedure.

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/