AIM
EUROPEAN BRANDS ASSOCIATION

Avenue de Gaulois 9
B-1040 Brussels
Belgium
Tel: +32 2 736 0305
TR: 107438267901
www.aim.be

POSITION PAPER

Comments on the draft Digital Services Act

5th March 2021

AIM, the European Brands Association, is grateful to the European Commission for its considered draft Digital Services Act ("DSA"), which should help to ensure that the European Union remains at the vanguard of protecting online consumer and business trust, safeguarding both rights and citizens.

The digital transformation has indeed brought many benefits but also risks and challenges in recent years, including the exponential growth in online offers of counterfeit and other illegal goods. Protecting consumers and providing them with trusted, safe and innovative goods is in the DNA of every branded goods manufacturer and should also be embedded in any intermediary and retailer, on- or offline. As such, the DSA is the opportunity to ensure that:

- European consumers and businesses are **protected equally on- and offline** against rogue traders and (illegal) unfair competition;
- Online service providers play their part in maintaining a clean and fair online ecosystem, in particular by exercising appropriate control over those parts of the value chain that are within their purview. This includes:
    - reasonable due diligence to know with whom they enter business relationships ("**Know Your Business Customer**");
    - legal obligations to employ **proactive, including technical, measures to prevent offers for illegal goods** appearing on their sites. Voluntary measures are insufficient to tackle counterfeiting online;
    - rapidly (and permanently) **removing such offers** when they are identified and **prohibiting repeat offenders** from accessing their services;
- **Information about infringements** is provided on a proactive basis to law enforcement, including customs and market surveillance, authorities allowing for effective risk analysis and targeting. Consumers also deserve such transparency, especially being informed when they have previously purchased a product that has since been removed as it was illegal.
- Rapid and efficient **notice and action procedures** are established, including the treatment of brand holders as "trusted flaggers", given that they alone can authenticate their products.

We trust that the detail in the following pages is of use and look forward to working with the policy makers going forward on this important file.

1. Overview

A horizontal instrument to prevent legal and practical fragmentation in the single market is to be welcomed, provided that sectoral realities are addressed. Starting from the agreed baseline of **that which is illegal offline is also illegal online**[1], we must be sure not to confuse two highly important but very separate issues: illegal goods and the freedom of expression. Preventive measures to stop illegal (including counterfeit, non-compliant and sub-standard) goods from being offered to consumers are very different from the monitoring of opinion or user-generated content: on the contrary, they are obvious due diligence and consumer protection measures that all offline retailers regard as standard business practice. There is no good reason why consumers should enjoy less protection in the online environment. Similarly, removing or disabling access to offers of illegal goods has no relation to "the observance of the principle of freedom of expression" (Recital 22). Although in its impact assessment[2] the European Commission states that the sale of products online can affect the freedom of expression in certain cases, we feel that this is a rather theoretical concept. In our view, an illegal product is an illegal product, regardless of its nature, and should be removed.

The promotion of new digital services should not be at the expense of either consumer protection or existing businesses that also rely upon the safe, predictable and trusted online environment to reach their markets. **Any business, whatever its size and sector, must abide by both EU and national law.** Fair trading practices, including appropriate due diligence, should be regarded as a basic cost of doing business by all. Everyone involved in the chain between the counterfeiter and the consumer should play their appropriate part in maintaining a clean and trusted online environment: as the platforms are the only parties that have visibility over the entire chain, they should systematically provide relevant information, especially to law enforcement. Overall, while we appreciate that not all platforms have the same capacity or reach, we should guard against giving any impression that smaller platforms do not have to operate within both this and other laws, including our consumer protection and intellectual property frameworks.

We welcome the clarification that **all providers of intermediary services are in scope** irrespective of their place of establishment or residence, insofar as they provide services in the Union (Article 1). European consumers, businesses and Law Enforcement Authorities should no longer be expected to deal with the tsunami of illegal goods arriving in the EU from rogue traders established in third countries who deliberately evade our laws.

2. Liability and due diligence

We welcome the confirmation in Article 5 that a service provider with **actual knowledge** does not benefit from the exemption from liability, but clarification on what an active role and knowledge actually are is needed to provide legal certainty. In particular with regard to Article 5(3) (c.f. Article 3(1)(c)), most platforms do modify the listings for goods, some grouping them within specific and proprietary category indicators, some mentioning the brand holder as the source (even when the seller has no connection whatsoever with that brand holder), some mandating the use of stock (genuine) images (effectively preventing any differentiation between genuine and counterfeit goods) and some even suggesting selling prices. Would the liability exemption apply when platforms offer paid-for services enabling sellers to promote their content? Would platforms' algorithms that rank offers according to non-public criteria qualify as "selecting or modifying the information"?

A clear definition of "active" based on CJEU jurisprudence[3] should be provided. We would also suggest that a service provider that does not verify the identity of its users in accordance with Article 22 should not benefit

[1] Wording used several time by the Commission, including by Executive Vice-President Vestager

[2] *229. Content moderation decisions by private companies, be it in assessing legality or compliance with their own terms of reference, can impede freedom of expression, in terms of freedom to share information and to hold opinions, but also in terms of freedom for citizens to receive information. While the sale of goods might be seen as less related to freedom of expression, speech can also be reflected in goods, such as books, clothing items or symbols, and restrictive measures on the sale of such artefacts can affect freedom of expression. (…)*

[3] For example, L'Oréal v eBay International, C324-09, judgment of 12 July 2011

from the liability exemption. Further, Article 5(3) should be amended to include reference to, for example, liability under product safety and intellectual property laws.

We are disappointed that the Commission chose not to render **proactive and preventive checks for illegal goods** mandatory; again in comparison to the offline environment where retailers are obliged to carry and display legal goods, it is unfortunate that online service providers are assumed to owe a lesser duty of care to consumers. We welcome the clarification in Article 6 that there is no good reason for platforms not to proactively carry out their own investigations to find and remove illegal goods, ending any spurious claims that by doing so the platforms were concerned that they would lose the benefit of the liability exemption. However, the wording in Recital 25 as to carrying out such "voluntary" activities "in good faith and in a diligent manner" again reinforces the distinction between off- and online business norms; brick and mortar retailers do not "voluntarily" employ best efforts to carry legal stock and "comply with the requirements of EU law". This provision must not be read as providing for a blanket exemption from any liability: platforms are paid for their services, many also for sales and fulfilment, thus it is important for them to play their part in maintaining a clean and legal value chain.

We strongly believe that the DSA should include a requirement for all hosting service providers to put in place a **"stay down" mechanism**, which would require them to ensure that an illegal product, which they have agreed to take down, does not reappear on their platform. Once identified as illegal, by proactive measures or following a judicial decision or third party notice, that listing and identical or equivalent postings/content should be permanently removed and remain inaccessible thereafter. Unfortunately, such products reappear all too rapidly today, forcing right holders to find and notify the same offers over and over again – a waste of resources on all sides – while leaving consumers exposed to the risks of buying illegal goods. From a practical perspective, most platforms are already equipped with tools (mainly based on key words and image recognition technologies) allowing for the easy identification of products which have been taken down previously. From a legal perspective, this stay down mechanism, which is specific, limited and proportionate, would be compatible with the Commission's choice against a general monitoring obligation.

Verifying the identity of the seller using a platform's services to offer goods to consumers, or using best efforts (including technical means) to prevent counterfeit and other illegal goods from appearing on the platform, is not a "general monitoring obligation" (Recital 28, Article 7). On the contrary, it is a targeted, appropriate business measure that is better seen as a "due diligence obligation" within Recitals 34 and 35. We are pleased to see the obligation on platforms **to collect and verify certain information from traders** - just as it would be unthinkable for physical retailers to enter into business contracts for goods or services without any verification of the identity of the other party, this should not be the norm online. However, we do not see why this should be limited to platforms and traders alone (Recitals 49 and 50, Article 22). Any digital intermediaries (in business to business relations), including domain name registrars, web hosting providers, marketplaces and online advertisers, should employ effective "Know Your Business Customer" verification measures. Simply stated: an entity from which any online service provider is taking money and which is in turn taking money from consumers should be identifiable. Once again this does not affect freedom of speech or general online anonymity: if someone buys something from you they have a right to know who you are and who to contact in case of a problem.

Certain information should also be made available to consumers so that they know with whom they are entering a distance agreement and to whom they are giving their personal data and/or payment details: this should already be the case under Article 5 of Directive 2000/31 but this obligation is often overlooked or ignored. Providing no, or manifestly incorrect, information should be a reason to take down related listings (upon third party notice or proactively) until and unless it is rectified. There should also be appropriate safeguards to prevent or deal with business sellers misrepresenting themselves as private individuals, as is already provided in the Platform-to-Business Regulation.

While clearly all operators must follow the law, as stipulated in Article 9, the (reactive) **provision of information** upon request only is a missed opportunity. According to the EUIPO and OECD[4], some 6.8% of all imports into the EU are counterfeit: if law enforcement is to be able to address this flood of illegal goods they need access to data to develop robust risk assessment techniques to be able to target the correct consignments. Regular provision of such data, with full respect of applicable laws, would be of huge benefit, allowing our stretched law enforcement colleagues to maximise their efforts and minimising the need for lengthy, repetitive and unnecessary communication procedures for all. As currently drafted Article 9 will unfortunately have little practical effect against the volume of counterfeits imported into the EU, and will again shift the responsibility away from the party facilitating that trade to the public sector and its (limited) resources.

Right holders welcome the obligation for user-friendly **notice and action mechanisms** detailed in Article 14, especially the ability to include several listings in one notice, although we would also appreciate clarity that notices can be filed in relation to all listings by one seller. We would also welcome clarity that the "explanation of the reasons" as required by para. 2(a) should not be unnecessarily broad; for example, "trade mark infringement", with reference to the trade mark registration number, should suffice. However an important step in the procedure has been omitted: platforms should have an obligation to **inform consumers** when a product they have previously bought has since been removed from sale as illegal/counterfeit. Consumers should have the right to know if the product they have purchased is not genuine, and more informed consumers are better equipped to resist future rogue trading attempts. The health and safety of consumers is of paramount concern and it is difficult to understand why more care is taken to inform rogue traders that the listing has been taken down than the consumers who have been the unwitting victims thereof.

While we fully support **transparency measures** that would oblige the platform to inform the seller of the reasoning for the take down, and provide a dispute mechanism if appropriate, again this is not akin to human opinion as to harmful content: counterfeits are illegal. As clearly stated in Recital 12, "the sale of non-compliant or counterfeit products" is an illegal activity. While the right holder is (correctly) obliged to provide evidence as to why the listing is illegal in its notice, currently many platforms do not require the same level of (or indeed, any) proof from sellers alleging the contrary: given that they are the only party who has access to the actual goods this unequal treatment may be open to abuse. If there is a dispute between a right holder and an online trader (including an appeal) as to the legality of the product, the burden of proving that the item is genuine should lie with the seller.

We would also like to stress that right holders cannot "attempt to resolve conflicts relating to [illegal] content without involving" intermediaries (Recital 26). Right holders do not know the account holder, seller or logistical distribution details: only the platforms have that visibility. Absent cooperation from the platforms both right holders and Law Enforcement Authorities are obliged to conduct resource-intensive investigation and ex post enforcement to safeguard the market and consumers. We would therefore appreciate an amendment to Article 22(5) to clarify that **the verified contact details and identity of the trader should also be provided to Law Enforcement Agencies and right holders** to allow them to further investigate and eventually pursue legal action. Further, we must guard against Recital 26 being interpreted as mandating contact with the seller before any court order can be sought, as in the case of counterfeit goods this is quite often simply impossible.

As drafted Article 22 requires the online platform to delete the information once the relationship with the trader is terminated: this would make it impossible for consumers or right holders to bring action against an identified seller once that account has been terminated. Instead, Article 22 should require the intermediary to update the information that it has collected and verified if and when necessary and to keep that verified information for as long as called for under applicable statutes of limitations.

We support the concept of **trusted flaggers**, but recommend that this be amended to specifically include individual intellectual property right holders and not only representative/collective interest organisations (Recital 46, Article 19). Brand holders themselves are best placed to confirm the authenticity of their goods and

[4] EUIPO/OECD study "Trends in Trade in Counterfeit and Pirated Goods" , March 2019

so can assist in taking down counterfeit products faster with less bureaucratic burden; the extra layer of requiring an intermediary representative would only add complexity and risk excluding smaller companies that cannot afford to outsource such online monitoring to paid third party service providers. Also, if trusted flagger status is awarded to a service provider that has multiple clients, losing such status should be linked to each individual client so that other clients are not unfairly affected. Finally, while we support trusted flaggers' notices being given priority treatment, we would appreciate clarity that this includes both more rapid consideration and action; such notices should result in automated take down as there will be no need for further verifications.

Strong provisions against **repeat offenders** are sorely needed. We would dispute the idea that spurious right holder notices are just as prevalent as repeat rogue sellers as is indicated by the tone of Recital 47 and Article 20: while of course there should be safeguards to prevent any misuse of the notification system, this should not be conflated with repeat infringers who deliberately and wilfully defraud and damage European consumers. We are also disappointed to see that repeat offenders may only be suspended temporarily from the platform with no possibility of **permanent exclusion**: this runs contra both to fair trading practices and consumer protection goals. Those who deliberately and repeatedly infringe the law should not be permitted to continue so to do with impunity.

Further, it is of concern to see that someone who "frequently provides manifestly illegal content" is to be pre-warned (again) that they are to be, at best temporarily, suspended. A frequent repeat offender surely does not merit such protection. Right holders expend huge resources in trying to clean platforms of rogue sellers who abuse their services in repeatedly offering illegal goods to consumers: to allow them to return to their nefarious practices after only a "reasonable" period seems both manifestly illogical and patently dangerous. This also does nothing to prevent such sellers jumping between different accounts and sites. We also stress that only the platforms know if those sellers have registered several related accounts and offer counterfeits of several brands, thus maximising their illegal profits and mitigating their own risks. As such, we suggest clarification that Article 20 will apply on a seller and not just account level. As repeat infringers frequently jump between sites, we also recommend that data on illegal goods are shared across platforms.

Platforms must be transparent with regards to their **repeat offender policies**. Given the large amount of discretion enjoyed by platforms, the Regulation, or subsequent Guidelines, should specify the minimum information that must be included in platforms' terms and conditions and repeat offender policies (Art 20(4)) as well as the type of information to be considered as manifestly illegal content (Recital 47). Operating under multiple accounts or uploading images with blurred logos should be considered "misuse" and lead to permanent restriction of the seller.

3. Very large online platforms

In defining "very large online platforms" we recommend that the wording of Article 25(1) be clarified, so that the "active recipients" figure includes those who access the platform and not only those who make a purchase; absent such wording we are concerned that figures based on monthly sales would artificially reduce the number of active users.

With regard to the very large online platforms' risk assessment duties laid down in Article 26, the **systemic risk of the sale of counterfeit and other illegal goods** is clearly within para. 1(a), but we are disappointed that no reference is made to the protection of intellectual property in Article 17 of the Charter on Fundamental Rights in para 1(b): this should also be explicitly referenced so as to prevent any misinterpretation that would suggest that it is somehow a "lesser" fundamental right.

While we of course support the mitigation steps laid out in Article 27, again we stress that all platforms, regardless of their size, should mirror that which is expected in the offline world and employ basic due diligence measures to ensure both the legality of the goods that they make available and the protection of the consumers to whom they are sold. There should be a **baseline of such proactive measures applied by all platforms**, of any size, who facilitate the sale of goods to European consumers. The offer of prohibited goods such as firearms,

drugs or CITES articles would not be permitted even if the platform were relatively small; some measures must apply across the board.

Relying on the parties who have no visibility over, or participation in, the supply chain from seller to consumer not only shifts the burden of consumer protection from the platform to right holders and law enforcement, it also by default relies on the parties with the least knowledge and information to take action. Further, the best practices identified by the Board and potential Commission Guidelines **should be applied, as appropriate, to all online players**. This is especially important for start-ups so that they can build these business practices into their models ab initio rather than attempting to retrofit their operations when they reach critical size.

All AIM members strongly believe in the necessity of protecting personal data as laid down in the GDPR. However, we stress that the **GDPR does not apply to commercial data and neither was it ever intended to provide a shield for those carrying out illegal activities**. As we have pointed out several times, neither right holders nor law enforcement authorities know the sellers, logistics providers or distribution routes employed by rogue sellers but the platforms do, especially where they also provide their own fulfilment centres and transporters. If we are ever to stem the tide of counterfeit and other illegal goods online it is imperative that platforms share data about the entities behind these sales with both law enforcement and right holders, under the appropriate safeguards and within legal parameters. Article 31 must be amended accordingly. While we understand the importance of researchers being able to access such data, with due respect they do not have the ability to fight against this illegal trade.

4. Due diligence

We are very pleased to see reference to the development of **standardised electronic notices** in Article 34, but would urge caution with the idea that once developed they should be voluntary. An obligatory minimum level of harmonisation would be of benefit to all in the online space and allow the development of an agreed nomenclature so that databases (including eventually the Enforcement Database) can be interoperable.

If codes of conduct are to be drawn up in the intellectual property and consumer protection fields, we believe that a multi-stakeholder approach would be the best way to deliver practical and effective results. We therefore suggest that Article 35(2) be amended to specifically include both consumer organisations and right holders.

5. Implementation, cooperation, sanctions and enforcement

With regards to the enforcement provisions, we are again surprised that there is no possibility for the **permanent removal of the illegal content or permanent suspension of the rogue trader** under Article 41 and would strongly advocate that such stay down obligations be enacted.

Under Article 42, we would suggest that in addition to the 6% fine, providers of intermediary services that infringe this Regulation should also **lose the liability exemption**. This is the logical corollary for providing that such exemptions are conditional upon fulfilling certain obligations.

We would appreciate clarification in the text that right holders, consumer organisations and law enforcement authorities may bring **complaints under Article 43**. We would also suggest that industry and consumer associations be considered as regular interlocutors for the Board under Article 48(5).

For further information please contact:
Amaury.Libbrecht@aim.be
Marie.Pattullo@aim.be