8 September 2020

Ref: Open public consultation on the Digital Services Act package.
https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package

Introduction

The Transnational Alliance to Combat Illicit Trade (TRACIT) is an independent, private sector initiative to mitigate the economic and social damages of illicit trade by strengthening government enforcement mechanisms and mobilizing businesses across industry sectors most impacted by illicit trade. Our member companies are multi-national corporations, all of which operate extensively in European markets.

We appreciate the opportunity to provide our views to the open public consultation on the Digital Services Act package. We agree that this is an important evidence-gathering exercise, and we are hopeful that you find value in our recommendations.

In our view, there is an urgent need to modernize the outdated legal framework governing eCommerce, and the DSA is a powerful opportunity to improve transparency and accountability online.

Consumers are entitled to an online browsing and shopping experience that is safe and secure from fraud. Online platforms connecting people and those that profit from commerce over their websites should be responsible, comply with the law and recognize the ethical/moral responsibility to assure consumers a safe and trusted environment.

The same consumer protections that exist for the brick-and-mortar stores should be applied to online marketplaces to ensure only legitimate and compliant products and services are sold on their sites. Therefore, we recommend that the DSA include provisions that require ecommerce platforms – both commercial and social – to step up and take responsibility for maintaining safe and legitimate product sales.

Recommendations for consideration

1. Improve verification requirements of eCommerce platform suppliers

Consumers deserve to know basic identifying information about who is selling the products they use, and they should have a way to contact a seller in case a consumer product appears to be stolen, counterfeit or dangerous. Brick-and-mortar retailers have clearly identifiable

names and business addresses and consumers are readily able to approach those retailers to raise concerns. However, online marketplaces do not always require third party sellers on their platforms to provide similar transparency for consumers.

To more effectively stop counterfeit/infringing product listings before they go live, strengthen effectiveness of Notice-and-Takedown (NTD) programs and address of recidivism and the endless cycle of takedown requests, we suggest that regulations require platforms to:

- Verify the seller's identity, location, and contact information.
- Require the seller to verify and attest that its goods are not illegal in any shape or form.
- Condition the seller's use of the platform on agreeing not to sell illegal products and consenting to being sued in court of platform jurisdiction.
- Display the seller's identity, location, and contact information; where the goods are made; and from where the goods will be shipped.
- Require sellers to use images that accurately depict the actual goods offered for sale and that the seller owns or has permission to use.
- Use technology to screen for illegal products before a seller's goods appear on the platform.
- Implement a timely takedown process for removing listings for counterfeit goods.
- Terminate sellers that have listed or sold counterfeit goods three times.
- Screen sellers to prevent terminated sellers from rejoining or remaining on the platform under a different alias or storefront.
- Share an infringing seller's information with law enforcement and, upon request, the owner of the registered trademark

Where a personal account becomes a business account, additional information should be required, as the relationship between user and platform has changed. Information required could include contact information listing name and street address, as well as banking details or other identity checks and verification practices. This information should be vetted for accuracy on sign-up, as well as at reasonable, regular intervals, or where an account has been flagged as high risk. If a platform allows users to have multiple accounts, these should be clearly linked so that if one account is found to be engaging in the selling of counterfeits, the other accounts can be reviewed.

2. Publishing information on ecommerce suppliers

To ensure that there is more transparency and accountability online and to facilitate the ability of consumers to more effectively make choices that protect them from fraud, we recommend that DSA require platforms to:

- Provide to the public the full name and contact information of the vendor.

- Provide to the public information about whether the listed vendor is the manufacturer, importer, reseller and/or retailer of the product.
- Notify the consumer prior to purchase of any given product if the vendor supplying a product is different from the vendor named on the product listing page.

3. Establish a new benchmark for contributory trademark liability for selling counterfeit goods on behalf of third-party sellers

Safe harbor from contributory infringement should be reserved for platforms that follow a set of measures [to be] delineated by the DSA. We therefore recommend that DSA introduce clear provisions holding online marketplaces liable when their platforms facilitate counterfeiting.

EU laws should introduce liability provisions that make clear how internet actors are liable when their platforms help users engage in unlawful conduct relative to specific categories of products that are highly regulated, and further accounts for the responsibilities of online marketplaces that take possession of and stock counterfeit products; facilitate payments for those products; package, ship, and handle administration for selling counterfeit products; and earn profit from the sale of counterfeit products.

4. Put in place post-discovery requirements

While we prefer measures and regulations that pro-actively prevent counterfeiters from exploiting vulnerabilities in eCommerce platforms, once a counterfeit has been discovered we believe that consumer protection measures should be put in place to guard against repeat activity. These post-discovery measures would require platforms to:

- Implement a “three strike” or similar system that permanently bans bad actors from conducting illicit business on their platforms. Such bans should be extended to such bad actors who would register on the same platform under different aliases or be able to jump to other platforms.
- Require platforms to inform consumers that have bought a product from a listing that is subsequently taken down for being counterfeit.
- Notify law enforcement of sellers (potentially “high volume sellers”) who have been permanently removed from the platform following multiple and successful notice and takedown complaints.
- Notify right holders who have products listed by sellers who have had other listing successfully removed due to a successful notice and takedown compliant by another right holder.
- Require destruction (sustainably) of goods held in warehouses / fulfilment centers operated by an ecommerce platform following the removal of a corresponding listing due to a successful notice and takedown compliant, or delivery up to law enforcement where that seller has been reported to law enforcement.

5. Address fraudulent advertising online

Fraudulent advertising is rapidly emerging as a new risk to consumers shopping online – presenting a new gateway to the massive world of counterfeiting and piracy available throughout the Internet. An extensive report on this issue has been published by the Transnational Alliance to Combat Illicit Trade (TRACIT) and the American Apparel and Footwear Association (AAFA).

The problem with fraudulent advertising is that the advertisements are of such professional quality that they easily deceive consumers, and when they are directed to a site from an advert on well-known and familiar website or app, they are more likely to regard the destination site as legitimate and trustworthy than if they had found it via a search engine or accidentally. This places extra responsibility on sites that host and provide optimisation for advertising or receive payment for doing so.

The lack of sufficient policies and procedures to verify users' true identity and to conduct the necessary vetting and due diligence during the onboarding process is a system weakness across multiple Internet-based platforms for social networking and shopping.

- *Establish enhanced "Know Your Business Customer" protocols.* It is imperative that websites and social media platforms know who they are working with when accepting paid advertising. By gathering and verifying an appropriate amount of data on who is utilising their advertising services, they will be better able to proactively identify bad actors, avoid recidivist infringing activity from previously removed accounts, provide information to law enforcement. Data collected could include individual/business name and street address (proven with recognised ID), phone number, email, and a proof of business registration.
- *Require rigorous review of advertisement prior to publication.* To ensure that their terms of service are being adhered to, and that no innocent consumers are being defrauded by fraudulent, scam advertising, all adverts published on a site or platform should be reviewed for infringing content, both algorithmically and where high risk has been flagged, manually. In addition, the external sites to which such adverts link should also be reviewed to determine their legality and authenticity.
- *Enforce effective reactive measures against fraudulent advertisers.* To act as an effective deterrent to illegal advertising activities, sites and platforms must establish strong, effective, and enforced measures against advertisers who have been found to infringe their terms of service. This should go beyond termination of the advertising agreement and include removal of the infringer's account and blocking the advertiser from the website or platform.
- *Ensure consumers and rights holders can report and share information about fraudulent advertisers.* Until such time that advertising on websites and social media platforms have a robust system to prevent bad actors, there needs to be avenues for consumers and rights holders to share information that can be used to dismantle criminal networks currently operating on their platforms. Currently, while adverts can

be reported and removed, platforms must be willing to receive trend and data-sharing information that could assist them in blocking bad actors accessing advertising.

- *Require post-discovery measures.* Consumers who have clicked on an advertisement which has subsequently been removed due to a successful notice and takedown compliant (Facebook has implemented this as part of the counterfeit PPE measures) should be notified. Additionally, a "report" functionality for consumers should be made available to assist consumers to report incidences where they suspect an advert to be counterfeit. Right holders can then opt-in to receive these notifications (as above - WeChat has implemented this functionality).

6. Require greater automation to manage the volume of potentially counterfeit listings

As the volume of goods sold on online platforms is vast and growing, it is impossible for platforms to keep up with a manual review of all listings; therefore, automated risk management tools are key to flag high-risk listings. Manual review is still important for these flagged listings to ensure they have not been erroneously caught in the filter, but these automated tools should keep the volume of listings needing review to a manageable level.

Filters should track brand names with keywords such as "replica" or "knock-off", as well as copyrighted images or images frequently used to sell fakes, items listed in categories not manufactured by the listed brand, or items sold from countries where the brand has no business presence. Unusual traffic or behaviour on an account should also be monitored, as it could be a sign the account has been compromised or changed ownership.

Where possible, machine learning could be employed to continuously improve these automated systems – by feeding in data on confirmed counterfeit listings, the algorithms will be better able to detect similar listings in future.

7. Improve contributions to assist law enforcement

Greater cooperation between platforms and law enforcement in prosecuting criminals who sell counterfeits and perpetrate fraud on the platforms.

Cooperation with law enforcement will help to keep criminals off platforms; it will ensure that the appropriate action is taken against prolific infringers abusing platforms for their own gain, and set an example as a public deterrent to other potential sellers of counterfeits. Platforms should support law enforcement efforts to tackle counterfeiters online and offline, and proactively reach out to the relevant law enforcement authorities when a seller is found to be consistently dealing in a significant volume of counterfeits.