eCommerce and Fraudulent Advertising

TRACIT Principles & Positions

Introduction

The Transnational Alliance to Combat Illicit Trade (TRACIT) is an independent, private sector trade association focused solely on mitigating 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 with a vested interest in protecting their brands and consumers.

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.

Similar—and in some cases more stringent—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 these sites. Therefore, we advocate for legislated consumer protections to resolve conflicting sets of obligations for eCommerce platforms – both commercial and social – and better enable them to step up and take responsibility for maintaining safe and legitimate product sales.

We start from the premise that our joint goal should be to stop fake, pirated and illicit goods from being offered in the first place.

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 potentially unsafe. 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 are offered online, to strengthen effectiveness of Notice-and-Takedown (NTD) programs and to address recidivism and the endless cycle of takedown requests, we recommend requiring online platforms to:

1. Prominently publish a list of what can and cannot be sold on the eCommerce marketplace for sellers and buyers.
2. Condition the seller's use of the platform on agreeing not to sell illegal products and consenting to being sued in a court.
3. For business accounts, require and verify the seller's identity, physical address, contact information, banking details and other identity checks (e.g., business license, chamber of commerce registration ID), along with where the goods are made and from where the goods will be shipped.
    a. If a platform allows users to have multiple accounts, these should be linked so that if one account is found to be selling counterfeits, the other accounts can be readily reviewed.
    b. Identity verification should be refreshed for accuracy at regular intervals, and when an account has been flagged as high risk.
    c. Require the seller to verify and attest when its goods are regulated in destination markets and that they are in compliance with destination market regulations and requirements.
    d. Require the seller to attest they are authorized to use the images on its product listing sites, and they accurately depict the goods sold.
4. Display the seller's identity, location, and contact information.
5. Use technology to actively screen for illegal products or products prohibited by the eCommerce market's terms of use before a seller's goods appear on the platform.
6. Implement a speedy takedown process for removing listings for counterfeit goods.

2. Establish a registration and licensing program

- Require an **e-business license**, according to where goods are sold, for sellers engaging in intra- and inter-state commerce.
- Establish a **central registry** (ideally, managed by a highly secure, disinterested party or industry group) to maintain the licenses.
- Establish a Foreign Supplier Verification Program (FSVP), such as that mandated by the U.S. Food Safety Modernization Act (FSMA), including requirements for documentation, verification, indemnity and recourse.
- Violation of terms of service would result in suspension or revocation of licenses.

3. Publish 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 platforms be required 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.

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

Online marketplaces currently have limited enforceable incentives to police, monitor or otherwise vet their sellers and the products that are being offered on their platforms, in compliance with their terms of service. Brand owners and consumers are left to rely on a range of differing, self-imposed and voluntary processes and procedures offered but not always enforced by marketplaces, many of which have had limited success in halting on-line counterfeiters and infringers.

If further progress is to be made identifying and taking down counterfeits and otherwise illicit product offerings, then laws clarifying the responsibility of platforms for proactive and timely action are essential, along with further cooperation between brand owners and platforms. In this regard, secondary infringement liability is a helpful tool, but it has its limitations. On-line marketplaces should have some legal obligations to make their sites safer for consumers and provide more transparency as to the identity of their sellers.

Evidence of the need to clarify responsiblities and associated liability can be found in the U.S. Copyright Office report on Section 512 of the Digital Milleniuum Copyright Act (DMCA) (1998) in May 2020. The Report explains that DMCA safe harbors were designed to provide "strong incentives for Service Providers and copyright owners to cooperate to detect and deal with copyright infringement that takes place in the online networked environment." The Report concludes that there has been enormous change in the Internet since 1998 and that the safe harbor is unbalanced. Congress intended to incentivize cooperation between online service providers and rightsholders, but cooperation is limited and voluntary, and cannot be the only answer.

Safe harbor from contributory infringement should be reserved for platforms that follow a set of measures. Online marketplaces should be held liable when their platforms facilitate counterfeiting, according to the role they play in facilitating the sale of counterfeit goods and with regards to the existence and efficiencies of controls they have implemented to prevent and to react to issues. Specific provisions should hold online platforms liable when their platforms:

- Help users engage in unlawful conduct relative to specific categories of products that are highly regulated.
- Take possession of and stock counterfeit products.
- Facilitate payments for those products.
- Package, ship, and handle administration for selling counterfeit products.
- Profit from the sale of counterfeit products.

5. 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 system (e.g., two-strike or three-strike) that terminates and permanently bans sellers that have listed or sold counterfeits, regardless of whether this was done through one or several seller accounts.
- Prevent terminated sellers from rejoining or remaining on the platform under a different alias or storefront.
- Notify: (i) consumers that have bought a product from the seller to enable the customer to pursue a return or avoid the seller in future transactions; (ii) e-commerce platform coalitions so that (other) platforms are aware of illicit sellers already flagged or identified as high risk; (iii) law enforcement of sellers who have been permanently removed from the platform; (iv) the owner of the registered trademark, upon request.
- Destroy, or deliver to law enforcement, goods held in warehouses/fulfilment centers following the removal of a corresponding listing.
- Share consumer complaints about counterfeit products with affected brand.

6. 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. 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. Consequently, we recommend the following:

- Require e-commerce marketplaces to monitor and prevent fraudulent advertising on their platforms. Care should be given to vetting customer posted reviews to ensure that those reviews associated with fraudulent advertisements and products are not comingled with customer reviews of legitimate products.

- *Establish enhanced "Know Your Business Customer" protocols.* It is imperative that websites and social media platforms know with whom they are working when accepting paid advertising. By gathering and verifying an appropriate amount of data on who is utilizing their advertising services, they will be better able to proactively identify bad actors, avoid recidivism from previously removed accounts, and provide information to law enforcement. Data collected could include individual/business name and street address (proven with recognized ID), phone number, email, and a proof of business registration.
- *Require rigorous review of advertisement prior to publication.* The eCommerce marketplace should publish a list for sellers and buyers of what can and cannot be sold over its platform. To ensure that their terms of service are being adhered to, and that no innocent consumers are being defrauded by fraudulent advertising, all adverts published on a 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, 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 to include removal of the infringer's account and block the advertiser from the website or platform.
- *Ensure consumers and rights holders can report and share information about fraudulent advertisers.* 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 been removed should be notified. *(Facebook has implemented this as part of the counterfeit PPE measures.)* Additionally, a "report" functionality should be made available to assist consumers to report incidences where they suspect an advert to be counterfeit. *(WeChat has implemented this functionality.)*

7. Restore transparency for the WHOIS Domain Name Database

WHOIS domain name registration data plays an important role in protecting consumers and businesses from criminal networks, and in cyber security and cyber investigations. The WHOIS database is essentially the publicly available directory of who has registered a particular Internet domain name. It provides the name, address, phone number, email address and other technical information that is essential for tracking down who owns a domain name. This data is critical for companies and other stakeholders to identify who is

operating a website that may be engaged in criminal activity such as sending malicious emails (spam, phishing), conducting cyber-attacks, violating intellectual property rights or committing fraud under a brand name.

Implementation of the European Union General Data Protection Regulation (GDPR) has effectively blocked access to the data needed by businesses, law enforcement agencies and other stakeholders to maintain cyber security. Efforts by the Internet Corporation for the Assigned Names and Numbers (ICANN) to develop access models that work around the EU GDP have proven unsuccessful. Congress should:

- Restore domain name transparency.
- Lock and suspend suspicious domain names.
- Authorize brands and their accredited service providers to have access to WhoIs information.

8. 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 a manual review of listings to keep pace with the fraud. 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 behavior on an account should also be monitored, as it could be a sign the account has been compromised or changed ownership.
- Online marketplaces should use technology to screen vendors to assure they were not previously terminated (for counterfeit listing as well as other fraud), or their products delisted under different names.
- 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 the future.

9. Law enforcement

Greater and more proactive support from eCommerce marketplaces can help law enforcement prosecute criminals who sell counterfeits and perpetrate fraud on the platforms. This will help keep criminals off platforms and assure that the appropriate action is taken against prolific infringers, setting 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.
- Law enforcement tools must be modernized. There should be increased information sharing between brands, government agencies and law enforcement. Border agents should develop a database on importers deemed "trusted," and establish a national product hazard list.
- Law enforcement must notify the rights holder and provide adequate time for response and investigation before destroying confiscated counterfeited products. Any evidence (goods or documentation, electronic or otherwise) should be quarantined and retained until such time that the rights holder or law enforcement authorizes that destruction. Costs of sustainable destruction shall be paid by the infringer or platform, and evidence of such destruction retained and provided to rights holder as proof.
- Penalties must be increased.

#########