International Trademark Association Singapore Branch Office
3 Temasek Avenue
Centennial Tower #21-34
Singapore 039190
+65 6549 7452
www.inta.org

Input to the ASEAN IPR Action Plan 2026–2035

Focusing on IP Protection Online

The International Trademark Association (INTA) is a global not-for-profit association with more than 6,700 member organizations from over 181 countries. Its members include a broad cross section of businesses that own and use trademarks and other intellectual property, as well as law firms and other professionals who assist in the use, protection, and enforcement of IP rights. INTA welcomes the opportunity to provide the ASEAN Member States with Recommended Best Practices for Online Marketplaces.

INTA first published a guide of Best Practices for Addressing the Sale of Counterfeits on the Internet in 2008. In June 2021, INTA published an updated best practices document, Addressing the Sale of Counterfeits on the Internet, which included several new, stronger provisions to reflect the growth of the Internet, technological advances, and the increasing severity of counterfeiting including global online counterfeiting in recent years.[1]

In November 2023, INTA's Board of Directors passed yet another resolution, affirming the importance of identifying clear obligations for Online Marketplaces and brand owners with respect to the products offered through Online Marketplaces.[2]

INTA recommends that any Guidelines define "online marketplace operators" as "parties which manage the operation of Online marketplaces." INTA's 2023 board resolution, for example, defines Online Marketplaces as entities that:

1) Provide consumer-facing platforms that facilitate third-party sales, payment, shipping, and delivery of physical goods;

2) Are used by third-party sellers for these purposes; and

3) Have contractual or equivalent relationships with consumers governing their use of the platform.

INTA acknowledges that counterfeiting cannot be solved by single groups of stakeholders and therefore recommends governments engage a broader coalition of stakeholders, including search engine advertising services, search engines, payment service providers, logistics and fulfillment companies, domain name registrars and registries, web hosting companies, and social media platforms. These actors can play a role in enabling counterfeit sales through their services, and also have the capacity to disrupt such activity. INTA encourages these entities to adopt due diligence procedures, cooperate with law enforcement, and maintain transparency in how they handle IP violations.

For example, key recommendations for these additional parties could include:

- **Search engine advertising services** should have a clear and effective complaint process publicly available to report ads for counterfeit products and facilitate efficient filtering and takedown processes in an ongoing, proactive fashion.

[1] https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/Addressing_the_Sale_of_Counterfeits_on_the_Internet_June_2021_edit.pdf
[2] https://www.inta.org/wp-content/uploads/public-files/advocacy/board-resolutions/20231114_Establishing-a-Framework-for-Protecting-Consumers-Final.pdf

International Trademark Association, Inc., is a 501c(6) not-for-profit member association incorporated in the State of New York, with its headquarters office at 655 Third Ave., 10F, New York City, New York, USA.

New York | Beijing | Brussels | Washington, D.C. Metro Area | Singapore | Santiago

- **Search engines** should terminate a counterfeit seller's account and remove the search results leading to the illegal counterfeiting content by delisting the content from their index. Search engines should design their systems to the extent possible to prioritize search results for the promotion of authentic over counterfeit goods.
- **Payment Service Providers** should have policies in place prohibiting the use of their services for the sale of goods that are determined to be counterfeit. Such policies should include a "chargeback reason code" permitting the payee to receive a refund without returning the goods to the merchant where the goods have been determined to be counterfeit by the trademark owner, a customs or law enforcement agency, or another neutral expert.
- **Logistics companies** should: (i) have comprehensive and detailed "know your customer" policy before providing services; (ii) share information with enforcement agencies and brand owners actively investigating counterfeiting activities; and (iii) have mechanisms in place to refuse to provide services to those found to be involved in counterfeiting activities.
- **Domain name registrars and registries and web hosting companies** should adopt, publish, and enforce IP rights policies to address and minimize misuse of their services.
- **Social media sites** should use proactive filtering programs to facilitate the removal of paid advertising and organic postings (user generated content) that advertise the sale of counterfeit merchandise. Sites should verify the identity of their users selling counterfeit merchandise and provide details to brand owners whose rights have been violated.

INTA recommends that any guidelines developed by the ASEAN Member States clearly articulate responsibilities for these additional actors to create a more comprehensive framework for addressing counterfeiting.

The following best practices for Online Marketplaces were identified through research and practical experience of members of INTA's Anticounterfeiting Committee which includes Rights Owners, Ecommerce and Social media platforms and legal practitioners from the ASEAN region as well as elsewhere.

For Consideration by ASEAN Member States When Developing E-commerce Guidelines: Recommended Best Practices for Online Marketplaces

1. Clear Intellectual Property Rights (IPR) Policies

To take action against sellers of counterfeit goods, online platforms should clearly and explicitly prohibit the sale of counterfeits and other IP-infringing goods. These terms of service should be easily accessible, not just to sellers to highlight the policy against sale of such products, but also to consumers to highlight the risks associated with the purchase of counterfeits.

Infringing products should be clearly defined by the platform to avoid any confusion or possible loopholes for infringers to exploit.

The terms that sellers agree to in order to sell on a platform should also set out non-negotiable penalties for non-compliance and should treat users selling in significant quantities as business accounts rather than as personal accounts for the purposes of data requirements and enforcement.

Examples of good practices identified include:

- Terms of service should be easily accessible to both sellers and consumers
- A user agreement should be signed by sellers that clearly prohibits the violation of laws, third-party IPR, and the IPR policies of the platform

- Terms should apply to any user selling on the platform; where there are certain rules which only apply to specific sellers on the platform (e.g. stricter rules for business accounts), this should be clearly communicated
- Terms should be enforced in a consistent manner.
- Resources should be available for educating consumers and sellers on the risks of counterfeits, especially after a seller has received a notice of infringement
- Consumers should be informed if they have bought a product from a listing that is subsequently taken down for being counterfeit
- A clear repeat infringer policy should be set out, stating how penalties might escalate for recidivist behavior

2. Notice and Takedown System for Brand Owners to Report Infringing Content

As a first point for tackling counterfeits, IPR owners should have the ability to notify platforms through the submission of takedown notices identifying suspected infringing content when they have a good-faith belief that a seller is engaged in the sale of counterfeits. This should be an easily accessible portal online rather than just an email address or online web form.

Examples of good practices include:

- As long as the IPR owner has clearly indicated the reason for suspecting infringement, no test purchase or physical proof should be required
- Data requirements from rights holders should also be balanced and reasonable
    - The process should not be overly burdensome, requiring unnecessary paperwork or requiring court actions
    - There should be a "trusted notifier" approach with reduced evidence requirements for IPR owners who have proved their notices to be consistently genuine and reliable
- Turnaround for acting on valid notices should be kept to a minimum: no longer than seven days, but ideally under 48 hours
- Portals for notice and takedown should allow for multiple reports (bulk reporting) rather than requiring multiple separate reports
- Where possible, for rejected notices, platforms should provide clear, actionable feedback to allow IPR owners to improve their future notices
- Platforms should consider allowing buyers and sellers to report suspected sellers of counterfeits or listings, while recognizing that these users will not necessarily be able to tell when a product is counterfeit and may have other motives for reporting

3. Seller Verification and Know Your Customer (KYC) Measures

As a first approach, a platform should aim to conduct due diligence checks on sellers intending to use their platform to identify sellers of counterfeits before they may begin abusing the platform to defraud consumers with infringing products. By collecting and verifying a seller's identifying information on sign-up, and at regular intervals thereafter, platforms can more easily identify previously banned or sanctioned users from setting up a new account to continue infringing activity. It will also allow for any secondary/linked accounts to be identified when action is taken against a user.

Furthermore, should law enforcement authorities or brand owners wish to pursue criminal or civil action against an infringing seller, such data can be invaluable for identifying these targets. Examples of the data that might be collected are:

- For companies and for individuals: a registered and/or verified address , contact number, email address, or other verified contact information that brand owners or law enforcement can use to contact these sellers (e.g. for cease and desist purposes, investigation notices, etc).
- Bank account details and details on bank account ownership
- Copies of the seller's national identity card/passport, when possible

Examples of good practice include:

- **Prevention of Re-Registration and Circumvention by Banned or Blacklisted Sellers**: The platform should implement robust mechanisms to prevent individuals or entities that have been banned or blacklisted from re-entering the platform. This includes preventing the use of alternate identification documents, multiple identities, or other tactics to circumvent the verification process. Systems should be in place to track and flag known fraudulent behaviors, such as repeated use of the same or linked addresses, email accounts, phone numbers, and bank details, making it difficult for blacklisted individuals to operate under different aliases or evade detection. Platforms should also monitor behavioral patterns that may indicate attempts to bypass the system (e.g., using multiple accounts from the same IP address or device).
- **Account Linking and Monitoring**: A mechanism to identify and link multiple accounts under a single seller should be in place. Any attempts to operate several accounts should trigger an alert or additional checks, particularly if a seller is found to have previously violated platform policies.
- **Verification on Sign-Up and Ongoing Vetting:** Information should be vetted for accuracy on sign-up, as well as at regular intervals, to ensure that the details are up to date and consistent. Platforms may also consider implementing random audits or more frequent checks for high-risk categories.
- **Consumer Protection**: The platform should ensure that consumer protections that exist for brick-and-mortar stores should be applied to Online Marketplaces, including verification of basic identifying information (i.e., full name and contact details of the seller).
- **Visibility of Verified Seller Information**: Verified seller details should be clearly visible to consumers, enabling consumers to make informed choices and to purchase from trusted sellers (within the restrictions of local competition laws).
- **Limitation on the Number of Stores per Verified Seller**: To prevent misuse of the platform by bad actors, a verified individual should only be permitted to open and operate a limited number of stores. This helps mitigate the risk of fraudulent sellers who attempt to spread their activities across multiple stores, which could evade detection or enforcement. Platforms may set a maximum number of stores per individual or entity, and any attempt to exceed that limit should trigger a manual review or require special authorization.

4. Proactive Monitoring of Listings and Sellers

The volume of goods sold online is vast and growing as more people turn to e-commerce for their shopping needs. As the volume of legitimate goods increases, so too does the volume of counterfeits and other IP-infringing goods on these platforms. As such, only so much monitoring can be expected from IP teams at e-commerce platforms and rights holders.

To manage the volume of infringing content that requires manual review, automated tools should be used to block listings that are clearly infringing and flag those that are possibly infringing but require further review. Machine learning could be employed to improve these automated systems with input from brands on trends that they see used by bad actors.

Platforms should also work with IPR owners to develop lists of keywords frequently seen in the sale of counterfeit goods, as well as other key indicators such as price points and categories of products that are or are not manufactured by their company.

Sellers' activity should also be monitored for "red flags" of high-risk behaviour; for example incomplete or unverified information provided on request, significant volume of notice and takedown against listings, customer complaints/negative reviews due to counterfeit items received, sudden change in behaviour on account (prompting re-verification of data in case account has changed hands or been hacked).

Examples of good practices include:

- Using automated risk management tools to flag high-risk listings. Filters should track:
  - brand names with known counterfeit-related keywords including, but not limited to, "replica", "AAA", "1:1", "dupe" or "copy"
  - copyrighted images or images frequently used to sell fakes
  - items listed in categories not manufactured by the listed brand
  - items sold from jurisdictions where the brand has no business presence

- Manual review , but making use of automated tools to help with the volume of listings

5. Data Sharing with Brand Owners and Law Enforcement

It is evident that no one entity (IPR owners, platforms, or government/law enforcement) can single-handedly tackle online counterfeiting. Each group has different intelligence, data sets and capabilities. As such, it is key that within the bounds of relevant data protection laws, tri-partite data sharing should be facilitated between the different parties for the purposes of undertaking criminal action against those confirmed to be selling counterfeit goods.

Platform liability

While online platforms, as third-party service providers, benefit from a "safe harbor" against liability for the sale of counterfeits, this should only extend so far as the platform has demonstrated that it is not directly facilitating the sale of these counterfeits. As per the 2023 INTA "Consumer Protection Framework" Resolution, International Trademark Association supports a framework for assessing liability of Online Marketplaces for the third-party sale of counterfeit goods according to the following:

1. The framework recognizes liability of an Online Marketplace for third-party sales of specific counterfeit goods when it:

a. Has intentionally induced a third party to sell those specific counterfeit goods; or

b. Has actual knowledge of specific counterfeit goods being offered on its website or platform, and although it has the ability to do so, does not remove their offering; or

c. If neither 1.a. nor 1.b. apply, has failed to take reasonable steps to prevent and mitigate the sale of counterfeit goods.

Examples of Best Practices at the Jurisdiction Level

The below jurisdictions are setting good standards for anticounterfeiting legislation beyond just providing safe harbor for platforms doing the bare minimum. These should be seen as good examples of what can be done at the jurisdiction level and should be considered by ASEAN Member States if enacting e-commerce or intellectual property regulations.

- **European Union (Digital Services Act)**

Effectively replacing the e-Commerce Directive, in 2022 the European Digital Services Act (DSA) was published, with additional requirements implemented for online platforms, especially Very Large Online Platforms (VLOPs), i.e. those with over 45 million monthly users in the EU. The DSA came fully into effect on February 17, 2024 for all digital platforms operating in the EU. Below is an overview of relevant obligations for all online platforms (beyond notice and takedown (NTD)):

1. A clear redress mechanism for users to challenge decisions made against them
2. Prioritization of reports from Trusted Flaggers[3]
3. Suspension of users who have been repeatedly providing infringing content following a warning, or who have been repeatedly submitting bad faith notices
4. Know Your Business Customer (KYBC) checks on new sellers, including vetting the provided information through reliable services, and making best efforts to do the same for existing sellers.

Additionally, for **VLOPs** the following obligations also apply:

5. Conducting annual assessments on any systemic risks stemming from the use of their services
6. Annual independent audits from an external auditor confirming compliance with the DSA obligations
7. Transparency reporting on measures, including a publicly available database on advertisements, including who paid for the advertisements and on whose behalf, and the human resources dedicated to content moderation

The penalty for non-compliance with the DSA obligations is determined by the EU Member State, with the maximum penalty not exceeding 6 percent of the intermediary's total worldwide annual turnover. For VLOPs, this penalty may be assigned by the European Commission directly.

- **China (E-Commerce Law, effective 2019)**

China's E-Commerce Law sets out specific measures for the sale of counterfeits online, covering platform operators and sellers on these platforms, as well as others selling "through the internet or other information networks," thereby covering social media and messaging apps. Obligations for platforms are set out below:

1. Platforms should act as a depository of data released on their infrastructure; this includes supporting enquiries into transaction records. Such information should be held for three years from the date of transaction.
2. Platforms are obliged to report to the relevant authorities any breach of the E-Commerce Law, including the obligation not to sell illegal products.
3. Platforms have a duty of care regarding the quality of products sold by vendors on their sites to protect consumer health and safety. Any platform which "knows or should have known" that a vendor is selling goods that could pose a health and safety risk, or fails to check the qualifications of a vendor selling goods relating to consumer health and safety, may incur joint liability with the vendor.

[3] Trusted Flagger status is assigned by the relevant "Digital Services Coordinator" of each member state.

4. Platforms must establish their own IP protection procedures and strengthen cooperation with rights holders.
5. In addition to NTD measures, platforms should require prima facie evidence from vendors who submit a counter-notice to prove lack of infringement.

- **United States (INFORM Consumers Act)**

In the United States, counterfeiting is addressed through the Lanham Act and the Trademark Counterfeiting Act. There have, however, been several efforts recently to implement specific legislation in relation to online counterfeiting

1. The INFORM Consumers Act passed in 2023. This Act requires platforms to collect identifying information (bank account, contact details, and Tax ID information) from any third party selling "high volumes"(defined as 200 sales amounting to USD 5,000 per year). The Act also requires platforms to suspend sellers who refuse to provide this information or supply false information, and requires a mechanism for consumers to report suspicious activity to the platform.
2. The SHOP SAFE Act has been presented for consideration by the Congress several times since 2021, including being passed by the House of Representatives in 2022 as part of the America COMPETES Act. This Act would amend the Lanham Act to establish contributory liability for platforms facilitating the sale of counterfeits that pose a risk to consumer health and safety unless they implement best practices including:
    a. Verifying the identity, business address, and contact details of sellers on the platform
    b. Displaying the above information as well as jurisdiction of origin and manufacture of the products being sold, as well as the location from which the product is being shipped
    c. Terminating the accounts of sellers who have sold or advertised counterfeits more than three times
    d. Requiring sellers to consent to the jurisdiction of U.S. courts with respect to claims related to their selling on the platform

Neither INFORM nor the proposed SHOP SAFE Act impose criminal liability, rather they impose civil liability.

- **Vietnam**

One identified example in the ASEAN region is the current draft e-commerce law in Vietnam. This draft is currently under review, but sets out potential additions to the law that would set a strong precedent for other ASEAN member states. Key provisions include accountability for platforms and stronger compliance requirements for sellers.

Articles 19 and 20 of the draft state that platforms must:

1. verify seller identities
2. ensure transparency in business and product information
3. screen content before publication
4. cooperate with the authorities in investigations
5. provide transactional data upon request
6. jointly bear responsibility and compensate for damages in case of failure to handle infringements promptly

Article 21 of the draft requires sellers to:

1. complete electronic identification
2. disclose full business details, including:
    a. trade names
    b. addresses
    c. tax codes
    d. personal identification numbers

Appendix A: Platform IPR and Brand Protection Reporting

E-commerce Companies:

Bukalapak[4]: active in Indonesia

- Bukalapak IPR Protection Newsletter 2023
- Bukalapak Terms of Service
- Bukalapak Statement on Protecting IPR (2021)

Carousell: active Singapore, Malaysia, Indonesia, the Philippines

- Carousell Counterfeit Policy
- Carousell Rights Owner Program (CROP)

Lazada: active in Indonesia, Malaysia, Singapore, Vietnam, Thailand, and the Philippines. Part of the Alibaba Group.

- Lazada IPR Policy
- Lazada IPR Protection Home Page
- Alibaba International IP Protection Platform[5]

Shopee: active in Indonesia, Vietnam, Thailand, Philippines, Malaysia, and Singapore

- Shopee Brand Protection site

TikTok Shop: active in Malaysia, the Philippines, Singapore, Thailand, and Vietnam.

- TikTok Shop IPR Report 2024
- TikTok Shop IP Protection Center

Tokopedia: active in Indonesia

- Content Infringement Reporting Procedure
- Tokopedia IP Protection Platform

Social Media and Messaging Companies:

Meta

- Meta Transparency Center – Third-Party Intellectual Property Infringement
- Repeated intellectual property infringer policy for Meta
- Intellectual Property Report (2023)

Facebook

- *Help Center - Intellectual Property*

Instagram

[4] Bukalapak announced in January 2025 that the platform will stop selling all physical goods, and going forward will only sell digital services
[5] Following restructuring in 2023, Lazada is now fully under the Alibaba International umbrella

- *What happens if you repeatedly post content on Instagram or Threads that violates someone else's intellectual property rights*

WhatsApp

- *Intellectual Property Policy: Your Copyrights and Trademarks*

Telegram

No specific anti-counterfeiting measures exist on Telegram. Below is a link to the page for “third-party account verification”:

- Page Verification Guidelines

TikTok

- TikTok Brand Safety Center
- Intellectual Property Policy