



July 2026

**NOUS INVESTIGATIVE
SOLUTIONS**

NOUS INTELLIGENCE BRIEF JULY 2026 EDITION

**www.nous.co.th
info@nous.co.th
065-936-8500**

Beyond Notice and Takedown

What Thailand's New Online IP Enforcement Coalition Means for Brand Owners

Thailand's July 2026 enforcement agreement improves cooperation among government, police and a major online marketplace. The practical challenge is to convert faster takedowns into intelligence that identifies repeat sellers, distributors and upstream supply networks.

NOUS Investigative Solutions | 18 July 2026

NOTICE AND TAKEDOWN REMOVES A LISTING. INVESTIGATION IDENTIFIES THE BUSINESS BEHIND IT.

Thailand has taken another significant step towards strengthening the enforcement of intellectual property rights in online markets. On 11 July 2026, the Department of Intellectual Property (DIP) signed a memorandum of understanding with the Central Investigation Bureau, represented by the Economic Crime Suppression Division, and Shopee Thailand. The agreement is intended to improve information sharing, investigations and law-enforcement action against online sellers of infringing goods. [1]

The development is important because it potentially creates a more direct bridge between platform intelligence, rights-holder complaints and criminal investigation. Brand owners should not, however, interpret the agreement as meaning that conventional notice-and-takedown programmes will now be sufficient. Removing an individual listing remains useful, but it rarely identifies the commercial operation behind the account. Effective deterrence requires a move from listing-level enforcement to seller-network investigation.

Thailand's expanding enforcement network

The July agreement forms part of a broader public-private effort to address infringement across physical and online markets. The DIP reported that its internet intellectual-property cooperation network has grown to 45 organisations: three agencies under the Ministry of Commerce, 37 private-sector rights holders and five online platforms - Lazada, Shopee, TikTok Shop, Nex Gen Commerce and LINE. Unilever was announced as the latest rights holder intending to join the network and implement notice-and-takedown measures. [1]

Thailand also reported substantial enforcement activity during the first half of 2026: 456 intellectual-property infringement cases, 1,654,698 seized items and assessed damages exceeding THB 786 million. The DIP stated that enforcement efforts are focused on manufacturing sources, distribution hubs and major offenders, alongside rapid coordination with platforms to block or suspend infringing sales. [1]

These figures demonstrate institutional activity and increased attention. They do not, by themselves, show whether enforcement has permanently disrupted the supply networks responsible for repeated infringement. Case and seizure totals are useful operational indicators, but they should not be treated as measures of sustained deterrence without evidence that the underlying operators and supply channels have been disabled.

The gap between removing content and disrupting a network

A platform takedown normally addresses the visible component of infringement: the product listing, advertisement, video, livestream or seller account that has been reported. The underlying operator may remain largely unaffected. A seller can recreate a listing under a modified description, move inventory to another account, switch platforms or redirect customers to private messaging channels. Several apparently

independent storefronts may also be controlled by the same individual, family group, distributor or fulfilment operation.

The 2026 Special 301 Report issued by the Office of the United States Trade Representative provides an important counterpoint to Thailand's enforcement announcement. The report states that Thailand remains on the Watch List, while acknowledging positive working relationships with Thai police and Customs, improved seizure efficiency, action against warehouses and distribution centres, and successful enforcement against major piracy services. [2]

At the same time, USTR records continued concerns that counterfeit and pirated goods remain readily available, particularly online; that enforcement may focus on small operators instead of high-level distributors and manufacturers; and that greater action is needed against upstream suppliers. It also notes that, although some rights holders report positive results from takedown procedures under Thailand's 2021 e-commerce MOU, others continue to report growing online sales of counterfeit and pirated goods. [2]

The implication is not that takedown programmes have failed. They perform a different function from investigation. Takedowns reduce immediate visibility and interrupt sales. Investigations establish who controls the operation, where the goods originate, how apparently separate accounts are connected and which targets are sufficiently important to justify escalation.

From storefronts to connected entities

For a brand-protection team, the principal analytical question should not be how many listings were removed. It should be how many commercially significant seller networks were identified and disrupted.

A network-level assessment looks for recurring links between apparently separate sellers. Depending on the available evidence, relevant indicators may include:

- common telephone numbers, messaging accounts or email addresses;
- repeated payment instructions, beneficiary names or bank details;
- identical return addresses, shipping origins or courier patterns;
- shared product photographs, descriptions, spelling errors or account-creation behaviour;
- common packaging, batch markings or counterfeit characteristics;
- overlapping social-media accounts, external websites or private chat channels;
- the same warehouse, fulfilment provider, importer or wholesale source; and
- coordinated pricing changes and simultaneous re-listing after enforcement action.

No single indicator necessarily proves common control. When several indicators converge, however, a collection of apparently low-value storefronts may reveal a substantially more important distribution operation.

Why controlled test purchases matter

Online monitoring captures what a seller presents publicly. A controlled test purchase can reveal how the transaction operates in practice. Depending on the case, it may disclose payment instructions, recipient names, telephone numbers, courier information, shipping locations, invoice details, packaging methods and return addresses. Examination of the delivered product can also help determine whether stock sold through different accounts originated from a common source.

The evidential value lies not simply in confirming that a product is counterfeit. It lies in connecting a digital storefront to physical goods, transaction records and real-world logistics. Test purchases should therefore be planned rather than conducted as isolated purchases by different teams. Product selection, seller communications, payment records, screen captures, delivery tracking, receipt of the parcel and examination of the goods should be documented consistently. Where litigation or criminal enforcement is contemplated, procedures should be coordinated with local legal counsel to preserve evidential integrity.

When should a case move beyond takedown?

Not every online infringement requires a full investigation. High-volume monitoring programmes inevitably identify small, intermittent and commercially insignificant sellers. Escalation is more justified when one or more of the following conditions are present:

Repeated reappearance. The seller returns after previous removals or recreates the same operation through new accounts.

Multiple connected storefronts. Different accounts appear linked through contact, payment, delivery, content or product indicators.

Material inventory. Test purchases, sales data or seller communications suggest wholesale quantities or continuing access to supply.

Consumer-safety exposure. The products include medicines, cosmetics, automotive parts, electrical goods, food, beverages or other safety-sensitive items.

Cross-platform migration. The operator moves among marketplaces, social media, chat applications and independent websites.

Upstream potential. Available evidence points towards a warehouse, importer, manufacturer or significant distributor.

Commercial harm. The activity materially affects pricing, authorised distributors, a product launch or consumer confidence.

These indicators allow brands to allocate investigative resources according to commercial harm and deterrence potential rather than simply the number of visible listings.

A practical 90-day response framework

The new enforcement environment gives brand owners an opportunity to review how information obtained from online platforms is used. A practical initial framework is:

Days 1-30: Consolidate marketplace, social-media and historical takedown data. Identify repeat sellers and group accounts according to common attributes rather than treating them as unrelated complaints.

Days 31-60: Subject priority clusters to targeted test purchases and enhanced open-source investigation. The objective is to establish connections among storefronts, payments, communications, delivery infrastructure and physical products.

Days 61-90: Assess each network for escalation. Potential responses may include further platform action, warning letters, civil proceedings, referral to law enforcement or a coordinated approach involving several platforms and rights holders.

The purpose is not to investigate every seller. It is to distinguish disposable accounts from durable commercial operations and to focus resources on targets whose disruption would have a meaningful market effect.

What the July agreement can achieve

The July 2026 MOU is encouraging because it explicitly includes information sharing, investigation and law enforcement - not merely the removal of content. This may improve the ability of the DIP, the Economic Crime Suppression Division and Shopee to connect platform activity with identifiable offenders. [\[1\]](#)

Its long-term impact will depend on implementation: the speed and quality of information exchange, the criteria used to identify priority offenders, the ability to connect multiple accounts and whether enforcement reaches warehouses, suppliers and organisers rather than ending with individual storefronts.

For rights holders, the strategic conclusion is clear. Platform reporting should remain an important first response, but it should feed into a broader intelligence process. Thailand's strengthened public-private cooperation creates an opportunity to move beyond counting removed listings. Brand owners should use

that opportunity to identify repeat operators, map distribution relationships and build evidence against the entities capable of sustaining infringement at scale.

NOUS PERSPECTIVE

A mature online brand-protection programme should measure not only listings removed, but repeat operators identified, networks mapped, upstream targets developed and infringement that does not return.

References

- [1] Ministry of Commerce / Department of Intellectual Property, *"Ministry of Commerce Forges Multi-Agency Coalition to Tighten IP Enforcement Across Physical and Online Marketplaces, Mobilising the New Generation Under Do Not Buy, Do Not Use, Do Not Support Intellectual Property Infringement Campaign,"* 11 July 2026. [Official PDF](#) (accessed 18 July 2026).
- [2] Office of the United States Trade Representative, *2026 Special 301 Report*, Thailand section, pp. 92-93, 30 April 2026. [Official PDF](#) (accessed 18 July 2026).

Citation method: Bracketed references [1] and [2] identify the source supporting the preceding factual statement or paragraph. Unreferenced evaluative and operational passages are NOUS analysis.