ASIAN-PACIFIC POSTAL UNION

Article 03/2026
Published on

KNOWLEDGE CENTER

Revenue Protection in the Postal Sector

1. Introduction

Every postal item carries a promise of payment. The sender pays through a stamp, a printed label, a prepaid envelope or a business account, and the post undertakes to carry the item to its destination. Revenue protection is the set of controls that makes sure this promise is kept: that the postage is genuine, that it matches the weight and service, that it is collected before the item enters the network, and that any duties or charges due along the way are correctly declared and paid.

For many years, this was treated as a narrow operational matter, mostly about spotting short-paid letters at the sorting centers during random checks. That view no longer holds. Postage is now bought online, printed at home, generated through third-party platforms and resold on marketplaces. Parcels have replaced letters as the growth segment, and each parcel carries far more revenue than a letter. At the same time, most postal operators in the Asia-Pacific region are under pressure to reduce dependence on government support and to finance the Universal Service Obligation (USO) from their own earnings.

In that setting, revenue that is earned but never collected is a direct hit to sustainability of the postal operator. This article looks at where postal revenue leaks, why the problem has become more serious in recent years, and what postal administrations, regulators and regional bodies can do about it.

2. Where Postal Revenue Leaks

Revenue loss rarely comes from one source. It builds up quietly at different points of the value chain, and the main ones are:

- **Counterfeit stamps and prepaid products:** Forged stamps, prepaid envelopes and packets, often printed and sold online in bulk below face value. Buyers are sometimes small businesses who genuinely believe they have found a discount.
- **Counterfeit and fraudulent labels:** Shipping labels produced from stolen account credentials, copied tracking numbers or manipulated online postage platforms. With parcels, a single fraudulent label can represent the value of dozens of letters.
- **Short-paid and under-declared items:** Items carrying less postage than their weight, size or service requires, whether by mistake or by design. Manual weighing and manual entry at counters remain a weak point in many administrations. Further, volumetric pricing is not strictly enforced by many operators due to lack of resources.
- **Account and acceptance fraud:** Business accounts opened with false details, dormant accounts taken over by third parties, or large volumes inducted without verification.

- **Internal leakage:** Under-invoicing at counters, items inserted midway in the delivery chain without booking, and manipulation of accounts. Where posts also run savings and remittance services, the exposure extends to customer funds.
- **International mail and customs:** Poor quality customs declarations, undervalued e-commerce items and gaps in dispatch data that weaken both customs revenue and the settlement of accounts between operators.

These categories overlap. A counterfeit label used to move undeclared goods is at once a postal revenue loss, a customs revenue loss and a security risk. This is why revenue protection sits so naturally alongside the postal security agenda.

3. A Shared Problem Across the Region

Revenue leakage is sometimes seen as a problem of large, highly digitized posts. The experience of the Asia-Pacific region suggests otherwise. Cases have surfaced in operators of very different sizes and structures:

- **Australia:** Between 2018 and 2019, a syndicate allegedly imported 2.3 tonnes of counterfeit Australia Post prepaid satchels from abroad and sold them on eBay. Australia Post estimated the cost of the fraud at about AUD 2 million. In November 2025, it launched a Counterfeit Detection Tool that monitors online marketplaces and has since helped remove several million dollars' worth of fake postage from sale.
- **Malaysia:** In 2016, enforcement officers acting on a tip-off from Pos Malaysia seized 15,000 counterfeit prepaid Pos Laju envelopes worth RM 99,300 in Port Klang. The envelopes were believed to have been printed abroad and were sold in bulk at about RM 5 each, against the official price of RM 6.36. Pos Malaysia responded by adding new security features to its envelopes.
- **Hong Kong, China:** Hongkong Post has issued repeated public alerts, most recently in 2025 and 2026, about fake websites and SMS messages using its name to collect postage payments from the public. Such impersonation diverts money that customers believe they are paying to the post, and it chips away at public trust.

The forms differ, from counterfeit products to internal fraud to impersonation, but the pattern is the same. Revenue that should have reached the post did not, and in most cases the loss was found late, after the money had gone.

4. Why the Issue Has Become Urgent

Three developments have pushed revenue protection higher up the agenda.

(i) E-commerce and digital postage have multiplied the exposure

Online postage and label generation have made sending easier, but they have also given fraudsters new points of entry. Where public audit data exists, the numbers are sobering. The USPS Office of Inspector General (OIG) estimated in September 2026 that the United States Postal Service lost USD 1.6 billion in FY 2025 through accepting counterfeit postage labels, and that about 97 percent of such labels were still processed for delivery. A separate OIG audit in June 2026 found nearly

8,900 instances of counterfeit stamps offered online within about two months, often at 20 to 50 percent below face value. Few operators in the region publish comparable data, but there is little reason to believe that the same tools and platforms are not being used against them.

(ii) Customs regimes are tightening

The suspension of the United States de minimis exemption on 29 August 2025 led to an 81 percent drop in postal traffic to the US within a day, with 88 operators suspending some or all services. The European Union has applied a flat EUR 3 customs charge on low-value B2C consignments since 1 July 2026. As duty-free thresholds disappear, the accuracy of declared values and descriptions becomes a direct revenue question for governments, and posts are expected to carry their share of that responsibility.

(iii) Revenue fraud and illicit trade are increasingly linked

Counterfeit postage gives criminals anonymity. A fake label or stamp hides the real sender, and that makes it attractive for moving narcotics, counterfeit medicines and contraband. Revenue protection, in other words, is no longer only a finance question. It is also a question of network integrity.

The experience elsewhere also shows that the problem can be brought under control. Royal Mail completed its switch to barcoded stamps in 2023 and reports that counterfeit stamps in its network have since fallen by around 90 percent. The lesson for the region is that securing the product, and having the means to read it, makes a measurable difference.

5. Reinforcement from the Interregional Forum in Bangkok

In February 2026, the Asian-Pacific Postal Union (APPU) and the Postal Union of the Americas, Spain and Portugal (PUASP) jointly organized the Interregional Forum on Security as a Key Element for the Postal Service in Bangkok, with the support of the Universal Postal Union (UPU) and funded by the United States Postal Service (USPS). Importance of revenue protection was an important agenda of the forum, raised by operators, customs officials and industry speakers from both regions. Some of the points that came through were:

- **Fraud prevention starts at onboarding:** The revenue investigations session, led by the US Postal Inspection Service, stressed that controls should begin when a customer account is opened. Addresses, phone numbers and email IDs should be validated, and accounts opened online without any postal employee involvement deserve particular care. Dormant accounts are a known target, as fraudsters locate them and take them over to look like legitimate customers.
- **Too much public data helps the fraudster:** Tracking numbers displayed on public websites are being harvested and reused on fraudulent labels. Posts were encouraged to review how much information they expose and to add 2D barcodes with encrypted account data to labels, while monitoring for duplicates.
- **Mail processing equipment is an underused asset:** Many sorting machines already capture data that can flag duplicate, reused or unpaid pieces and labels from invalid accounts.

- **Remedies must go beyond detection:** Website takedown requests, administrative and financial penalties, withdrawal of courtesy services, public awareness campaigns and holding e-commerce partners and fulfilment centres accountable were all presented as practical tools.
- **Stamp authentication technology is maturing:** The UPU presented WNS 2.0, built on more than 122,000 registered stamps, which now uses AI-based analysis of stamp images and perforations. Its industrial version can be fitted to domestic sorting centres without IT development and can check up to 12 stamps per second.
- **Data quality is revenue quality:** According to the UPU, 5 to 10 percent of items with electronic advance data (EAD) are rejected owing to poor data quality, often because of generic descriptions. The Asia-Pacific region recorded ITMATT compliance of 90.55% in January 2026, which is encouraging but still leaves room for misdeclared items to pass.
- **The scale of illicit trade is large:** The UPU-TRACIT guide on illicit pharmaceuticals estimates that around 58 percent of all drug seizures happen through mail channels.

The UPU's closing message on revenue protection summed it up well: the standards exist, the expertise exists, and the funding exists. What is often missing is commitment at the level of the designated operator.

6. Building Blocks for Revenue Protection

There is no single solution, and the right mix will differ between a large operator with automated hubs and a small island post with one office of exchange. Postal administrations may, however, consider the following building blocks.

(i) Treat revenue protection as a programme, not a task
Fragmented efforts rarely work. Revenue protection needs an ownerships at the highst level, a documented strategy, defined roles across retail, processing, finance, IT and security, and measurable targets. Without this, weaknesses are often known internally but not acted upon until someone exploits them.

(ii) Secure the product itself
Barcoded stamps, labels with 2D barcodes and encrypted data, and security features on prepaid envelopes and satchels make counterfeiting harder and detection easier. The investment pays off once the network can read and validate these features at scale.

(iii) Strengthen controls at the counter and at acceptance
Integrating weighing scales with postal IT systems removes much of the scope for manual error and under-invoicing. Validation of customers at account opening, checks on bulk volumes at induction, and booking alerts that flag items entering the chain without payment should become routine.

(iv) Use the data already available
Sorting machines, tracking events, counter systems and EDI messages generate large volumes of data. Analysed properly, this data can point to duplicate labels, suspicious accounts, unusual volumes and recurring addresses. AI-based tools can help, but even basic exception reporting can

recover significant revenue.

(v) Watch the online marketplace
Most counterfeit postage reaching the network is sold on e-commerce platforms and social media. Posts need a structured process for monitoring listings, issuing takedown requests and working with platforms, as Australia Post now does. Speed matters: a listing that stays online for a month can do far more damage than one removed in a week.

(vi) Make Post-Customs cooperation work in practice
Accurate declarations protect customs revenue and the post's own credibility. A formal memorandum of understanding between customs and post, as encouraged by the WCO-UPU guidelines, helps clarify roles on examination, data sharing and risk assessment. The trilateral MoU signed in March 2025 between Mongol Post, the Customs General Administration and the General Police Department of Mongolia is a good regional example.

(vii) Build awareness, inside and outside
Staff at retail and processing units need to know what counterfeit postage looks like and what to do when they find it. The UPU's Trainpost platform now includes a dedicated course on revenue protection. Equally, the public should be told plainly that discounted stamps, envelopes and labels from unofficial sources are likely to be fake, and that official channels never ask for postage payments through unsolicited links.

7. The Role of Stakeholders and Regional Cooperation

Designated operators cannot deal with this alone. Counterfeit postage is sold on platforms that posts do not control, and the legal tools to act against sellers usually sit with governments. In many countries, postal laws are outdated, and they say little about the sale of counterfeit postage on e-commerce sites or the obligations of the platforms that host it. In many countries, cases like this are taken under consumer protection and criminal law, which worked, but a clearer basis in postal legislation would help.
The gap has been recognized at the global level. In 2025, the United States developed a proposal for the UPU Congress asking the Postal Operations Council and its Postal Security Group to raise awareness of revenue protection, engage member governments and regulators, push for stronger protocols for e-commerce platforms selling postage, and set up a secure channel for posts to share fraud trends in real time. How much difference this makes will depend on how actively member countries take it up at home.
At the regional level, the APPU has already shown, with partners such as PUASP and the UPU, that joint work on security certification, EAD and Post-Customs cooperation delivers results. Revenue protection could be added to this agenda through shared training, a regional exchange of information on counterfeit trends, and support for smaller operators who lack the scale to invest in detection technology. UPU funding mechanisms, including support already extended for security equipment in least developed countries could be extended to revenue protection tools as well.

8. Conclusion

For a sector working hard to stay financially sustainable, revenue protection may be one of the

most cost-effective investments available. Every rupee, ringgit, yen or baht recovered from fraud is revenue already earned, without new products or new customers. The experience of operators that have acted decisively shows that losses can fall sharply once posts secure their products, use their data and work together with customs, regulators and platforms.

The Bangkok forum confirmed that much of the groundwork is already in place, through security certification, EAD systems and Post-Customs cooperation. Building revenue protection on that foundation is the logical next step. A post that knows its postage is genuine, its declarations are accurate and its accounts are clean is better placed to protect both its finances and the trust that people place in the postal network.

Written by:
Mr. Sandeep KP
Consultant, APPU
sandeep@appu-bureau.org