Title: The Rise of Scam Hubs is no Longer a Domestic Problem: Why the Palermo Convention Matters to the Philippines

A scam was once imagined as a single deceptive message. It was a fake investment pitch, a suspicious link, or a stranger pretending to be in love. Today, in the Philippines, the scam has become something more organized. It has rooms, routers, phones, scripts, cryptocurrency wallets, fake identities, foreign handlers, trafficked workers, and, in some cases, the appearance of a lawful business.

This is why the United Nations Convention against Transnational Organized Crime, more commonly known as the Palermo Convention, matters urgently to the Philippines. The Convention was adopted by the United Nations General Assembly in 2000, entered into force in 2003, and is described by the United Nations Office on Drugs and Crime (UNODC) as the main international instrument against transnational organized crime. It is a treaty about criminal systems that survive because they cross borders. On December 14, 2000, the Philippines signed the said treaty. Under the Palermo Convention, our country is expected to punish organized criminal groups, criminalize money laundering, corruption, and obstruction of justice, cooperate with other countries through extradition, mutual legal assistance, intelligence-sharing, and law enforcement coordination, protect victims and witnesses, and create domestic laws and institutions for effective investigation and prosecution.

The Philippines should treat foreign-linked scam hubs not as isolated cybercrime incidents, but as transnational organized crime under the Palermo Convention. This is because recent scam-hub cases show a recurring pattern: foreign actors operate or direct schemes from Philippine territory, victims are targeted abroad, workers may be trafficked or coerced, proceeds are moved through digital and cryptocurrency channels, and the true beneficiaries may be hidden behind corporate, property, or financial arrangements. A purely domestic response may close a node, but only a transnational response can dismantle the network.

Scam hubs are organized criminal systems

The Palermo Convention defines an organized criminal group as “a structured group of three or more persons, existing for a period of time, acting together to commit serious crimes for financial or material benefit.” It also applies to transnational offenses involving an organized criminal group. An offense is transnational when it is committed in more than one State, planned or controlled in another State, involves a group active in more than one State, or has substantial effects in another State.

In Parañaque City, the National Bureau of Investigation (NBI) dismantled an alleged online scamming operation that combined romance fraud, cryptocurrency schemes, and artificial intelligence tools to target foreign victims. Seventeen individuals were arrested, including fourteen Filipinos and three foreign nationals. Investigators reported a call center-like setup linked to a suspected fraudulent investment platform. The NBI's forensic findings indicated that victims were targeted abroad, including in the United States, Bangkok, and parts of Europe.

This case is important because it shows the basic structure of a modern scam hub. It is not merely one person deceiving another. It is a coordinated operation involving identity fabrication, emotional manipulation, digital tools, payment channels, and foreign victims. The crime begins in one place, continues in another, and is rarely confined to one jurisdiction.

Moreover, the Philippine National Police Anti-Cybercrime Group (PNP-ACG) arrested thirty-nine individuals, including eight Chinese nationals and one Taiwanese national, for allegedly operating an online scam hub from three condominium units. Police said the group used romance and investment fraud, layered digital wallets, AI-enhanced social engineering, pre-registered SIM cards, and fraudulent cryptocurrency platforms. The PNP-ACG also said that some groups splintered into smaller "guerrilla-type" operations after Philippine Offshore Gaming Operations (POGO) were declared illegal by the Anti-POGO Act of 2025. That detail is crucial. It means enforcement pressure may not eliminate scam hubs; it may simply force them to mutate. The criminal compound becomes a condominium unit. The POGO office becomes a residential operation. The visible hub becomes a dispersed network.

Domestic enforcement alone misreads the nature of the crime

It may be argued that scam hubs are already covered by domestic laws: cybercrime law, anti-trafficking law, immigration law, securities regulation, access-device law, and anti-money laundering law. While it is true that Philippine law is indispensable and domestic legal institutions are important in preventing scam hubs, both Philippine law and institutions are not sufficient. The life of a scam hub does not begin and end its life solely in the Philippines.

In the Pasay City raid, authorities arrested 401 foreign nationals, including Chinese, Vietnamese, Korean, Malaysian, Indonesian, Myanmar, and Madagascan nationals. Authorities reported signs of cryptocurrency fraud, love and investment scams, spamming, text blasters, and one-time password generators. AP likewise reported that the detained individuals were suspected of involvement in illegal online gaming operations, cryptocurrency schemes, romance scams, and investment scams. And that some online gambling outfits had relocated to countries such as Cambodia and Myanmar. In contrast, others remained in the Philippines and continue to scam over the internet.

The Pasay case demonstrates why the Palermo Convention is needed. The suspects came from several countries. The victims may be outside the Philippines. The money may be stored or moved through digital wallets and foreign-controlled accounts. The evidence may be scattered across messaging platforms, financial intermediaries, telecom systems, and cloud servers across countries. The Philippines can raid a local site, but it may need other States to identify victims, preserve digital evidence, trace funds, deport or extradite suspects, and establish the full structure of the criminal group.

This is precisely the gap the Palermo Convention addresses. Its purpose is to promote cooperation to prevent and combat transnational organized crime more effectively. It creates a legal framework for extradition, mutual legal assistance, law enforcement cooperation, confiscation, victim protection, and prevention.

The Palermo Convention turns raids into network disruption

The Palermo Convention matters because it changes the goal of enforcement. The goal should not only be to arrest the people found inside a room. The goal should be to dismantle the organization behind the room.

First, the Convention supports law-enforcement cooperation. Article 27 requires States Parties to cooperate closely, establish secure channels of communication, exchange information on suspects and proceeds of crime, coordinate inquiries, and respond to transnational organized crime committed through modern technology. This is directly relevant to scam hubs. A Philippine agency may know where the computers are, but a foreign agency may know who the victims are. A Philippine investigator may identify a wallet address, but another jurisdiction may have information on the exchange account, subscriber identity, or cash-out location. Without international cooperation, each State sees only one fragment of the criminal design.

Second, the Convention supports mutual legal assistance. Article 18 requires the designation of central authorities to receive and execute requests for assistance. This matters because scam-hub cases often require bank records, immigration files, corporate documents, digital evidence, witness testimony, and victim statements from abroad.

Third, the Convention supports extradition. Article 16 treats covered offenses as extraditable between States Parties and allows the Convention, in some circumstances, to serve as a legal basis for extradition. This matters where organizers, financiers, recruiters, or technology providers are not physically present in the Philippines.

Fourth, the Convention supports asset tracing and confiscation. The Convention provides mechanisms for identifying, tracing, freezing, seizing, and confiscating proceeds of crime. It also recognizes the importance of returning confiscated proceeds to requesting States so they may compensate victims or restore property to legitimate owners. This is essential because scam hubs are profit-driven. If enforcement only stops at arrest, the organization may survive. But if enforcement reaches the money, the organization is weakened.

The Palermo Convention is especially relevant because scam hubs depend on money laundering. The Malate case allegedly involved layered digital wallets used to conceal the source of illicit proceeds. The Parañaque case allegedly involved cryptocurrency wallets linked to a suspected fraudulent investment platform. The Pasay case involved alleged cryptocurrency, romance, and investment scams.

Article 7 of the Palermo Convention requires States Parties to establish regulatory and supervisory regimes for banks, non-bank financial institutions, and other bodies susceptible to money laundering. It emphasizes customer identification, record-keeping, suspicious transaction reporting, financial intelligence units, and cooperation among law enforcement and financial regulatory authorities at both national and international levels. This is where the scam-hub issue becomes larger than cybercrime. A scammer can deceive a victim, but an organized criminal group needs infrastructure to receive, move, conceal, and enjoy the proceeds. That infrastructure may include crypto wallets, mule accounts, shell companies, false identities, property leases, local incorporators, payment processors, and foreign accounts.

The legal implication is clear that the Philippines must not only identify who typed the messages. It must identify who owned the wallets, who supplied the SIM cards, who leased the units, who registered the businesses, who controlled the platforms, who handled cash-outs, and who ultimately received the proceeds.

Human trafficking makes the issue more urgent

The scam-hub problem is not only about money. It is also about people.

The Bamban, Tarlac case illustrates this. AP reported that a Philippine court convicted former Bamban Mayor Alice Guo and seven Filipino and Chinese co-accused of human trafficking connected to an illegal online gaming complex where foreign nationals were forced to conduct scams. The court sentenced Guo and her co-accused to life imprisonment, imposed fines, and ordered compensation for the victims. AP also reported that online scam centers in Southeast Asia have trapped large numbers of people in conditions of forced criminality, where victims are compelled to exploit others through false romance, fake investments, and illegal gambling schemes.

This matters because enforcement must avoid a simplistic assumption that everyone inside a scam hub is equally culpable. Some may be organizers. Some may be recruiters. Some may be financiers. Some may be local enablers. Others may be trafficked persons forced to participate in criminal activity.

The Palermo Convention's Trafficking Protocol is still relevant in this regard. The Convention contains provisions on victim assistance, witness protection, cooperation with law enforcement, and prevention. It recognizes that organized crime cannot be fought only by punishment. A serious Philippine response should therefore distinguish between the criminal enterprise and the persons trapped within it. The State must prosecute the architects without misclassifying victims as willing offenders.

The broader regional pattern

The Philippine scam-hub problem is part of a larger Southeast Asian crisis. UNODC warned in 2025 that transnational organized crime groups in East and Southeast Asia are moving into more vulnerable and underprepared areas as enforcement pressure increases. The UNODC also identified scam compounds in Cambodia, Laos, Myanmar, and the Philippines as being displaced by crackdowns, only to reappear in other areas and purpose-built business parks.

This regional pattern matters because it shows the limits of lone-country enforcement. If the Philippines acts alone, syndicates may move abroad. If other States act alone, syndicates may move into the Philippines. If enforcement focuses only on buildings, syndicates may shift to residential units. If enforcement focuses only on workers, the financiers remain untouched.

What the Philippines should do

The Philippines has already accepted the logic of the Palermo Convention. It signed the Convention on December 14, 2000, and ratified it on May 28, 2002. Executive Order No. 265 (2004) also recognized that the Convention encourages coordinated national policy, legislative, administrative, and law-enforcement approaches to prevent and combat transnational crime more effectively.

The issue now is implementation.

A Palermo-based response to scam hubs should include at least five commitments.

First, the Philippines should make financial investigation a central part of every scam-hub raid. Seized devices should lead not only to cybercrime charges but also to asset tracing, suspicious-transaction reports, beneficial ownership inquiries, and possible forfeiture.

Second, the Philippines should strengthen beneficial ownership and corporate transparency. Article 31 of the Convention urges States to reduce opportunities for organized criminal groups to participate in lawful markets with proceeds of crime, including by preventing the misuse of legal persons.

Third, the Philippines should pursue mutual legal assistance from the beginning before the domestic case has weakened where victims, suspects, platforms, bank accounts, or crypto exchanges are abroad.

Fourth, law enforcement should adopt victim-sensitive screening. Scam hubs may contain both offenders and trafficked persons. A worker forced to commit fraud under threat should not be treated the same as a financier or syndicate leader.

Fifth, the Philippines should treat scam hubs as a regional security and governance issue. They are not merely private crimes committed by private offenders. They test the integrity of immigration systems, local licensing, property markets, digital finance, corporate registration, and anti-corruption institutions.

The Palermo Convention matters because it helps the Philippines see the scam hub correctly. The room filled with computers is only the visible part of the crime. Behind it may be recruiters, handlers, property lessors, corporate fronts, crypto wallets, foreign victims, trafficked workers, corrupt facilitators, and offshore beneficiaries.

The latest cases from Parañaque, Malate, Pasay, and Bamban show that scam hubs are becoming more adaptive, technologically advanced, and transnational. They use AI tools to deceive, cryptocurrency to move proceeds, foreign nationals to direct operations, and the Philippine territory as a convenient base. Treating them merely as local cybercrime incidents risks mistaking the symptom for the system.

The Philippines must therefore use the Palermo Convention not as a ceremonial treaty, but as an operational legal framework. The task is not only to raid scam hubs. It is to identify organized criminal groups, protect trafficked persons, trace funds, cooperate with foreign jurisdictions, confiscate criminal proceeds, and close legal spaces that allow foreign-led syndicates to operate under local cover.

In the end, the question is not whether the Philippines can enforce its laws within its own territory. It can, and it must. The deeper question is whether Philippine enforcement can prevent the full architecture of a crime designed to cross borders. That is where the Palermo Convention becomes indispensable. It reminds us that in the face of transnational organized crime, sovereignty is not defended by acting alone. It is defended by cooperating well.

Disclaimer