GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

MINIMIZING RISKS OF CRIMINAL EXPOSURE TO SCAM COMPOUNDS IN CORPORATE SUPPLY CHAINS

A GUIDE FOR SUPPLIERS AND PARTNERS

Lindsey Kennedy | Nathan Paul Southern

JANUARY 2026

ACKNOWLEDGEMENTS

The authors would like to thank the Government of Norway and the Government of Canada for supporting the research and publication of this policy brief.

ABOUT THE AUTHORS

Lindsey Kennedy is an investigative journalist and research director at The Eyewitness Project, which specializes in the overlaps between organized crime, conflict and corruption. Her work focuses on cyber scam operations, human trafficking, illicit commodity flows and environmental crime, and has been featured in *Foreign Policy*, *The Guardian*, HuffPost, Al Jazeera, *The Sydney Morning Herald* and NPR. She has co-authored Global Initiative Against Transnational Organized Crime (GI-TOC) reports on trafficking in the Mekong region.

Nathan Paul Southern is a non-traditional security specialist, director of operations at The Eyewitness Project and PhD candidate in international relations at the University of St Andrews. He specializes in the overlaps between conflict, organized crime and corruption, and has consulted on reports for the Brookings Institution, the GI-TOC and the Institute for Integrated Transitions, and written for Al Jazeera, *Foreign Policy*, HuffPost and the *South China Morning Post*.

Cover: © *Lillian Suwanrumpha via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

SUMMARY

Highly organized cyber scams in South East Asia are invariably run from so-called scam compounds, which are purpose built or modified buildings that meet precise requirements. The compounds provide crucial infrastructure for various forms of online scams, fraud and related cybercrime.

This policy brief is the second in a two-part series on how private businesses can avoid buying from, selling to or partnering with criminal actors in the cyber scam industry. In part one, we covered the pre-operational phase of scam compounds and looked at ways in which developers, funders and construction contractors can identify high-risk developments and distance themselves before compounds are even built.

Here, in part two, we focus on compounds that are already operational. The brief looks at how existing or potential suppliers and partners can recognize red flags that these criminal activities are taking place and what they can do in response. This is particularly relevant for companies in the utilities, telecoms and order fulfilment/shipping sectors, as well as tech companies that develop ride-hailing, food delivery and 'super apps'.[1]

Key points

Companies at risk of acting as suppliers to scam compounds can play a central role in disrupting this industry in three key ways:

- Incorporating prevention of exploitation for forced criminality into their existing policies on human trafficking and ethical business practices, in a way that empowers employees at all levels to flag concerns through internal reporting systems.
- Companies should enhance training of internal machine learning models to recognize red flags, suspicious orders and patterns that suggest that new scam compounds may be emerging.
- Finally, companies can contribute to the cyber scam response by engaging with broader information-sharing mechanisms wherever possible within their industries and across sectors, and by complying with data sharing requests and subpoenas from law enforcement and legal teams relating to customer data linked to scam compounds.

INTRODUCTION

In jurisdictions where political connections between organized criminal groups and local or national authorities constrain an effective policy response, proactive collaboration with the private sector is essential for identifying and tackling the cyber scam epidemic. Once indicators emerge that cyber scams are being perpetrated from a particular location, feeder industries and suppliers willing to share information or implement AI-driven systems to flag suspicious activity can collectively help to build a vital picture of these operations. In particular, they can shed light on the criminal actors who are profiting, and how compounds interlink.

Cyber scam compounds, like any other licit or illicit enterprise, source physical products and on-premise services from a range of suppliers to meet their daily operational needs. Not all of these suppliers may be able to refuse service to compounds directly – in some cases, it may be impractical, illegal or unethical to do so. However, even those that cannot cut ties can provide crucial assistance by improving detection models for suspicious transactions, tracing scams to specific locations, linking payments to scam locations and even exposing new scam compounds as they emerge.

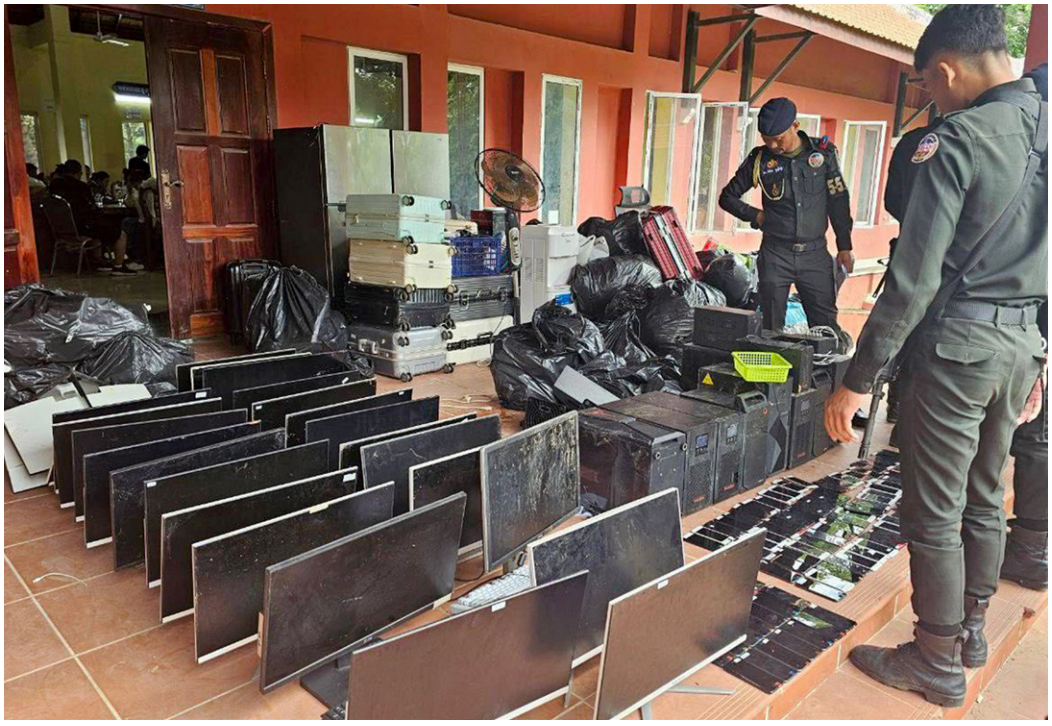
For these reasons, this policy brief focuses on localized order fulfilment and delivery companies that serve relatively small geographical areas or work with niche, regional supply chains. For example, it looks at those that partner with regional warehouses of larger e-commerce companies to meet demand in specific areas that are at high risk of hosting scam compounds. Actors in this sub-category of shipping/delivery suppliers are more likely to know and track exactly what products they collect and deliver, and more likely to understand how this could prove significant in the local context of scam compound exposure risk. This creates greater potential for targeted engagement, analyzing data to detect unusual patterns in demand that raise red flags and identifying a local presence that law enforcement bodies could collaborate with.

The research for this policy brief included visits to scam compounds in Cambodia and Laos – mainly to the exterior of such sites, but sometimes also the interior of temporarily disused facilities – and interviews with survivors. Researchers from the Global Initiative Against Transnational Organized Crime (GI-TOC) met with real estate agents that advertise for tenants for compounds, analyzed media reports, reviewed photos and videos from inside compounds and scoured corporate listings and addresses. Alongside analysis of open-source satellite imagery and pinned locations of company names listed on Google Maps inside inaccessible compound hubs, the researchers were able to compose a picture of how scam compounds are typically structured and what services they tend to offer onsite.

WHY DO COMPANIES SUPPLY THE CYBER SCAM INDUSTRY?

When assessing why a company acts as a supplier or partner with a scam compound, we first need to consider two questions:

- Has the supplier been made aware of the criminal exposure risk of dealing with this compound?
- Is the company concerned about the risks associated with criminal exposure or is it distancing itself from the scam compound industry as a genuine priority?



Military police with computers, smartphones and other equipment seized in July 2025 during a raid on a scam centre in Kandal province, Cambodia. *© JSTR/Pool/AFP via Getty Images*

FIGURE 1 Suppliers can be located within a quadrant of criminal risk awareness and willingness to engage with the cyber scam industry.

The answers to these questions create four broad possibilities, depicted in each quadrant of the grid above.

1. The entity has no idea that it is supplying a scam compound and would not willingly have done so.
2. The entity was not directly made aware that they are supplying a scam compound, but is not concerned about the potential criminal exposure risks.
3. The entity is aware (or is likely to be aware) that it is supplying a scam compound and, despite reluctance and concerns, has continued to do so.
4. The entity is aware that it is supplying a criminal compound and willingly or enthusiastically continues to do so.

Distinguishing between these categories helps to assess the extent to which an entity is actively complicit in the criminal enterprise, as opposed to viewing involvement as a necessary or unavoidable evil or simply being unaware that they play any role at all. This represents a broad spectrum of reasons for engaging with the scam industry and acts as a starting point for considering what might convince an entity to cease supplying a scam compound or to assist with efforts to disrupt its activities.

For example, the images below show companies that are clearly seeking customers in the forced criminality space and/or are companies that are based within scam compounds, meaning they fit within quadrant 4. The image on the left advertises a transport service that picks up undocumented workers (i.e. individuals at high risk of trafficking) from Chinese border areas and brings them to a range of locations in Laos, Myanmar, Cambodia and elsewhere that are strongly associated with the scam compound industry. The centre image is an advertisement for a range of services for scam companies that move teams into compounds inside the Golden Triangle Special Economic Zone (SEZ) in Laos. On the right, a real estate company representing a suspected scam compound location in Sihanoukville, Cambodia, lists its services, facilities, and office and dormitory furniture for sale, as well as related management and cleaning fees. Depending on the degree of involvement, engagement with these companies will require different considerations.

Advertisements shared on Telegram groups in August 2025 targeting 'grey area' businesses working in the scam and online gambling space. *Photos supplied*

Taking a closer look at companies potentially situated in quadrant 3 exposes deep and vested interests in the cyber scam industry. Field research indicates that many scam compounds and companies are part-owned or managed by, or otherwise closely linked to, powerful political figures, meaning that attempts to shut down the industry are at times directly at odds with the personal financial interests of those responsible for making such policy decisions. For example, scam compounds in Myanmar reportedly rely on towers provided by Mytel, a joint venture between the Myanmar military and Viettel, a Vietnamese state-owned defence enterprise.[2]

This quadrant may also include foreign government-linked telecoms services that offer their products in high-risk cyber scam jurisdictions. For example, in one mixed-use compound to which a GI-TOC research team gained entry in February 2025 – and where the team collected evidence of forced criminality – the building's Wi-Fi was provided by routers labelled China Mobile,[3] a Chinese state-owned telecoms provider.

The use of telecoms networks may also make it more difficult for actors to detect red flags and raise the alarm. For example, organizations that trace the origin of scam calls internationally and intercept and block them before they reach potential victims rely on the cooperation of private telecoms and internet providers all along the chain.[4] If these companies have political backing, investment or protection, it may be impossible to make them comply.

WHERE DO SCAM COMPOUNDS INTERACT WITH OUTSIDE SUPPLIERS?

Owners of large, self-contained compounds typically provide most core services as a package. However, regardless of whether a criminal group deals directly with external suppliers or the compound manages most of the supply chain on their behalf, mapping where and how these suppliers interact with the industry is crucial. This mapping can assist in identifying who has the potential to cut lifelines to criminal actors and what steps they can take to achieve this.

This section summarizes the kinds of suppliers and services that are commissioned to help scam compounds meet their critical requirements (see Figure 2) and identifies the points of contact this creates with supply chains beyond the compound.

Critical requirement: Reliable power

Primary sector: Utilities

Scam companies need reliable power 24/7. Typically, scam compounds source electricity from the national grid or, in borderland areas, from that of a neighbouring country.[5] However, some larger hubs include power stations as part of their development plans,[6] and we witnessed examples of remote compound sites installing solar panels, which may be a step towards self-sufficient, on-site power generation.[7]

Thailand has cut the power supply to scam compound cities in Myanmar at various points (including in February 2025 – see the section below), but these cities appeared to have survived by switching to diesel generators.[8] Criminally exposed SEZs housing forced labour operations in South East Asia are often located in the vicinity of new Chinese-funded hydroelectric dams[9] or coal-fired power plants.[10] However, we were unable to ascertain whether these SEZs benefit from the supply or are simply installing themselves in areas where there are official Chinese infrastructure projects to create the illusion of legitimacy.

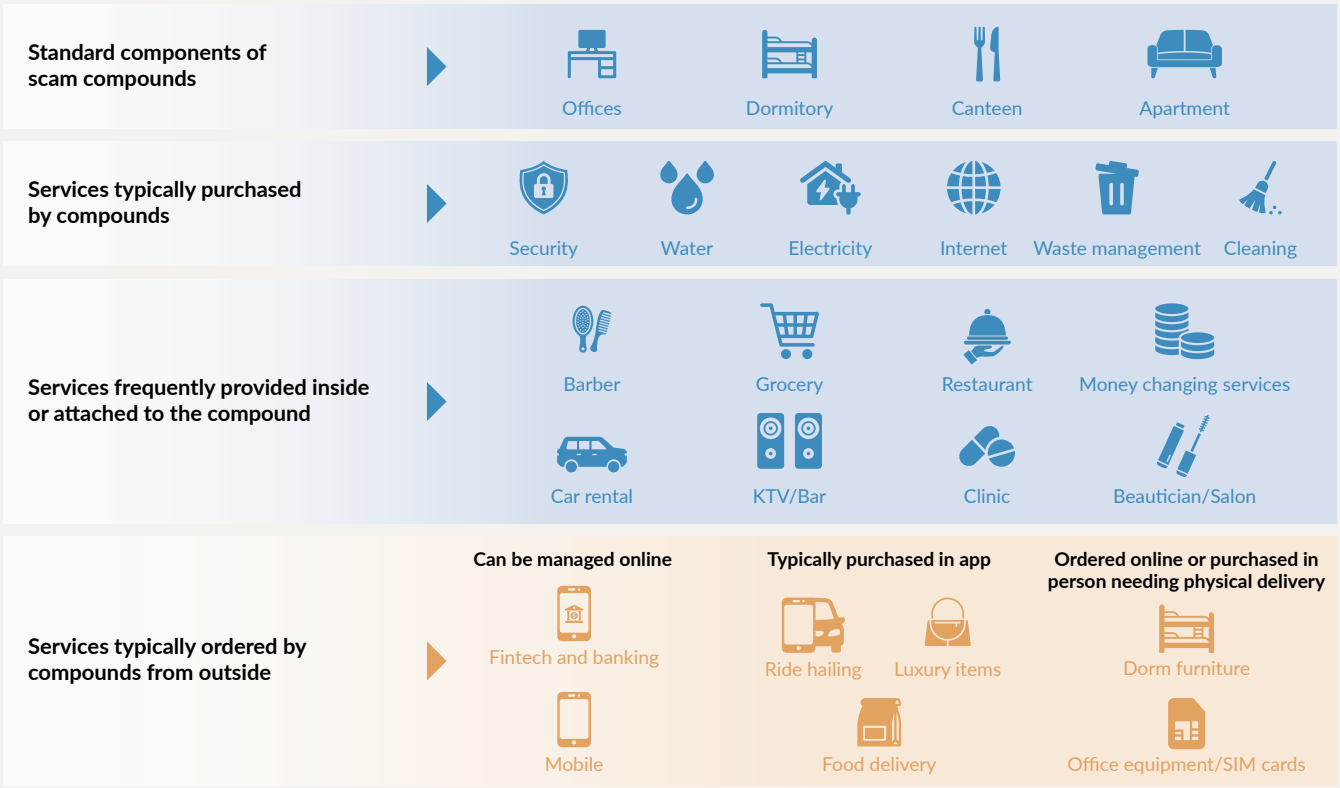


FIGURE 2 Services and facilities usually provided inside scam compounds or ordered from outside.

Practical and ethical considerations

In February 2025, under pressure from China, the Thai government shut off electricity, internet access and fuel supply to five locations in Tachileik, Myawaddy and Payathonzu – areas that are all alleged to be hubs of cyber scam and human trafficking activity in Myanmar.[11] While this was designed to target and disrupt scam compounds,[12] it had the unintended effect of depriving local residents of these resources and services, while criminal syndicates appeared to find workarounds to keep operating.[13] This highlights how disadvantaged communities often bear the brunt of abrupt policy moves, while also raising the question of why the Thai authorities would partner with Myanmar companies to supply a region dominated by scam hubs in the first place.[14] Thailand's energy sector is dominated by three state-owned utility companies,[15] but these are permitted to supply border towns in Myanmar with electricity without seeking central government approval.[16] Simply cutting off all access to utilities or shutting down private companies that serve scam compounds may prove to be short-sighted or excessively heavy handed; more nuanced, targeted responses are needed to address these issues in the long term. ■

Critical requirement: Waste management

Primary sector: Utilities

Public or private waste collection companies need to come to the compound location to take away refuse, although some remote compounds appear to have their own systems in place or use unbranded trucks for collection.[17] It is worth noting that denying service altogether would create significant harm beyond the compound. Those without an effective system in place are often surrounded by mountains of waste dumped directly or in plastic bags,[18] sometimes with visible chemical seepage into waterways.[19] This has obvious ramifications for the natural environment, nearby agriculture and public health.

Critical requirement: Clean water

Primary sector: Utilities

Secondary sector: Shipping/delivery

A water tower in Vientiane, Laos. Water supply is a critical service for scam compounds, and some have infrastructure for their own supply. *© Oleksandr Rupeta/NurPhoto via Getty Images*

In urban areas, supply of clean running water for scam compounds is likely to be provided by standard public or private water companies. Remote compounds may have their own sources or developers may build sewerage and water supply pipes as part of their agreement – for example, Boten SEZ in Laos includes a water treatment plant that reportedly produces 10 000 cubic metres of water per day.[20] Rooftop water tanks and towers are also common, and the owner of one remote compound hub in Cambodia has also built a reservoir nearby,[21] with the capacity to store 440 000 cubic metres of water.[22]

It is common to see large volumes of drinking water (in tanks or bottles) being delivered to the gates of sealed-off compounds and carried inside by staff or guards.[23] Noting these large deliveries to compounds that are as yet unoccupied or temporarily vacant can help make rough estimates of how many people are about to be transported or trafficked to the compound. It can also provide an indication that buildings that have supposedly been shut down are being prepared for occupation again.[24]

Critical requirement: Internet access

Primary sector: Telecoms

A cell tower in Shwe Kokko, Myanmar, from where some 250 people were rescued from online scam centres in February 2025. Cyber scam companies are dependent on high-speed internet, and some make provision for private cell towers.
© Brent Lewin/Bloomberg via Getty Images

Cyber scam companies cannot operate without high-speed internet, whether using Wi-Fi or through reliable mobile network coverage. Compounds are likely to offer access to their own Wi-Fi networks or satellite links. Scam compound investors sometimes own their own internet companies. For example, the Zhengheng Group, which was sanctioned by the UK and its allies in December 2023 for involvement in Cambodian scam compounds,[25] listed among its group Net1, an internet provider and cybersecurity company.[26] Net1 claimed on its website to route internet traffic through China using a submarine cable.[27] Scam companies leasing space inside compounds are sometimes offered the option of setting up contracts directly with internet providers.[28] Alternatively, they may purchase mobile data packages.[29]

Suppliers include mobile network providers and carriers, many of which advertise low-cost, high-volume data packages prominently on outer walls or in the immediate vicinity of scam compounds,[30] as well as internet service providers (sometimes offering dedicated Wi-Fi to compounds, including from Chinese providers).[31] Other suppliers include virtual private network companies that offer private business connections and satellite providers.[32]

Private cell towers are also increasingly common on the roofs of buildings, including in Cambodia and Laos, both in major cities[33] and in borderland areas and SEZs.[34] Responsibility and permissions required for constructing smaller cell towers vary by country, but decisions on where larger towers are placed are typically made jointly between government ministers and telecoms providers.[35] Compounds may be able to hire engineers to construct small tower boosters. For satellite providers, once a country or region has coverage, individual buyers (including compounds) need only buy the receiver equipment and pay a monthly subscription for access.[36]

Scam compounds may have benefited from services provided by international companies. In early 2025, a report in the Cambodian *Khmer Times* claimed that representatives had visited Cambodia and announced that the country was a priority for market expansion.[37] Thai police, according to a report in the *Thai Examiner*, also reportedly disrupted smuggling rings transporting Starlink satellite receivers for use in Golden Triangle SEZ scam compounds in April 2024[38] (and again in March 2025, according to video footage posted by MSN).[39] According to a BBC report, SpaceX, the parent company of Starlink, announced that it had taken remedial action in October 2025 by cutting Starlink satellite communication links to more than 2 500 devices used by scam compounds in Myanmar.[40]

Inconsistent solutions to transnational problems

Part of the challenge for companies trying to keep their supply chains clean – and to ensure they are not being used unknowingly by scam companies – is a lack of cohesion between different jurisdictions. For example, in 2019, the US Federal Communications Commission (FCC) introduced legislation allowing mobile network carriers to block suspected 'robocalls' based on call analytics.[41] This was followed by rules in 2021 to prevent spoofing[42] by requiring every company that calls a US number using Voice over Internet Protocol (VoIP) to adopt the STIR/SHAKEN protocol, which uses a cryptographic certificate system to verify that the number is legitimate.[43]

This should mean that any company using VoIP technology to make calls to a US number would need to register that number properly, with digital proof that they own the number they are calling from. In the absence of such proof, the number will not display a 'verified' label to reassure the recipient, and the mobile carrier can decide to block it.[44] Combined with other tracing efforts, this approach appears to have had a marked impact on reducing spoofed call attempts within the US, which fell from a high of 2.5 billion per month in February 2021 to less than 500 million per month in January 2024.[45]

However, for the system to work on international calls, all countries must comply. Otherwise, the call will pass through networks along the chain that do not participate and cannot verify legitimacy, meaning carriers either flag everything or nothing as potential fraud.[46] By June 2023, the US and Canada had fully implemented the system, while it was under development in France.[47] However, in the same month, the UK regulator Ofcom rejected proposals to implement the protocol.[48] Ofcom cited fears that it would cause disruptions for UK businesses as well as concerns that the system focused on verifying non-fraudulent calls rather than detecting fraudulent ones and tracing their source to identify criminals.[49]

The not-for-profit European Telecommunications Standard Institute is developing similar regulations to STIR/SHAKEN, tailored to the European market but with global application in mind. However, these systems can only work if they are universally standardized or at least mutually compatible and properly implemented by all carriers along the chain. ■

Critical requirement: Phone numbers

Primary sector: Telecoms

Secondary sectors: Delivery, super apps

Online scam operations generally require high volumes of unique phone numbers that can be used simultaneously to make first contact with as many potential victims as possible. This might be through phone calls or SMS or text messages, social media accounts or messaging apps like WhatsApp and Telegram.[50] Usually, a scam group will focus on acquiring phone numbers with the same country code as the target country, or the country they claim to be based in (if these differ).[51] There are two main ways to do this: either by buying virtual phone numbers through a third-party operator or by purchasing physical SIM cards from carriers in that country in bulk.

Virtual phone numbers are also used by legitimate organizations that employ a remote workforce or base call centres offshore for customer support or sales.[52] These companies typically simulate a local presence in a customer's country or state in order to build trust – much like cyber scam groups running scams and illegal gambling sites wanting to create the illusion of legitimacy and accountability.

Numbers can also be spoofed by scam companies using VoIP technologies. VoIP software converts a phone call from an analogue signal into a digital one. Calls are made and received from computers, and routed through a private branch exchange (PBX). These services configure internal phone lines within an organization. It is possible to tweak the PBX files to display the outgoing number to be anything you choose. Again, this is often used by legitimate companies to ensure that remote employees can call customers using a consistent business number. However, it also means that cyber scam groups can use this technology to convince victims they are official and legitimate.[53] Such technology can also enable a scammer to call a person from a number belonging to a family member or friend, if they are able to uncover those numbers.

Virtual phone numbers, either purchased through a third party or created using a PBX, are considerably cheaper, easier and faster to acquire than physical SIM cards. However, the Industry Traceback Group (ITG)[54] noted in January 2024 that while VoIP providers remained the most popular originators of unlawful robocalls, there had been an increase in calls from mobile networks that appeared to rely on SIM boxes,[55] likely due to increased difficulty in getting calls through to consumers. The ITG also noted in October 2023 that there had been a general shift from spoofed numbers to rotations through real (assigned) numbers (attributed to the domestic success of STIR/SHAKEN). Some of these numbers were only used once or twice before being abandoned, prompting the ITG to cite the need for a number trace mechanism to establish how illicit actors were able to acquire such a high volume of phone numbers.[56]

SIM cards (or eSIMs) originate from genuine network providers that assign the unique numbers. Various companies (especially providers to the call centre industry) sell virtual numbers that use VoIP technology to make and receive calls and messages using internet connections, but some countries restrict the ability of companies to sell virtual numbers for their country code for use overseas. SIM cards may be bought directly from vendors at markets, physical shops or in bulk online. During the research period, we found vendors on e-commerce sites like Alibaba selling UK SIM cards, for example, by the hundreds, with worldwide delivery that would then need to be fulfilled by local partners.

Critical requirement: False base stations (stingrays)

Primary sector: Telecoms

Mobile devices automatically connect to the nearest cell tower or to base stations. A false base station is a relatively new and insidious technique that mimics real network towers, so that passing mobile devices connect to them instead of real towers. The false base station can then use SMS blasters to send out mass spam or scam messages to all phones or devices connected to their network. This approach has been deployed by fraudsters using mobile units in Hong Kong[57] and Bangkok[58] to send millions of messages in a matter of days.

In Phnom Penh, Cambodia, false base stations mostly appear to operate consistently from the same locations, and there are indicators that they are used as a tool by scam compounds in the city to target potential victims passing by the towers. Given they rely on proximity and geolocation, these criminal groups do not need to go through the trouble of acquiring phone numbers. Typically, these SMS messages are written in Chinese rather than Khmer. Some messages pretend to be from companies like Telegram or contain malicious links, but most advertise illegal gambling sites with close links to the scam and forced labour industry.[59]

Concrete examples include messages advertising NagaWorld online casino that are delivered when outside NagaWorld's premises, suggesting that the SMS blaster is in the immediate vicinity of NagaWorld.[60] Other hotspots included the area around the former Phnom Penh Airport, which appeared to have been designed to target visitors arriving in the country (messages are received by both overseas numbers and local Cambodian numbers, which can be purchased as 'tourist SIMs' at the arrivals gate).[61] By November 2025, scam text operators were also targeting arrivals at the newly opened airport serving Phnom Penh.[62]

A similar situation was observed near Sihanoukville's Golden Lion roundabout, in the heart of the casino tourism area. There, only non-Cambodian numbers appeared to be targeted, suggesting the intended market is international visitors.[63] There are also unconfirmed reports that scam groups linked to a Cambodian–Australian hotel and casino developer group operates mobile units from vehicles driven around Phnom Penh.[64]

Critical requirement: Transport for workers

Related sectors: Shipping/delivery, super apps

Trafficked workers and willing employees need to be picked up from arrival points and driven between compounds if relocated or sold. In the likely case that these workers' movements are tightly restricted, transport will be arranged for them, including locally for appointments etc. For example, 'models' housed onsite to work as romantic interests in video calls need to be kept looking aesthetically pleasing for these calls. While the GI-TOC's research indicates that some models accept these roles willingly and are relatively free to leave the compound, others appear to be duped by misleading job adverts,[65] exposed to sexual exploitation,[66] and in some cases are permitted to leave the premises only for beauty treatments.[67]

Scam companies appear mostly to hire their own drivers and own or hire their own cars and vans.[68] However, researchers have observed a marked increase in the number of Chinese-owned car rental companies establishing branch offices inside existing or under-construction scam compound developments,[69] suggesting that this is a growing trend. Rental companies that hire out cars and vans or car showrooms selling these vehicles can also be sources of information. Meanwhile, luxury cars used by criminal organizations are often imported through contacts in government or security services who are exempt from high import taxes.[70]

In some cases, scam companies and compounds may also use drivers on an ad hoc basis through ride-hailing apps, or certain employees who are permitted to leave the premises may call these drivers to the premises. This underlines once again the need for broader awareness raising among people and industries potentially in contact with cyber scam operations and the importance of providing them with guidelines and points of contact for sharing their observations and data.

Critical requirement: Shipping

Primary sector: Shipping/delivery

Secondary sector: Telecoms

Real estate projects purpose-built as scam compounds will typically include extensive space for dormitory accommodation for workers.[71] However, research has found that other hotels and apartment buildings are converted according to the needs of the scam company leasing the space. This means they will likely need to bulk buy equipment, furniture, mobile phones, computer hardware and other office supplies.

Workers at scam operations, especially those tasked with finding potential scam victims, generally need to manage multiple fake personas simultaneously. Communication apps linked to phone numbers (e.g. WhatsApp, Signal and Telegram) only allow one account per device, meaning the worker needs to have a separate physical device for each such account they use. This creates high demand for dozens of mobile phones per person, as well as computers and other IT hardware needed to operate the scam out of the office (for example, hard drives, cables/adapters and multi-port chargers for phones). Depending on the type of operation, there may also be video equipment and other specialized technology.[72]

Scam companies may buy these items directly, but some equipment or infrastructure is likely to be installed by the compound owner's teams or real estate agents in advance. Moreover, devices purchased in bulk – especially from international online retailers such as Alibaba and Taobao – need to be shipped to the location by delivery partners. This has coincided with the rise of companies like ZTO, which partners with major online retailers like Alibaba and advertises fulfilment warehouses in the Chinese city of Guangzhou and Yunnan province, which has overland delivery via Vietnam or the Golden Triangle region. We documented posters detailing ZTO's delivery prices inside a temporarily abandoned scam compound in Kampot, Cambodia, in April 2023.[73] In April 2025, signs advertising ZTO services were displayed opposite the entrance to a compound on the outskirts Vientiane, Laos (on a private road serving only this compound).[74]

Compounds also tend to be evacuated periodically, with workers moved or sold to another location, creating the illusion of a meaningful crackdown before these spaces are replenished. This cycle has created a thriving trade in warehouses selling second-hand scam compound supplies.[75] At two warehouses in Phnom Penh, shop owners explained that everything they sold was originally from China. However, they acknowledged that they receive inventories (dormitory and office furniture, casino floor equipment, computer hardware etc.) from representatives of in-country 'online' companies, a commonly used local euphemism for scam and gambling operations. Interviewees suggested that these companies appear to call in a hurry as they clear out their premises. These warehouses sell disassembled bunkbeds for as little as US$35 each (and US$5 for a mattress), and they can provide around 100 beds at a time.[76] However, labels on items for sale indicated that most had initially been shipped in from overseas, predominantly China and Thailand.[77]

Critical requirement: Grocery and food delivery

Primary sector: Super apps

As noted in part one of this series, workers at scam centres are usually unable to leave the premises. This means that workers and bosses may rely heavily on food delivery apps and super apps for their daily basics, especially if they lack sufficient food or want a break from canteen food. Some of these super apps appear to have been developed exclusively for use inside a scam hub.[78] However, as discussed in the next section, data collected by other popular regional or country-specific super apps could be used to help identify scam compounds and key personnel.

WHAT DATA DO SUPPLIERS POSSESS AND WHY DOES IT MATTER?

Cutting off the supply of key products and services to criminally exposed compounds is a rapid way of disrupting scam operations, but may not be possible for practical, safety, ethical or legal reasons. However, companies that find they are unwittingly or unavoidably supplying criminal groups can still be an invaluable source of data and information.

This applies most clearly in the context of formal transnational police investigations, where sensitive personal and payment information is legally requested. However, pertinent information can also be shared with non-governmental organizations and researchers, so long as it is anonymized, non-identifiable data that reveals or corroborates broader patterns. This can be used to blow the whistle on suspicious activity, bring attention to emerging criminal hubs, or highlight changing trends in consumer demand and behaviour in the cyber scam compound and forced labour industries.

Indicators and recommendations

Data already held by utilities, telecoms, shipping/delivery companies and super apps can help disrupt the pernicious scam industry in three main ways, as set out below.

Flagging suspicious orders and improving detection models

Companies collect a wealth of data on customers that can be analyzed for suspicious patterns. Identifying red flags and building these into their order systems – or using them to train internal AI-driven detection systems – could help block suspicious orders or pinpoint developing tactics used by criminals involved in forced online criminality.

Utility companies: Dramatic surges in demand for electricity by a single customer or cluster of customers in one location (especially if the location is classed as residential or the buyer is not a business customer) may indicate that the building is densely occupied, possibly with online workers. Other suspicious electricity demand patterns include overnight increases or other indications of unusual work shifts. Additional considerations include water usage or waste that far outstrips normal occupancy for a

A view of Laos's Golden Triangle Special Economic Zone, which has been identified as a centre for cybercrime. *© STR/AFP via Getty Images*

given building. This means that private sector workers (such as refuse collectors) could theoretically provide invaluable insights and visual assessments indicating whether a building appears suspicious or whether people are unable to leave. For example, if there is an excessive security presence or very few motorbikes and other vehicles parked outside compared to the number of people that would be likely to produce the volume of refuse collected, this could indicate that the building is housing online scam workers. It is unlikely that these workers would report concerns to authorities, especially in areas where authorities provide protection to cyber scam operations, but for investigators and NGOs, collaborating with private sector actors who are amenable to cooperating to establish internal reporting mechanisms or engaging such workers directly can shed light on human trafficking patterns.

Telecoms: In remote areas that lack reliable Wi-Fi access, scam compounds may rely on data and local SIM cards from providers that offer generous data packages.[79] As described above, one tactic is to bulk-buy SIM cards from the target country to set up WhatsApp accounts on multiple mobile phones, then replace those foreign SIM cards with local SIM cards that can be topped up cheaply (while retaining the original foreign WhatsApp phone number).[80] This means that overseas orders, or large volumes of SIM cards purchased by individuals, should raise red flags for network providers, as should clusters of SIM cards from their network connecting overseas when roaming or mobile services are switched on.

Order fulfilment/shipping companies: On-the-ground research and survivor interviews since 2022 suggest that scam and illegal gambling companies rotate between different locations on a semi-regular basis (some reports suggest once every six months).[81] This often necessitates selling trafficked workers on to another company, either domestically or internationally, and clearing out their offices and dormitories for a brief period before replenishment with a new cohort or an entirely different scam company. This may be reflected in ordering, shipping or delivery patterns – especially of items that would not normally be replaced in such a short timeframe (e.g. bunkbeds, computer monitors) – to the same location in similar quantities on a semi-regular basis.

Large quantities of devices set to a language not usually in demand in the delivery location provide an indication that they will be used by a large group of foreign workers, thereby flagging the risk of trafficking and forced labour. For example, we discovered a large batch of identical Thai-language computer keyboards at a scam compound resale warehouse in Cambodia, produced by Bangkok-headquartered Signo Technology Co. Ltd.[82] This is a relatively small company whose listed online resellers and delivery partners are all Thai or South East Asia-focused. The fact that the company's entire disclosed client list consists of a relatively small and primarily local or regional set of partners suggests there could be scope for direct engagement and collaboration in finding ways to flag suspicious orders.

Super apps: Apps that offer food delivery may be able to detect unusual patterns such as a new clustering of one type of restaurant or shop in a dense area and/or a correspondingly high demand for delivery emanating from a single location (or small cluster of locations). In a high-risk location for scams and human trafficking this is often an indication that large numbers of people from a particular country or region have been placed in a particular building and may suggest they are unable to leave. If the order originates from a known scam compound, changes in order patterns likely reflect changes in the demographics of trafficking victims.

Identifying criminal actors and financial flows

Once a scam compound has already been identified or is under investigation, data held by its suppliers could be vital in unmasking who wields executive power at this location, who owns or leases the property, and in identifying other criminal actors based at or linked to the location.

While sharing personal information on specific individuals is likely to require an official police request or subpoena, all categories of providers covered in this report will hold identifying data on their users (e.g. verified identities, phone numbers linked to addresses and payment information). This could help identify actors operating inside compounds and/or disrupt criminal activity, especially when this information is cross-referenced with data linked to bank accounts and cryptocurrency wallets.

Utilities: Utility companies need to bill their customers, whether personal or corporate, which means that they will have a name and payment information on file linked to addresses identified as scam compounds.

Telecoms: Many countries have legislation in place requiring SIM cards to be registered to individuals using photo identification (a passport or driving license). They may also restrict the number of SIM cards one person can buy/register.[83] Collecting this information is typically the responsibility of the network provider. Even if not mandated to do so, it is likely that the phone company will have payment details on file for any data plans or top-ups that can be used to identify the owner of a phone number either linked to scam activity or connecting to a cell tower in a known scam compound location.

Furthermore, cryptocurrency wallets are generally linked to phone numbers, and access to any online service necessitates an internet provider and an IP address. This means that network providers and internet service providers may be able to provide or corroborate vital information linking illicit financial flows in cryptocurrencies to specific people or locations. High-level suppliers to compounds – such as telecom companies that physically construct rooftop cell towers – are best placed to identify the contract holder and thus the compound owner (or, at the very least, the individuals who negotiated the service and manage this on the owner's behalf).

Order fulfilment/shipping companies: E-commerce sites and large-scale shipping companies tend to expect payment in advance instead of accepting cash on delivery. This means that they will likely have a real name or company name associated with the payment method used, which can help identify buyers. Even when an order is placed with an online retailer rather than the shipping company itself, e-commerce sites typically share customer data with logistics, delivery and fulfilment partners for functional and data analytics purposes.[84]

Super apps: Online orders may be made through delivery and super apps (linked to bank accounts, cards, names and addresses). Data on clients of delivery and super apps, including real names, account details and payment information, will be held by these service providers. Casino investors and scam compound owners often develop their own fintech and super apps to address this issue (or for exclusive use inside the compound development), creating an extra wall between the scam company and external financial systems. These super apps may also be designed specifically to facilitate cryptocurrency transactions, especially to switch between holdings in Tether[85] and fiat currencies without interacting directly with banking systems. However, scam compound owners may try to make these apps compatible with established banking or super apps, including to pay bills (such as utilities) directly, creating points of interaction with suppliers where personal information is again potentially visible.

Tracing criminal activity to specific scam compounds

Customer and order data collected by companies that supply scam compounds could be used to identify criminal actors and connect the dots between online criminal activity and specific locations. By monitoring patterns and changes in demand, this could act as an early warning system, providing insights into where scam compounds are likely to move next.

Utilities: High-level analysis of changing patterns in utilities demand – including water, electricity and demand for waste collection – could provide vital evidence to help confirm whether a compound that had been ordered to close following a raid has reopened. Such analysis could also provide intelligence on which locations were at full capacity and when, while also corroborating timelines provided by survivors of human trafficking detailing when they were sold and transferred between locations.

Telecoms: International phone companies and network providers route calls, including international calls and those made using VoIP technology, to their ultimate destination. Tracing back to the root of a scam call means jumping through a number of 'hops' – points at which call traffic is re-routed through different providers to avoid being flagged en route to its final destination.[86] The ITG reported that private-led efforts successfully traced 3 737 numbers in 2023 (each with the capacity to make millions of calls) to 699 providers, with an average of 5.9 hops per traceback.[87] This can be a painstaking process, but it means that network providers working collaboratively can trace a scam call all the way from its end receiver to the initial cell tower. This can link a particular scam to a specific compound, strengthening a fraud case against an existing operator or potentially pin-pointing a new location altogether.

Order fulfilment/shipping companies: Mobile devices and SIM cards purchased in bulk, especially from major international online retailers, need to be physically brought to the location by delivery partners in-country. Depending on how comprehensive their databases are, order fulfilment companies may have records of the specific SIM cards (i.e. with phone numbers) or international mobile equipment identity (IMEI) numbers of mobile devices they sent or delivered to a particular location. If these numbers are later flagged as fraudulent – or device data such as an IMEI number is captured

by investigators into scams – order fulfilment and shipping companies could cross-reference this with their delivery histories to check whether they delivered these items (and to where/whom).

Super apps: Building on the ability to detect patterns in restaurant types and demand dynamics concentrated in one location, these delivery apps could go a step further by creating ways for their workers to report concerns.

Researchers have observed a strong presence of taxi and *tuk-tuk* drivers based outside scam compounds across South East Asia.[88] Often these drivers act as spotters or an extra layer of security for compounds, including by alerting compound staff to people they do not recognize,[89] trailing unfamiliar vehicles that pass close to compounds,[90] or intimidating unwelcome visitors when they approach.[91] However, amenable drivers based in locations where they witness people coming in and out of compounds, or who are regularly hired to make pick-ups and drop-offs at compounds, often provide intelligence that proves invaluable to investigations into a specific compound and/or locations connected to it.[92] These drivers typically work for one or more ride-hailing apps, meaning that, in some cases, journey, location and user data will be recorded on the app's servers.

CONCLUSION

Companies at risk of acting as suppliers to scam compounds can play a crucial role in disrupting this criminal economy in three key ways:

- Companies should incorporate forced criminality into their existing policies on human trafficking and ethical business practices, in a way that empowers employees at all levels to flag concerns through internal reporting systems. This includes acknowledging common indicators of scam compounds and illicit activity, and incorporating this into training and company policies.
- Companies should enhance training of their internal machine-learning models to recognize red flags, suspicious orders and patterns that suggest that new scam compounds may be emerging. If they have sufficient resources, companies may wish to analyze this data themselves to produce in-house reports or documentation showing emerging patterns and trends. Alternatively, they could commit to collating and anonymizing raw data and making this available to researchers, journalists, and non-governmental and civil society organizations to help map and pre-empt the spread of scam compounds to new locations.
- Companies can contribute to the cyber scam response by engaging with broader information-sharing mechanisms wherever possible within their industries and across sectors, and by complying with data-sharing requests and subpoenas from law enforcement and legal teams relating to customer data linked to scam compounds. This may also require advocating for clearer guidelines in jurisdictions where they operate.

However, using this data effectively to tackle the crisis will also require the input of governments, corporate registries, international policing bodies and civil society. Companies need regulation that enables them to share data where possible and to clarify where and when they can decide to deny service to potential criminal operations. Careful analysis is needed to identify orders of product types and quantities that are clearly intended for criminal activity so that these can be flagged.

Flagging procedures would have similarities to the way in which large volumes of potentially criminally intended combinations of products in the pharmaceutical industry are required by the US Drug Enforcement Administration to trigger suspicious order monitoring alerts.[93] Utility companies and mobile network providers should engage in ongoing dialogue with government ministers to highlight risk areas for scam compounds and devise plans for rolling out coverage to people who need it, without inadvertently facilitating criminals.

Ultimately, tackling corruption, exploitation and criminal exposure in transnational supply chains requires transnational action. For efforts to succeed, governments across the Association of Southeast Asian Nations, China and beyond need to agree on policies for monitoring, information sharing and enforcement. Without multi-jurisdictional policy cooperation, scam companies will simply seek out new supply routes and continue to grow and adapt.

NOTES

1 A super app is a single application that integrates several services, such as e-commerce, fiat payments and cryptocurrency transactions, on the same online platform.
2 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia.
3 Fieldwork, Phnom Penh, Cambodia, February 2025.
4 An example of one such organization is the Industry Traceback Group; see: https://tracebacks.org.
5 James Reddick, Thailand cuts power to Myanmar scam hubs, The Record, 5 February 2025, https://therecord.media/thailand-cuts-power-scam-compounds-myanmar.
6 Lulu Luo and Jonathan Head, The shadowy Chinese firms that own chunks of Cambodia, *The Guardian*, 25 September 2023, https://www.bbc.co.uk/news/world-asia-66851049.
7 Fieldwork by GI-TOC researchers, Bokor Mountain, Kampot, March 2025 and various locations in Laos, April 2025.
8 James Reddick, Thailand cuts power to Myanmar scam hubs, The Record, 5 February 2025, https://therecord.media/thailand-cuts-power-scam-compounds-myanmar.
9 Fieldwork trips in the Mekong areas of Laos and Koh Kong province, Cambodia, 2022 to 2025.
10 Inclusive Development International, Botum Sakor coal power plant, The People's Map of Global China, 1 March 2022, https://thepeoplesmap.net/project/botum-sakor-coal-power-plant/.
11 Prachatai, Thailand cuts power to Myanmar's scam hubs. But will it make a difference?, 10 February 2025, https://prachataienglish.com/node/11302.
12 Kocha Olarn and Ross Adkin, Power cut to site of global, billion-dollar scam industry. But will it halt the swindling?, CNN, 5 February 2025, https://edition.cnn.com/2025/02/05/asia/myanmar-thailand-scam-power-cuts-intl-hnk/index.html.
13 RFA Burmese, Thailand's power and fuel cuts hurting ordinary Myanmar residents, 11 March 2025, https://www.rfa.org/english/myanmar/2025/03/11/myanmar-thailand-fuel-price-spike/.
14 *The Nation*, PEA clarifies on supply of electricity to border areas of neighbouring countries, 29 January 2025, https://www.nationthailand.com/news/general/40045695.
15 Supasit Boonsanong et al, Electricity regulation in Thailand: Overview, Practical Law Country Q&A, Thomson Reuters, August 2019, https://www.tilleke.com/wp-content/uploads/2019/09/Tilleke-Gibbins-Electricity-regulation-in-Thailand-overview.pdf.
16 *The Nation*, PEA clarifies on supply of electricity to border areas of neighbouring countries, 29 January 2025, https://www.nationthailand.com/news/general/40045695.
17 Fieldwork, Bokor Mountain, Kampot, March 2025.
18 Fieldwork, Dara Sakor, March 2025.
19 Fieldwork, Boten SEZ, April 2025.
20 *The Vientiane Times*, PM gives advice on development of Boten SEZ, 26 September 2023, https://www.vientianetimes.org.la/freefreenews/freecontent_187_PM_gives_y23.php.
21 Fieldwork, Bokor Mountain, Kampot, March 2025.
22 Hong Raksmey, Exploring the natural wonders of Bokor, *The Phnom Penh Post*, 5 June 2024, https://web.archive.org/web/20240605043614/https://www.phnompenhpost.com/travel/exploring-the-natural-wonders-of-bokor.
23 Fieldwork, Boten SEZ, April 2025.
24 Fieldwork, Jinshui and 'China Town', Sihanoukville, April 2023.
25 UK Government, Office of Financial Sanctions Implementation, Financial sanctions notice, HM Treasury, 8 December 2023, https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf.
26 Archived version of the now deleted Zhengheng Group website on the Internet Archive, May 2023, https://web.archive.org/web/20230528034435/http://zhgroup.com.kh/en/.
27 Archived version of the Net1 website on the Internet Archive, June 2023, https://web.archive.org/web/20230609115628/https://net1.com.kh/.
28 This was explained to the authors during an undercover tour of a mixed-use scam compound and apartment building in Phnom Penh, January 2025.

29 Interview with a trafficking survivor from a compound in Chrey Thum, Cambodia, January 2025.
30 Fieldwork at various locations in Cambodia and Laos, January to April 2025.
31 Examples of Chinese modems were seen in one mixed-use complex housing apartments and a scam compound in Phnom Penh visited by GI-TOC researchers in February 2024.
32 According to reporting by The Record from Recorded Future News, a Thai law enforcement unit confiscated Starlink satellite internet transmitters in Myanmar. As with many widely sold connectivity products, there is no suggestion that the manufacturer controlled or knew about the end use of these devices. The operation was carried out by the Thai Army's Ratchamanu Task Force. See James Reddick, Thai officers intercept Starlink transmitters allegedly headed to Myanmar scam compounds, The Record, 24 March 2025, https://therecord.media/thai-officers-intercept-starlink-transmitters-myanmar-cyber-scam-compounds.
33 Fieldwork in Phnom Penh, February 2025.
34 Fieldwork in Boten, April 2025, and Bavet, April 2024.
35 The Better Cambodia, Cambodia's plan for nationwide internet and digital transformation by 2027, 6 February 2025, https://thebettercambodia.com/cambodias-plan-for-nationwide-internet-and-digital-transformation-by-2027/.
36 Kinza Yasar, Starlink, TechTarget, 7 October 2024, https://www.techtarget.com/whatis/definition/Starlink.
37 *Khmer Times*, Starlink – SpaceX says Cambodia is a priority among its tech targets in 2025, 21 February 2025, https://www.khmertimeskh.com/501643386/starlink-spacex-says-cambodia-is-a-priority-among-its-investment-targets-in-2025/.
38 James Morris and Son Nguyen, Scammer's plan to use SpaceX Starlink satellites in transnational scam network targeting Thailand with deception, 14 April 2024, https://www.thaiexaminer.com/thai-news-foreigners/2024/04/14/plan-to-use-spacex-starlink-satellites-in-world-scam-network-thai-laos-mekong-border/.
39 Newsflare, Chinese 'scammer' caught with 38 boxes of Elon Musk Starlink satellite dishes in Thailand, MSN, March 2025, https://www.msn.com/en-gb/video/viral/chinese-scammer-caught-with-38-boxes-of-elon-musk-starlink-satellite-dishes-in-thailand/vi-AA1BDNAH.
40 Jonathan Head and Rachel Hagan, SpaceX says it has cut Starlink services to Myanmar scam camps, BBC, 22 October 2025, https://www.bbc.co.uk/news/articles/cpd2e5541d1o.
41 Nillay Patel, Robocalls now get blocked by your carrier by default, The Verge, 6 June 2019, https://www.theverge.com/2019/6/6/18655334/robocalls-blocked-default-carrier-providers-fcc-ajit-pai.
42 Ofcom, Number spoofing scams, 16 January 2023, https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/phone-spoof-scam.
43 ATIS-SIP Forum IP-NNI Task Force, Shaken: Frequently asked questions, August 2020, https://sti-ga.atis.org/wp-content/uploads/2020/08/shaken-faq.pdf.
44 Ibid.
45 Industry Traceback Group, Letter addressed to the secretary of the FCC, 1 May 2024, https://www.fcc.gov/ecfs/document/105010043202095/1.
46 Katia Gonzalez, Thinking beyond STIR/SHAKEN: What can enterprises do today to fight robocalls?, BICS, 17 August 2023, https://bics.com/blog/blog-robocalls-stir-shaken/.
47 Ibid.
48 Industry Traceback Group, Letter addressed to the secretary of the FCC, 1 May 2024, https://www.fcc.gov/ecfs/document/105010043202095/1.
49 Ibid.
50 Based on dozens of interviews by the authors with people who survived being trafficked to scam compounds in South East Asia and the UAE between 2022 and 2025.
51 Ibid.
52 Toni Matthews-El and Rob Watts, What is a virtual phone number and how does it work?, Forbes, 29 May 2024, https://www.forbes.com/advisor/business/software/what-is-a-virtual-phone-number/.
53 Correy Cummings, Vishing, Wangiri and other VoIP fraud tactics on the rise, Tech Republic, 19 November 2024, https://www.techrepublic.com/article/voip-fraud/.
54 Industry Traceback Group is a private company appointed by the US FCC to manage tracebacks into illegal robocalls.
55 Industry Traceback Group, Letter addressed to the secretary of the FCC, 1 May 2024, https://www.fcc.gov/ecfs/document/105010043202095/1.
56 Joshua M Bercu, Prepared testimony to the Senate Committee on Commerce, Science & Transportation, Hearing on protecting Americans from robocalls, 24 October 2023, https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181.
57 Eric Priezkains, SMS blaster smishing fraudster arrested in Hong Kong, Comms Risk, 24 February 2025, https://commsrisk.com/sms-blaster-smishing-fraudster-arrested-in-hong-kong/.
58 Eric Priezkains, Police find SMS blaster that sent a million smishing messages in 3 days, Comms Risk, 22 November 2024, https://commsrisk.com/police-find-sms-blaster-that-sent-a-million-smishing-messages-in-3-days/.
59 Monitoring and analysis of scam text examples compiled by the authors in Cambodia, January to May 2025.
60 Evidence for this was provided in scam text messages received by the authors outside the NagaWorld casino complex, Phnom Penh, March 2025.
61 Fieldwork in Phnom Penh, January to March 2025.
62 Fieldwork in Phnom Penh, November 2025
63 Fieldwork in Sihanoukville, March 2025

64 Intelligence from police source, Phnom Penh, March 2025.
65 Analysis of job advertisements posted on Telegram channels, January to May 2025.
66 GI-TOC, Compound crime: Cyber scam operations in South East Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.
67 Information provided by a beautician whose customers include a number of scam compound models, Cambodia, May 2024.
68 Based on fieldwork at scam hubs in Cambodia and multiple interviews with survivors of forced online criminality in South East Asia and the UAE conducted between 2022 and 2025.
69 Field research in various locations across Cambodia, January to March 2025.
70 Information provided by a police source in Phnom Penh, February 2025.
71 GI-TOC, Compound crime: Cyber scam operations in South East Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.
72 Based on multiple interviews with survivors of forced online criminality conducted between 2022 and 2025.
73 Fieldwork, Bokor Mountain, Kampot, April 2023.
74 Fieldwork, Vientiane, April 2025.
75 Visits to warehouses that supply second-hand goods to scam compounds near Phnom Penh, March 2025.
76 Ibid.
77 Ibid.
78 Danielle Keeton-Olsen and Mech Dara, Rescue reveals scam compound at Koh Kong's UDG, VOD, 24 August 2022, https://vodenglish.news/rescue-reveals-scam-compound-at-koh-kongs-udg/.
79 Interview with Filipino trafficking survivor held in Chrey Thum, Phnom Penh, January 2025.
80 Ibid.
81 Interviews with various survivors, 2023 to 2025.
82 See Pro Series Signo, https://www.signo-technology.com/product/166.
83 James Whitehead, TRC tightens control on SIM card vendors, *Khmer Times*, 10 May 2024, https://www.khmertimeskh.com/501485835/trc-tightens-control-on-sim-card-vendors/.
84 Arkadiusz Kawa and Justyna Swiatowiec-Szczepańska, Logistics as a value in e-commerce and its influence on satisfaction in industries: a multilevel analysis, *Journal of Business & Industrial Marketing*, December 2021, https://www.emerald.com/insight/content/doi/10.1108/jbim-09-2020-0429/full/html#abstract.
85 Tether is a stablecoin that is pegged to the US dollar at a rate of 1:1. This cryptocurrency has been widely exploited by criminals for money laundering purposes in jurisdictions around the world. See Oliver Bullough, How Tether became money-launderers' dream currency, *The Economist*, 4 July 2025, https://www.economist.com/1843/2025/07/04/how-tether-became-money-launderers-dream-currency.
86 Joshua M Bercu, Prepared testimony to the Senate Committee on Commerce, Science & Transportation, Hearing on protecting Americans from robocalls, 24 October 2023, https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181.
87 Industry Traceback Group, Letter addressed to the secretary of the FCC, 1 May 2024, https://www.fcc.gov/ecfs/document/105010043202095/1.
88 Field research in Cambodia, Laos and the Philippines, 2022 to 2025.
89 Field research in Vientiane, April 2025.
90 Field research in Bavet, April 2024.
91 Field research in Sihanoukville, May 2023.
92 Field research in Cambodia, Laos, Philippines, Mae Sot–Myawaddy border (Thailand) and the UAE, 2022 to 2025.
93 US Department of Justice, Drug Enforcement Administration, Diversion Control Division, https://www.deadiversion.usdoj.gov/about-us.html.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net