Humanity Research Consultancy | Local insights, global impact

The Scam Compounds Brief Special Issue

Mapping the Global Expansion of Chinese-speaking Scam Syndicates, 2010–2026

Mina Chiang | August 2026

Humanity Research Consultancy | Local insights, global impact

The Scam Compounds Brief – Special Issue

Mapping the Global Expansion of Chinese-speaking Scam Syndicates, 2010–2026

About this Brief

The Scam Compounds Brief is an ongoing analytical series by Humanity Research Consultancy (HRC) that examines the evolution of transnational criminal networks, primarily Chinese-speaking syndicates, operating scam facilities. Each issue identifies emerging operational patterns, enforcement actions, and structural shifts across affected jurisdictions.

By drawing on open-source intelligence — including content from niche social media platforms — the brief translates and contextualises information that is often inaccessible to international audiences. The series periodically synthesises broader trends and surfaces specific leads that may not be fully documented elsewhere. This provides unique insight into the shifting dynamics of the online scam industry. The brief aims to promote greater visibility and scrutiny, equipping governments, law enforcement, researchers, and civil society with the evidence needed to address these evolving threats.

How to cite this publication

Chiang, M. (2026, August). *Mapping the Global Expansion of Chinese-speaking Scam Syndicates, 2010–2026*. Humanity Research Consultancy.

Sources and verification note

This briefing draws on official statements, open-source reporting, court judgments, and monitored online channels, including Chinese-language sources and closed messaging platforms. Where information cannot be independently verified, it is indicated as reported or alleged. Identifying details are removed to protect individuals at risk.

Notice on access to sensitive content

For security and ethical reasons, direct links to social media posts that may indicate criminal activity are not published in this brief. Such materials can be made available upon request to law enforcement authorities or accredited researchers, subject to appropriate verification of credentials.

Humanity Research Consultancy | Local insights, global impact

Content

Note: Although the title covers the period 2010–2026, the year 2026 was still ongoing at the time of writing. This report seeks to include as many publicly documented cases as possible up to mid-August 2026. Additional significant cases may emerge during the remainder of the year and are therefore not reflected in this edition.

Introduction

As law enforcement pressure on scam compounds has intensified across Southeast Asia, increasing attention has been paid to reports of scam operations emerging in new regions. Much of the recent discussion has described this trend as the start of expansion of scam compounds beyond Southeast Asia. While this reflects genuine concerns about the international spread of these criminal networks, such characterisation risks oversimplifying both their history and their organisational evolution.

By documenting historical and contemporary cases from 2010 to 2026, this report provides a chronological overview of the global footprint of Chinese-speaking scam syndicates and offers a framework for understanding both the continuity and transformation of their overseas operations.

This report seeks to make three contributions.

First, it demonstrates that the overseas expansion of Chinese-speaking scam operations is not a new phenomenon. The cases documented in this report show that Chinese-speaking syndicates have established scam operations overseas for at least 16 years, long before the emergence of the large-scale scam compounds associated with Cambodia and Myanmar. The recent appearance of scam operations in new jurisdictions should therefore be understood as part of a much longer pattern of transnational criminal expansion rather than an entirely new development. By 2017, the Chinese government claimed that scam operations of various sizes, established by Taiwanese and Chinese nationals, had been identified in at least 40 countries, primarily targeting Chinese-speaking victims.[1]

Second, this report argues that describing recent developments simply as the expansion of scam compounds can be misleading. Although Chinese-speaking scam syndicates are increasingly exploring new jurisdictions, most documented overseas operations follow an “outpost scam model” orchestrated by a single leadership team, rather than the multi-tenant landlord–tenant industrial park model characteristic of scam compounds. This distinction is important because the two models are enabled by fundamentally different operational logics. Outpost scam operations are typically smaller and may be harder to detect, but they are often easier to dismantle once identified. In contrast, scam compounds are larger, purpose-built criminal ecosystems that are more visible yet considerably harder to address due to their entrenched infrastructure and frequent protection from corrupt political elites and security forces. Nevertheless, there are growing signs that criminal groups are attempting to replicate the broader scam compound ecosystem in selected countries.

[1] https://www.mps.gov.cn/n2255079/n5590589/n5747791/n5778470/c5772552/content.html

Table 1. Law Enforcement Implications of the Outpost Scam Model and Scam Compound Model

Scam outpost model	**Scam compound model**
Financial investigations are generally more straightforward, as evidence typically relates to a single scam organisation. However, the same leadership may operate multiple outposts across one or more jurisdictions.	Investigations often uncover multiple scam companies with different lifespans, scam methods, and target victims operating within the same compound.
Fewer resources and personnel are typically required for a single raid due to the small scam operations (e.g. villas, apartments, offices, hotels).	Raids require substantial law enforcement resources due to the large scam operations. Accountability should extend beyond scam operators to compound owners and facilitators.
Harder to detect due to their small scale and concealed nature, but generally easier to dismantle once identified.	Easier to identify but harder to dismantle due to infrastructure and protection from corrupt political elites. Sanctions, diplomatic engagement, and accountability for enabling actors may be necessary to sustain enforcement outcomes.
Since at least 2010 (and continuing).	Emerged at scale from around 2020, with signs of expansion into new jurisdictions.

Third, the historical cases documented in this report point to two possible explanations that deserve further research. Several countries hosted Chinese-speaking scam operations before the COVID-19 pandemic but have no publicly reported cases after 2020. One explanation is that criminal groups have tested different jurisdictions over time and moved away from countries with stronger law enforcement responses. Another is that scam operations continue to exist in some countries but remain undetected because of limited local enforcement, reporting, or public disclosure. It is also worth noting that many early overseas scam operations were uncovered only through coordinated multinational investigations rather than locally initiated law enforcement efforts (e.g. the January 2018 cases in the Czech Republic, Poland, and Slovenia). By documenting both historical and recent cases, this report aims to present a more complete picture of the long-term and global footprint of Chinese-speaking scam syndicates.

This report is structured with a high-level analysis and discussion of limitations, followed by country profiles covering 45 countries. Readers are encouraged to read the analytical sections first and then use the country profiles strategically, for example by using the search function (e.g. Ctrl+F) to quickly locate specific countries and cases of interest.

Analysis

The Long History of Operating Overseas

Chinese-speaking scammers have operated overseas for at least 16 years. This report identified scam operations in at least one-fifth of the world's countries since as early as 2010, demonstrating that cross-border relocation is not a recent phenomenon. However, the scale of these operations varied considerably. Most early overseas scam sites operated from rented villas, apartments, or office buildings and typically involved dozens to hundreds of scammers under a single management structure.

Even during this early period, however, these operations were already connected through transnational criminal networks. Large joint enforcement actions illustrate that scam syndicates operated across multiple jurisdictions. In the "3.10" operation in 2011, police from China, Taiwan, Cambodia, Indonesia, Malaysia, and Thailand arrested 598 suspects and dismantled 106 scam sites operated by a single transnational scam syndicate. The suspects included 410 Taiwanese and 186 Chinese nationals, and the reported losses exceeded RMB 70 million (approximately USD 11 million in 2011).[2]

Similarly, the "9.28" operation in 2011 involved networks spread across eight Southeast Asian countries, including Indonesia, Cambodia, the Philippines, Vietnam, Thailand, Laos, Malaysia, and Singapore. Authorities dismantled 162 sites, arrested 828 suspects, including 532 Chinese, 284 Taiwanese, and 12 other nationalities, and linked the networks to approximately RMB 220 million (approximately USD 34 million in 2011) in losses.[3]

The Involvement of Forced Criminality Since 2015

Some reports have suggested that the widespread use of human trafficking, forced labour, and slave labour emerged only with the rise of scam compounds after 2020. However, the cases documented in this report demonstrate that these practices can be traced back to at least 2015. Some early overseas scam operations were already characterised by deceptive recruitment (e.g. the October 2015 case in Indonesia), passport confiscation (e.g. the July 2016 case in Greece), poor living conditions, excessively long working hours (e.g. the August 2015 case in Australia), and restrictions on workers' freedom of movement. Nevertheless, the available evidence suggests that these earlier operations generally involved lower levels of violence and sometimes continued to pay workers, albeit under coercive conditions.

The emergence of large-scale scam compounds marked a significant escalation in both the scale and severity of abuse. Testimonies increasingly describe systematic violence, including frequent use of

---

[2] https://www.chinanews.com/shipin/2011/06-15/news39912.html
[3] https://web.archive.org/web/20210903122258/http://www.gov.cn/jrzg/2011-09/28/content_1958955.htm

electric shocks, severe beatings, prolonged detention, torture, and deaths. This escalation may be linked to the compound management model itself. Unlike the earlier outpost scam model, companies operating within scam compounds typically rely on compound management to control workers' movements through armed guards, high perimeter walls, barred windows, and other physical security measures.

The landlord-tenant structure therefore enables scam companies to outsource confinement and coercion while concentrating on maximising fraud operations. It also creates an environment of impunity. Tenant companies can employ extreme violence to discipline workers with relatively little concern about escape or law enforcement intervention, as compound management typically arranges political protection and corruption to shield the compound from external scrutiny.

From Telephone to Internet-Based Fraud

Chinese-speaking scam syndicates have continuously adapted their operating methods. Early operations primarily relied on telecommunications fraud, for example, using phone calls to impersonate government officials or telecommunications providers. This model depended heavily on voice conversations, making it easier to target victims who spoke the same language and shared similar cultural contexts. Over the past decade, however, criminal groups have increasingly shifted to internet-based fraud, including investment scams, romance scams, cryptocurrency fraud, fake online gambling, and other social media-enabled schemes.

The Globalisation of Victim Targeting

As the ringleaders of these syndicates are predominantly Chinese-speaking, China and Taiwan were the earliest and most significant targets of their operations. For years, scammers primarily targeted victims who shared the same language and cultural background before expanding overseas. The first wave largely focused on victims in China and Taiwan, while a second wave increasingly targeted Chinese diaspora communities, prompting Chinese police, embassies, and consulates around the world to issue repeated warnings about scams impersonating Chinese police, embassies, and other authorities.[4] In 2016, Chinese public security authorities nationwide filed 630,000 telecom fraud cases, resulting in economic losses of RMB 18 billion (approximately USD 2.7 billion, at the 2016 average exchange rate). That same year, police cracked 83,000 telecom and internet fraud cases and apprehended 34,000 suspects.[5]

The subsequent shift from telephone-based fraud to internet-enabled scams significantly accelerated this internationalisation. Unlike voice calls, online messaging allows scammers to rely on translation software, AI-assisted tools, and scripted conversations, removing the need to speak the victim's

[4] See, for example, https://gaj.cq.gov.cn/sy_245/bmdt/202505/t20250516_14627394.html
[5] https://www.mps.gov.cn/n2255079/n5590589/n5747791/n5778470/c5772552/content.html

language fluently or conceal a foreign accent. This has lowered the barriers to targeting victims worldwide and enabled Chinese-speaking scam syndicates to diversify far beyond the Chinese-speaking community.

At the same time, scam operations now draw workers and trafficking victims from at least 80 countries, while Chinese-speaking actors continue to predominate among identified ringleaders.[6] The nationalities of scam workers correspond to the target markets they are assigned to, allowing syndicates to exploit native language skills and cultural familiarity to improve the credibility and effectiveness of their scams.

Table 2. The Globalisation of Chinese-speaking Scam Syndicates

	Ringleaders	**Scam workers (voluntary and involuntary)**	**Primary target victims**
Historical (pre-2020)	Predominantly Chinese-speaking, including Chinese and Taiwanese nationals	Predominantly Chinese-speaking, with occasional recruits from other Asian countries	Predominantly Chinese-speaking victims, including those in China, Taiwan, and the Chinese diaspora
Present	Predominantly Chinese-speaking, although ringleaders from other Asian countries are increasingly adopting the model	Individuals from at least 80 countries, including both willing participants and victims of human trafficking	Global

Demography of the Suspects

Both male and female suspects were identified across many documented operations. Men consistently accounted for the majority of those arrested, though exceptions exist (e.g. The September 2011 case in Laos). Notably, the ringleaders and senior managers identified in court judgments and law enforcement investigations were overwhelmingly male.

The majority of identified suspects were between 20 and 40 years old, reflecting the industry's demand for digitally literate and working-age adults. However, notable exceptions were documented. In recent years, law enforcement agencies have increasingly identified underage individuals in scam operations, suggesting that criminal groups are expanding recruitment to younger age groups.[7] Owing to limited demographic information in many official reports, the full age profile of those involved remains unclear.

---

[6] https://www.iom.int/explainer/key-facts-human-trafficking-online-scam-operations

[7] See, for example: https://www.twreporter.org/a/human-trafficking-scam-gangs-and-violence-juvenile-delinquency

The Organisational Model

The defining feature of recent years is not the overseas movement of scammers, but the emergence of the scam compound model. Unlike earlier operations, scam compounds host multiple scam "companies"[8] under different leaderships, sharing office space, accommodation, and infrastructure. This organisational model was particularly noticeable in Cambodia, Myanmar, Laos, Philippines, Dubai after 2020. Earlier overseas scam operations were overwhelmingly organised under a single leadership team.

Notably, although early overseas scam operations were typically organised under a single leadership rather than the later compound model, individual scam sites were often components of wider criminal networks. A single syndicate could operate multiple scam sites simultaneously within the same country or across different jurisdictions, sharing recruiters, managers, logistics, and money laundering channels. For example, in Australia, Taiwanese ringleaders operated scam call centres from two separate luxury houses in Brisbane (Morningside and South Brisbane) that were not physically connected but functioned under the same criminal organisation.[9] The later emergence of the scam compound model therefore represented a shift in organisational efficiency and scale, rather than the beginning of multi-site or transnational coordination among Chinese-speaking scam syndicates.

In almost every jurisdiction where scam operations expanded into industrial-scale compounds employing thousands of workers, credible reporting has documented systemic corruption, or collusion between criminal groups and local elites. This suggests that while scammers can operate almost anywhere, the development of the scam compound model depends on an enabling political and governance environment.

Table 3. Comparison between the scam outpost model and the scam compound model

	Scam outpost model	**Scam compound model**
Strategy for evading law enforcement	Operates covertly, frequently relocates, and seeks to avoid attracting attention from neighbouring communities.	Relies on protection from compound owners, who often ensure local political elites benefit from scam profits. Operations are therefore more overt and less reliant on concealment.
Scale of operations	Typically dozens to hundreds of scammers at a single site.	Hundreds to tens of thousands of workers within a single compound from multiple scam companies.

[8] The company structure is how scam bosses usually present themselves to their workers, often with company names, employment contracts and clear commission systems, although the actual treatment might differ significantly from the promises. Some might have official registration records in certain jurisdictions, while the majority do not.
[9] https://mil.sina.cn/zgjq/2016-04-19/detail-ifxriqqx3038078.d.html?vt=4

Type of premises	Usually operates from a single apartment, villa, or other private property (e.g. former embassy buildings as in the November 2023 case in Malaysia). Property owners may have little or no knowledge of the scam operations.	Purpose-built or converted industrial park. Onsite facilities typically include offices, dormitory, restaurants, brothels, and in some cases, torture chamber and incinerators[10]. Compound owners, or the landlords, are generally aware of the criminal activities. Compounds typically contain multiple buildings or a large multi-storey building accommodating numerous scam companies.
Human trafficking, forced criminality, and violence	Exploitation and coercion occur, but violence tends to be less systematic, likely due to the smaller organisational structure and fewer guards.	Human trafficking, forced criminality, and violence are common. Layered management structures and dedicated security personnel enable more systematic coercion and control over workers. Political protection enables impunity to crime.
Firearms	Less commonly encountered.	Frequently recovered.
Scam types	Usually specialises in a single scam method under one leadership.	Multiple scam methods often operate simultaneously, as different scam companies under separate leadership rent space within the same compound.

Expansion by Seasoned Cybercrime Organisers

Several cases documented in this report suggest that new scam operations are often established by seasoned cybercrime organisers rather than newcomers. For example, the Lixin Group expanded from Cambodia to Georgia; the ringleader of the North Macedonia operation had previously established scam centres in Japan, the Netherlands, Montenegro, and Türkiye; a joint Dubai-Armenia recruitment advertisement promoted a "very mature operating model"; and testimonies from Malaysia (Forest City), Vietnam, Pakistan, Uganda, and Madagascar described workers and managers who had previously worked in scam operations elsewhere.

From Authority Impersonation to the Chinese Romance-Investment (Pig-butchering) Scams

Early overseas operations documented in this report were dominated by authority impersonation scams and online gambling scams targeting Chinese-speaking victims. By contrast, pig-butchering scams

[10] See, for example: https://www.taisounds.com/news/content/88/220553. The existence of incinerators in some scam compounds was also confirmed privately to HRC by Cambodian local legal professionals.

became increasingly prominent from around 2019 onwards. The significance of this shift is reflected in the fact that "pig-butchering scam" (杀猪盘) was selected as one of China's Top Ten New Media Buzzwords of 2019.[11]

By 2019, "pig butchering" scams had become one of the most damaging forms of online fraud in China. Between January and August 2019, these scams caused losses of RMB 3.88 billion (USD 550 million), accounting for 21.3% of all financial losses from telecommunications and online fraud nationwide.[12] The average loss per victim was RMB 181,000 (USD 26,000), approximately 4.8 times higher than the average loss across other fraud types.[13]

Table 4. Traditional Romance Scam vs. "Pig Butchering" Scam

Feature	Traditional Romance Scam	"Pig Butchering" Scam (Sha Zhu Pan)
Core Pretext	The scammer asks for direct financial help using excuses like sudden medical emergencies, travel costs, or legal trouble.	The scammers typically guide victims towards fraudulent investment, crypto, forex, or gambling platforms.
Operational Model	Usually operated by individuals or small, loosely organised groups.	Highly industrialised. Run by massive syndicates with psychological scriptwriters, dedicated IT teams, professional customer service, and money-laundering networks.
Psychological Tactics	Relies purely on emotional attachment and guilt; usually a slower build-up.	Exploits the psychological desire for a shared future, creating the illusion of "let's make money together to build our life."

[11] http://www.moe.gov.cn/s78/A19/A19_ztzl/ztzl_yywzfw/shenghuoxz/201912/t20191213_411939.html
[12] https://news.cctv.com/2019/09/07/ARTI97p1gbnl2wYuhWMtOejh190907.shtml
[13] https://news.cctv.com/2019/09/07/ARTI97p1gbnl2wYuhWMtOejh190907.shtml

Limitation

Incomplete visibility of scam operations. This report is based on documented law enforcement operations and media reports, supplemented by court judgments, survivor testimonies, and open-source intelligence, including Telegram channels. However, many scam operations are likely never detected, raided, or publicly reported. As a result, the global footprint presented in this report should be regarded as a minimum estimate, and the actual geographic spread is likely to be substantially larger.

Incomplete information on suspect nationalities. In some cases, only Taiwanese suspects were identified in publicly available sources. However, it is likely that Chinese nationals were also active in the same locations and during the same period. This reflects broader limitations in data availability and transparency. Chinese authorities frequently publish aggregated statistics on overseas fraud but do not always disclose the underlying case details. For example, in 2017, Chinese authorities stated that scam operations established by Chinese and Taiwanese nationals had been identified in more than 40 countries[14], yet no official list of those countries or corresponding case information were found. Differences in reporting practices and restrictions on public access to Chinese court judgments further limit the ability to reconstruct individual cases.

Limited information on scam operational duration. For most cases, publicly available sources do not indicate how long the scam operation had been active before it was dismantled. Consequently, this report cannot systematically assess the lifespan or stability of overseas scam operations.

Exclusion of enabling hubs. This report focuses on countries where Chinese-speaking scam operators have established a physical operational presence, such as scam outposts or compounds. It does not attempt to comprehensively map the broader transnational ecosystem that enables these operations. Other jurisdictions play important supporting roles. For example, Between September 2006 and April 2009, more than 400 Taiwanese nationals were arrested in South Korea for withdrawing proceeds on behalf of international telephone scam networks.[15] Similarly, many identified ringleaders of Chinese-origin scam compounds hold Vanuatu passports.[16] Singapore, too, has uncovered major money laundering networks linked to online scams and illegal gambling in Cambodia.[17] These cases demonstrate how jurisdictions without significant scam operations may nevertheless play a critical role.

[14] https://www.mps.gov.cn/n2255079/n5590589/n5747791/n5778470/c5772552/content.html
[15] https://news.ltn.com.tw/news/politics/breakingnews/1993852
[16] See, for example: https://www.yogonet.com/zh-TW/%E5%9C%8B%E9%9A%9B/%E6%96%B0%E8%81%9E-a/2025/02/04/94081%E5%90%8D%E6%B6%89%E5%AB%8C%E5%A4%A7%E8%A6%8F%E6%A8%A1%E8%A9%90%E9%A8%99%E7%9A%84%E4%B8%AD%E5%9C%8B%E8%B3%AD%E5%8D%9A%E5%A4%A7%E4%BD%AC%E5%9C%A8%E9%BB%91%E5%B1%B1%E8%A2%AB%E6%8D%95
[17] https://www.straitstimes.com/singapore/billion-dollar-money-laundering-case-9-out-of-10-accused-in-s-pore-have-cambodian-links

Exclusion of small cases and cases of isolated reports. This report focuses on scam operations that demonstrate a degree of organisational and managerial capacity. As a general approach, it does not include cases in which fewer than 10 suspects were arrested in a single operation, as such cases often involve small groups acting independently. Instead, the report prioritises operations involving larger, coordinated groups that exhibit evidence of structured recruitment and management. This threshold is intended to distinguish organised scam enterprises from isolated individuals engaging in opportunistic fraud. This report excludes countries supported only by isolated reports. For example, one scam group was reportedly established in Hungary in 2017 before relocating to Spain several months later.[18] As no further reports or corroborating evidence were identified, Hungary was not included in this analysis.

Distinguishing suspects from trafficking victims. Many law enforcement agencies and government statements do not distinguish between criminal suspects and potential victims of human trafficking when reporting the outcomes of scam operations. As a result, the reported number of "fraud suspects" should be interpreted with caution, as some individuals may have been trafficked into scam operations and compelled to participate under coercion. For example, Chinese authorities announced that 41,000 fraud suspects were transferred from Myanmar to China in 2023.[19] It is likely that some of those transferred were survivors of human trafficking.

Scope and depth of case summaries. This report aims to demonstrate the breadth and global spread of scam operations organised by Chinese-speaking ringleaders, rather than provide comprehensive case studies of each operation. Individual cases are therefore presented in a concise format. Readers are encouraged to use the citations, dates, locations, and key details such as the number and nationalities of suspects as starting points for further research. Many cases are supported by additional media reports in multiple languages (particularly Chinese, English, and the local language(s) of the countries where the scammers operated), court judgments, and government statements that provide substantially greater detail than can be included in this report.

Southeast Asia

Cambodia

Cambodia was one of the earliest and most persistent overseas bases for Chinese-speaking fraud networks. Between 2011 and 2016, nearly 300 people were deported from Cambodia to Taiwan, while

[18] https://web.archive.org/web/20210902032313/https://www.jiemian.com/article/1615647.html
[19] https://m.gmw.cn/2024-01/05/content_1303621919.htm

additional Chinese nationals were returned to China, many in connection with online or telecommunications fraud.[20]

In October 2015, Cambodian police arrested 166 Chinese nationals in Sihanoukville Province. The suspects had rented hotels and large villas and were accused of targeting victims in more than 20 Chinese cities and provinces. Their methods included impersonating employees of banks, telecommunications providers, health insurance agencies, police forces, and postal authorities. Victims were pressured to disclose personal information or transfer money to overseas accounts under the pretence that they were implicated in crimes such as money laundering or drug trafficking. In March 2016, another 38 Chinese nationals wanted by Chinese police were arrested in Cambodia for similar activities.[21]

In 2020, Chinese police dismantled a major "pig butchering" syndicate that had established multiple scam sites in Cambodia (Phnom Penh and Poipet), the Philippines (Manila), and Guangzhou, China between 2018 and 2019. The network consisted of nearly 1,000 members and defrauded victims in China of more than RMB 400 million (USD 57 million) through fraudulent investment schemes. During a nationwide coordinated operation involving more than 3,000 police officers, authorities arrested 868 suspects, with 492 formally detained. Investigators found that the syndicate operated multiple scam sites under the same criminal organisation, using fake investment platforms, WeChat groups, and cryptocurrency products to carry out "pig butchering" scams.[22]

Since 2021, Cambodia has emerged as one of the world's largest hubs for Chinese-speaking scam compounds. The United Nations estimated in 2023 that approximately 100,000 people in Cambodia may be held in situations where they are forced to carry out online scams, concentrated primarily in Sihanoukville, but also in Phnom Penh, Kandal, Pursat, Koh Kong, Bavet (Svay Rieng), Oddar Meanchey, including the Dara Sakor and Heng He (Heng Thmor Da) Special Economic Zones. Scam operations have expanded into heavily fortified complexes hosting multiple scam companies.[23] UNODC estimates that cyber-enabled fraud originating from Southeast Asia generated between USD 18 billion and USD 37 billion in losses in 2023 alone, with Cambodia serving as one of the region's principal operational hubs.[24]

HRC's previous report found that the continued expansion of scam compounds in Cambodia is enabled by systemic corruption rather than isolated instances of official misconduct. Our research documented

---

[20] https://news.ifeng.com/c/7fcW0ugaXq9
[21] https://www.epochtimes.com/b5/16/3/4/n4653754.htm
[22] https://m.news.cctv.com/2021/06/02/ARTIWx3Br9Md41nwtXm2pawy210602.shtml
[23] https://bangkok.ohchr.org/reports/online-scam-operations-and-trafficking-forced-criminality-southeast-asia-recommendations
[24] https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

recurring patterns in which politically connected individuals and business elites benefited from scam operations through ownership interests and selective law enforcement. These relationships have allowed scam compounds to operate openly, expand into large-scale developments, and adapt to periodic enforcement campaigns.[25]

Indonesia

Indonesia hosted some of the largest Chinese-speaking fraud operations uncovered during the mid-2010s. In October 2015, a joint operation involving Chinese, Indonesian, Taiwanese, and Hong Kong authorities dismantled eight scam centres across Indonesia. A total of 224 suspects were arrested, including 86 Chinese and 138 Taiwanese nationals. The operation helped solve more than 3,000 telecommunications fraud cases, including cases involving victims in Hong Kong. Some individuals later reported that they had been recruited under the false promise of legitimate overseas employment, without knowing they would be involved in scam operations. Upon arrival, their passports were confiscated and they were prohibited from contacting their families.[26] [27]

In August 2016, Indonesian police dismantled a Taiwanese-led fraud operation in Jakarta, arresting 31 suspects, including 11 Taiwanese nationals and 20 Chinese nationals. In July 2017, Indonesian police conducted coordinated raids across Jakarta, Surabaya, Bali, and Batam, arresting 149 suspects, including 143 Chinese nationals, six Taiwanese nationals, and five Indonesians suspected of assisting the operation. The syndicate operated from rented luxury houses, impersonated Chinese police officers and targeted victims in China. The group had been operating since late 2016 or early 2017 and was estimated to have defrauded victims of up to IDR 6 trillion (approximately USD 450 million).[28] [29]

In November 2019, Indonesian police arrested 91 suspects, including 85 Chinese nationals and six Indonesians, during coordinated raids in Jakarta, South Tangerang, and Malang. Operating from six locations in Greater Jakarta and eight rented houses in Malang, the syndicate impersonated Chinese police officers, prosecutors, courts, and banks to defraud victims in China. Police seized 192 mobile phones, while investigators estimated losses of approximately IDR 36 billion (around USD 2.6 million).[30]

In June 2024, Indonesian immigration authorities raided a villa in Bali and arrested 103 suspects, including 102 Taiwanese nationals and one Hong Kong national, linked to a suspected cyber-enabled

---

25 https://www.humanity-consultancy.com/publications/policies-and-patterns-state-abetted-transnational-crime-in-cambodia-as-a-global-security-threat

26 https://www.mps.gov.cn:8090/n2255079/n4876594/n5104076/n5104079/c5109908/content.html

27 https://tv.cctv.com/2015/11/10/VIDE1447159504647323.shtml?spm=C53156045404.P8kLhvFclptK.0.0

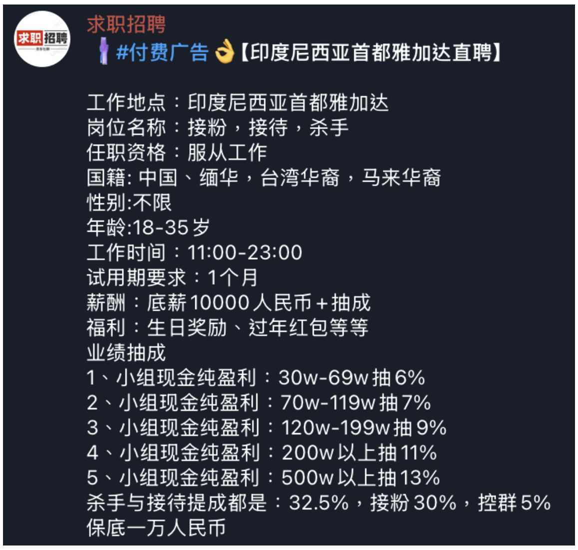
28 https://www.storm.mg/article/165995

29 https://en.antaranews.com/news/112270/indonesia-fights-cyber-fraud-syndicate-from-china

30 https://www.thejakartapost.com/news/2019/11/26/dozens-of-chinese-nationals-arrested-for-scamming-people-in-china

fraud operation. According to Indonesian authorities, the group allegedly conducted online scams targeting victims in Malaysia.[31]

Telegram channels monitored by HRC continued to regularly advertise scam-related recruitment to Indonesia (see, for example, Figure 1), suggesting that Indonesia remains a regularly exploited destination for Chinese-speaking scam syndicates and that the actual number of scam operations may be substantially higher than those uncovered by law enforcement.

<table>
<tr>
<td>

求职招聘
#付费广告 👌【印度尼西亚首都雅加达直聘】

工作地点：印度尼西亚首都雅加达
岗位名称：接粉，接待，杀手
任职资格：服从工作
国籍: 中国、缅华，台湾华裔，马来华裔
性别:不限
年龄:18-35岁
工作时间：11:00-23:00
试用期要求：1个月
薪酬：底薪10000人民币+抽成
福利：生日奖励、过年红包等等
业绩抽成
1、小组现金纯盈利：30w-69w抽6%
2、小组现金纯盈利：70w-119w抽7%
3、小组现金纯盈利：120w-199w抽9%
4、小组现金纯盈利：200w以上抽11%
5、小组现金纯盈利：500w以上抽13%
杀手与接待提成都是：32.5%，接粉30%，控群5%
保底一万人民币

Figure 1. Screenshot of a Chinese-language Telegram channel advertising scam-related job roles and commission structures.
</td>
<td>
Job Recruitment
#Paid Advertisement 👌【Direct Hire in Jakarta, Capital of Indonesia】

Work location: Jakarta, capital of Indonesia
Position titles: Initial grooming specialist (接粉), Host/Attendant (接待), Killer (杀手)
Job requirement: Obedient to work
Nationality: Chinese, Burmese-Chinese, Taiwanese-Chinese, Malaysian-Chinese
Gender: No restriction
Age: 18–35 years old
Working hours: 11:00–23:00
Probation period: 1 month
Salary: Base salary 10,000 RMB + commission
Benefits: Birthday bonus, Lunar New Year red envelope, etc.

Performance commission structure:
1. Group net profit 300,000–690,000: 6% commission
2. Group net profit 700,000–1,190,000: 7% commission
3. Group net profit 1,200,000–1,990,000: 9% commission
4. Group net profit 2,000,000 and above: 11% commission
5. Group net profit 5,000,000 and above: 13% commission

Killer and Host commission both at 32.5%; Initial grooming specialist at 30%; Group controller at 5%. Guaranteed floor: 10,000 RMB
</td>
</tr>
</table>

Laos

In September 2011, Lao police arrested 32 Chinese suspects operating from two villas in Vientiane. The group had been employed by Taiwanese organisers and recruited Chinese workers on short-term tourist visas, organised them into three operational tiers with scripted roles impersonating courts, police, and prosecutors, and placed more than 19,200 fraudulent calls within eight days. Twenty-one of the 32 arrested suspects were women, suggesting a large calling workforce structured around scripted telephone contact. The Laos case is an early example of the labour-intensive call-centre model later reproduced across Southeast Asia. Organisers supplied scripts, technical systems, accommodation, and management, while recruited workers conducted high-volume calls from rented villas.[32]

[31] https://news.pts.org.tw/article/703428
[32] https://www.055110.com/law/1/13219.html

Since at least 2022, Laos has become one of Southeast Asia's principal hubs for Chinese-speaking scam compounds, particularly in and around the Golden Triangle Special Economic Zone and other special economic zones. Estimates show that approximately 85,000 people are working in scam centres in Laos, making it the third-largest concentration in the region after Myanmar and Cambodia.[33]

Between January and June 2026, authorities carried out 44 operations, arresting 4,482 suspects from 25 nationalities in connection with online scams, cybercrime, and illegal gambling. In July 2026 alone, 1,044 additional suspects were detained during nationwide operations.[34]

Malaysia

In March 2016, Chinese and Malaysian authorities raided five telecommunications fraud call centres and arrested 119 people, including 52 Taiwanese, 65 Chinese, and two Malaysian nationals.[35]

In November 2023, Malaysian authorities dismantled a transnational investment scam syndicate operating from a bungalow in Kuala Lumpur that had previously served as the office and residence of a foreign consulate. Police arrested 28 suspects, including 13 Malaysians, seven Chinese nationals, four Bruneians, and four South Koreans. The syndicate maintained the appearance of an active consulate by retaining the building's signage and employing armed security guards, while operating a fraudulent cryptocurrency investment scheme targeting victims in Malaysia, Brunei, South Korea, and China.[36]

In July 2026, Malaysian authorities dismantled two major scam syndicates operating from Forest City, Johor, arresting 335 suspects, including 309 Chinese nationals, 19 Indonesians, four Myanmar nationals, and three Malaysians.[37] Police raided 27 apartments and five bungalows used as operational bases, seizing 313 computers, 1,557 mobile phones, 17 laptops, and 10 modems. The two syndicates allegedly conducted fake cryptocurrency investment and romance scams targeting victims primarily in China and Indonesia. Authorities also reported that some suspects had previously worked in scam centres elsewhere in Southeast Asia, suggesting that Forest City had become a relocation destination as enforcement pressure intensified in neighbouring countries.[38]

---

33 https://web.archive.org/web/20241009004548/https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

34 https://laotiantimes.com/2026/07/06/laos-arrests-more-than-4400-in-cybercrime-crackdown-during-first-half-of-2026

35 https://www.hkcd.com.hk/content/2016-04/17/content_996133.html

36 https://www.freemalaysiatoday.com/category/nation/2023/11/29/cops-raid-crypto-scam-syndicate-based-in-ex-consulates-bungalow

37 https://www.bbc.co.uk/news/articles/cx2kvlye1k5o

38 https://www.channelnewsasia.com/asia/malaysia-forest-city-johor-scam-syndicates-call-centres-6282901

Myanmar

Since at least 2009, the Kokang Four Families, a group of Myanmar nationals of Kokang Chinese (Han Chinese) descent, began expanding from traditional organised crime into organised cybercrime. Although culturally and linguistically Chinese-speaking, they held Myanmar citizenship and controlled significant political, military, and economic power in the Kokang Self-Administered Zone.

From 2009, the Bai family exploited its political and military influence in Kokang to establish 41 scam compounds. According to Chinese prosecutors, the family attracted scam financiers ("gold masters") to operate within these compounds, charging rent, security fees, recruitment fees, and profit-sharing commissions. The compounds were linked to fraud, online gambling, homicide, and other organised crimes, generating more than RMB 20 billion (around USD 3.0 billion) in proceeds.[39] [40]

From 2009, the Wei family developed 31 scam compounds, including Henry (亨利) and Weisheng (威胜). In addition to collecting rent and protection fees from tenant scam companies, the family operated casinos, entertainment venues, and businesses linked to gambling, prostitution, and drug trafficking. Armed personnel controlled the compounds and protected scam operations, while allowing tenant companies to violently discipline workers through beatings, torture, unlawful detention, and killings.[41]

From 2015, the Ming family established industrialised scam compounds, including Wohu Villa (卧虎山庄)[42] and Yuxiang International Group (玉祥国际集团). At their peak, the compounds housed nearly 10,000 scam workers. The family provided armed protection and permitted tenant companies to use systematic violence, including unlawful detention, torture, rape, and murder, against workers who resisted management or failed to meet fraud targets.[43]

From 2018, the Liu family developed 28 scam compounds, including Triumph Building (凯旋大楼) and Rose Manor (玫瑰庄园), through the Fully Light Group (福利来集团). The family attracted scam financiers (tenants) by providing premises, internet infrastructure, investment partnerships, and armed protection. According to Chinese authorities, the compounds were used to facilitate telecommunications fraud, extortion, unlawful detention, and other organised crimes targeting Chinese citizens.[44]

---

[39] http://www.cppsup.com/news/show.aspx?id=10556

[40] https://www.i-cable.com/%E6%96%B0%E8%81%9E%E8%B3%87%E8%A8%8A/%E4%B8%AD%E5%9C%8B%E5%9C%A8%E7%B7%9A/392935/%E7%B7%AC%E5%8C%97%E7%99%BD%E5%AE%B6%E7%8A%AF%E7%BD%AA%E9%9B%86%E5%9C%98%E4%B8%BB%E6%A1%88%E4%B8%80%E5%AF%A9-%E9%A6%96%E8%85%A6%E7%99%BD%E6%89%80%E6%88%90%E7%AD%8921%E4%BA%BA%E6%8E%A7%E6%AE%BA

[41] https://www.piyao.org.cn/20251015/7e35c97dae9f4f3897ba7d779a67400e/c.html

[42] The Wohu Villa, or "Tiger-resting Manor" was documented in HRC's publication in 2023. See: https://www.humanity-consultancy.com/publications/hrc-briefing-guidance-on-responding-to-victims-in-forced-scam-labour

[43] https://www.news.cn/20241230/a5ce27c3812f47518f2dc7f237e24e24/c.html

[44] https://www.chinanews.com.cn/gn/2025/10-15/10498585.shtml

In 2023, the UN estimates that approximately 120,000 people may be trapped in online scam operations in Myanmar. The largest concentrations are located along the Thai border in Myawaddy Township, particularly in Shwe Kokko and KK Park, with additional compounds documented in Dongmei Park, Huanya International City, and other developments in Karen State.[45] In 2023, large-scale cooperation between Chinese authorities and multiple actors in Myanmar resulted in the transfer of 41,000 telecommunications and online fraud suspects to China.[46]

Following mounting pressure from neighbouring countries, large-scale enforcement operations began in 2025. Myanmar authorities detained more than 13,000 foreign nationals from 47 countries during raids targeting major scam hubs around KK Park and Shwe Kokko. The operations also resulted in the seizure of more than 3,000 computers, 21,000 mobile phones, and 102 Starlink terminals, while hundreds of buildings associated with scam operations were demolished.[47] [48]

Philippines

The Philippines has been used as a base for Chinese-speaking telecommunications fraud since at least 2010. In 2010, 24 Chinese nationals were arrested from a scam operation in Manila. The Chinese scam syndicate impersonated Chinese police and judicial officials.[49]

In November 2016, Taiwanese and Philippine police arrested a group operating from a luxury residence, including 19 Taiwanese and five Chinese suspects.[50] In January 2018, Chinese and Philippine authorities dismantled six telecommunications fraud sites in Manila, Vigan, and other locations, arresting 151 suspects, including 73 Chinese and 78 Taiwanese.[51]

In October 2019, Philippine authorities dismantled a major Chinese-operated "pig butchering" scam centre in Manila, arresting 512 suspects. The syndicate used online social platforms to cultivate romantic or friendly relationships with victims before persuading them to make increasingly large investments through fraudulent investment schemes, disappearing with the funds once substantial sums had been transferred.[52]

---

45 https://bangkok.ohchr.org/reports/online-scam-operations-and-trafficking-forced-criminality-southeast-asia-recommendations
46 https://m.gmw.cn/2024-01/05/content_1303621919.htm
47 https://apnews.com/article/myanmar-scam-hubs-detainees-repatriation-e4d814fecf29b4da56dc81cc8ec096c5
48 https://www.wired.com/story/myanmar-kk-park-scam-compound-destruction/
49 https://www.mps.gov.cn/n2253534/n2253535/c4137765/content.html
50 https://web.archive.org/web/20161201143752/http://news.ftv.com.tw/NewsContent.aspx?ntype=class&sno=2016B22S08M1
51 https://news.sina.com.cn/o/2018-04-04/doc-ifyteqtq3814380.shtml
52 https://www.mps.gov.cn/n2255079/n4242954/n4841045/n4841074/c6782220/content.html

Since at least 2020, the Philippines has been one of Southeast Asia's largest hubs for Chinese-speaking scam operations. Major raids in 2023 alone uncovered approximately 1,300 workers at Clark Sun Valley Hub in Pampanga, more than 2,700 workers at Xinchuang Network Technology in Las Piñas, and around 640 workers at Rivendell Global Gaming in Pasay, illustrating the industrial scale of these operations. In 2024, UNODC documented that major POGO compounds housed thousands of workers from more than 20 nationalities and functioned as large-scale scam centres engaging in cyber-enabled fraud, human trafficking, illegal detention, and online gambling.[53] [54]

Following President Ferdinand Marcos Jr.'s announcement in July 2024 banning all POGOs, Philippine authorities significantly intensified enforcement, arresting thousands of Filipino and foreign nationals involved in scam operations and deporting at least 3,000 foreign nationals linked to scam centres.[55]

Despite the ban, enforcement actions indicate that scam operations have persisted, albeit in smaller and more dispersed forms. In February 2025, authorities raided a suspected scam hub in Pasay City and arrested 401 foreign nationals, including 207 Chinese, 132 Vietnamese, 24 South Koreans, 14 Indonesians, 12 Myanmar nationals, 11 Malaysians, and one Madagascan national, while discovering evidence of cryptocurrency fraud, romance scams, investment scams, and illegal online gambling.[56]

Telegram channels monitored by HRC continued to regularly advertise scam-related recruitment to the Philippines, suggesting that the Philippines remains a regularly exploited destination for Chinese-speaking scam syndicates in 2026. The actual number of scam operations may be substantially higher than those uncovered by law enforcement.

Thailand

In December 2015, Thai and Chinese authorities dismantled a fraud operation in Bangkok, arresting 30 suspects, including 13 Taiwanese nationals, 14 Chinese nationals, and three Thai nationals. According to Chinese police, the syndicate had recruited Chinese workers under the promise of high-paying overseas jobs before deploying them to Thailand on tourist visas to conduct police-impersonation fraud targeting victims in China. Operating from rented villas and detached houses in Bangkok, the group was linked to more than 300 fraud cases across China, causing losses of over RMB 30 million (approximately USD 4.6 million) within three months. Investigators found that the operation had placed more than 2.45 million fraudulent telephone calls during the same period.[57]

[53] https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
[54] https://www.asahi.com/ajw/articles/14943302
[55] https://www.state.gov/reports/2025-trafficking-in-persons-report/philippines/
[56] https://www.pna.gov.ph/index.php/articles/1244996
[57] https://web.archive.org/web/20210902104314/https://www.chinanews.com/gn/2016/02-25/7772829.shtml

In March 2024, Thai authorities dismantled one of the country's largest Chinese-operated fraud centres in Nakhon Si Thammarat, arresting 71 suspects, including 52 Chinese nationals and 19 Thai nationals. The syndicate used 5 units of a 4-story shophouse hotel with 22 rooms and targeted victims in multiple countries using multilingual scam scripts in Chinese, Japanese, Russian, and Thai. Authorities seized 223 computers, 1,001 mobile phones, and 298 SIM cards. In 2025, a Thai court sentenced 70 members of the network to prison terms of up to 24 years.[58]

In July 2025, police arrested 17 Chinese nationals operating a scam centre from a luxury villa in Chiang Mai that allegedly defrauded more than 100,000 victims in China of over USD 14 million.[59] Later that month, authorities raided another luxury residence in Chiang Mai and arrested 18 Chinese nationals involved in a separate call centre operation.[60]

Timor-Leste

In August 2025, authorities raided a hotel suspected of hosting a scam operation, detaining about 30 foreign nationals from China, Indonesia, and Malaysia. Investigators seized SIM cards, Starlink, and other communications devices.[61]

In September 2025, UNODC warned that organised crime groups were exploiting the Oecusse Digital Centre free trade zone through criminal foreign direct investment, shell companies, and regulatory loopholes to establish scam operations. The report identified Timor-Leste as an emerging destination for scam syndicates seeking jurisdictions with limited regulatory capacity and less experience combating transnational organised crime.[62]

In June and July 2026, Timorese authorities dismantled multiple scam compounds in Dili, arresting 314 suspects, primarily Chinese and Indonesian nationals. Authorities seized laptops, thousands of SIM cards, Starlink terminals, and other equipment associated with online fraud.[63] [64]

---

58 https://www.dsi.go.th/en/Detail/2695bdbae55d9f8f8410870d9f9bb046

59 https://www.channelnewsasia.com/asia/thailand-chiang-mai-chinese-nationals-scam-centre-network-police-5215866

60 https://www.bangkokpost.com/thailand/general/3079589/police-raid-luxury-house-arrest-18-chinese-call-centre-fraudsters

61 https://www.abc.net.au/news/2025-09-20/organised-crime-scam-centres-move-into-pacific-united-nations/105775972

62 https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf

63 https://www.abc.net.au/news/2026-07-15/timor-scam-compound-chinese-indonesians-cambodians-arrested/106913210

64

Vietnam

In 2011, Vietnam was one of eight Southeast Asian countries involved in the coordinated "9.28" operation against cross-border telecommunications fraud, reflecting its early role as a destination for Chinese-speaking scam groups. In December 2019, Vietnamese and Chinese police dismantled two telecommunications fraud centres in Da Nang, arresting 21 Chinese suspects linked to more than 1,400 fraud cases involving losses exceeding RMB 7 million (approximately USD 1 million).[65]

In June 2024, Vietnamese police dismantled five fraud centres in Ho Chi Minh City and arrested 19 Chinese nationals. According to Chinese authorities, the syndicate had relocated from Cambodia, rented hotel rooms, and targeted victims in China using fake online lending schemes. Investigators recovered computers, mobile phones, and other equipment used in the operation.[66]

In June 2026, Ho Chi Minh City police uncovered a transnational fraud operation after discovering 83 Chinese nationals occupying an entire hotel. Most had allegedly entered Vietnam illegally from Cambodia and were in the process of installing computers to establish an online scam operation targeting victims in multiple countries. Police stated that the operation had not yet become operational at the time of the raid. During the wider enforcement campaign, authorities also identified nearly 300 foreign nationals suspected of immigration, gambling, employment, or online fraud-related violations.[67]

In the same week, Vietnamese police disrupted a transnational criminal group attempting to establish a large-scale online scam centre linked to Cambodian scam syndicates. Authorities arrested four suspects, including one Chinese national and three Vietnamese nationals, and found that the group had rented multiple resorts, farmstays, and villas in Hanoi, Lao Cai, and Phu Tho to accommodate dozens of workers. Investigators stated that many of the recruits had previously worked in scam centres in Cambodia, concluding that the operation was close to becoming operational before it was dismantled.[68]

East Asia

Mongolia

In October 2019, Mongolian authorities arrested approximately 800 Chinese nationals during coordinated raids on four locations in Ulaanbaatar following a two-month investigation into a transnational cybercrime

[65] https://www.cneb.gov.cn/2019/12/13/ARTI1576168152372474.shtml
[66] https://english.news.cn/20240626/8798e90192db4d5995b456fc0090f654/c.html
[67] https://english.vov.vn/en/society/83-chinese-nationals-found-preparing-alleged-online-scam-operation-in-hcmc-post1305867.vov
[68] https://www.reuters.com/legal/government/vietnam-police-bust-group-planning-large-scale-online-scam-centre-2026-06-12/

syndicate. Authorities alleged that the suspects were involved in fraud, illegal gambling, computer hacking, identity theft, and money laundering. All suspects were reported to have entered Mongolia on 30-day tourist visas.[69] [70]

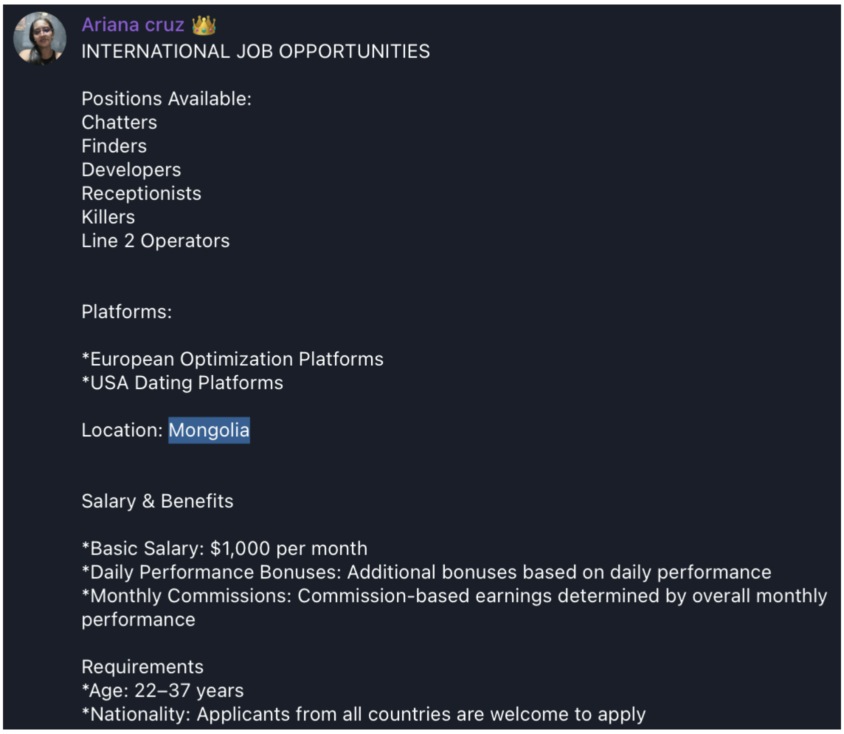


Figure 2. Recruitment post observed by HRC advertising scam-related roles in Mongolia in August 2026. The advertised positions, commission-based salary structure, and references to European and U.S. target platforms are consistent with recruitment for online scam operations.

Japan

Evidence from Japan suggests that Chinese-speaking scam groups had established operational bases in the country by at least 2017. In January 2017, more than 30 Taiwanese nationals were arrested in Fukuoka Prefecture for allegedly operating a call centre targeting victims in China.[71] In April 2019, Japanese police arrested another ten Taiwanese nationals, aged between 19 and 44, and searched an office in Yamanashi Prefecture, where they discovered Chinese-language scam manuals, contact lists, and telephone numbers.[72]

---

69 https://www.hk01.com/%E5%8D%B3%E6%99%82%E4%B8%AD%E5%9C%8B/393233/%E9%9B%BB%E8%A8%8A%E8%A9%90%E9%A8%99-%E8%92%99%E5%8F%A4%E5%9C%8B%E9%80%AE%E6%8D%95800%E5%90%8D%E4%B8%AD%E5%9C%8B%E4%BA%BA-%E6%B6%89%E9%9D%9E%E6%B3%95%E8%B3%AD%E5%8D%9A%E8%A9%90%E9%A8%99%E6%B4%97%E9%8C%A2%E7%AD%89%E7%8A%AF%E7%BD%AA

70 https://legal.people.com.cn/n1/2019/1107/c42510-31443671.html

71 https://news.ltn.com.tw/news/politics/breakingnews/1937233

72 https://www.cna.com.tw/news/asoc/201904180225.aspx

The Japan cases also reveal how scam groups reproduced their methods across borders. A case uncovered in 2018 showed that experienced Taiwanese scammers had begun training foreign recruits in Taiwan. Japanese and Thai recruits were reportedly brought to Taiwan for organised instruction before being sent to establish call centres targeting people in their own countries. This suggests that Taiwan-based organisers were not merely relocating existing groups, but were transferring operational knowledge and management systems to new national teams.[73]

South Korea

In December 2017, following a joint investigation by Taiwanese and South Korean authorities, police arrested 59 suspects, including 50 Taiwanese nationals, 7 Chinese nationals, and 2 South Korean nationals in Jeju. The group had rented two villa blocks as a scam call centre, targeting victims in mainland China through authority impersonation scams, and using Jeju's visa-free entry scheme to facilitate the movement of personnel.[74] [75]

West Asia

Armenia

In August 2016, Armenian authorities raided six properties rented by Chinese-speaking criminal groups and arrested 129 suspects, including 51 Chinese and 78 Taiwanese nationals. According to China's Ministry of Public Security, the group had rented residential properties at high prices, sealed windows, and soundproofed the premises before carrying out telecom fraud targeting victims across at least 13 Chinese provinces. More than 50 cases involving losses exceeding RMB 7 million (approximately USD 1.05 million) were initially identified.[76]

In May 2026, Armenia's Ministry of Internal Affairs announced that it had dismantled an "Asian criminal syndicate" engaged in gambling scams. The police released raid footage showing a large office-like facility and multiple arrests.[77]

Between June and July 2026, HRC identified multiple Chinese-language Telegram channels serving the Chinese-speaking community in Armenia. Beyond community information and commercial advertisements, these channels featured recruitment for scam-related positions, online gambling, escort services, encrypted networks, dedicated internet connections, overseas IP services, and other technical

73 https://www.mirrormedia.mg/story/20180808inv002
74 https://web.archive.org/web/20210902032421/https://www.setn.com/news.aspx?newsid=566954
75 https://www.yna.co.kr/view/AKR20171227068300004
76 https://news.cctv.com/2016/09/08/ARTIz7zhkFUSkxi24R2At4lj160908.shtml
77 https://armenpress.am/en/article/1250274

support. While each service may have legitimate uses individually, their combination suggests the emergence of a broader criminal ecosystem rather than isolated activities.

HRC has observed similar patterns in Cambodia and Myanmar, where Chinese-language Telegram channels function as marketplaces connecting recruitment, technical infrastructure, accommodation, entertainment, and other services supporting scam operations. The emergence of multiple channels with comparable characteristics in Armenia, together with the recent police raid on an Asian-operated online fraud network, suggests that elements of this organisational model may be taking root in a new jurisdiction.

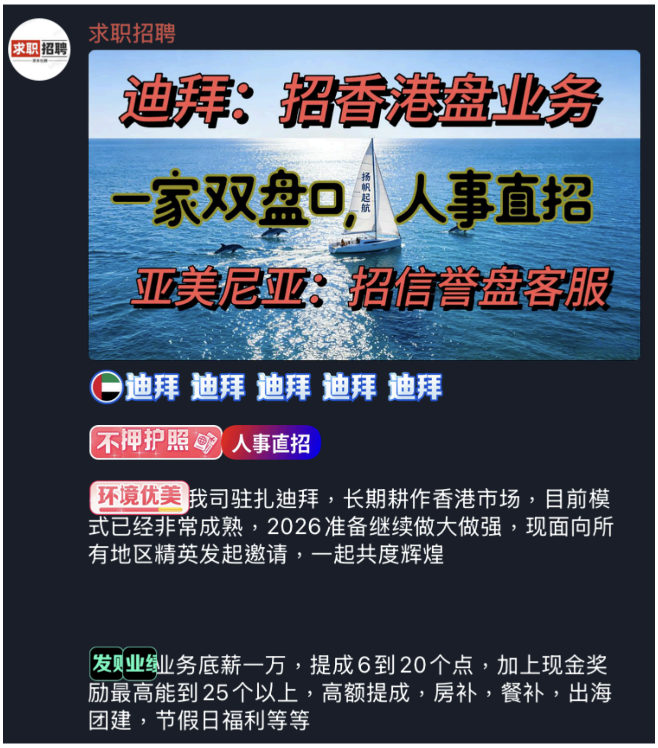


Figure 3. Recruitment post for positions in Dubai and Armenia that appears to relate to scam operations, despite using vague language.

[In the graph]
Dubai: Recruiting Hong Kong Market Operations
One company, dual markets, direct recruitment
Armenia: Recruiting Credit-based Gambling Platform Customer Service

[Text]
🇦🇪 Dubai Dubai Dubai Dubai Dubai

🏷️ No passport confiscation | Direct HR recruitment

Good environment: Our company is based in Dubai, has been working in the Hong Kong market long-term, and the model is already very mature. In 2026, we plan to continue growing and strengthening. We are now inviting elites from all regions to join us and share in the glory together.

Benefit: Base salary of 10,000, commission 6 to 20 points, plus cash bonuses that can reach 25 points and above, high commission, housing allowance, meal allowance, team building trips, holiday benefits, etc.

Georgia

In 2021, Taiwanese fugitive Hsu Ming-chin (Thomas Xu) expanded the Cambodia-based Lixin Group into Batumi, Georgia.[78] According to the 2025 UNODC report, Lixin (identified as "Business Group 2") had registered at least 25 companies in Georgia, with investments concentrated in Batumi, a city increasingly associated with online gambling and cyber-enabled fraud similar to that documented in Southeast Asia.[79]

78 https://www.occrp.org/en/investigation/the-phantom-investor-how-a-wanted-meth-kingpin-posed-as-a-tycoon-in-georgia

79 https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

Chinese court judgments also linked Lixin in Cambodia to the recruitment of Chinese nationals for large-scale scam call centres.[80]

In 2023, Taiwanese authorities investigated reports of a scam operation in Georgia in which approximately 400 trafficked workers were allegedly confined in a hotel and forced to conduct telecommunications fraud. According to victims, workers who failed to meet performance targets were subjected to torture, including waterboarding and electric shocks. Taiwan's Criminal Investigation Bureau confirmed that it had rescued three Taiwanese victims following requests for assistance and found evidence that Taiwanese criminal groups were active in Georgia, using third-country passports to facilitate entry and establish scam centres.[81]

Türkiye

In May 2016, Türkiye authorities arrested 52 Taiwanese and 30 Chinese nationals suspected of fraud.[82] In March 2021, Turkish authorities raided a scam call centre operating from nine rented villas in Silivri, near Istanbul, arresting 119 Chinese nationals. Police identified 18 suspects and 101 apparent victims of human trafficking, who had been recruited with false job offers, including positions for programmers and network engineers. Upon arrival, their passports were confiscated, they were prohibited from leaving the premises, and forced to conduct cryptocurrency-related scams targeting victims in China. The operation was uncovered after two workers escaped and alerted police. Authorities seized 712 mobile phones, 677 SIM cards, 112 computers, and approximately TRY 1.5 million (USD 198,000) in cash.[83]

In May 2021, Türkiye gendarmerie dismantled an online fraud group in Kemer, Antalya Province, and rescued 33 Taiwanese nationals reportedly under the control of human traffickers. In November 2021, another fraud group involving 27 Taiwanese nationals was dismantled.[84]

80 https://www.occrp.org/en/investigation/major-cambodia-based-real-estate-conglomerate-linked-to-scam-gambling-operations

81 https://tw.news.yahoo.com/400%E8%B1%AC%E4%BB%94%E9%81%AD%E5%9B%9A%E5%96%AC%E6%B2%BB%E4%BA%9E-%E7%81%8C%E6%B0%B4%E9%9B%BB%E6%93%8A%E7%A7%81%E5%88%91-%E8%AD%A6%E6%95%91%E5%87%BA3%E4%BA%BA-060431499.html

82 https://news.ltn.com.tw/news/politics/breakingnews/1903732

83 https://www.dw.com/zh-hant/%E6%B6%89%E5%AB%8C%E9%9B%BB%E4%BF%A1%E8%A9%90%E9%A8%99%E5%9C%9F%E8%80%B3%E5%85%B6%E8%AD%A6%E6%96%B9%E9%80%AE%E6%8D%95119%E5%90%8D%E8%8F%AF%E4%BA%BA/a-56862147

84 https://web.archive.org/web/20211129080513/https://www.cna.com.tw/news/aopl/202111270061.aspx

United Arab Emirates

In 2021, the Consulate-General of China in Dubai warned that Chinese nationals were being lured to Dubai through high-paying job advertisements, only to have their passports confiscated and be forced into online scams and illegal gambling operations after arrival.[85]

In August 2023, Chinese authorities prosecuted 21 Chinese nationals for operating investment scams from Dubai since 2019. According to the court, the group recruited "salespersons" and "lecturers", purchased WeChat accounts, and targeted victims in China through fake investment schemes.[86]

In 2024, HRC documented at least seven suspected scam compounds across Dubai and neighbouring Ajman, including operations in Dubai Silicon Oasis, Phoenix Industrial Park, Dubai Investment Park (DIP), Rahaba Residence, the Prince Compound, and Al Ghoroub Tower in Ajman. Evidence collected by HRC, including survivor testimonies, leaked documents, and open-source intelligence, indicated that these compounds were predominantly managed by Chinese-speaking criminal groups and operated in a manner similar to scam compounds in Cambodia and Myanmar. HRC also documented the scale of several individual operations. A survivor from Dubai Investment Park reported that his company employed approximately 200 staff, primarily Chinese nationals, and generated an estimated USD 2.9–4.3 million per month through online gambling fraud. At Rahaba Residence, survivor testimony described a complex of 20 eight-storey apartment blocks used for scam operations, while leaked data from the Prince Compound suggested at least 300 Chinese scammers were working there.[87]

In 2026, Dubai Police announced one of the largest international enforcement operations against scam centres outside Southeast Asia. Working with the FBI and Chinese authorities, police dismantled nine scam centres and arrested 276 suspects, the majority reportedly from Southeast Asia, in connection with cryptocurrency investment fraud targeting victims worldwide.[88]

HRC's monitoring also indicates that, since at least 2022, Chinese-language Telegram channels have openly advertised recruitment for scam-related positions in Dubai. These recruitment channels frequently discuss Dubai alongside established scam destinations such as Cambodia and Myanmar, suggesting that recruiters view them as part of the same transnational labour market rather than distinct operating environments. The persistence and volume of such recruitment activity over several years indicate that

[85] https://dubai.china-consulate.gov.cn/zytz/202102/t20210223_9917924.htm
[86] https://news.qq.com/rain/a/20230830A091K900
[87] https://www.humanity-consultancy.com/publications/hrc-briefing--uncovering-the-spread-of-human-trafficking-for-online-fraud-into-laos-and-dubai
[88] https://www.justice.gov/opa/pr/coordinated-takedown-scam-centers-leads-least-276-arrests-alleged-managers-and-recruiters

Dubai has become an established destination within the Chinese-speaking scam ecosystem, rather than an emerging or isolated location.

South Asia

India

In 2020, a Chinese court convicted 44 defendants for operating a telecommunications fraud syndicate based in India between 2015 and 2016. The operation was organised from a two-storey villa on the outskirts of an Indian city and recruited more than 40 Chinese nationals to conduct police-impersonation fraud targeting victims across China. The syndicate placed fraudulent calls to more than 300,000 people, defrauding victims of over RMB 50 million (approximately USD 7.5 million).[89]

Nepal

In December 2019, Nepalese police arrested 122 Chinese nationals during coordinated raids on nine houses in Kathmandu in what authorities described as the country's largest crackdown involving foreign nationals. Investigators suspected the group of preparing cyber fraud operations and found the properties configured as dormitory-style accommodation with workstations. Police seized more than 700 mobile phones, 331 laptops, nearly 100 desktop computers, along with SIM cards and USB drives. The operation was conducted in coordination with China's National Central Bureau.[90]

Pakistan

In July 2025, Pakistan's National Cyber Crime Investigation Agency (NCCIA) raided a scam call centre in Faisalabad, arresting 149 suspects involved in Ponzi schemes and investment fraud. The suspects included 78 Pakistanis, 48 Chinese nationals, 8 Nigerians, 6 Bangladeshis, 4 Filipinos, 2 Sri Lankans, 2 Myanmar nationals, and 1 Zimbabwean national.[91]

In August 2026, Pakistani authorities raided an illegal scam call centre operating from a luxury residential compound in the outskirts of Islamabad, detaining 258 foreign nationals, including 40 Chinese nationals, 170 Vietnamese nationals, and citizens of several other Asian countries.[92]

---

89 https://web.archive.org/web/20210903122304/https://www.chinacourt.org/article/detail/2019/01/id/3639284.shtml
90 https://www.securityweek.com/nepal-arrests-122-chinese-over-suspected-cyber-scam/
91 https://www.dawn.com/news/1922894/149-arrested-for-online-fraud-in-raid-on-factory-in-faisalabad
92 https://orientaldaily.on.cc/content/%E5%85%A9%E5%B2%B8%E5%9C%8B%E9%9A%9B/odn-20260819-0819_00178_029/%E5%B7%B4%E5%9F%BA%E6%96%AF%E5%9D%A6%E6%90%97%E9%9B%BB%E8%A9%90%E4%B8%AD%E5%BF%83--%E6%8B%98258%E4%BA%BA

An apparent testimony from one arrested Chinese scam worker suggests that the operation relocated from a scam compound in Sihanoukville, Cambodia, to Pakistan in early 2025 following intensified law enforcement pressure.[93] According to the account, workers had little choice but to relocate because their passports were held by the company, although the individual acknowledged willingly participating in scam activities in the hope of earning money. The testimony also describes surprise that Pakistani authorities successfully raided the operation, reflecting a belief that Pakistan would provide a safe haven from law enforcement. Following extensive international media coverage, the individual anticipated deportation to China and subsequent criminal prosecution. While the authenticity of the testimony cannot be independently verified, it is consistent with broader evidence of scam syndicates relocating to new jurisdictions in response to crackdowns elsewhere.

Sri Lanka

In May 2012, Chinese authorities announced the dismantling of a major Taiwanese-led transnational telecommunications fraud network that operated call centres in Sri Lanka alongside Thailand, Malaysia, Indonesia, Cambodia, and Fiji. The coordinated operation across six countries resulted in the arrest of 482 suspects, including 286 Taiwanese and 177 Chinese nationals, and the dismantling of 35 operational sites. According to China's Ministry of Public Security, the syndicate was linked to more than 510 telecommunications fraud cases across 30 provinces in China, causing losses exceeding RMB 73 million (approximately USD 11 million).[94]

In June 2024, Sri Lankan authorities arrested at least 200 foreign nationals, the majority of whom were Indian nationals, in connection with online financial scams. The suspects also included Chinese, Bangladeshi, Pakistani, and Nepali nationals.[95] In October 2024, Sri Lankan authorities arrested more than 230 Chinese nationals during a series of raids targeting cyber-enabled scam operations. Police also detained a small number of Vietnamese, Thai, and Filipino nationals and seized hundreds of computers and mobile phones.[96]

In March 2026, authorities arrested 135 Chinese nationals operating a scam centre;[97] in April, another 152 foreign nationals, including 133 Chinese, were detained at a hotel-based operation;[98] By May 2026, Sri Lankan police reported having arrested more than 1,000 foreign nationals, mainly from China,

---

[93] https://t.me/YMNY222/2901

[94] https://web.archive.org/web/20210903122303/https://www.chinacourt.org/article/detail/2012/05/id/519207.shtml

[95] https://indianexpress.com/article/world/indian-nationals-arrested-sri-lanka-cybercrime-operations-police-9422963/

[96] https://www.scmp.com/news/asia/south-asia/article/3282534/hundreds-chinese-men-arrested-sri-lanka-over-online-scams

[97] https://www.abc.net.au/news/2026-05-22/fears-scam-operations-relocating-sri-lanka/106708344

[98] https://www.malaymail.com/news/world/2026/04/04/sri-lanka-arrests-152-foreigners-over-hotel-based-cyberscam-ring/215028

Vietnam, and India, for alleged involvement in cybercrime since the beginning of the year.[99] Authorities and researchers attributed the increase to the relocation of Chinese-speaking scam syndicates from Cambodia and Myanmar, attracted by Sri Lanka's relatively relaxed visa regime, developed telecommunications infrastructure, and comparatively weak cybercrime enforcement.

Central Asia

Kazakhstan

In July 2026, South Korean and Kazakh authorities conducted a joint operation in Almaty, Kazakhstan, arresting 19 South Korean nationals involved in a voice phishing syndicate. Police stated that several ringleaders, including a Chinese national believed to have led the organisation, remained at large. Investigators found that the group had relocated from Cambodia to Vietnam, and later to Kazakhstan following intensified law enforcement pressure in Southeast Asia. The syndicate operated a call centre impersonating financial regulators, prosecutors, and courts to defraud victims in South Korea. Authorities identified 16 victims with confirmed losses of approximately KRW 600 million (USD 440,000), although investigators estimated that losses from the group's operations in Cambodia and Vietnam amounted to several billion won.[100]

While the nationalities of those prosecuted were not disclosed, Kazakhstan's Ministry of Internal Affairs reported that the country recorded more than 22,000 cyber fraud cases in 2024, resulting in losses of approximately 45.5 billion tenge (USD 90 million). Authorities stated that 1,564 suspects were held criminally liable for cyber fraud during the year, with cases concentrated in Astana, Almaty, and Karaganda. The ministry also highlighted increasing international cooperation to dismantle transnational fraud networks and ongoing legislative reforms to strengthen SIM card registration and disrupt telecommunications fraud.[101]

Europe

Croatia

In January 2018, Croatian police arrested 61 Taiwanese nationals accused of operating a telecommunications fraud network targeting Chinese citizens. Investigators alleged that two ringleaders had recruited 59 Taiwanese victims with promises of well-paid jobs in Europe before confiscating their passports, restricting their freedom of movement, and forcing them to conduct police-impersonation fraud

[99] https://www.japantimes.co.jp/news/2026/05/20/asia-pacific/crime-legal/southeast-asia-scam-sri-lanka/
[100] https://www.ettoday.net/news/20260805/3213682.htm
[101] https://www.chinanews.com.cn/gj/2025/03-26/10389263.shtml

targeting victims in China. The group reportedly used standardised scam scripts and had completed more than 20 successful frauds worth nearly RMB 10 million (approximately USD 1.5 million). Authorities also found that the organisation had previously operated in Slovenia.[102] [103]

Czech Republic

In January 2018, Czech police arrested eight Taiwanese men in Prague following an INTERPOL Red Notice issued at the request of China. They were accused of impersonating Chinese police and prosecutors and defrauding Chinese-speaking women in Australia of approximately CZK 60 million (approximately USD 2.9 million in 2018). The case illustrates the geographic separation characteristic of these networks: suspects operated from Europe, impersonated Chinese authorities, and targeted victims in Australia.[104]

Greece

In July 2016, Greek police dismantled a large fraud network and arrested 125 suspects, including 122 Taiwanese nationals and three Greek nationals. Hiding in five luxury villas in the suburb of Athens, the group was also reportedly involved in illegal online gambling, particularly football matches. Investigators found that Taiwanese workers had been recruited in groups since 2014 and had their passports confiscated upon arrival.[105] [106] [107]

Latvia

In August 2017, Chinese and Latvian authorities dismantled a telecommunications fraud operation in Latvia targeting victims in China, arresting 111 suspects, including 110 Taiwanese nationals and one Latvian national. The syndicate used police-impersonation fraud, posing as mobile network operators and government officials to convince victims that their identities had been compromised or linked to serious financial crimes, before persuading them to transfer funds. Investigators estimated that the group had defrauded victims of nearly TWD 300 million (approximately USD 10 million) in just six months.[108] [109]

---

102 https://glashrvatske.hrt.hr/en/domestic/two-croatian-and-two-chinese-nationals-arrested-for-imprisoning-59-people-1881075
103 https://www.cna.com.tw/news/firstnews/201801250114.aspx
104 https://tw.news.yahoo.com/%E6%8D%B7%E5%85%8B%E6%B3%95%E9%99%A2%E8%A3%81%E6%B1%BA-8%E5%90%8D%E5%8F%B0%E7%B1%8D%E9%9B%BB%E4%BF%A1%E8%A9%90%E6%AC%BA%E5%AB%8C%E7%8A%AF%E9%81%A3%E9%80%81%E4%B8%AD%E5%9C%8B-231448278.html
105 https://www.tovima.gr/2016/07/25/society/me-edra-tin-athina-stoiximatizan-se-agwnes-stin-asia/
106 https://www.chinatimes.com/realtimenews/20160723003950-260401?chdtv
107 https://web.archive.org/web/20210902070839/http://www.xinhuanet.com/world/2016-07/25/c_129173703.htm
108 https://www.chinatimes.com/realtimenews/20200604005238-260402?chdtv
109 https://www.rti.org.tw/news?uid=3&pid=189055&typeId=2

Montenegro

In January 2020, Taiwanese and Montenegrin authorities dismantled three telecommunications fraud call centres in Montenegro, repatriating 92 Taiwanese suspects to Taiwan. The syndicate, established in September 2019, targeted victims in China through police-impersonation fraud, with members posing as officials from China's telecommunications regulator and public security authorities. Investigators estimated that more than 2,000 victims were defrauded of over TWD 600 million (approximately USD 20 million) in just five months. Subsequent investigations uncovered a recruitment and training centre in Taiwan, where new members received telecommunications fraud training before being deployed to Montenegro. Authorities also traced the operation to Taiwanese financiers based in Malaysia and identified domestic money-laundering infrastructure supporting the network. Prosecutors also found evidence of coercion and human trafficking. At least one member had been recruited under the false promise of a "work exchange" programme, only to have her movements restricted and be forced to conduct scam calls. When she refused to participate, she was verbally abused and punished by repeatedly copying scam scripts. The organisers were subsequently charged under Taiwan's Human Trafficking Prevention Act.[110] [111]

North Macedonia

In May 2021, North Macedonian authorities dismantled a Taiwanese-operated telecommunications fraud call centre, arresting more than 30 suspects. Taiwanese prosecutors later charged 42 members of the syndicate, alleging that the organisation had established the operation in February 2021 after renting a luxury villa in a suburban area. The syndicate carried out police-impersonation fraud targeting victims in China, successfully defrauding at least 124 victims of RMB 13.27 million (approximately USD 2.1 million). To avoid attracting the attention of local authorities, members initially stayed at luxury hotels, including Hilton and Marriott properties, posing as business travellers before being transported to the scam centre. Prosecutors further revealed that the ringleader had previously established telecommunications fraud call centres in Japan, the Netherlands, Montenegro, and Türkiye, typically relocating every three to four months to evade law enforcement.[112][113]

Poland

In January 2018, Polish prosecutors announced the arrest of 48 Taiwanese suspects and two Polish nationals in connection with an international fraud group. The group had allegedly defrauded Chinese victims of approximately EUR 1.8 million over one year. The operation formed part of the same

---

[110] https://www.tcc.moj.gov.tw/295804/295830/657577/788306/post
[111] https://www.ettoday.net/news/20200603/1729230.htm
[112] https://www.cna.com.tw/news/asoc/202108180177.aspx
[113] https://judgment.judicial.gov.tw/FJUD/default.aspx

multinational law enforcement action targeting Chinese-speaking telecommunications fraud networks operating across Central and Eastern Europe.[114]

Slovenia

In January 2018, Slovenian authorities dismantled telecommunications fraud call centres in Maribor and Ljubljana as part of the same joint operation with Croatia. Police arrested four Taiwanese nationals and two Slovenians suspected of human trafficking and organised crime, while identifying 31 Taiwanese nationals as victims of trafficking who had allegedly been recruited to Europe, had their passports confiscated, and were forced to carry out fraud against victims in China.[115] [116]

Spain

From 2016, Chinese police traced a series of telecommunications fraud cases to sites in Madrid, Barcelona, and other Spanish locations. On 13 December 2016, Chinese and Spanish police dismantled 13 scam sites and arrested more than 200 suspects. The network was linked to more than EUR 16 million in losses.[117] [118]

United Kingdom

In April 2024, Isle of Man authorities raided offices linked to a Chinese-operated "pig-butchering" scam network as part of a wider fraud and money laundering investigation. Chinese court judgments and company records found that the syndicate had transferred nearly 100 Chinese workers from the Philippines to the Isle of Man in late 2021 to conduct investment scams targeting victims in China. The operation initially used the Seaview Hotel in Douglas before relocating to former bank offices. Chinese courts documented losses of at least RMB 38.87 million (approximately USD 5.3 million), although investigators believed the total losses were substantially higher.[119]

---

114 https://tw.news.yahoo.com/%E6%B3%A2%E8%98%AD%E9%80%AE48%E5%90%8D%E5%8F%B0%E7%81%A3%E8%A9%90%E6%AC%BA%E7%8A%AF-%E5%B9%B4%E6%95%B2%E8%A9%90%E5%A4%A7%E9%99%B8%E4%BA%BA6500%E8%90%AC-023932353.html

115 https://vijesti.hrt.hr/svijet/kina-od-slovenije-trazi-izrucenje-uhicenih-tajvanaca-iz-call-centara-817182

116 https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=TCHM%2c107%2c%e6%8a%97%2c951%2c20181108%2c1

117 https://www.chinanews.com.cn/m/gn/2017/12-26/8409552.shtml

118 https://www.xinhuanet.com/world/2018-06/02/c_1122927474.htm

119 https://www.bbc.co.uk/news/articles/cz6x1ql1yelo

Oceania

Australia

In August 2015, Australian police dismantled a Chinese-speaking telecommunications fraud operation in Brisbane, rescuing 58 Taiwanese nationals who had been lured to Australia with false promises of working holiday opportunities. Victims were confined in two luxury houses, forced to work seven days a week making fraudulent telephone calls to victims in China, and received no wages. Some reported working 12-hour shifts, having their freedom of movement restricted, and being subjected to exploitative living conditions. Australian authorities arrested two Taiwanese ringleaders and one Australian accomplice.[120]

Fiji

In 2011, following six months of intensive investigation, Chinese public security authorities uncovered a major cross-border telecommunications fraud syndicate (the “11.29” case). The syndicate maintained scam platforms and call-centre operations in six countries (Thailand, Malaysia, Indonesia, Cambodia, Sri Lanka, and Fiji) as well as in China and Taiwan. Sites used to withdraw and transfer criminal proceeds were located in Thailand and Taiwan. The operation was linked to more than 510 telecommunications fraud cases across 30 provinces in China, resulting in losses exceeding RMB 73 million (approximately USD 11.3 million at the 2011 exchange rate). In May 2012, coordinated raids dismantled 35 sites and arrested 482 suspects, including 286 Taiwanese nationals.[121]

In August 2017, Fijian and Chinese authorities conducted a joint operation that resulted in the deportation of 77 Chinese nationals suspected of operating a telecommunications and online fraud centre targeting victims in China. According to the Fiji Police Force, the group was linked to more than 50 fraud cases involving losses exceeding RMB 6 million (approximately USD 900,000). Chinese authorities stated that the Fiji-based operation formed part of a larger criminal network spanning China, Indonesia, and Fiji, involving more than 200 suspects.[122] [123]

Palau

On New Year's Eve 2019 and in a subsequent raid in mid-2020, Palauan authorities detained more than 200 workers, the majority of whom were Chinese nationals, during operations targeting suspected online

---

[120] https://www.setn.com/news/139532
[121] https://web.archive.org/web/20210903122303/https://www.chinacourt.org/article/detail/2012/05/id/519207.shtml
[122] https://www.occrp.org/en/news/china-77-telecom-and-online-fraud-suspects-arrested-in-fiji-and-flown-to-china
[123] https://www.fijivillage.com/news-feature/Chinese-nationals-involved-in-telecom-and-online-fraud-cases---Fiji-Police-kr2s95/

gambling centres. Through interviews with some of the detainees and other informants, investigators gained insight into the organisation and operation of the criminal networks. However, a comprehensive criminal investigation was not carried out because most of the detainees were rapidly deported for immigration offences.[124]

In January 2025, Palauan authorities raided two suspected online scam centres in Koror. Investigators found evidence that the operations employed workers from China, Malaysia, and Vietnam, many of whom had entered Palau on work visas sponsored by local companies. At least 12 foreign workers were detained and later deported, as Palau lacked the legal framework to prosecute cyber-enabled fraud. Digital forensic analysis revealed Chinese-language scam scripts, online gambling platforms, cryptocurrency fraud, and sophisticated workforce management systems. One operation employed at least 21 workers and was estimated to have operated for more than two and a half years, generating at least USD 200,000 per month. Investigators also identified links between cryptocurrency transactions associated with the operation and Cambodia's Huione Group, highlighting the integration of Palau-based operations into the wider Southeast Asian scam ecosystem.[125]

Africa

Angola

In August 2024, Angolan authorities dismantled a Chinese-operated cybercrime network in Luanda, arresting 46 Chinese nationals. More than 100 Angolan nationals were also found in marketing and customer-support roles. The group allegedly operated an illegal online casino from the Sunshine Hotel in Talatona, offering more than 400 online gambling games and targeting victims in Brazil and Nigeria. According to investigators, the online games were designed to ensure users lost money, encouraging repeated deposits while creating the illusion of possible winnings. Police stated that the operation also extracted banking information and personal data from users, indicating that financial theft extended beyond gambling losses.[126] [127] [128]

Egypt

124 https://www.occrp.org/en/investigation/pacific-gambit-inside-the-chinese-communist-party-and-triad-push-into-palau
125 https://www.occrp.org/en/investigation/foreign-workers-local-sponsors-inside-palaus-hotel-scam-centers
126 https://allafrica.com/stories/202408290256.html
127 https://www.angola24horas.com/sociedade/item/30310-chineses-detidos-em-luanda-por-gestao-fraudulenta-de-mais-400-jogos-online
128 https://www.giranoticias.com/sociedade/2024/08/20338-detidos-chineses-em-luanda-por-gestao-fraudulenta-de-jogos-online.html

In July 2014, Egyptian authorities dismantled a telecommunications fraud syndicate in Alexandria, arresting 96 suspects, including 40 Taiwanese and 56 Chinese nationals. The group had established multiple scam call centres targeting victims in China. In 2015, an Egyptian court sentenced the Taiwanese ringleader to five years' imprisonment, while the remaining suspects received two-year prison sentences and fines of USD 17,500 each.[129]

Eswatini

In 2026, Eswatini launched a major crackdown on a Chinese-linked "pig-butchering" syndicate, initially arresting 88 foreign nationals before the number rose to more than 200 as investigations expanded. The suspects included nationals from China, Taiwan, the Philippines, Malaysia, Indonesia, Cambodia, and Brazil. Authorities later arrested a Chinese national, identified as the suspected kingpin, and dismantled multiple operational sites across Mbabane, Hawane, Woodlands, and Ezulwini. The suspects were accused of operating online investment and gambling scams, money laundering, and immigration offences.[130] [131] [132]

Kenya

In November 2014, Kenyan police discovered a group in Nairobi involving 28 Taiwanese nationals and 48 Chinese nationals. The suspects allegedly impersonated Chinese police, prosecutors, and judicial authorities and targeted more than 100 victims. In April 2016, Kenyan police dismantled another Chinese-speaking fraud group involving 19 Chinese and 22 Taiwanese nationals.[133]

Madagascar

In May 2026, the Chinese Embassy in Madagascar warned that, as Southeast Asian countries intensified crackdowns on scam compounds, some telecommunications fraud operators and their support personnel had begun relocating to Madagascar in an attempt to rebuild their criminal networks.[134] Around the same time, testimonies from apparent Chinese trafficking survivors began to emerge on Telegram, describing exploitative conditions within scam operations in Madagascar.[135]

In July 2026, the Malagasy Ministry of Justice announced that hundreds of people had been arrested in connection with scam operations, with some suspects prosecuted and others repatriated to their countries of origin. Authorities stated that scam operations, initially concentrated in Antananarivo and

[129] https://www.chinatimes.com/realtimenews/20160303003576-260407?chdtv
[130] https://times.co.sz/31697/news/how-arrested-foreigners-ran-pig-butchering-scam/
[131] https://www.eswatiniobserver.com/no-arrests-home-affairs-gambling/
[132] https://times.co.sz/31772/news/suspect-pig-butchering-kingpin-nabbed/
[133] https://www.xinhuanet.com//world/2016-04/13/c_1118603285.htm
[134] https://finance.sina.com.cn/wm/2026-05-27/doc-inhzivfi1586828.shtml
[135] https://t.me/fz190/11701

Toamasina, had expanded to several regions of the country. In response, Madagascar established a multi-agency task force and strengthened international cooperation with countries including China, the United States, South Africa, Kenya, and Rwanda to combat transnational scam networks and human trafficking.[136]

Separately, Ugandan survivors interviewed by HRC reported that some Ugandan returnees from scam compounds in Southeast Asia were later recruited by Chinese business owners to work in Madagascar after struggling with compounded debts and poverty, suggesting continued cross-border movement of personnel within the scam ecosystem. According to these survivors, Chinese-speaking scam operators frequently offer a substantial "red envelope" (joining bonus) to new recruits, providing immediate cash to individuals in financial distress and creating a strong incentive to re-enter scam operations despite their previous experiences.[137]

Nigeria

In December 2024, the Nigerian authorities conducted an operation resulting in the arrest of more than 700 suspects, including 148 Chinese nationals and 40 Philippine nationals, during a raid on a seven-storey building in Victoria Island, Lagos. Nigerian authorities stated that the syndicate was involved in online fraud schemes, including pig-butchering and fraudulent investment scams, and used a Nigerian-registered company to recruit and train local personnel in cyber-enabled fraud.[138]

Uganda

In early 2016, Chinese authorities announced the dismantling of what was then the largest single telecommunications fraud case at the time by value. The syndicate was accused of defrauding victims of more than RMB 100 million (approximately USD 15 million at the time). The operation had been conducted from Uganda and was allegedly masterminded by a Taiwanese ringleader. A total of 62 suspects were arrested, including 10 Taiwanese nationals. According to reports, the police investigation found that the operation was orchestrated by Taiwanese suspects, who centrally recruited call-centre operators in China, arranged their overseas travel, and managed their accommodation, meals, and training.[139]

In July 2026, Ugandan authorities arrested more than 1,000 foreign nationals, the majority reportedly Chinese nationals, during raids on multiple locations in Kampala and Wakiso District. Investigators

---

136 https://newsmada.com/2026/07/31/traite-des-etres-humains-des-centaines-dinterpellations-liees-au-scamming-a-madagascar/

137 Conversation with Ugandan survivors in August 2026.

138 https://punchng.com/efcc-nis-expel-another-51-foreigners-jailed-for-cyberfraud-offences/

139 https://www.zaobao.com.sg/special/report/politic/taiwan/story20160424-608845

alleged that the compounds operated as online scam centres and fraudulent call centres targeting victims both within Uganda and abroad. Authorities also seized hundreds of computers, servers, mobile phones, and other digital devices.[140]

Figure 4. Accommodation and office environment of a scam operation managed by Chinese-speaking ringleaders in Uganda (November 2025). Survivors interviewed by HRC reported that many workers had previously been deported following raids in Dubai or had relocated from scam compounds in Cambodia and Myanmar. Workers included nationals of Uganda, Kenya, Nigeria, Sudan, and Tanzania. The operation reportedly targeted victims in Europe, primarily the United Kingdom, offering a basic salary of USD 30 per month plus a USD 30 commission for each successfully scammed victim. Photo: Anonymous survivor (shared with HRC).

Zambia

In April 2024, Zambian authorities dismantled a Chinese-operated cyber fraud network based in Lusaka, arresting 77 suspects, including 22 Chinese nationals who later pleaded guilty to cyber-related offences. The operation centred on a Chinese-run company alleged to have recruited dozens of young Zambians as call-centre agents to conduct online scams using scripted conversations on platforms such as WhatsApp and Telegram. Scammed victims were located in Zambia as well as Singapore, Peru, the United Arab Emirates, and several African countries. Authorities seized more than 13,000 SIM cards, 11 SIM boxes used to disguise call origins, firearms, ammunition, and other equipment, highlighting the sophisticated and transnational nature of the operation. In June, the Lusaka Magistrates' Court

[140] https://chimpreports.com/breaking-1000-foreign-nationals-arrested-in-sweeping-uganda-cybercrime-crackdown/

sentenced the suspects to prison terms ranging from seven to eleven years and imposed fines ranging from USD 1,500 to USD 3,000.[141] [142]

Americas

Dominican Republic

In December 2017, Taiwanese and Dominican authorities dismantled two Taiwanese-run telephone scam operations based in the Dominican Republic, arresting 37 suspects. Since 2014, the syndicates have established scam call centres targeting victims in China through police-impersonation ("fake police and prosecutor") fraud. The operations were financed by Taiwanese investors and supported by members of the local Taiwanese diaspora, who arranged accommodation, logistics, and translation services for the fraudsters. Prosecutors estimated that the syndicates defrauded victims of at least TWD 140 million (approximately USD 4.6 million) over a two-month period. Investigators also found that financiers increasingly adopted a cross-investment model, investing in multiple scam operations simultaneously to diversify risk.[143] [144]

Paraguay

In January 2015, Paraguayan authorities discovered approximately 80 Taiwanese nationals living in two rented mansions in the Paraná Country Club in Hernandarias. Investigators found that the occupants' passports were being held by a single individual, raising suspicions of human trafficking and forced labour. Although the properties contained large numbers of computers, mobile phones, and communications equipment, authorities did not publicly confirm that the group was operating a telecommunications fraud centre.[145]

However, court records from a separate case later showed that Paraguay formed part of a large transnational scam network operating between 2013 and 2016. The Taiwan-based Lizhan syndicate (立展詐欺集團) established call centres in both Paraguay and the Dominican Republic, with personnel moving between the two countries. The organisation operated at least seven specialised call-centre teams targeting victims in China. These court records suggest that Paraguay was not an isolated location, but one component of a broader overseas operational network.[146]

---

[141] https://www.bbc.co.uk/news/articles/c999dyxenx0o
[142] https://www.cna.com.tw/news/aopl/202406080185.aspx
[143] https://www.chinatimes.com/newspapers/20171212000429-260106?chdtv
[144] https://judgment.judicial.gov.tw/FJUD/default.aspx
[145] https://www.abc.com.py/nacionales/extrana-detencion-de-chinos-1326908.html
[146] https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=TCHM%2c115%2c%e4%b8%8a%e8%a8%b4%2c8%2c20260407%2c1&ot=in

Peru

In October 2023, Peruvian police rescued 44 Asian trafficking victims from a telecommunications fraud operation in Lima and arrested eight suspects, including six Taiwanese nationals and two Peruvians. The victims comprised 43 Malaysians and one Taiwanese national, who had been recruited through fake casino job advertisements, trafficked to Peru via Amsterdam, had their passports confiscated, and were forced to impersonate police and judicial officials in telephone scams targeting companies in Malaysia and Taiwan. According to investigators, the operation was run by a Taiwanese criminal group known as "Red Dragon".[147]

Conclusion

This report documents the global expansion of Chinese-speaking scam syndicates across 45 countries between 2010 and 2026, demonstrating that the internationalisation of these networks long predates the emergence of large-scale scam compounds. It also argues that distinguishing between the outpost scam model and the scam compound model is essential for understanding how these operations evolve and for developing more effective law enforcement responses.

As scam syndicates expand, the primary concern should not simply be the appearance of new scam sites, but attempts to replicate the scam compound model. Early signs of this broader ecosystem are emerging in countries such as Armenia, Malaysia, and Sri Lanka. Above all, the international community should closely monitor systemic corruption, which remains one of the greatest enablers of scam compounds, allowing criminal groups to operate and expand with relative impunity.

Finally, this report highlights an important research gap. Public reporting largely focuses on raids and arrests, while the subsequent criminal justice process remains poorly documented. It is often unclear whether suspects were prosecuted locally, repatriated, or released, and even less is known about trial outcomes. The long-term outcomes of convicted offenders are similarly underexplored. The cases documented in this report suggest that authorities are unlikely to arrest their way out of the problem. Many scam operators are repeat offenders, returning to the industry after serving prison sentences, while some are wanted. Future research should therefore examine the full criminal justice process, from arrest and prosecution to sentencing, rehabilitation, and reoffending.

[147] https://www.cna.com.tw/news/aopl/202310100012.aspx