REGIONAL SUPPORT OFFICE
THE BALI PROCESS

TRAPPED IN DECEIT

RESPONDING TO THE TRAFFICKING IN PERSONS FUELLING THE EXPANSION OF SOUTHEAST ASIA'S ONLINE SCAM CENTRES

POLICY BRIEF **APRIL 2023**

REGIONAL SUPPORT OFFICE
THE BALI PROCESS

Acknowledgements

This policy brief was made possible through support from the Australian Government's Department of Home Affairs and Bali Process Members. The Bali Process Regional Support Office is grateful for their commitment to supporting responses to trafficking in persons, people smuggling and related transnational crime across the Bali Process Member region.

This report was written, designed and edited by:

- Ryan Winch, Transnational Crime & Technology Programme Manager
- Lindsay Erjavic, Transnational Crime & Technology Programme Assistant
- Sebastian Higginson, Communications and Engagement Programme Manager
- David Scott, RSO Co-Manager (Australia)

www.baliprocess.net

This report is part of the Bali Process Regional Support Office's (RSO) efforts to provide detailed data, analysis, and policy recommendations to Bali Process Members in support of their endeavours to counter trafficking in persons, people smuggling and related transnational crime. The designations used by this publication do not indicate the expression of any opinion by the Bali Process or the Bali Process RSO concerning the legal status of any country, territory or city or concerning the delineation of its borders.

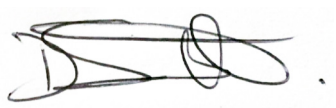
Foreword

Online scam centres are upending traditional patterns of trafficking in persons, leading traffickers to operate in new and often unexpected ways. This includes the increased use of cryptocurrencies to move money across borders and launder their profits, a growing emphasis on using technology as a recruitment tool, and the trafficking of victims from far-flung geographies and socially diverse backgrounds. As responses continue to be discussed, it's the victims who are paying the price. Transnational crime will continue to profit by taking advantage of both trafficking victims living within scam compounds, who are being forced to participate in scamming under threat of violence, and victims of scams, who will continue to be cheated out of huge sums of money until strengthened coordinated responses can be put into action.

As a result, a rapidly implementable regional response is needed to effectively combat the transnational crime organisations operating online scam centres. As policymakers, diplomats and government officials, we must acknowledge the urgent need for well-coordinated regional responses to counter the transnational crime groups that operate these centres. This will require enhanced information and intelligence-sharing and engagement through both formal and informal communication channels, alongside connecting policymakers, consular officials, border and immigration officials, judicial authorities, and law enforcement with one another, as well as with their private sector counterparts.

Trafficking is increasingly facilitated online, with the current online scam centre crisis a clear embodiment of this. To enact durable solutions, we need to work with those who understand the online landscape best – social media platforms and the technology industry at large. Engaging with civil society organisations working to prevent and respond to technology-facilitated trafficking in persons will also be essential. Joint conversations between the technology sector, civil society and law enforcement are too rare, and while all sides are working to respond, siloed approaches are leading to many responses being either inefficient or incomplete.

The RSO is well-positioned to coordinate responses to counter the rising prevalence of online scam centres. With the broad membership of the Bali Process, the RSO has the mandate and capacity to bring together governments, law enforcement, private companies, and civil society organisations to implement solutions together. Further to this, the RSO has the unique capacity to engage at the operational, policy, and capacity-building levels, providing us with the potential to coordinate a truly holistic response. This brief presents a clear set of response activities to move forward at each of these levels, aiming to start discussions about the next steps forward and to advance discussions about innovative potential response strategies. The RSO is committed to continuing to work with our partners to turn these ideas into action and looks forward to seeing trafficking in persons related to these scam centres, as well as the organised crime groups operating them, in decline as soon as possible.



David Scott
RSO Co-Manager
(Australia)

Sukmo Yuwono
RSO Co-Manager
(Indonesia)

Table of Contents

I. Introduction

While online scams are far from a new phenomenon, their increasing formalisation as a profit generator for transnational organised crime in the Asia-Pacific, alongside the increasingly deceptive and brutal strategies used by these criminal organisations to administer these scams, necessitates an urgent intensifying of efforts to combat them.

Scams ranging from the infamous "Nigerian prince scam" to the use of fake dating profiles to emotionally pressure unwitting individuals to transfer funds have long been reported around the globe. Advocacy efforts have raised public awareness of these techniques and law enforcement have long-ago developed a relatively effective toolkit to respond to these situations when scams are reported. However, online scam centres operating across the Asia-Pacific region today go far beyond these more traditional scam strategies, employing entire teams of scammers to target specific individuals, making use of realistic yet fraudulent websites, mobile applications (apps), and investment tools to defraud victims, and implementing increasingly complex forms of psychological manipulation to build trust with, and extract money from, potential victims.

In addition to the scams, far-reaching recruitment efforts by scam operations have led to the trafficking of thousands of individuals. A significant amount of the labour being used within online scam operations is reported to be forced labour. Victims are trafficked into online scam centres, where they're subsequently forced to administer the scams via threats of violent reprisals. High walls, armed guards and barbed wire surround many of the compounds. Cramped conditions, back-breaking working hours, physical, verbal, and sexual abuse, and, in some cases, the ever-present threat of being sold to another transnational organised crime organisation or transferred to even more abusive roles within a transnational crime group's operation, characterise the victims' experience inside scam operations.

Figure I. Example of a job advertisement that is reportedly tied to a scam centre operation.

This situation has clear benefits for transnational organised crime. Trafficking victims work alongside those running scams voluntarily and are being forced to defraud scam victims. All the profits from this flow directly to criminals' pockets, as well as to those of unscrupulous businesspeople, and, in many cases, corrupt bureaucrats and law enforcement officials, who are also essential to facilitating these operations. Scam centres are, under present circumstances, largely low-risk, high-reward operations, that have become increasingly lucrative as scam techniques continue to improve. Some initial hopes that scam compounds would close or diminish after the lifting of COVID restrictions have now faded, as scam centres continue to operate, and in many cases, increase in scale. For transnational organised crime, the effectiveness of the scams is too large of a potential income generator to shift away from, particularly as responses to date have yet to effectively prevent their operation, prosecute the high-level criminals who are funding and coordinating them, or reduce the efficacy of their scams in a substantial manner.

The acknowledgement of this reality, alongside growing awareness amongst law enforcement and policymakers of the scam centres' significant scale, is prompting increasing momentum towards implementing solutions. Consequently, if momentum continues in a positive direction, response efforts should soon lead scam centres to become more challenging to operate, with both their funders and their management facing a real risk of arrest and conviction. In parallel, conversations about how to ensure victims of trafficking (VoT) can be identified and able to more frictionlessly access services is ongoing, with a growing acknowledgement that more coordinated service provision efforts are needed.

II. Summary of Recommendations

While a wide-ranging response is needed to effectively address the challenges posed by online scam centres, some challenges are more pressing than others. This includes, for example, ensuring access to services for victims of trafficking, and improving cross-border collaboration between regional law enforcement agencies so investigations lead to prosecutions more regularly. Similarly, some proposed responses appear more likely than others to have a significant impact on the situation. As a result, the RSO proposes to prioritise the implementation of the following five recommendations:

1. **Launch regularised regional forums for multi-disciplinary groups of international counterparts to coordinate at the operational and policy levels;**

2. **Clarify communication channels between law enforcement, policymakers and the private sector and support efforts to develop clearer guidelines related to electronic evidence requests and the rapid removal of potentially harmful online materials;**

3. **Update or develop guidelines to support consular officials in assisting victims of trafficking who are attempting to leave scam centres or who are seeking support after having left;**

4. **Intensify research and data collection efforts to quantify the scale of the online scams crisis, including developing estimates of trafficking victim numbers, as well as the number of scam centres currently operating and their revenues;**

5. **Launch large-scale awareness-raising campaigns to prevent the trafficking of at-risk populations across Southeast Asia, as well as other significant source countries and transit points.**

Additional context on each of these recommendations is provided throughout the remainder of the Brief, particularly through section VI: The Path Forward, alongside the broader set of recommended responses proposed by the RSO.

III. Objectives

The objectives of this brief are three-fold:

- First, to outline the novel elements of trafficking in persons related to online scam centres, ensuring that policymakers and law enforcement have a clear understanding of the current situation.
- Second, to highlight the challenges that have slowed responses to date, seeking to direct attention to some of the primary causes which have facilitated the proliferation of online scam centres.
- Third, to outline potential solutions to overcoming these challenges, working to start a conversation about how law enforcement, policymakers and other relevant partners can effectively respond.

IV. Methodology

The primary source of information for this brief was the Thematic Dialogue on Preventing and Responding to Online Scam Enterprises, a regional event hosted by the RSO in Bangkok to discuss the increasing impact of trafficking in persons related to online scam centres on Bali Process Member States, as well as the international community more broadly. The event provided a forum for coordinated international response strategies to be discussed and brought together 19 Member States, 2 member organisations, and 10 partner and observer organisations. Insights attained during this event have been supplemented with information collected through subsequent bilateral conversations and interviews with key law enforcement, consular partners, and research institutions. The RSO's research has also been complemented by a range of media reports and open-source information relating to the scam centre crisis, transnational organised crime and trafficking in persons.

V. The Situation

This current scam centre crisis emerged through the period of intense pandemic-related border restrictions and lockdowns during 2020-21. The lockdowns and border closures forced organised crime groups to adjust their means of operation and find new streams of income as cross-border trafficking in drugs, illegal wildlife and people was significantly curtailed. In parallel, this period was characterised by an unprecedented spike in internet user traffic, mainly through chat applications, social media, video games, and dating apps to socialise and connect with one another. These conditions created fertile ground for effectively scamming victims and scaling-up trafficking recruitment.

Casinos, resorts and apartment blocks during the same period faced significant economic challenges as well, as tourism ground to a halt and many living in urban centres chose to move from large cities to smaller towns and villages. Given that many transnational organised crime groups already owned properties or had connections with casino operators and real estate moguls, they sought to find ways to continue to use these resources to support their operations. The result was the rapid growth of online scam centres.

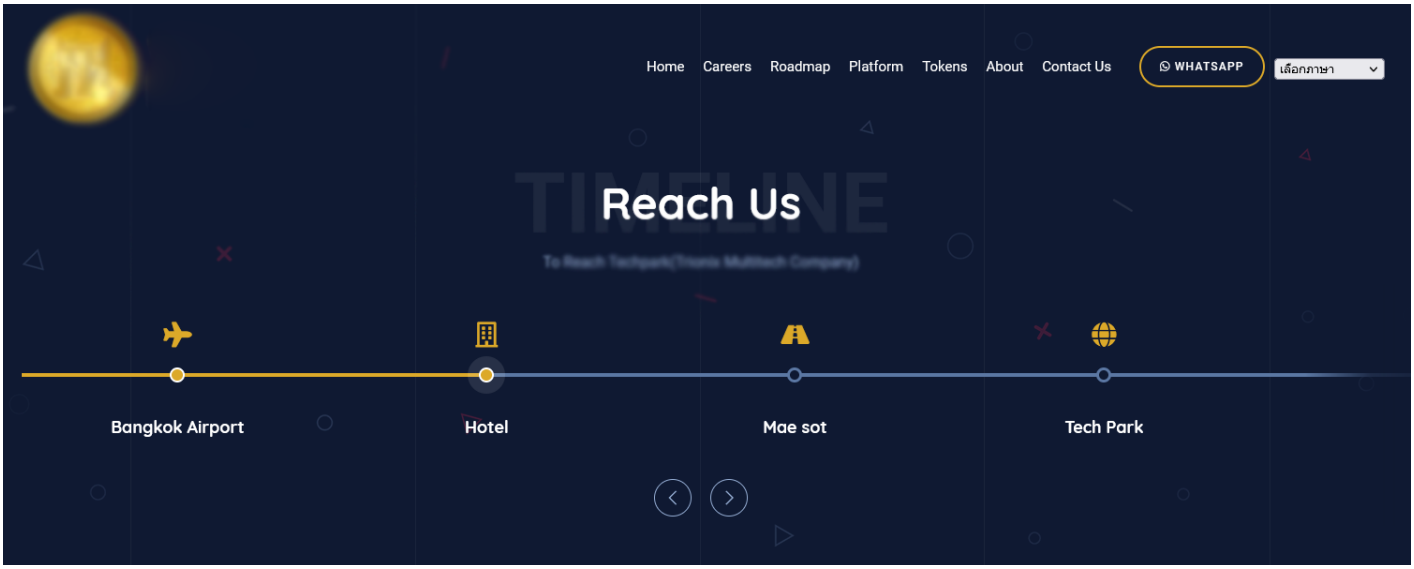


Figure II. A website promoting an itinerary for potential trafficking victims transiting through Thailand to a reported scam centre in Myanmar.

ONLINE SCAM RECRUITMENT PIPELINE

RECRUITMENT PIPELINES

- Recruiters actively seek out potential victims, highlighting high wages, reasonable work hours, and comfortable working conditions.
- Many scam centres have dedicated recruiters assigned to attracting more victims.
- Recruitment often targets friends and family of recruiters or other victims, using existing relationships to build trust with potential trafficking victims, and convincing them to travel to work in scam centres.
- False or misleading job advertisements are also a primary means of attracting victims, with job ads being placed on popular job search websites and social media platforms.
- Recruitment through online job ads, and social media more widely, has created the possibility of targeting potential victims anywhere in the world. Victims of trafficking from every continent except for Australia and the Antarctic have been trafficked into scam operations.

TRAVEL AND TRANSIT

- Victims travel independently to scam centres or nearby cities based on the promise of having been "hired."
- Some victims are aware they're travelling to work on online scams, while others believe they are travelling to work for companies such as investment firms, casinos, or cryptocurrency exchanges.
- Those taking positions in scam centres voluntarily are themselves at risk of becoming victims, as they are often prevented from leaving scam centres after they have arrived - a particular risk for those who prove to be effective scammers.
- Often victims travel to more seemingly legitimate locations where they are told they will be based, before being trafficked elsewhere.
- Bangkok in particular is a transit hub, with transnational crime groups meeting victims at airports and bus stations, before travelling with them to border regions and trafficking the victims across borders.

ARRIVAL

- For those travelling to scam centres independently, it is often in the first hours that the true gravity of their situation is revealed, with victims frequently having their passports taken away and being locked inside the scam centres soon after their arrival.
- Victims' freedom of movement is immediately restricted, with most scam centres having a significant security presence, including high walls, guard stations and barbed wire. Victims in most circumstances are not able to leave these compounds or move freely throughout them, only being permitted in certain parts of the compound at certain times.
- Victims are usually put in cramped dorm-style accommodations, which are frequently reported to be unsanitary and overcrowded.

FURTHER TRAFFICKING

- Victims are reported to be bought and sold by different transnational crime groups operating various scam centres. This buying has been institutionalised to the point where markets exist on communication applications, such as WeChat and Line, with traffickers posting victim profiles and prices (often based on factors including technical skills, languages spoken, or country of origin).
  - This can involve trafficking between scam operations in the same city, but can also involve victims being trafficked between regions, or across borders.

Barbed wire, guard stations and dormitory-style accommodations were installed into properties across many parts of Southeast Asia, congregating most often in areas known for lax regulation of online businesses, as well as the existence of government and law enforcement corruption. As infrastructure around these centres continued to develop, trafficking in persons increased in line with the growing scale of operations. Subsequently, scam operators developed strategies for scamming more effectively, and through this, shifted scam operations from a present, but largely peripheral crime, into a central profit generator for many criminal organisations. While it remains difficult to determine the revenue of scam centres precisely, estimates are consistently in the billions of dollars, with some reaching into the tens of billions.

Although COVID-19-related restrictions have now nearly all been lifted, these massive revenues, investments in physical infrastructure already a sunk cost, as well as the now well-established relationships and networks needed to provide a consistent supply of trafficked labour having been developed, online scam centres have continued to operate, or, according to some reports, continued to increase in scale.

PIG BUTCHERING

While online scam centres have been reported to run a range of scams, using a variety of strategies, by far the most commonly reported is the so-called "pig butchering scam." Pig butchering is a reference to the strategy used by scammers to slowly "fatten" victims up (build a strong relationship) before "butchering" scam victims (stealing their money) one piece at a time (Figure III).

Scammers running pig butchering operations most often create fake profiles on dating sites (eg. Tinder, Hinge), social media platforms (eg. Facebook, Tik Tok), or other online forums to establish relationships, usually romantic ones, with potential victims. In other cases, scammers message potential victims through SMS or messaging apps, such as WeChat, WhatsApp or Line, pretending to have messaged a wrong number before working to start developing relationships with those who respond. Former trafficking victims report each scammer can target hundreds of individual phone numbers each day, looking for those willing to respond and engage in conversation.

Once false personas are well-developed and a connection with a potential victim has been made, the scammers will typically use emotional manipulation to gain their victim's trust and affection over an extended period, often weeks or months. After a strong rapport with potential victims is established, scammers will begin asking for money, personal information, or, most frequently, to have victims put their money into some form of investment scheme or cryptocurrency trading, often via a fraudulent app or website developed by the scam organisation.

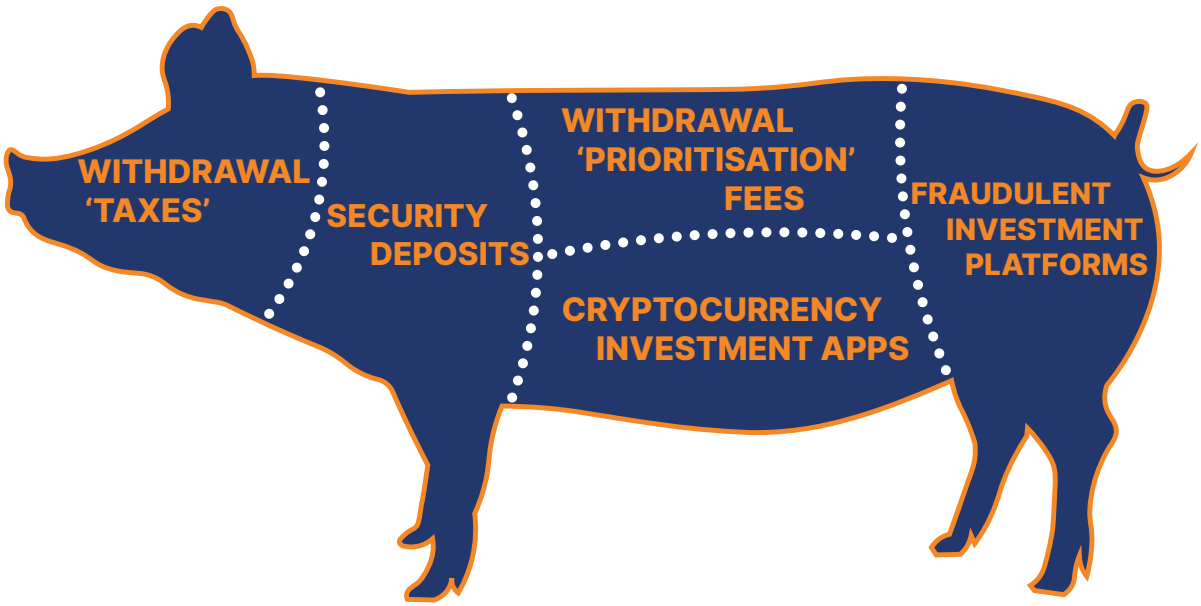


Figure III. Representation of several common strategies used to defraud scam victims.

The resources available to scammers working within scam centres are what make the scams so believable. Teams of researchers, voice actors and investment specialists support the scams, helping to build and keep track of the back stories for the fake personas, and to answer the questions of potential scam victims convincingly, even using voice and video calls. The scale of scam centres also allows them to take risks that individual scammers may not have the resources to facilitate. For example, investment schemes will often pay out earnings to victims on one or several occasions, working to convince victims that it is secure to deposit ever-increasing amounts of money. This level of risk, whereby scam victims potentially could choose not to invest further, leaving scammers taking a loss, is only possible in a sustainable manner because of the scale and the large amounts of capital available within large scam operations. This level of sophistication suggests why scam centres have been so effective to date, and why in many cases they have been able to scam thousands, and sometimes into the millions of dollars, from often well-educated and financially literate individuals.

TRAFFICKING PATTERNS AND VICTIM PROFILES

The reported trafficking patterns mark a notable departure from those observed prior to the pandemic. Firstly, they upend traditional routes and patterns used by human traffickers, with source and destination countries often being the reverse of what had been seen in the past. Whereas in the past VoTs would regularly be trafficked from Myanmar into Thailand for example, now trafficking victims are going from Thailand into Myanmar. Secondly, the typical profile of victims is much broader than has traditionally been the case. The utilisation of online recruiting tactics effectively eliminates geographic barriers to reaching potential victims, meaning that anyone online is now a potential target for traffickers. While most trafficking victims for online scam centres continue to come from Southeast Asia, online recruiting has expanded trafficking routes across the globe in an alarming and unprecedented manner (Figure IV). Victims have been reported from regions as diverse as the Middle East, East Africa, Central Asia, and South America. Until recently, scam centres had been operating largely in Cambodia, with smaller numbers located in Lao PDR and Myanmar. However, there are signs of a growing shift into Myanmar. Some reports have noted this is the result of crackdowns, potentially initiated in response to intensifying international pressure, that have taken place in Cambodia. This law enforcement response has pushed transnational organised crime to move operations into jurisdictions where law enforcement investigations are less likely and where they perceive there is greater freedom to operate.

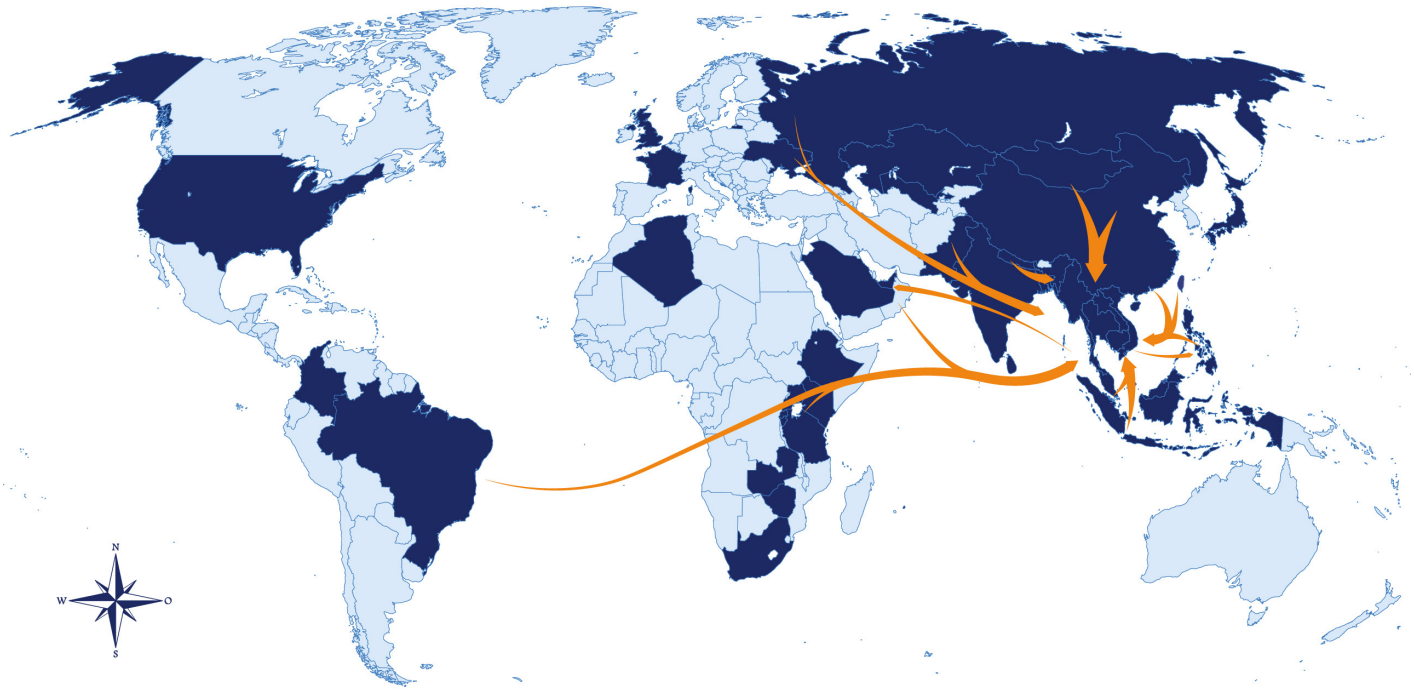


Figure IV. Reported countries of origin for online scam centre trafficking victims (dark blue) alongside generalised trafficking in persons patterns towards online scam centres.

Other reports indicate that the growth of scam centres in Myanmar signifies an overall growth of the scam industry, and rather than representing a shift from Cambodia, they represent a spread of online scam centres into new localities, particularly those with weak rule of law. Smaller but still meaningful numbers of scam centres tied to regional transnational organised crime networks have also been reported in the Philippines, Thailand, Malaysia and the United Arab Emirates.

Personal connections, particularly through friend and family networks are a primary means through which trafficking victims are recruited. Designated recruiters are a part of most scam operations, working full-time to draw additional trafficking victims into the centres. Many of the recruiters are trafficking victims themselves, forced to recruit others through the threat of violent reprisals if recruitment quotas aren't met. In some cases, it has been reported that recruiters are offered their freedom in exchange for recruiting others to replace them, often leading them to desperately recruit friends and family members to allow themselves to escape the centre. However, victims caught contacting the police, civil society groups offering support, or attempting to escape are often brutally punished.

Evidence of severe punishments within the scam centres is now widely available online, with electrocution, beatings, solitary confinement and food deprivation all tools used by scam centre operators to control victims and prevent efforts to report illegal behaviour or escape.

Figure V. Trafficking patterns towards online scam centres in Southeast Asia.

Morale is often maintained within scam centres by promising that victims will be released at a set date. Workers are told if they work hard, scam effectively and don't attempt to escape, they can expect to be released after a set period, often around six months. This promise of freedom rarely becomes a reality. Instead, victims are sold onto other scam centres in the weeks or days leading to their scheduled "release". Victims in some scam centres can spend months without sunlight, locked inside single buildings for extended periods of time, with accommodation often being windowless, or where windows are covered to prevent anyone from seeing the conditions inside. In other situations, some movement within the compounds is possible though only between specific buildings (between the office and accommodation most often), and usually only during specific hours of the day under the careful watch of guards.

Online job advertisements are another significant recruitment tool. Opportunities to work at a "cryptocurrency exchange", "tech park", or an "IT start-up" are posted on social media, as well as on job search and recruitment websites, and offer high salaries, benefits, and comfortable working conditions. A few scam centres have even developed recruitment websites, filled with images of Silicon-Valley-style offices and promises of a comfortable lifestyle for staff working there. Positions advertised can range from translators to positions such as sales representatives, IT support, cryptocurrency analysts, models, or human resources specialists.

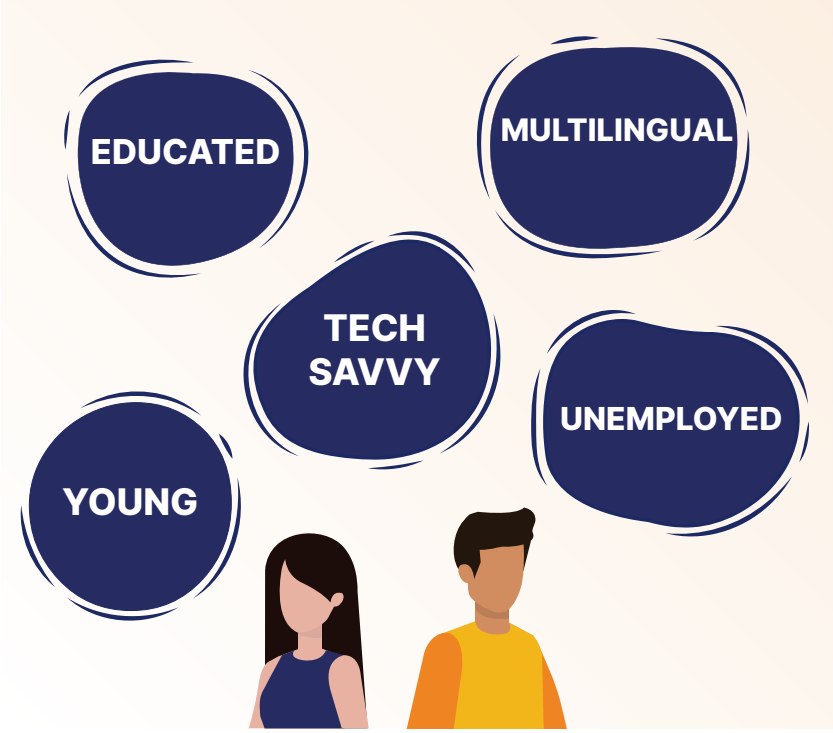


Figure VI. Demographics frequently targeted by scam centre recruiters.

Given the skills needed to operate scams effectively, primarily computer literacy and language skills, the demographics scam centre recruiters target differs significantly from traditional trafficking victim profiles. Trafficking victims for scam centres are typically young, between the ages of 18 and 35, tech savvy, multilingual and educated (Figure VI). Many of those freed from scam centres have degrees, some at the graduate level. Proficiency in English and Chinese are particularly valuable to facilitate communication with both scam victims and the foreign crime bosses funding the scam operations, along with the knowledge of finance, investment, and cryptocurrencies, which is necessary for ensuring scams can be as accurate and convincing as possible.

To facilitate trafficking to the scam centres, victims will most often travel voluntarily, believing they are travelling to legitimate job opportunities and are then either detained in the location they travelled to, or smuggled across borders. Bangkok has become a growing transit hub, as jobs are increasingly advertised as being in Thailand, with transnational crime groups meeting victims at airports or bus stations, before continuing to border regions and forcibly trafficking them across borders.

VI. The Path Forward

INTENSIFYING CROSS-BORDER LAW ENFORCEMENT COLLABORATION

Responses to the growth of online scam centres have begun, and in many cases are making an impact. There are now many instances of specific scam centres being closed, although a number of these cases have reportedly relocated rather than fully ending operations. Further, a significant number of victims have been freed from scam centres with the help of law enforcement or consular officials. These responses, while impactful in specific cases, remain piecemeal, with different understandings of the situation hindering work between national and international counterparts, and with investigations and communication often stopping at national borders. The key challenge, therefore, is how to best ensure regional partners have open lines of communication with each other and can best collaborate in their efforts to counter online scam centres.

Impactful solutions to the scams centre crisis will require addressing these challenges. Intelligence sharing across borders and coordination on regional investigations are needed to ensure criminals cannot simply flee across borders when facing arrest, and that scam centres cannot relocate to new areas when faced with closure. In a similar vein, the challenges of conducting investigations given the ongoing political crisis in Myanmar means that neighbouring countries have a significant role to play in preventing the proliferation of scam centres there. Ensuring online scam centres are shut down, rather than relocated, is essential to preventing their spread.

On a related note, scam centres operate in most cases near borders, often using cross-border telecommunication services and electricity supplies. Reports indicate that in Thailand new cell towers and power lines have been built on multiple occasions in the vicinity of new casino developments across from their borders, many of which appear to be scam centres. The provision of these services directly facilitates the operation of the scam centres. The cutting of cross-border services to the scam centres/casinos, therefore, represents low-hanging fruit in terms of counter-scam centre efforts that could be quickly implemented. Without accessible power and electricity, many scam centres would be forced to cease operations or seek more expensive and difficult-to-connect services nationally.

RECOMMENDATIONS FOR RESPONDING

Launch regularised forums for multi-disciplinary groups of international counterparts to coordinate at the operational and policy levels.

- Coordination through the formation of task forces and coordination groups can act to address specific cases, communicate trafficking patterns, and share intelligence on transnational organised crime structures and operations. A key part of this should be the development of open communication channels between investigators allowing for more regular discussions to take place between counterparts. To facilitate this, the designation of focal points, alongside the appointment of focal agencies within national law enforcement, are important first steps to facilitating this type of open communication and coordination.
- In support of this coordination, multi-disciplinary working groups or teams should be designated – both nationally and regionally. These groups would bring together investigators working to address cybercrime, transnational crime financing, trafficking in persons/people smuggling, money laundering, and any other law enforcement departments investigating elements of online scam centres. Nationally, this would ensure investigators are clear on who is leading investigations, and facilitate faster, more consistent sharing of information. At the regional level, by bringing together this diverse group of law enforcement, and by having coordination meetings with all countries whose citizens are regularly trafficked into scam centres, cross-border investigations will be able to lead to more consistent prosecutions, while also facilitating data sharing that is important to more accurately understanding the full scope of the situation.

Clear standard operating procedures (SOPs) should be developed and implemented to facilitate the rapid sharing of intelligence and evidence.

- Where communication challenges exist, clear and consistent standard operating procedures specific to online scam centre investigations should be developed to facilitate faster and more standardised collaboration, particularly related to intelligence sharing and joint investigations. Clearer and more defined procedures will better support law enforcement in understanding how and when to engage with regional counterparts and will reduce the time needed to attain approvals for sharing specific pieces of evidence, thereby ensuring information being shared is up-to-date and in the hands of the investigators who can act on it.

Intensify research and data collection efforts to quantify the scale of the online scams crisis, including developing estimates of trafficking victim numbers, as well as the number of scam centres currently operating and their revenues.

- Additional research is needed to make sure law enforcement and governments have a consistent understanding of transnational organised crime structures, trends in online scam centre geographies, and TIP trafficking routes. Additional data collection, through regional analysis of victim demographics, analyses of scam centres' online presences, and more detailed understandings of trafficking patterns, will better inform both law enforcement and policymakers as they strive to implement evidence-based solutions.

Prevent the cross-border provision of power and telecoms services to scam centres.

- Online scam centres regularly operate using electricity and telecommunication services from neighbouring countries, and countries cutting these services into identified online scam areas have the potential to greatly hinder operations. Additionally, verification that any new infrastructure being developed is not being constructed to support online scam centres should be done prior to any new services being developed.

IMPLEMENTING SYSTEMATIC STRATEGIES TO COUNTER TRANSNATIONAL ORGANISED CRIME

Transnational organised crime groups are at the centre of online scam centre operations. The need to address transnational organised crime as a whole, rather than just investigating lower-level individuals such as scam centre managers, is vital to responding not only to scam centres, but also for responding to the full range of crimes perpetrated by transnational organised crime – including drug trafficking, illegal wildlife trafficking, and money laundering. While dismantling transnational organised crime groups at scale is an enormous task and one that extends well beyond targeted responses to online scams centres, efforts to respond to online scam centres will only be possible through weakening and systemically addressing the underlying conditions that facilitate the existence of and the continued ability of organised crime to generate massive profits.

One of the most effective means of accomplishing this would be through focusing on financial investigations, cryptocurrency tracing and anti-money laundering. Investigations in this vein have the advantage of being possible even where cross-border investigations are difficult and international law enforcement is lacking, with seizing assets as they cross borders and denying access to the international financial system being one potential strategy for reducing scam centres' profits.

To move forward with these types of investigations, law enforcement in many countries has reported the need for increased capacity, particularly tied to cryptocurrencies. Cryptocurrency transactions, which are increasingly traceable, are erroneously seen by many transnational organised crime groups as anonymous, creating the potential for relatively straightforward investigations to identify the exchanges they are moving their money through, a step that can allow law enforcement to obtain their identities. This is particularly important as cryptocurrencies are being used at scale by scam centres and transnational organised crime in their broader operations as a means of paying their staff, extracting money from victims and moving their earnings across borders.

Corruption also needs to be addressed, with the close proximity of scam centres to law enforcement offices in many locations, and the lack of follow-up investigations after removing specific victims from within scam centres, representing areas of particular concern. Levels of corruption, it is important to note, vary across countries where scam centres are found, as well as between localities and specific departments within each country. In many cases though, scam centres are operating so openly and in such clear violation of local laws and international human rights standards that it is evident corruption must be present to allow for their continued operation. Corruption should be seen as a central factor in the continued operation and growth of scam centres, as well as the trafficking in persons tied to them.

Figure VII. A view of the Mekong's Golden Triangle.

Finally, greater law enforcement presence in special economic zones (SEZs) is needed to interrupt transnational organised crime operations within them. Corruption, a lack of capacity and a lack of clear guidelines for local law enforcement about the applicability of national laws within the SEZs are reported to be barriers to effective enforcement of the rule of law. Awareness raising is needed and clarifications should be issued to all law enforcement working nearby to SEZs throughout Southeast Asia, clarifying that the rule of law still applies in these zones, and providing resources to these law enforcement offices to investigate serious crimes including trafficking in persons, people smuggling, drug trafficking and illegal wildlife crime.

RECOMMENDATIONS FOR RESPONDING

Greater capability development is needed to facilitate anti-money laundering investigations, particularly related to cryptocurrency.

- While coordinating investigations across borders can take time and require international collaboration, which can be less effective than desired during many investigations, national efforts can deny transnational organised crime access to the international banking system and make it more difficult to move funds across borders. By increasing the complexity of money laundering efforts by transnational organised crime, law enforcement and financial regulators can make online scam operations more labour-intensive and expensive to operate, reducing the profit margins of the operations, and discouraging their further proliferation.
- In addition, law enforcement's awareness of cryptocurrency tracing remains lacking within many contexts, with law enforcement, reportedly, at times falsely assuming that cryptocurrency transactions are untraceable. Similarly, many transnational organised crime groups are reportedly moving funds through cryptocurrency exchanges without taking all possible precautions, suggesting they believe either that cryptocurrencies are anonymous, or that law enforcement does not have the capacity to trace their transactions. Through building awareness of the efficacy of cryptocurrency tracing and building capacity to conduct cryptocurrency investigations, there appears to be significant potential to identify the beneficiaries of scam operations, as well as to seize the profits of these operations as they move through crypto exchanges.
- Bolstering financial investigations creates the possibility of identifying those receiving the profits of scam centres, allowing them to be arrested if they are living in countries where law enforcement is proactively investigating scam cases. It also creates an evidence base that will allow key transnational organised crime to be arrested as they travel, either while in transit or at their destination points, thereby restricting their movement. At a minimum, this can serve as a powerful tool for deterring criminals from investing in scam centres moving forward. Optimistically, it can weaken or break down their operations and potentially lead to the arrest of key transnational organised crime figures.

Intensified anti-corruption efforts, particularly through increased political pressure from the international community.

- Where scam centres are operating openly, it is apparent that corruption linked with, at least some senior government and/or law enforcement officials must be present. The high-level nature of this corruption means that measures such as developing or strengthening anti-corruption commissions, or implementing improved corruption reporting channels are unlikely to be sufficient, though these measures may be helpful in areas where scam centres are operating without such deeply entrenched corruption.
- Intensified political pressure from the international community, potentially tied to consequences in terms of trade relationships or development funding, is one potential pathway to reducing corruption and seeing scam centres closed. This pressure should be as well coordinated as possible from a range of international partners to be effective.

Need to build awareness of regulations around SEZs and ensure the rule of law is enforced within them.

- Law enforcement in some countries report they do not have the authority to enforce laws within SEZs. Therefore, awareness needs to be increased about which laws do and do not apply within SEZs, the ability of law enforcement to operate in these zones, and how to prevent transnational organised crime from operating openly within these zones.

Investigators need to follow up on leads related to online scam centres, particularly where criminal activity is openly apparent.

- This is particularly noteworthy in the context where law enforcement enter scam centres at the request of consular officials or international law enforcement counterparts to free specific individuals. Knowing there is one case of trafficking within a locality, law enforcement investigations into others working in these scam centres is critical to ensure they are not also trafficking victims. Particularly in cases where clear indicators such as barbed wire around the compound and armed guards are present, law enforcement should proactively look to build on these initial cases, for example through interviewing those they free from the scam centre to assess the degree of criminality occurring within a given compound.
- Local law enforcement responding to trafficking cases tied to suspected scam centres should refer these cases and pass all relevant evidence to dedicated national law enforcement focal points. This will ensure adequate resources are provided to the investigations while having the added benefit of reducing the potential for local political considerations or conflicts of interest from influencing investigations.

STEPPING-UP ENGAGEMENT WITH THE PRIVATE SECTOR

While private sector actors, particularly a number of leading social media companies, have already taken steps to prevent trafficking in persons through their platforms, the complexity of trafficking for online scam centres means that intensified public-private collaboration would bring significant benefits in support of curbing trafficking to scam centres. Traffickers use a breadth of online means to recruit victims to scam centres, including through messaging apps, job boards, online forums, social media platforms, and, by some accounts, online games.

One proposed collaborative response would involve working with leading tech companies to support the development of a verification process for job advertisements on social media platforms and job boards. This could take several forms. For example, one strategy would be for only verified businesses to be able to post job ads. Alternatively, another strategy could be to develop an artificial intelligence (AI) tool that would flag job ads that contained certain trafficking red flags. A more manual process of reporting could also be scaled up, with tech company employees, law enforcement, consular officials and civil society organisations working jointly to flag and take down suspected illegitimate job advertisements. Nuanced tools will need to be put in place to ensure legitimate businesses are not prevented from posting job advertisements and that verification processes aren't overly strenuous, driving users onto alternative platforms. The goal for any of these solutions is to ensure that those applying for jobs are exposed to fewer fraudulent job ads, or, at minimum, that they are aware of the risk they are taking as they reply to job ads that appear suspicious.

Currently, even when fraudulent job ads or potentially harmful posts are found online, it is difficult in most cases to have these posts taken down. While some platforms have clear methods of reporting posts, many do not, and response times from all platforms are often too long, allowing posts to continue to be seen by potential victims while they are reviewed by platform moderators. Similarly, for law enforcement and prosecutors to effectively investigate and prosecute cases related to trafficking for online scams, they must have the ability to quickly and easily request electronic evidence from the tech companies and platforms involved. This includes access to communication records, user data, and other electronic evidence that may be crucial to building a case against traffickers. Without streamlined processes for requesting and obtaining this evidence, law enforcement efforts to combat trafficking for online scams will continue to be hindered. Some platforms do have user-friendly portals for requesting this type of evidence, but even where portals exist, oftentimes awareness of them is lacking within law enforcement. Therefore, increased public-private collaboration is needed to develop clear and efficient protocols for requesting and sharing electronic evidence, while balancing these needs with the privacy and security of user data.

RECOMMENDATIONS FOR RESPONDING

Work with social media companies and job websites to develop tools which can more effectively identify posts which may be tied to scam centres.

- The development and use of screening software could identify indicators like job locations, common languages, or frequent patterns in how jobs are described, and through this could flag or facilitate the removal of posts most likely to be tied to trafficking. On platforms with human moderators, such software could forward high-risk posts to moderation teams for review or produce warning labels to be attached to the posts. While removal of all high-risk posts would be ideal, where this isn't possible, flagging posts as risky would also be an effective solution that would let job seekers and potential trafficking victims more directly access information about human trafficking risks, assisting them in making informed decisions about which roles to apply for.

Creating clearer communication channels between law enforcement, policy makers and the private sector.

- Clear communication channels between law enforcement, policy makers and the private sector do not exist, and where communication does occur, it doesn't occur with enough frequency to respond to quickly changing situations such as the scam centre crisis. Of note, mechanisms allowing law enforcement to report fraudulent pages or request digital evidence from social media platforms do not currently exist in a standardised way. Many platforms do have methods for this type of reporting, but where this is the case law enforcement is oftentimes uninformed on how to use them. Clearer and more consistent international guidelines around jurisdictional standards, methods for requesting evidence, and how to report illegal activity online are needed so that all platforms have straightforward protocols, and criminals can't simply migrate to platforms with lower security standards.
- To address these challenges, a broader set of private sector actors need to come to the table. Although some leading social media companies engage quite readily, many private sector companies do not engage at all, particularly those based in East and Southeast Asia. Effective solutions require all major platforms to buy into coordinated responses, or at least be open about challenges in communication, fraudulent post identification and removal, and allowing for policymakers to work towards remedying these barriers. In this regard, roundtables and working groups to bring together key actors to discuss improved coordination could be a strong start in addressing this.

Policymakers need to work with tech companies to set minimum standards for post removal, including setting minimum response times for having flagged posts reviewed.

- The development of guidelines for private companies could create accountability mechanisms, and further encourage the investigation of, and action against, potentially fraudulent posts and job advertisements. This could start with voluntary guidelines – allowing tech companies to buy in, and regional companies to join discussions around these guidelines. Such guidelines could create a level playing field between social media companies, job websites and other technology platforms, ensuring no single company faces commercial repercussions for their engagement.

PROVIDING CLEARER GUIDANCE AND PROTOCOLS FOR CONSULAR OFFICIALS

While there is widespread concern related to scam centres as a profit generator for transnational organised crime, conversations surrounding those forced into operating the scams are complex, with a range of responses from different governments having been implemented to date. These approaches are varied and, in many cases, have slowed or prevented the repatriation of trafficking victims to their country of origin or have prevented them from accessing services aiming to assist victims of trafficking. These issues have emerged largely as a result of disagreements over their criminal culpability for the scams they have been operating.

The root causes of this challenge stem from not only different laws and legal frameworks in different jurisdictions regarding cases of forced criminality but also because the lines between criminal and victim are particularly blurry in many cases tied to online scam centres. In these cases, those working in scam centres are reported to cross between the two categories, victim and offender, over time. For example, some labourers begin as forced labour, but later, potentially incentivised by the profits from the scams, choose voluntarily to continue working at the scam centres. Inversely, some scam centre labourers may begin working voluntarily but later become forced labour when their managers at the scam centres prevent them from leaving. These blurred lines between victims and offenders significantly complicate the work of consular officials, law enforcement and prosecutors in determining the status of individuals involved in online scams.

These blurred lines have led consular officials to make determinations based on frequently incomplete information or speculation, inferring from small pieces of available evidence, before making determinations related to consular support. In some cases, for example, the value of an individual's phone has been used to make judgements about the individual's role within a scam operation. Those with expensive phones have been interpreted as more likely to have profited personally from the scam operations, and therefore more likely to be offenders. Given the fact that many operating scams are reported to have access to multiple phones at any given time to operate the scams, it is possible they simply were supplied with expensive phones as a tool to facilitate scams – for example, the need for an iPhone to use iMessage.

Furthermore, ransom payments have emerged as a particularly challenging issue related to freeing victims from online scam centres. Consular officials have been providing different levels of support and guidance regarding these payments, which has complicated responses for other consular officials offering alternative advice. Specifically, there have been several reported cases where embassies have made direct payments to scam centres to free their citizens. More regularly, consular officials from some countries encourage victims trapped in scam centres to pay for their freedom, which is facilitated either through families or friends sending money to the scam centres, or from the "wages" earned by VoTs being used to buy their freedom over time. These ransom payments complicate the situation for consular officials advising against providing payments, as scam centre operators increasingly expect payments to be made in return for freeing victims. Many consular officials caution against making ransom payments as continuing to make payments in exchange for victims' freedom runs the risk of encouraging transnational crime organisations to scale up their trafficking efforts, with the expectation that each victim they traffic will result in a significant payment when they are released.

Visa overstay fines also represent a substantial barrier to victims being able to return to their home country once they have escaped or been removed from a scam centre. Consular officials report challenges working with local law enforcement to excuse these visa overstay fines and a lack of resources or protocols for supporting visa overstay fine repayment, leading to many victims being confined by local law enforcement until fines are paid. Many victims are revictimized in this way after having been freed from scam centres, with their families having to send through substantial money to cover the fines, as well as the cost-of-living expenses while victims are held in detention.

RECOMMENDATIONS FOR RESPONDING

Need to develop updated guidelines featuring best practices for consular officials.

- Responses, to the extent possible, need to be standardised at the regional level. Conversations with relevant actors should be organised to allow best practices to be put forward and clear guidelines for consular officials to be developed, providing improved tools for differentiating victims from perpetrators. This will allow not only for more accurate victim identification but also for cases to be managed more quickly by consular officials, allowing them to respond to a greater number of cases.
- Guidance by consular officials regarding ransom payments should be standardised amongst all those working to respond, or, alternatively, if a common approach isn't feasible, information on any payments made should be shared between consular officials responding to assist their counterparts in making informed decisions regarding guidance offered to their nationals.

Clear protocols are needed to ensure victims aren't required to pay visa overstay fines.

- Trafficking victims should not be re-victimised by law enforcement as a result of bureaucratic protocols. Clearer standards should be developed in countries that have identified scam centres so that victims are exempted from visa fees or overstay fines. Similarly, consular officials should be empowered to pressure local law enforcement to release trafficking victims from detention. Consular officials should also, where relevant, be connected to national anti-corruption authorities to report cases of extortion when scam centre victims are detained in violation of local laws and regulations.

Updated legal frameworks needed in some contexts to ensure victims do not face charges in cases of forced criminality.

- Where relevant, laws should be updated so that trafficking victims are not revictimized by their national legal system, or the legal system of the country they have been trafficked to. Where criminality is forced through manipulation, violence, food deprivation, or similar strategies, victims should not be held legally accountable. Victims in these cases should furthermore be given full access to services provided to other VoTs.

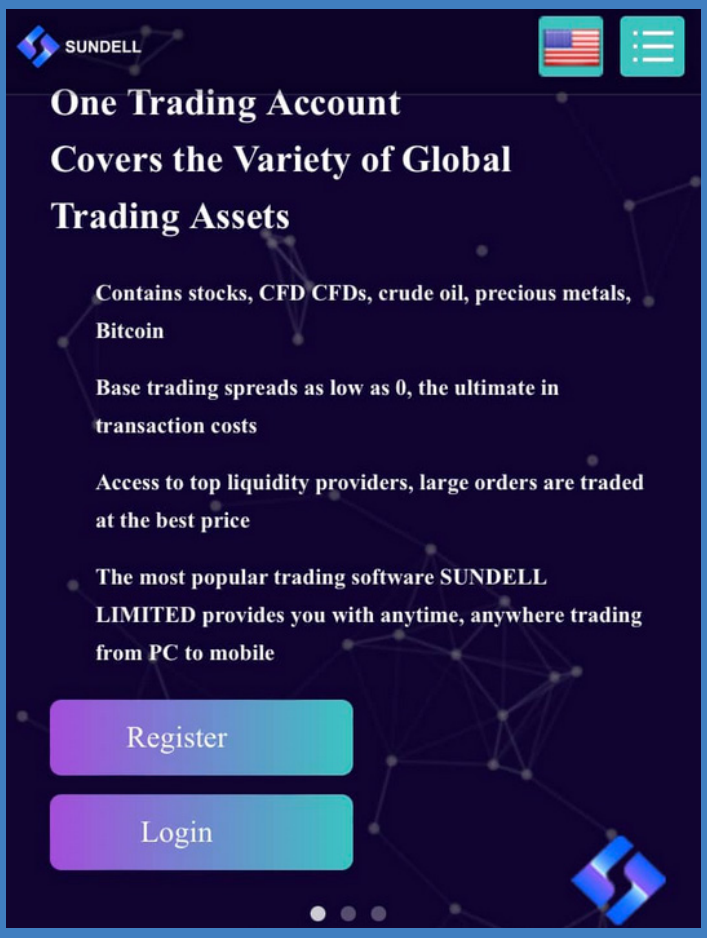


Figure VIII. Example of a reported fraudulent trading platform.

PREVENTING TRAFFICKING THROUGH AWARENESS RAISING

With the new patterns of trafficking in persons tied to online scam centres, past awareness campaigns, as well as trainings tied to trafficking risk and screening for potential trafficking victims at border checkpoints, have quickly become incomplete, and awareness-raising efforts from the past are therefore in urgent need of supplementation.

Those fitting the most common profiles of victims – relatively well-educated, tech-savvy individuals – often do not understand they could be at risk of being trafficked. As a result, they are in many instances not adequately suspicious of the job opportunities being advertised by scam centres. Past advocacy work by governments and civil society groups has built awareness of risks for job seekers in many industries, such as the fishing industry or the garment sector. White-collar desk jobs though have rarely been at the centre of counter-trafficking advocacy campaigns in the Asia-Pacific. Particularly given the resources online scam centres are putting into their recruitment efforts, including using fraudulent company websites, allowing potential trafficking victims to speak with "human resources departments" and providing victims with dubious contracts, greater awareness is needed about how to spot high-risk opportunities amongst target populations.

In addition to this, frontline border officers working to screen for potential trafficking victims at borders have been trained to look for specific demographics in their effort to identify potential trafficking victims. This type of training can be deeply engrained, with many victim identification practices integrated into core training curricula for new recruits and therefore having been used by border officers throughout their careers. Now, as victim profiles have rapidly shifted, there is a need to refresh their understanding of what a typical victim profile looks like, ensuring that they are able to screen effectively for trafficking victims headed towards online scam centres. This is a particularly pressing need in hotspot regions and transit points, where the density of potential victims is likely to be the highest.

RECOMMENDATIONS FOR RESPONDING

Launch awareness-raising campaigns to prevent the trafficking of at-risk populations.

- Targeted awareness-raising campaigns can support efforts to reach at-risk populations and to build a deeper understanding of how to identify job opportunities that may be tied to trafficking in persons, especially fraudulent job advertisements. Building awareness in target populations that they are at risk of trafficking should go some distance towards assisting job-seekers to be more sceptical of job advertisements found online, especially those that seem too good to be true. This could be supplemented by more specific efforts to highlight specific risks, such as travelling across borders for jobs without valid work visas. Campaigns should look to operate at a number of levels, starting within social media platforms and job search websites, but also including elements along trafficking routes, such as within airports and at border crossings.

Building awareness of new victim profiles with customs, immigration and border officials.

- Ensuring frontline officers have the information needed to identify potential victims accurately and effectively is important to improving trafficking prevention. Strategies for addressing this could include awareness-raising events and champions/focal points within immigration departments being assigned to ensure the information on changing trafficking profiles is proactively shared with their colleagues. Additionally, the widespread distribution of handbooks, toolkits or quick reference guides that provide updated information can assist in raising awareness amongst law enforcement officials.

VII. Conclusion

The fact that scam centres are operating so openly, in many cases in clear view of the public, is indicative of both why this issue will be so hard to address – corruption, entrenched interests, and the need for greater political will remain a significant barrier. However, it also highlights why the international community can be confident impactful solutions can be implemented. Law enforcement knows where many of these scam centres are located, have the potential to see in many cases how they're moving their profits, and there are clear ideas of how to begin responding. What is needed now is coordination, motivation, and a sense of urgency. If law enforcement and policymakers can come together, and if coordination with the private sector can be done in a more structured and thoughtful manner, it will be only a matter of time before the profits of scam centres diminish and organised crime groups view these scam operations more as a hindrance than as a reliable means of generating profits.

While the challenges faced in responding to online scam centres are numerous, it is encouraging to see so many proposals for action have been put forward, and that some are already being implemented. This policy brief has laid out the central challenges in implementing these solutions, providing an anchor to conversations around scam centres and where response efforts should be focussed. In unison, the brief has put forward a range of potential solutions, albeit in most cases in relatively general terms, based in large part on feedback received during the RSO's Thematic Dialogue on Preventing and Responding to Online Scam Enterprises. These response options will need further refinement, alongside trial and error as the region looks to respond. Open conversation, ongoing problem-solving, and the allocation of significant resources will need to be put in place if these responses are going to have a real-world impact. The next steps will be defining, shaping whether scam centres become a long-term feature of the criminal landscape, or whether, through working together and concerted effort, they will soon be remembered as a trend of the past.

REGIONAL SUPPORT OFFICE
THE BALI PROCESS

Regional Support Office of the Bali Process (RSO)
27th Floor Rajanakarn Building
3 South Sathorn Road, Sathorn, Bangkok 10120, Thailand
Tel. +66 2 343 9477 Fax. +66 2 676 7337
info@rso.baliprocess.net

For further information on the Bali Process and the RSO please visit **www.baliprocess.net**