MEKONG
CLUB

# From Fake Job Ads to Human Trafficking

## The Horrifying Reality of the Human Trafficking Scam Trade

# Acknowledgements

We would like to thank everyone who was involved in producing this publication, from data collection to editing. Particularly, we want to acknowledge **Nolan Clack** from the Mekong Club for his coordination and writing efforts. We also want to thank **Matthew Friedman** from the Mekong Club for making this report possible. Lastly, a big thank you to **Matthew Keeler**, a volunteer from the Mekong Club, for supporting the proofreading and editing of this report.

In addition, but not secondarily, we must thank our external collaborators who helped write sections of this paper. A huge thank you to the following for their valuable contributions:

**Valentina Casulli** – Project Officer for Humanity Research Consultancy

**Mina Chiang** – Founder and Director for Humanity Research Consultancy

**Larry Cameron** – Chief Information Security Officer for Anti-Human Trafficking Intelligence Initiative

**Aaron Kahler** – Founder and Chief Executive Officer for Anti-Human Trafficking Intelligence Initiative

**Ian Mitchell –** Founder and Board Chair for The Knoble

**Please be advised that some of the content and visuals in this publication may be disturbing to some readers.**

# Table of Contents

## Executive Summary

This publication provides a comprehensive analysis of a new crime that emerged in 2022. It involves fraud, human trafficking, modern slavery, cryptocurrencies and money laundering, hereby referred to as the 'human trafficking scam trade'.

There are two victims to this crime, victims of human trafficking, and victims of the scams. This emerging trend of human trafficking involves individuals being lured into compounds in different regions across Southeast Asia. Whilst in the compounds, they are forced to scam others against their will, often trapped in debt bondage, and subjected to physical and sexual violence, along with other forms of abuse, if they refuse to comply.

One of the most common scams to emerge from the compounds is known as the 'pig butchering scam'. This involves the scammer building a trusting, sometimes romantic, relationship with the target before persuading them to invest money into a fake platform, only to later freeze their account and seize the money, 'butchering' the target.

We will highlight the key indicators of human trafficking, providing readers with a clear understanding of how victims are lured into these situations and the processes involved in the scamming operations. The paper also explores case studies that illustrate how the scammers operate and the tactics they use to evade detection. One of the challenges faced by law enforcement is the sophisticated methods used by the criminals to connect multiple IP addresses, making it difficult to trace the networks and disrupt the traffickers' operations.

To prevent these scams and similar types of fraud, we will recommend how individuals, organisations, and public sector partners can collaborate to raise awareness and take steps to prevent these crimes from occurring. This includes partnering with nonprofits to ensure prevention, detection, and remediation of such cases and to prevent criminal networks from hiding within private sector operations and supply chains. Additionally, we recommend exploring how traditional financial institutions can ensure funds generated from these crimes do not end up in their operations.

By understanding the key indicators and tactics that the criminals use, individuals and organisations can take steps to prevent these scams and protect vulnerable individuals from exploitation.

## Introduction

In the fight against modern slavery and trafficking, the private sector plays a crucial role as it serves as the primary channel for 70% of the flows of illicit activities. Money is at the core of this insidious crime, flowing in and out of different countries through various channels. Modern-day slavery generates an estimated US$150 billion in profits each year, a significant portion of which is being funnelled into the global financial system.

The financial services industry, being at the forefront of this system, has a unique opportunity to detect suspicious activities and trends associated with money laundering and slavery. Proper training can empower this industry to identify new forms of financial fraud, thereby reducing the risks associated with illegal and fraudulent businesses. As such, the financial services industry can take a proactive stance in the fight against modern slavery and trafficking.

According to estimates by the United Nations Interagency Project on Human Trafficking (UNIAP), someone becomes a victim of modern slavery every four seconds, with the criminal industry that fuels this practice earning over US$285,000 every minute. These statistics highlight the alarming scale and global reach of modern slavery and trafficking, which reduces human beings to mere commodities.

These crimes are not confined to any specific geographic region or industry; rather, they are prevalent across supply chains and affect individuals in both developed and developing nations. The immense profits generated by modern slavery and human trafficking make it one of the world's most lucrative criminal enterprises, second only to the drug trade. These profits are derived from the exploitation of an estimated 50 million people, making it a highly pervasive industry.

Due to its reliance on access to financial institutions, modern slavery and trafficking represent not only a destination for illicit proceeds but also a conduit for financing the entire process. Financial institutions are increasingly recognising their pivotal role in combating modern slavery and trafficking and are actively exploring ways to disrupt the flow of money that sustains this practice.

While the goal of completely eradicating modern-day slavery may be unrealistic, efforts to cut off its financial lifeline must not falter. By limiting the funds that support these heinous practices, we can help reduce the prevalence of modern slavery and human trafficking.

Recognition of modern slavery and human trafficking issues linked to cryptocurrencies is an emerging trend first seen toward the end of 2022. Traditional financial institutions need to be aware of how this could be used to launder money, and more specifically how it's linked to modern slavery and human trafficking. So, what are cryptocurrencies and how are they used to launder money?

Cryptocurrencies are a type of digital asset designed to work as a medium of exchange. They use cryptography to secure and verify transactions as well as to control the creation of new units. Since cryptocurrencies are decentralised and operate on a distributed ledger called the blockchain, this means that transactions are recorded across a network of computers, making them difficult to manipulate or hack. Although cryptocurrencies are commonly used for legitimate purposes such as purchasing goods and services, investing, and sending money to family and friends, they are also used for illicit activities such as money laundering. Cryptocurrencies can be used to launder money because they offer a level of anonymity and can be easily transferred across borders without the need for intermediaries like banks.

A common method of using cryptocurrencies to launder money is called the 'mixing' process. Mixing involves combining funds from multiple transactions or wallets and then redistributing them to new wallets. This can make it difficult to trace the origin of funds and link them to criminal activity. Another method of using cryptocurrencies for money laundering is 'tumbling' services. Tumbling services are online platforms that offer to break up large cryptocurrency transactions into smaller ones, which are then sent to multiple recipients to obscure the original source of the funds. Other methods include unregulated exchanges, peer-to-peer (P2P), prepaid cards, gaming sites and ATMs. Typically, with almost all the methods mentioned, transactions from criminals can then be used to launder money by converting the cryptocurrencies into cash or other assets.

The methods mentioned above are just some of the tactics used to conduct the  pig butchering scams that commonly emerge from the scamming compounds. Victims in the compounds are often recruited overseas via fake job advertisements, enticed by high salaries, free flights, dream jobs and the opportunity to experience a new country. However, upon arrival they will be trafficked to a compound and forced to defraud individuals worldwide, including those in the United States, Canada, Europe, and other developed nations. Those who refuse may be subjected to physical violence, food deprivation, electric shocks and consumption of illicit drugs to keep them from sleeping and continue scamming (Podkul and Lui, 2022).

Human rights advocates, law enforcement officials, rescuers, and victims of this form of human trafficking have reported that hundreds of thousands of individuals from China, Taiwan, Brazil, the United States, Ethiopia and other countries across the globe have been trafficked into the scamming compounds (Chiang and Casulli, 2023). Victims come from a range of backgrounds, many being English-speaking professionals and students educated to degree level.

The term 'pig butchering' has become widely recognised in the field of anti-money laundering and is often associated with the Association of Certified Anti-Money Laundering Specialists (ACAMS), although they did not coin the phrase.

ACAMS's global reputation as experts in this field coupled with their use of the term, has contributed to its widespread recognition. These types of scams, typically entail scammers making unsolicited contact with individuals, gaining their trust, and then deceiving them into investing in bogus ventures, this process is commonly referred to as the 'fattening of the pig'. Once the funds are obtained, the fraudsters 'butcher' the victim and then disappear without a trace.

In this publication, a team of experts has shared their collective knowledge to argue that the term currently used does not accurately reflect the gravity of the situation in terms of its impact on the financial system, the general public, and the victims who are coerced into carrying out the scams against their will. The act of modern slavery and human trafficking is at the heart of the issue, and as a more appropriate alternative, the authors have chosen to use the term 'human trafficking scam trade' throughout the remainder of this publication to refer to the crime as a whole. The term 'human trafficking scam trade' accurately captures the interconnectedness of these two types of crimes – human trafficking and fraud – and will be utilised within the context of this paper.

The objective of this publication is to increase awareness about the human trafficking scam trade among various stakeholders within the public and private sector, and the general public. It offers a detailed analysis of scams and provides valuable recommendations for action against this crime.

# **Inside the Human Trafficking Scam Trade:** How it Works and How it Preys on the Vulnerable

This section aims to shed light on the abhorrent crimes of human trafficking, modern slavery, and forced labour. It is essential to understand the indicators that differentiate this type of criminal activity from others before delving into its mechanics. Survivors of the scamming compounds face numerous indicators outlined by the International Labour Organization (ILO).

Restriction of movement. Survivors reported being unable to leave the building or scamming compound, and attempting to escape could result in severe physical violence or death.

Physical and sexual violence. Victims were subjected to physical and sexual violence, including beatings and electronic shocks, and some reported being raped.

Victims being openly sold between enslavers. Some victims were sold multiple times when their performance in scamming was low. One identified victim was sold for US$25,000.

Debt bondage. Victims were often told they owed the company/enslavers money and were charged bogus fees such as ‘floor-wearing fees’, ‘air-breathing fees’ and more.

Other indicators of human trafficking, modern slavery and forced labour include abuse of vulnerability, deception, isolation, intimidation and threats, retention of identity documents, withholding of wages, abusive working and living conditions, and excessive overwork (Chiang and Chen, 2022).

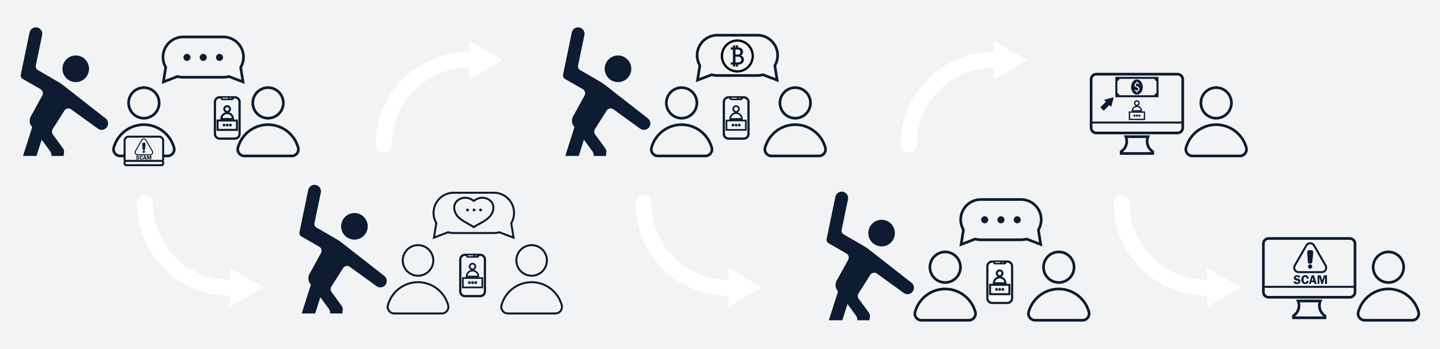
The different companies that operate in the scamming compounds often specialise in various scamming techniques; this includes targeting specific types of ‘clients’ or scamming victims.

The scams conducted by those in the compounds target people from the Western world, particularly North America and Western Europe, along with people across Asia in places such as Hong Kong, Taiwan and Thailand (Farivar, 2022). Criminals working in the compounds distribute Hong Kong, Thai and Taiwanese sim cards to the trafficking victims. These sim cards are used to contact and scam people from the respective areas. The victims who achieve a higher key performance indicator (KPI) will be tasked with scamming Hong Kongers, as the criminals generally make more money from such targets (TNAOT, 2021). Those with a lower KPI will scam targets from other nations across Asia.

## An Illustration of the Process

Vū is a victim of human trafficking where he is forced by criminals to contact people on dating apps to scam them. Vū is told by his captor to use a dating app to make contact with his victim, Ying, a successful and wealthy woman from Hong Kong looking for love. She is enticed by Vū's lies, and they build a relationship. From Ying's perspective, Vū appears to be very successful in the cryptocurrency space. Being wealthy, she is intrigued by his success and how she can get involved. Vū assures her of big returns, and she sends money to a fake website. As time goes by, Ying continues to speak with Vū and continues to invest. He continues to show her returns on investment and she continues to believe she is building her investment portfolio.

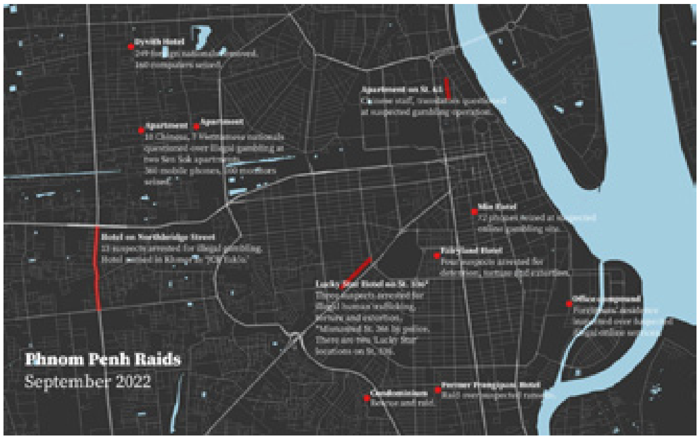
Eventually, Ying is ready to cash out. Vū informs her that she needs to invest a bit more to cover taxes before she can cash out. Ying wants her money back, and complies with the request. Upon this last transaction, Ying can no longer contact Vū about obtaining her funds. After investigating, she realises that she has fallen victim to a scam and lost hundreds of thousands of dollars. Ying has lost her money and Vū is still a victim forced to scam against his will. The only beneficiaries are his captors, who will continue to replicate and become better at this process through trial and error.



Victims in the compounds are given numerous mobile phones and computers, so they can carry out a large number of scams simultaneously at any given time. The process of the scam is thoroughly thought out and constructed by the traffickers with psychological tactics in mind for the purpose of inducing victims into investing in fake investment websites.

While some victims are fraudulently recruited to the compounds, others go voluntarily to conduct scams. Many of the latter are wanted by authorities in their home country. However, in both scenarios, they may be subject to violence, torture, and restrictions of movement, and become forced labourers (Chiang and Casulli, 2023). Some people in the compounds also become recruiters, getting paid thousands to lure others – even family and friends – into the compounds on fake job proposals. Some victims are forced to do this and others do so voluntarily.

In the past few years, amid the pandemic, a significant number of individuals from Southeast Asia, comprising a substantial number of Malaysians and Thais, have been deceived by job offers and subjected to enslavement. Several initially found themselves trapped in Cambodia, where they were detained and coerced into working in fraudulent call centres run by criminal organisations.



Source: Michael Dickison (2022)

Whilst international attention and media coverage of this crime began with a large focus on compounds in Cambodia, compounds have been operating in other nations such as Laos and Myanmar for similar periods of time, many operating in 'special economic zones'. However, there is currently not enough evidence to confidently illustrate the timeline of activities within the compounds across the different countries.

A growing focus on compounds in Cambodia, and increased scrutiny from national consulates and governments beyond the country's borders may have also led to more scamming compounds appearing in Myanmar.

The lack of support available to victims as a result of the coup in Myanmar allows for a breeding ground of compounds, particularly along the Myanmar-Thailand border .

Those conducting the scams will start the process by creating a charming persona that will appeal to the person they are targeting. Much like the example mentioned above, a male character that has recently been through a divorce, or has parents in ill health, would be presented to highly educated female victims to win their sympathy. Traffickers provide victims in the scamming compounds with playbooks instructing them on what to say to their target.

Through these interactions, the traffickers aim to learn more about the target's financial situation and personal characteristics. This will then influence the way in which the scam proceeds to increase the rate of success. The victims in the compounds are forced to continually build on relationships with targets, often working on numerous targets at any given time. After a trusting relationship has been established, they will then mention cryptocurrency and the success they have had in their cryptocurrency investments, gently suggesting the target invests some money into the site.

To begin with, the target will make financial returns from their investment in order to make the investment seem legitimate, encouraging them to invest more money into the site. However, the website or app used is in fact fake and allows the traffickers full access to the target's bank account and funds. Once the target feels comfortable to invest a large amount of money into the system, their accounts are frozen and emptied by the criminal companies operating in the scamming compounds.

### Step-by-step Summary of the Tactics Used by Victims Forced to Scam to Defraud Unsuspecting Victims of Their Funds:

The scammer initiates contact with the target, typically through social media or via a fake 'wrong number' text.

The scammer develops trust with the target by sharing personal information, generating empathy and emotional pressure, whilst also assessing the target's financial position.

The scammer gradually introduces the topic of cryptocurrency investment and convinces the target to invest.

The scammer persists in encouraging investment until the target transfers a significant amount to the fraudulent investment platform.

> "My company/enslaver specialised in scamming the North American market, and that's why they particularly want workers/slaves who understand English. My company has the ability to obtain endless new American phone numbers to send SMS to potential scamming victims. We send messages like 'hey are you going to the weekend party?' and once they reply 'you send it to the wrong person', we will reply really politely, and start making them fall in love with our characters. The goal is to make them invest in our platform. Some victims sold two houses and lost millions to my company/enslaver." (Chiang and Chen, 2022).
>
> **-Testimony from survivor forced to scam.**

# **Outsmarting the System:** Devious Tactics Employed by Traffickers to Avoid Detection and Continue Criminal Activities

The increasing prevalence of criminal organisations and their adoption of intricate techniques to evade detection and sustain their illicit operations has become a pressing issue. Their employment of covert methods, unorthodox payment mechanisms, deceitful ploys to attract targets and willingness to resort to violence are among the topics discussed in this section.

## How Criminal Networks are Staying Under the Radar with Money Flows

Sophisticated tactics to stay one step ahead of law enforcement agencies have made this crime one of the most challenging to track. One of the most common tactics is to use unconventional payment methods that make it difficult for authorities to track their activities. These methods include exchanging for cash, prepaid credit cards, gift cards, and peer-to-peer transactions.

Scammers have also used decentralised exchanges and decentralised finance (DeFi) platforms to launder their ill-gotten gains. These platforms allow them to move money around without leaving a trace, making it almost impossible for investigators to track down the source of the funds. In addition, scammers are using privacy coins and off-chain transactions to avoid detection.

Lastly, another tactic employed by the scammers is to use high-risk exchanges that are unregulated and offer anonymity to users. By using these exchanges, scammers can move large sums of money without drawing attention to themselves. They also use multiple output transactions, which allow them to send money to multiple addresses at the same time, making it harder for authorities to trace the flow of funds. The findings of our analysis revealed a total of 15 exchanges that were utilised, with a significant number of tokens linked to Ethereum crypto addresses, which are now defunct and have been identified as fraudulent. The level of organisation involved in these devious tactics is quite alarming, as measures have been put in place to evade detection and ensure the smooth running of their illegal activities. The rise of these devious tactics has made it imperative for authorities to remain vigilant and adopt new strategies to outsmart the scammers (ATII, 2023).

# Understanding the Various Illicit Activities Employed by Traffickers to Succeed in Their Deceptive Schemes

The scams perpetrated by criminals extend far beyond simply theft or fraud. In many cases, these individuals and organisations engage in a wide range of illegal activities to further their aims, often with the goal of evading detection and punishment, beyond the romance scam example from the start of the publication.

## Casinos

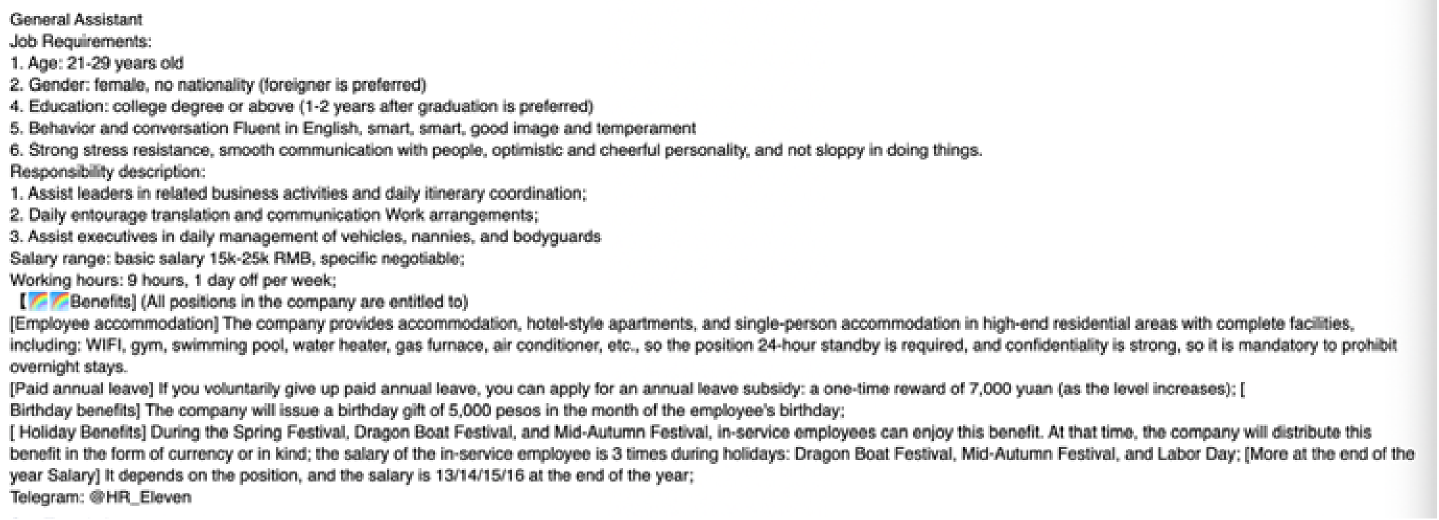
A tactic employed by scammers is the use of illegal gambling, often centred around casinos in locations such as Sihanoukville, Cambodia or casinos bordering other countries around the Kingdom. These casinos have been used to launder money and facilitate illicit financial transactions, all while providing a veneer of legitimacy to criminal enterprises (Gibbs, 2022).

## Deceptive Job Recruitment

Another tactic used by the criminal networks is the creation of fake recruitment campaigns which have lured unsuspecting abroad. This can be particularly damaging in areas where employment opportunities are scarce or underpaid, as individuals may be more likely to look for work overseas or accept jobs that appear 'too good to be true' out of desperation.

Five common recruitment methods to lure victims into the scamming compounds have been identified by Humanity Research Consultancy, who work directly with victims. The first method is to recruit through legal, primary job-matching websites where traffickers pretend to be regular companies such as gaming companies recruiting workers.

The second method is to recruit through private job-matching groups on social media and other online platforms where traffickers approach and lure victims.



General Assistant
Job Requirements:
1. Age: 21-29 years old
2. Gender: female, no nationality (foreigner is preferred)
4. Education: college degree or above (1-2 years after graduation is preferred)
5. Behavior and conversation Fluent in English, smart, smart, good image and temperament
6. Strong stress resistance, smooth communication with people, optimistic and cheerful personality, and not sloppy in doing things.
Responsibility description:
1. Assist leaders in related business activities and daily itinerary coordination;
2. Daily entourage translation and communication Work arrangements;
3. Assist executives in daily management of vehicles, nannies, and bodyguards
Salary range: basic salary 15k-25k RMB, specific negotiable;
Working hours: 9 hours, 1 day off per week;
【🌈🌈Benefits] (All positions in the company are entitled to)
[Employee accommodation] The company provides accommodation, hotel-style apartments, and single-person accommodation in high-end residential areas with complete facilities, including: WIFI, gym, swimming pool, water heater, gas furnace, air conditioner, etc., so the position 24-hour standby is required, and confidentiality is strong, so it is mandatory to prohibit overnight stays.
[Paid annual leave] If you voluntarily give up paid annual leave, you can apply for an annual leave subsidy: a one-time reward of 7,000 yuan (as the level increases); [ Birthday benefits] The company will issue a birthday gift of 5,000 pesos in the month of the employee's birthday;
[ Holiday Benefits] During the Spring Festival, Dragon Boat Festival, and Mid-Autumn Festival, in-service employees can enjoy this benefit. At that time, the company will distribute this benefit in the form of currency or in kind; the salary of the in-service employee is 3 times during holidays: Dragon Boat Festival, Mid-Autumn Festival, and Labor Day; [More at the end of the year Salary] It depends on the position, and the salary is 13/14/15/16 at the end of the year;
Telegram: @HR_Eleven

The third method involves recruiting victims through personal networks. Some victims reported being invited by their university or high school friends who were already working in Cambodia or Myanmar. In other cases, victims were assigned to the 'human resource' department in the scamming compound and were forced to lure 5 to 10 more victims to join the company.

The fourth recruitment method involves traffickers posing as a potential client to lure professionals. Traffickers pretend to be potential customers, inviting magicians, interior designers, and tour guides to visit Cambodia and provide services.

Lastly, victims can be kidnapped on the street. Some victims were kidnapped during their visit to Cambodia and forced to work in the scamming compounds (Chiang and Chen, 2022).

These recruitment methods demonstrate the lengths that traffickers will go to exploit vulnerable individuals for profit. It is imperative that law enforcement agencies, nonprofits and government agencies work together to crack down on these criminal activities and bring those responsible to justice.

## Fake Documentation

To further bolster their schemes, the traffickers may also create fake paperwork or documents, including passports and visas, to create the appearance of legitimacy. This can be particularly effective in cross-border criminal activity where the illusion of official documentation can help mask illegal activity through trafficking victims into compounds across countries (Abad, 2023).

## Custom Software

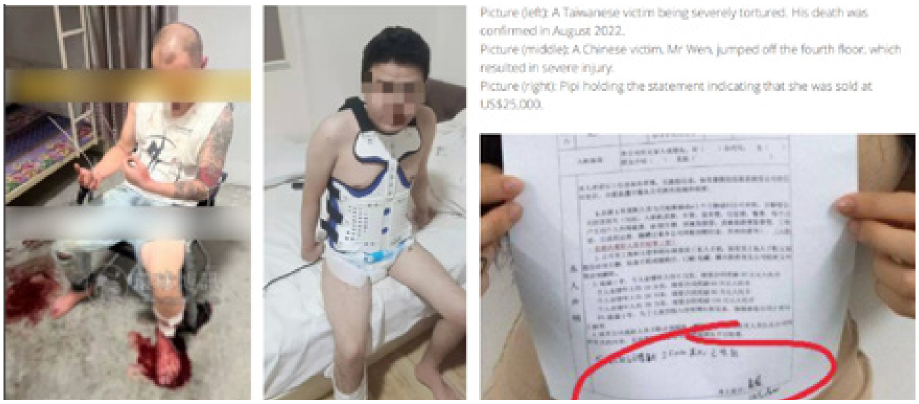
In their attempts to outsmart the system and avoid detection, scammers have used custom software that conceals their activity. This may involve the use of virtual private networks (VPNs) and other tools that obscure their online presence and protect their anonymity.

The use of custom software is particularly effective for the scammers as it enables them to create a false trail that leads investigators away from the true location or identity. By using advanced technology and tools, scammers can also manipulate data and create fake identities that are difficult to trace (Global Anti-Scam, 2022).

## Use of Violence

The use of violence and other extreme measures, such as torture, murder, or other human rights violations, have been documented in the scamming compounds and the criminal networks operating in relation to these crimes.

Criminal rings may use violent measures to intimidate victims and prevent them from reporting or escaping the scam compounds, and when the victim forced to scam refuses to comply. Victims may be threatened with physical harm or even death if they refuse to comply with the criminals' demands.



Picture (left): A Taiwanese victim being severely tortured. His death was confirmed in August 2022.
Picture (middle): A Chinese victim, Mr Wen, jumped off the fourth floor, which resulted in severe injury.
Picture (right): Pipi holding the statement indicating that she was sold at US$25,000.

Source: HRC Briefing (2022)

# **Unveiling the Multifaceted Consequences of the Human Trafficking Scam Trade:** Economic Loss, Psychological Trauma, Reputational Damage, and Implications for Financial Systems and Regulations.

The scams can leave a trail of destruction in their wake, affecting not only the victims who fall prey to them but also those who are coerced into carrying out the scams. Whether a victim is forced to scam or falls victim to the scam, the consequences are often devastating, ranging from financial ruin to deep psychological trauma. In this section, we'll explore the similarities in the impacts of the scams on these two types of victims and the steps we can take to help mitigate the harm caused by these insidious practices.

## **The Costly Aftermath:** Examining the Economic and Social Impact of Scams on Victims

### The Scam from the End Victims' Perspective

Many victims of these scams have lost substantial amounts of money, sometimes even their entire life savings, leaving them in dire financial straits. The shame and humiliation that comes with being scammed are often compounded by societal attitudes that blame and shame the victim. This can make it difficult for victims to seek help or talk about their experience with loved ones or law enforcement, leading to feelings of isolation and despair.

Scammers often target vulnerable individuals who may be experiencing difficult life events, such as divorce or the loss of a loved one, making them more susceptible to the tactics of the scammer. The psychological toll of being scammed can be devastating, with many victims suffering from anxiety, depression, and other mental health issues as a result. In some extreme cases, victims have even taken their own lives in the aftermath of being scammed.

It's important to recognise the severity of the impact that these scams have on victims and to take steps to prevent and address these crimes.

# The Impact on the Victims Being Forced to Scam

Victims who are forced into scamming experience unimaginable hardships while being held captive, and the aftermath of their release can be equally as challenging. The psychological and emotional scars they bear from their captivity can make it difficult to integrate back into society and rebuild their lives. Moreover, the shame of being lured into the compounds and the stigma attached to scamming others can exacerbate their trauma, often accompanied by the societal shame many victims are faced with surrounding what they've been through and the lack of survivor-centred support that is available to them.

The victims in the compounds are trapped in debt bondage, a form of modern slavery whereby the company they are being enslaved by claims they are owed money for things such as accommodation and travel costs to the compound, along with other deceptive items such as 'air-breathing fees' or 'keyboard-wearing fees'. Victims are forced to work in order to repay this debt.

Some of the victims are sold multiple times between different companies operating in the scamming compounds for tens of thousands of dollars. Often, the victims are sold for twice as much as they were originally purchased, doubling and sometimes tripling their debt. Company managers often claim they will release the victims for a fee which is paid by the victims themselves or by their family members back home. Numerous survivors face extreme financial difficulties during and after their time in the compounds as a result of the large payments demanded by the traffickers.

## Many victims remain in a state of vulnerability after being rescued and returning to their home countries. Reasons include:

Insufficient financial and psychological resources provided by the government to support survivors' reintegration journey.

A lack of understanding from authorities regarding the aspect of forced criminality that surrounds these victims' trafficking situation; they may be regarded as criminals for the scamming activities they have been forced to conduct and wrongly prosecuted or ostracised.

Societal discrimination towards trafficking victims. This can lead to victims being viewed as unintelligent and accused of wasting authorities' time. Such reactions generate a lot of shame around victim support. There are even cases where some victims are disowned by their families.

Survivors of these scams who return home often face significant challenges reintegrating into their communities. They may have difficulty finding employment or housing and may struggle with physical and emotional scars from their experience. These difficulties can leave them vulnerable to being re-trafficked, especially if they are unable to meet their basic needs or find support in their community.

One particular risk factor for re-trafficking is if the survivor chooses to travel abroad again in search of new opportunities. Traffickers may take advantage of their vulnerability and offer them false promises of employment or education, only to subject them to trafficking once again. It's crucial that survivors receive appropriate support and resources to help them reintegrate into their communities and reduce their risk of re-trafficking. This includes access to education and training programs, mental health services, and legal assistance (Chiang and Chen, 2022).

## Victims Story

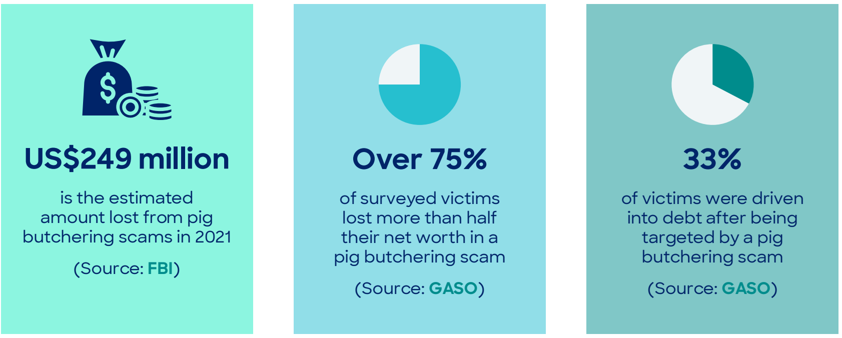
"I am a survivor of human trafficking and modern slavery. From April-September 2022, I was forced to work in a scamming compound in Sihanoukville, Cambodia and was sold 4 times for as much as $10,000 to different companies that operated within the compound. It was a hell-like experience as the compounds used violence to control us, restricted our freedom, and forced us to be complicit in the scamming of innocent individuals across the US and Europe. After several months, I was able to leave the compound with the help of both the Global Anti-Scam Organisation (GASO) and Humanity Research Consultancy (HRC)."

(Abdus, 2023)

## Impact of Online Scams on the Financial System and Emerging Fraud Regulations

The global issue of online scams is one of the worst financial crime's facing the world today. The scale of this issue is immense, and according to a recent report from the FBI's Internet Crime Complaint Center (IC3), internet scams increased to over US$10 billion in losses in 2022. This problem goes beyond financial crime, as it is linked to the suffering of innocent people. On one side of the equation, people's life savings are being stolen, while on the other side, human trafficking and modern slavery are occurring in order to make these scams possible, enabling monies to be mulled globally to fund complex and organised criminal enterprises.

### Quick Facts



**US$249 million**

is the estimated amount lost from pig butchering scams in 2021

(Source: **FBI**)

**Over 75%**

of surveyed victims lost more than half their net worth in a pig butchering scam

(Source: **GASO**)

**33%**

of victims were driven into debt after being targeted by a pig butchering scam

(Source: **GASO**)

Source: ACAMS (2023).

The scams target vulnerable individuals, and the attack vectors evolve and change with the need and vulnerability. The problem is that all people are vulnerable in one way or another, whether it be emotionally, financially, or socially. The increased sophistication of the criminals is now providing a way for them to scale using complex technologies to expand their reach and tailor their attacks.

Moreover, compounding this issue is the fact that traditionally, banks haven't placed as much attention on building robust anti-scam programs that leverage the power of their proactive anti-fraud defences. While most efforts to date have been largely focused on education and awareness, the more progressive banks have started to offer proactive education before a scam event occurs. However, advanced defences against scams to protect customers proactively and analytically are still nascent, and so are the industry solutions to assist banks.

As a result of the increase in activity, new and increased government attention has caused banks to enhance their anti-scam programs and deploy their robust defences against the emerging threat. The challenge of regulating emerging forms of fraud is significant, and there is a risk of contagion that must be addressed. The development of new technologies, including blockchain and artificial intelligence, can play a significant role in combating this problem. However, until these technologies are widely adopted, the financial system will continue to be vulnerable to these types of attacks.

The global scam problem is a complex issue that will require a multifaceted approach to address. The financial system will need to be better equipped to detect and prevent these scams from occurring, and education and awareness must continue to be a focus for both the private and public sectors. While it is an uphill battle, by working together, we can better understand how to be one step ahead of criminal activities.

# Exploring Real-life Case Studies of the Scams:
Responses, Lessons Learned and Strategies for Prevention

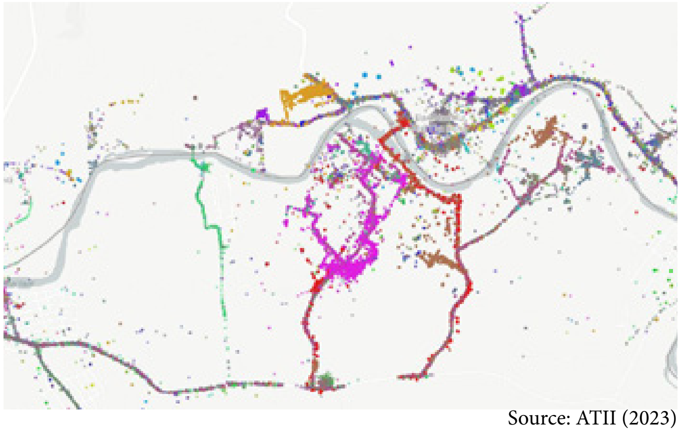
In this section, we will examine specific cases of the human trafficking scam trade, including common victim demographics, the perpetrators, and the outcomes of these fraudulent schemes. By analysing these case studies, we aim to identify common patterns and modus operandi of the scams, as well as how they have evolved over time. A visual map will be included to help better understand the scope of these scams. We'll also compare the cases across different regions and countries, identifying commonalities and patterns.

## Exploring the Use of International Internet Connections by Scammers to Commit Crimes

The rise of these international scams has become a growing concern for governments worldwide. In one instance, it was discovered that criminals were bringing internet connectivity from Thailand into Cambodia, and using it to commit fraud on a massive scale. An estimated 10,000 internet lines were used by the scammers to commit the scams. Shockingly, government employees were allegedly involved in the state-owned telecommunications company running cables across the border.

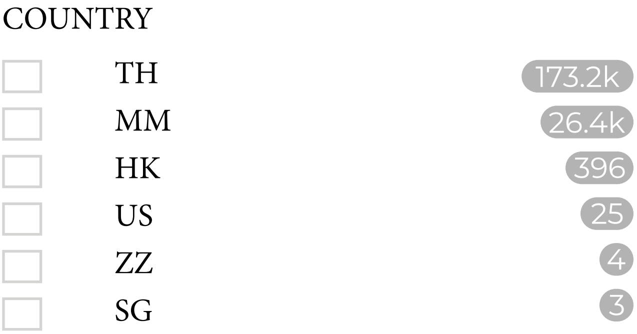
Authorities have taken steps to combat these crimes, including police raids to suppress call scammers by cutting off their internet access. In one operation, officers found 30 internet cables running across the Thai-Cambodian border, which were believed to serve the call scam gangs. The 10,000 plus internet lines supported from 30 internet cables led to the defrauding of many Thai nationals. Police have found that the cables were used to illegally extend internet access to the neighbouring country. During the raids, police arrested eight suspects, including government employees (Ngamkham, 2022).

By conducting a geo-fencing operation, a list of seven internet service providers (ISPs) and mobile carriers was obtained, along with a reverse lookup for the domain used on these IP addresses. An example has been provided below, which displays a small area around the compound. It was discovered that the majority of these IP addresses were located in Thailand, with a few clusters of activity found in the vicinity of the compounds in Myanmar.



Source: ATII (2023)

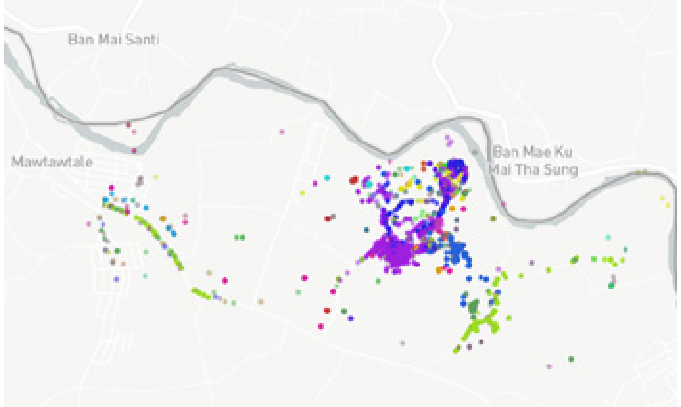
Various filters are available for pinpointing specific cross-border internet activity scenarios. By leveraging geo-location data and comparing it to a comprehensive database of IP address assignments and allocations by ISPs, analysts have identified a highly precise technique for detecting such activity. The analysis shows a large disparity between the numbers of hits in Thailand (172,000) and Myanmar (26,400) which is unusual as Myanmar should have the most hits.



| COUNTRY | | |
|---|---|---|
| □ | TH | 173.2k |
| □ | MM | 26.4k |
| □ | HK | 396 |
| □ | US | 25 |
| □ | ZZ | 4 |
| □ | SG | 3 |

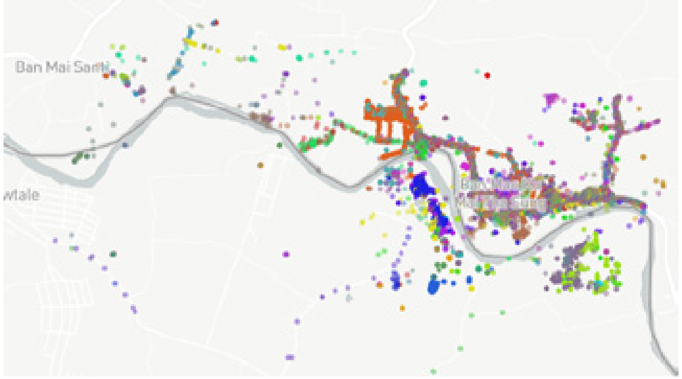
Source: ATII (2023)

In order to gain a more comprehensive understanding of the filters discussed above, the following illustration exclusively shows IP addresses assigned to Myanmar. By filtering out the IP addresses assigned to other countries, we can see that they are only present in their respective assigned country.



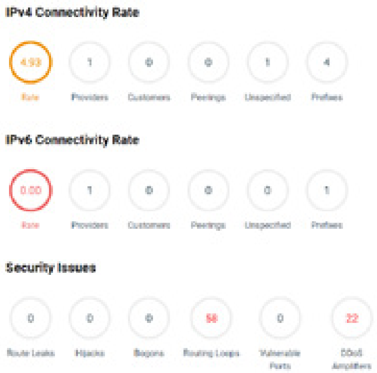
Source: ATII (2023)

By narrowing down our focus to IP addresses exclusively assigned to Thailand, we can develop a more comprehensive understanding of cross-border internet activity. The following illustration showcases the filtering process of IP addresses that belong to other countries, exposing that these addresses can only be located within the country they are assigned to – in this case, Thailand. This methodology allows for the identification and tracking of potentially fraudulent internet activity within a specific geographical location, as observed in the case of the cross-border scam cables.



Source: ATII (2023)

At a granular level, analysts have detected an IP address that is redirecting to a company in Thailand which has employed flawed applications that are transmitting GPS coordinates with inaccurate locations. The numerous routing loops found suggest that the criminals involved are either not wiring their network correctly or routing the internet traffic inefficiently. These issues can lead to connectivity problems, such as outages, delayed traffic, and latency as seen in the visual below.



IPv4 Connectivity Rate

4.93 Rate
1 Providers
0 Customers
0 Peerings
1 Unspecified
4 Prefixes

IPv6 Connectivity Rate

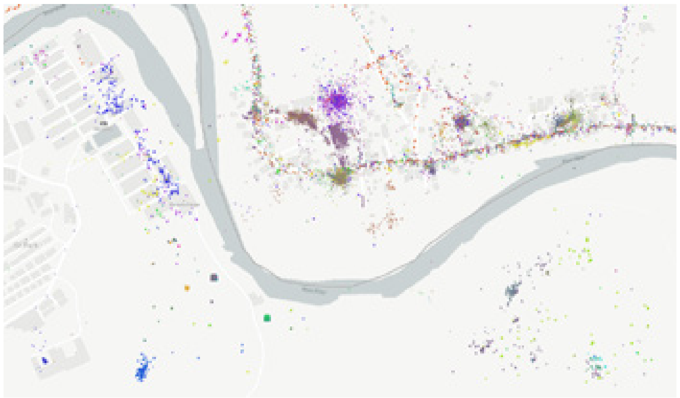
0.00 Rate
1 Providers
0 Customers
0 Peerings
0 Unspecified
1 Prefixes

Security Issues

0 Route Leaks
0 Hijacks
0 Bogons
58 Routing Loops
0 Vulnerable Ports
22 DDoS Amplifiers

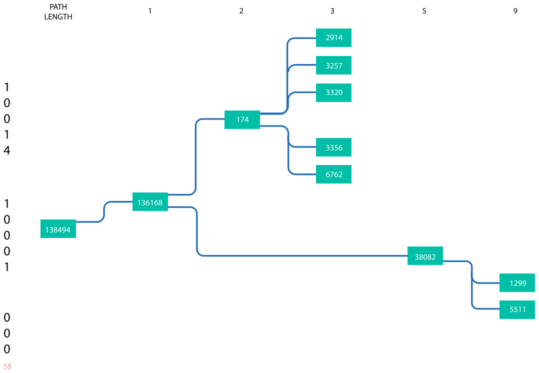
Source: ATII (2023)

A wider-scope visual of the compound area reveals significant activity on Thailand IP addresses in the Myanmar region, which would not typically be possible. This indicates that Thailand's internet infrastructure is being utilised in Myanmar, most likely through cross-border internet lines. Such cross-border activity can be detected and tracked using geo-location data and filtering of IP addresses assigned to other countries, as demonstrated in the previous sections above. This method is particularly useful in identifying and monitoring suspicious internet activity within a specific geographic area, as observed in the case of the cross-border scam cables.



Source: ATII (2023)

The issue of global networks is also relevant to this matter. A criminal network involved in this type of scamming utilises various tactics to obfuscate their original source by connecting nodes to several other IP addresses, as shown in the diagram below. This presents a significant challenge for law enforcement in attempting to trace the networks, internet exchange points, peers, and potential routes for internet traffic across the world. A clear visualisation, such as the one depicted below, can provide nonprofits and law enforcement with the necessary knowledge to disrupt the traffic for the ISPs being used.



Source: ATII (2023)

In conclusion, this case study highlights the high risk of exploitation that ISPs face from human trafficking scam trade. However, ISPs also have the opportunity to work with nonprofits to prevent, detect, and remediate such cases within their operations. By collaborating with these organisations, ISPs can play an active role in combating this heinous crime and protecting the vulnerable individuals who are most at risk.

The Complexities of Combating the Human Trafficking Scam Trade: A Deep Dive into the Challenges of Prevention and Prosecution.

## Countering Human Trafficking: Assessing the Effectiveness of Responses from Local Governments and Law Enforcement

Currently, one of the most successful means of exit from the scamming compounds is through intervention from the embassy of the victim's country of origin. There have been several cases whereby the embassy has contacted the Cambodian or Myanmar authorities to inform them that their citizens are trapped in the compounds.
An officer is then sent to the compound with a list of people to retrieve.

However, when embassies do not respond to the request of their citizens, recognise the nature of the crime as human trafficking, or have representation in the destinations, it is extremely difficult to rescue the victims.

### Examples of actions from the embassy that make rescuing victims extremely difficult are:

**No response**
to the request of their citizen

**No recognition**
of the crime as human trafficking

**No representatives**
in the destinations (Chiang and Casulli, 2023)

Victims are also faced with difficulties after successfully exiting the compound. Many do not hold valid visas as a result of being trapped in the compound for several months, and they must pay a fine for this. According to international norms, such fines must be waived for victims of human trafficking. However, if victims are not correctly identified as victims of human trafficking, or such policies are not properly understood by local law enforcement, victims may be left with no choice but to pay. There is no policy in place which allows this fine to be waived for victims of trafficking from the compounds and many do not have the means to pay this fine. As many do not have the means to cover the fine, many remain trapped in detention centres for several weeks or months.

Within the more affected countries across East and Southeast Asia, the non-punishment principle can be identified in numerous policies and conventions, asserting that victims must not be prosecuted for illicit activities they were forced to carry out as a result of their trafficking situation (ASEAN, 2015). However, many victims are still wrongly prosecuted and viewed as criminals. This may be due to numerous factors, such as lack of understanding with regard to identification of human trafficking victims and the situations they may face or lack of understanding and capacity regarding the appropriate laws in place to protect victims of human trafficking (RefWorld, 2012).

# Recommendations

## Recommendations for law enforcement and national governments:

It is imperative to establish a mandate for embassies that encompasses not only diplomatic responsibilities but also the provision of emergency support to their citizens. Countries must take proactive measures to support their citizens who are victims of human trafficking abroad.

Law enforcement agencies should be well-informed about the non-punishment principle. Achieving this can be facilitated through various methods such as training programs, case studies, and awareness-raising initiatives. Effective training and capacity-building should be provided to law enforcement bodies to enhance their understanding of the challenges faced by trafficking victims and their connection to the non-punishment principle from their enslavers.

Comprehensive support services, including legal aid, mental health assistance, employment opportunities, and financial support should be made available to survivors. These services should be accessible not only during their transition out of the trafficking situation but also throughout their reintegration process. Collaboration with local-anti-trafficking organisations can help establish and maintain such support systems.

Survivors of human trafficking should be treated as valuable informants in order to effectively prosecute traffickers from the source countries. Recognising survivors as key sources of information can greatly contribute to efforts aimed at bringing traffickers to justice (Chiang and Casulli, 2023).

## Recommendations for Anti-Trafficking Organisations

Collaboration with governments is necessary to establish and provide comprehensive support services to victims throughout their transition out of scamming compounds and during their reintegration process. This collaborative effort aims to ensure that victims receive the necessary assistance and support at each stage of their journey (Chiang and Casulli, 2023).

Ensuring that all members involved understand the non-punishment principle is essential. This will enable organisations to provide appropriate guidance and take necessary actions when interacting with survivors. Achieving this understanding can be accomplished through training programs, case studies, awareness campaigns, and similar initiatives.

It is crucial to give priority to engaging and communicating with governments that have not yet acknowledged their citizens as victims of human trafficking and modern slavery within scamming compounds.

# Countering Online Scams:
# Challenges and Recommendations in Prevention and Prosecution

Combatting the pig butchering scams is a complex challenge that requires the cooperation of various stakeholders. Law enforcement agencies have been working for decades to combat consumer scams, but the increasing sophistication of these scams has made it difficult for them to keep up. Private industry's supporting infrastructures and constructions have not been as present as for traditional third-party fraud, which further exacerbates the challenge. The prevention and prosecution of scams is a complex task that involves a multi-stakeholder approach, including law enforcement, financial institutions, nonprofits, and regulations.The role of each stakeholder, along with some of the challenges involved in preventing and prosecuting scams will be highlighted in this section.

To combat these scams and prevent their devastating impacts on victims, it's crucial to consider prevention and response measures. This section will explore various recommendations and suggestions for protecting oneself from falling victim to online scams, as well as improving detection and deterrence. Additionally, we will delve into suggestions for financial institutions, specifically banks, on how to ensure that laundered funds from the scams do not enter the traditional financial system. By implementing these measures, we can work towards a safe and more secure financial landscape, protecting both individuals and institutions from the harmful effects of the human trafficking scam trades.

## Staying Safe: How to Protect Yourself from Scammers and What to Do If You're Targeted

The increasing popularity of cryptocurrencies has led to the emergence of various schemes aimed at defrauding individuals, like the pig butchering scams. As a result, it's essential to take steps to protect yourself from these scams, and there are several measures you can take to do so.

Firstly, it's crucial to conduct thorough research before investing in any cryptocurrency. This involves checking the legitimacy of the project's website, whitepaper, and team. You should also review the project's social media channels and check for any suspicious activity or complaints. By doing your research, you can identify legitimate projects and avoid falling privy to fraudulent schemes.

Using trusted cryptocurrency exchanges and wallets is another critical measure to protect yourself from scams. You should only use exchanges that are well-established and have a reputation within the cryptocurrency community. Avoid using unregulated or new exchanges that haven't been vetted by the community. This way, you can ensure the safety of your digital assets and minimise the risk of fraud.

Phishing scams are another common tactic used by scammers to obtain login credentials and private keys. To avoid falling victim to these scams, it's crucial to double-check the URL of any website you visit and never give out sensitive information unless you are sure you are on a legitimate website. Additionally, never give away your private keys, as they are the keys to your digital wallet, and anyone with access to them can access your funds.

If you suspect that you have been targeted by the pig butchering scam or have fallen victim to one, it's essential to report it to your local authorities and the cryptocurrency community. Reporting such scams can help prevent others from falling victim to the same scam, and authorities can take action to investigate and shut down fraudulent operations.

By doing your research, avoiding get-rich-quick schemes, using trusted exchanges and wallets, being aware of phishing scams, and reporting suspicious activity, you can protect yourself from fraud and invest your money safely (Mitchell, 2022).

The single most significant challenge that law enforcement and banks face is that many victims of scams believe the scams to be legitimate. As a result, they often don't recognise that they are victims until it is too late. This delay in reporting the event reduces the chances of recovering the lost monies, and finding and prosecuting the criminals.

For example, scammers frequently operate across national borders, creating jurisdictional obstacles that complicate the task of tracking down the compounds and bringing criminal networks involved to justice. Additionally, many law enforcement agencies lack the necessary resources to effectively investigate and prosecute scams, which can make it difficult to protect victims and hold scammers accountable.

Another significant challenge faced by law enforcement agencies is the rapidly evolving nature of scam tactics. Scammers are constantly developing new techniques to evade detection, making it difficult for investigators to keep up. To address this challenge, it is crucial for law enforcement agencies to collaborate with other stakeholders, such as financial institutions and nonprofit organisations, to share information and resources. By working together, these groups can pool their expertise and resources to combat scams and bring those responsible to justice more effectively. Furthermore, it is crucial to educate consumers about the risks of scams and what steps they can take to protect themselves.

# Financial Institutions

One of the main issues is that many banks have not traditionally tracked scams or reported them to law enforcement. The Knoble survey suggested that under 50% of member banks tracked scams in 2022, even lower in the years prior. This is due in part to limitations of their anti-fraud programs, which can lead to a reduced number of cases being escalated to law enforcement. In addition, it minimises technology innovation surrounding scams, leaving victims vulnerable to increasingly sophisticated attacks. For example, scams may involve fake websites or phone numbers that look legitimate, making it difficult for financial institutions to distinguish between legitimate and fraudulent transactions. With limited resources, financial institutions may not have the necessary resources to monitor all transactions for potential fraud. This can especially be a challenge for smaller financial institutions that may not have the same level of resources as their larger counterparts.

Another significant challenge is that many of these scams originate internationally. Criminals often move money through multiple bank accounts, making it difficult for law enforcement to track down perpetrators, especially in countries with minimal law enforcement support or access to bank security professionals.

Lastly, customer privacy is also a crucial consideration for financial institutions. While fraud prevention is a top priority, financial institutions must also balance this with protecting customer data. This can be a delicate balance, as financial institutions need to ensure that they are not violating their customers' privacy rights while also detecting and preventing fraudulent transactions.

To address these challenges, financial institutions need to invest in fraud prevention technologies and tools. These may include fraud detection software, transaction monitoring systems, and other technologies that can help financial institutions detect and prevent the scams. Collaboration amongst law enforcement and nonprofits will enable the development of the right tools to play a vital role in preventing scams and protecting financial institutions' customers' financial well-being.

# Nonprofits

Nonprofits have a crucial role to play in the fight against these scams. Nonprofits have the data and sources to provide financial education to vulnerable populations, such as the elderly and those with limited financial literacy. They also play a pivotal role in providing insights on how to detect and train banking staff on the red flags related to these scams. By increasing awareness, sharing data, and providing education, nonprofits can help prevent individuals from becoming victims of scams, and help banks prevent money entering the traditional financial system.

However, nonprofits still face several challenges, starting with limited resources. The hardships of the 2020 pandemic severely cut resources and only amplified criminal activity, with the number of people in modern slavery and human trafficking victims increasing from 40 million to 50 million in recent years according to a recent ILO report. Many nonprofits couldn't sustain and were required to shut down. With the resources that were available, frugal spending and careful decision making have been required to stay afloat.

Lastly, limited expertise. Nonprofits may not have the in-house capacity that's necessary to identify and prevent scams effectively. Data and resource sharing amongst nonprofits does exist, but in limited capacity as each organisation is competing for funding. However, collaborations amongst the nonprofit world do exist and expertise is shared, but it is still an area that requires larger adaptation to be effective in working towards a common goal to prevent and detect the human trafficking scam trade from occurring.

To overcome these challenges, nonprofits will need to collaborate with other stakeholders, including law enforcement agencies and financial institutions, to share information and resources. By working together, they can maximise their impact and reach a wider audience. Nonprofits can also leverage technology to provide support to victims. The technology used can provide resources and assistance to victims, such as online support groups or counselling services.

# Regulations

Lastly, regulations can also be helpful in combating these scams by creating a legal framework that scammers must operate within. Governments can enact legislation that requires financial institutions to report scams to law enforcement agencies, increasing the chances of criminals being caught and prosecuted. Through enacting regulations that require financial institutions to implement robust anti-fraud programs that leverage advanced analytical technologies to detect and prevent scams, these crimes can be prevented before they even occur.

Nonetheless, regulations face several challenges, starting with limited reach, whether it be too broad or too narrow in scope. If regulations are too broad, they may unintentionally hinder legitimate businesses and innovation. On the other hand, if regulations are too narrow, they may not cover emerging scam tactics and technologies.

Moreover, scammers, like in the human trafficking scam trade, may also find ways to exploit loopholes or gaps in regulations, which can limit their effectiveness in preventing scams. This can be particularly true for online scams, where the scammers can easily adapt their tactics quickly to avoid regulatory oversight. For example, scammers may switch to new technology platforms or change the language used in their scams to avoid detection. Another example is changing locations to evade regulation as seen in an earlier section.

Limited enforcement and rapidly evolving scams are two additional challenges faced by regulators in preventing the scams. Even with strong regulations in place, scammers can continue their operations with impunity if regulations are not effectively enforced. Regulators may face challenges in identifying and tracking down scammers who operate across borders or use anonymous community methods to evade detection.

To address these challenges, regulators need to constantly update their regulations and enforcement strategies to keep pace with the changing nature of scams. Collaboration with other stakeholders, such as law enforcement agencies, financial institutions, and technology companies, can also help regulators stay informed about the latest scams and develop more effective measures to prevent them. Additionally, regulators can leverage technology and data analytics to better identify and track down the scammers involved and enforce regulations more effectively.

# Detection and Deterrence Related to Financial Institutions

In this section, we will explore various strategies and recommendations for improving the detection and deterrence of these scams, specifically with regards to financial institutions. We will examine the role banks have in preventing the flow of laundered funds from these scams into traditional financial systems and suggest potential measures that can be taken to address this issue.

As fraud fighters, we have a challenging job, but it is crucial that we do more to fight these scams. To improve the detection and deterrence of pig butchering scams related to financial institutions, we need to focus on the following:

## Programs

With many people falling prey to this scam and suffering significant financial losses, it's essential to establish formal programs to track these scams and develop comprehensive anti-scam policies, risks, appetites, taxonomies, and procedures. These programs will help financial institutions and law enforcement agencies better understand the nature of the scams, the tactics used by scammers, and how to detect and prevent these types of fraud from occurring in the future.

## Deterrence

To effectively deter the scammers, a creative approach is needed, which includes training, technologies, and programs designed to fight fraud and protect customers. As the threat of scams becomes more sophisticated, more and more of us need to step up and become protectors by staying vigilant and taking proactive measures to prevent the scammers from succeeding.

## Operational Treatment

Operational treatment is also crucial in fighting these scams. Financial institutions need to rethink their staffing models and look for resources to meet the challenge of more complicated fraud detection. One way to achieve this is by automating the traditional unauthorised fraud and deploying resources to protect the innocent. By doing so, we'll be one step ahead in preventing the scams.

## Collaboration

Financial institutions need to find ways to share information to fight these threats and mules. Building a scam/mule consortium can help detect mule activity and abnormal customer behaviour and assist in risk-scoring money movement to prevent further loss.

## Reporting

Encouraging victims who have fallen prey to scamming to report these incidents to law enforcement and financial institutions is critical in preventing further loss. Reporting can help institutions identify patterns and trends in scamming activities, enabling them to take action to prevent similar scams from occurring in the future.

In summary, to improve the detection and deterrence of the human trafficking scam trade and other emerging scams similar to these in the future, financial institutions need to establish formal anti-scam programs, take a creative approach to deter scammers, rethink their staffing models, collaborate to share information, and encourage victims to report scams. By implementing these measures, we can work together to prevent fraud and protect customers from falling prey (Mitchell, 2022).

## Conclusion

After exploring the human trafficking scam trade and its devastating impact on victims, it's clear that this crime is a serious issue that requires attention from individuals and organisations alike.

We've seen how the scam works, with fraudsters using sophisticated tactics to build trust with their victims and convince them to invest in fake schemes. Once the victims have invested, the fraudster disappears, leaving them with nothing and often in debt.

Additionally, we've examined the horrors of human trafficking and modern slavery that are linked to these scams and how it relates to the financial system. It is crucial that individuals and organisations take steps to raise awareness about this issue and prevent further instances of the human trafficking scam trade and other forms of human trafficking and forced labour from emerging. This includes advocating for stronger laws and regulations to protect vulnerable populations, supporting organisations that provide resources and assistance to victims, and promoting education and training programs to help individuals and companies identify and avoid potential scams and fraud. Both public and private sectors have a role to play, and through partnering with nonprofits and sharing meaningful data, as a global community we can address the root causes of human trafficking, fraud and money laundering as a result of poverty, inequality, and lack of opportunity. By working together, we can build a safe and more just world for all.

# Reference Bibliography

- Abad, M., (2023) ‘*Ph authorities supplied trafficked OFW with genuine travel documents*’ *RAPPLER*. Available at: https://www.rappler.com/nation/overseas-filipinos/philippine-authorities-supplied-trafficked-ofw-genuine-travel-documents. [Accessed: March 24, 2023].

- Abdus, S., (2023) ‘*I was once a victim of human trafficking, now I help bring other victims home safely from Cambodia to Bangladesh*’ *Humanity Research Consultancy*. Available at: https://humanity-consultancy.com/2023/02/20/i-was-once-a-victim-of-human-trafficking-now-i-help-bring-other-victims-home-safely-from-cambodia-to-bangladesh. [Accessed: March 15, 2023].

- ACAMS., (2022) ‘*Understanding pig butchering*’ *ACAMS*. Available at: https://www.acams.org/en/media/document/Pig-Butchering-Infographic. [Accessed: March 10, 2023].

- ASEAN, (2015) ‘*Convention Against Trafficking in Persons, Especially Women and Children’* Available at: https://asean.org/asean2020/wp-content/uploads/2021/01/ACTIP.pdf. [Accessed: April 3, 2023].

- ATII., (Personal Communication, March, 29, 2023) *‘Common Crypto Money Launder Practices: Pig Butchering Scams’ ATII* [PowerPoint Slides]. [Accessed: March 29, 2023].

- Chiang, M. and Casulli, V., (2023) ‘*Guidance on Responding to Victims in Forced Scam Labour’ Humanity Research Consultancy Briefing*. Available at: https://humanity-consultancy.com/wp-content/uploads/2023/04/HRC-Briefing-Guidance-on-Responding-to-Victims-in-Forced-Scam-Labour.pdf. [Accessed: April 25, 2023].

- Chiang, M. and Chen, S, (2022) ‘*HRC Briefing: Cyber Slayer in the Scamming Compounds*’ *Humanity Research Consultancy*. Available at: http://www.humanity-consultancy.com/wp-content/uploads/2022/09/HRC-Briefing_Cyber-Slavery-in-the-Scamming-Compounds.pdf. [Accessed: March 15, 2023].

- Farivar, C., (2022) ‘*How One man lost $1 million to a crypto ‘super scam’ called pig butchering*’ *Forbes*. Forbes Magazine. Available at: https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butchering-crypto-super-scam/?sh=479cf70ec8ed. [Accessed: April 16, 2023].

- Gibbs, E., (2022) ‘*Cambodia illegal gambling crackdown, 10k venues raided*’ *Casino.* Available at: https://www.casino.org/news/illegal-gambling-crackdown-in-cambodia-becomes-priority-10k-venues-raided. [Accessed: March 22, 2023].

- Global Anti-Scam., (2022) ‘*Metatrader has forex and crypto fraud*’ *Global Anti Scam Org*. Available at: https://www.globalantiscam.org/post/metatrader-has-fraud. [Accessed: March 26, 2023].

- Hunt, L., (2023) ‘*Focus on human trafficking shifts from Cambodia to Myanmar’ The Diplomat*. Available at: https://thediplomat.com/2023/02/focus-on-human-trafficking-shifts-from-cambodia-to-myanmar. [Accessed: April 13, 2023].

- Mitchell, I., (2022) ‘*An open letter to my fellow fraud fighters on fighting scams’ LinkedIn*. Available at: https://www.linkedin.com/pulse/open-letter-my-fellow-fraud-fighters-fighting-scams-mitchell-cafp. [Accessed: March 15, 2023].

- Ngamkham, W., (2022) ‘*Police find cross-border data cables serving call scammers in Cambodia’ Bangkok Post.* Available at: https://www.bangkokpost.com/thailand/general/2460499/police-find-cross-border-data-cables-serving-call-scammers-in-cambodia. [Accessed: April 1, 2023].

- Podkul, C. and Liu, C., (2022) ‘*How human traffickers force victims into Cyberscamming’ ProPublica*. Available at: https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming. [Accessed: March 15, 2023].

- *Refworld.,* (2012) ‘*The leader in Refugee Decision Support*’ *Refworld*. Available at: https://www.refworld.org/pdfid/543f75664.pdf. [Accessed: April 10, 2023].

- TNAOT., (2021) ’犯罪集团藏身柬埔寨跨国实施”比特币投资”诈骗 一女子被骗百万, 柬埔寨头条. 柬埔寨头条’*TNAOT*. Available at: https://www.tnaot.com/zh/m/detail/article/11706542?channel=84. [Accessed: March 16, 2023].

Contact us at:

✉ info@themekongclub.org

www.themekongclub.org

Follow us on:

@themekongclub

@themekongclub

@themekongclub

@themekongclub