2025

MEKONG CLUB

UNMASKING SCAM CENTERS: TYPOLOGIES , TACTICS , AND TARGETED INDUSTRIES

The Mekong Club | September 2025

2025

UNMASKING SCAM CENTERS: TYPOLOGIES, TACTICS , AND TARGETED INDUSTRIES

Authors: Balki Aydin
Sebastián Arévalo Sánchez

This publication was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the author[s] and do not necessarily reflect those of the United States Department of State.

INDEX

I. Executive Summary

This report aims to equip key industries, including social media companies, airlines, financial institutions and cryptocurrency companies, with an understanding of how their services may be misused by scam centers that engage in human trafficking and forced labor to carry out scamming activities.

Scam centers are organized operations, often run by criminal networks in Southeast Asia, that use deceptive tactics to carry out fraudulent activities. These operations have become notorious for their involvement in human trafficking-luring individuals with false promises of legitimate employment and high salaries and coercing them into executing fraudulent schemes through threats and violence. Scammers often advertise attractive job opportunities on social media and recruitment platforms, promising high salaries and targeting educated, computer-literate individuals, in fields like customer service or IT.

Trafficking in Persons (TIP) victims in scam centers are often deceived into accepting these offers but are instead forced to participate in scams, enduring threats, violence, and restricted freedom. TIP victims are often forced into modern slavery within scamming centers to conduct fraudulent activities, victimizing both the trafficked individuals and the targets of their scams.

Human trafficking is defined as the recruitment, transportation, transfer, harboring or receipt of persons, by means of threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, for the purpose of exploitation. Human trafficking can intersect with scam centers when criminal networks recruit or coerce individuals into working in fraudulent operations under exploitative conditions, making some scam centers a subset of trafficking.

This report breaks down scam center operations into a series of typologies, illustrating how these criminal enterprises exploit legitimate systems to recruit and control TIP victims, execute large scale online scams, and launder illicit proceeds. It examines the scamming process in five critical phases:

A. Recruitment
B. Transportation
C. Harboring and Receipt
D. Forced Criminality in Scam Operations
E. Money Laundering of Criminal Proceeds

Each phase represents a key stage in the scamming process, involving multiple industries and geographies. This industry-specific typology report seeks to help stakeholders identify vulnerabilities, detect red flags, and implement safeguards to prevent their infrastructure from being misused to facilitate scamming activities and financial crime. Ultimately, by understanding these evolving risks, stakeholders will be better positioned to disrupt exploitation, protect TIP victims of trafficking and scam targets, and mitigate the global impact of scam centers.

II. Who Should Read This Report?

This report is intended for stakeholders in industries that may be manipulated by scam centers engaged in human trafficking and forced labor to carry out fraudulent activities. Relevant sectors include social media platforms, technology providers (such as cloud or IT infrastructure services), airlines, the hospitality industry, financial institutions, cryptocurrency companies, law enforcement agencies and regulators.

III. Why Use Typologies?

Human trafficking into scam centers is a rapidly evolving form of transnational organized crime that combines human trafficking for forced criminality with sophisticated online scams. TIP victims are lured through fake job offers, trafficked across borders and forced to work for large-scale scamming operations targeting individuals worldwide.

Drawing on a typology, this report seeks to provide a general understanding of how scam centers operate and the industries that have a key role in addressing this issue. The report outlines the five key phases of trafficking into scam centers: recruitment, transportation, harboring and receipt, forced criminality in scam operations, and money laundering of criminal proceeds.

Each typology has the following elements:

A. Industry Overview: A summary of how the industry is exposed to scam centers and human trafficking, highlighting key trends and describing the forms of modern slavery most commonly observed in the sector.

B. Industry Red Flags: Key indicators of suspicious or high-risk activity within the industry that may suggest misuse, coercion, or fraudulent operations. These signs can help industry professionals detect and respond to potential misuse of services.

C. The Case: This section presents a composite case study illustrating how industry services can be manipulated in fraudulent or coercive schemes. While individual circumstances may vary, this example draws on recurring patterns observed across real incidents and investigations to provide a realistic understanding of risk exposure.

D. Questions and Actions: Outlines key questions and practical steps industry professionals should consider when evaluating potential misuse of their platforms or services. These focus on common vulnerabilities, behavioral red flags, and proactive measures to mitigate risk and protect consumers.

IV. How To Use This Report?

This tool can be applied across industries in several keyways:

A. Training Resource: It can be used to create workshops and training sessions for staff, using the case studies to help employees better identify risks and take action to prevent being manipulated by scam centers or inadvertently supporting modern slavery and forced labor. It also provides helpful input into employee reference tools, such as desktop manuals or checklists, that can aid staff in identifying risks in their daily work activities.

B. Raising Industry Awareness: It can be circulated within relevant industries to build awareness of the broader risks associated with scam operations and human trafficking. Many stakeholders mistakenly associate modern slavery only with sex trafficking, but human trafficking and forced labor are increasingly infiltrating a wide range of sectors.

C. Strengthening Risk Assessments: Industry professionals can use this tool as a reference point when assessing risks tied to customers, business partners, or transactions, ensuring the right questions are asked during onboarding, client assessments, transactional reviews, and partnership reviews.

D. Monitoring for Red Flags: Whether reviewing account activity, monitoring network traffic, analyzing customer behavior, or overseeing their platform use, this tool can assist organizations in identifying unusual patterns or indicators of misuse across financial, transportation, and communications systems.

E. Improve the Dialogue with Regulators: This report can help facilitate more constructive conversations with regulators and policymakers by providing insights into emerging risks and evolving criminal tactics. It can also support efforts to strengthen regulatory guidance and promote coordinated action against human trafficking, forced labor, and scam operations.

V. Common Traits of Scam Centers

Scam centers exploit TIP victims by forcing them to perpetrate online scams, such as cryptocurrency fraud, romance scams, or investment schemes. These centers share several core traits in their recruitment processes and methods to trap and control TIP victims, mirroring some aspects of modern slavery but tailored to the context of cybercrime. The key elements include deception, coercion, confinement, psychological manipulation, debt bondage, threats, and exploitation through illegal or exploitative contracts.

The primary method of recruitment is deception. TIP victims are lured with false promises of legitimate, well-paying jobs, often in fields like customer service, IT, or marketing. Recruiters target vulnerable populations, such as young people, unemployed individuals, or those in economically disadvantaged regions, through social media, job boards, or personal networks. These offers are designed to appear credible, with professional-looking advertisements or testimonials. TIP victims are often enticed with perks like free travel, accommodation, or high salaries, which seem like life-changing opportunities. In some cases, recruiters pose as reputable companies or misuse trusted relationships to gain TIP victims' confidence.

Once TIP victims arrive at scam centers, perpetrators employ a range of tactics to trap them and force participation in fraudulent activities. These methods ensure compliance and prevent escape:

A. **Physical Confinement:** TIP victims are often held in heavily guarded centers surrounded by high walls, security cameras, or armed guards. Movement is strictly controlled, with limited or no access to the outside world. Passports, identification documents, and personal belongings are confiscated to prevent escape.

B. **Psychological Manipulation and Emotional Abuse:** Perpetrators use fear, shame, and guilt to control TIP victims. They may threaten to expose victims' involvement in scams to their families or authorities, even if the TIP victims were coerced. TIP Victims are

often gaslighted into believing they are complicit, making them feel trapped by their own actions and they also believe that they will be prosecuted and shamed back in their countries once returned.

C. **Threats and Violence:** Physical abuse, including beatings or torture, is used to punish non-compliance or failed escape attempts. Threats are also directed at TIP victims' families, leveraging emotional bonds to ensure obedience. In some cases, perpetrators threaten legal action, claiming victims owe debts or have broken contracts.

D. **Debt Bondage:** TIP victims are often told they owe money for travel, accommodation, or "training" costs, creating a cycle of debt that is impossible to repay. Wages are withheld or manipulated to keep TIP victims financially dependent. In some cases, TIP victims are forced to pay fines for underperforming or breaking arbitrary rules.

E. **Exploitative Contracts:** TIP victims may be coerced into signing contracts that are illegal, vague, or heavily weighted against them. These contracts often include clauses that impose penalties for leaving or failing to meet scam quotas, further entrenching TIP victims in the operation.

F. **Forced Participation in Scams:** TIP victims are trained to execute scams, such as posing as romantic partners, financial advisors, or cryptocurrency experts. They are given scripts and monitored closely to ensure they meet daily targets. Refusal to participate results in punishment, while compliance may be incentivized with small rewards or promises of eventual release.

G. **Isolation and Surveillance:** TIP victims are cut off from external communication, with phones and internet access tightly controlled. They are often housed in dormitories with other victims, fostering an environment of mutual distrust. Surveillance systems monitor their activities, both online and offline, to prevent rebellion or escape.

H. **Exploitation of Vulnerabilities:** Perpetrators exploit TIP victims' cultural, linguistic, or economic vulnerabilities. For example, TIP victims may be recruited from countries with high unemployment rates and transported to foreign countries where they don't speak the language, making escape or seeking help nearly impossible.

The combination of physical, psychological, and financial controls creates a sense of hopelessness among victims. Many TIP victims initially believe they can work off their "debts" or earn their freedom, only to find the terms constantly shifting. The fear of violence, legal repercussions, or harm to loved ones keeps them compliant. Additionally, the isolation and constant surveillance make organizing or attempting escape extremely difficult. Even if TIP victims recognize the criminal nature of their work, they may feel powerless to leave due to the lack of resources, documentation, or knowledge of their surroundings.

In summary, scam centers operate by exploiting trust and desperation during recruitment, then using a sophisticated mix of coercion, confinement, and manipulation to force TIP victims into conducting scams. These operations thrive in regions with weak law enforcement or high corruption, making it critical to raise awareness and strengthen international efforts to combat this form of modern exploitation.

VI. Recruitment

Criminals often target individuals seeking employment and better opportunities by using deceptive tactics. They lure potential TIP victims with fraudulent job offers from fictitious companies, typically advertising roles such as customer service representatives, data analysts, or technical support staff. Scammers promote these fake job advertisements with promises of high salaries and favorable working conditions, often requiring little to no experience.

Social media platforms (e.g., Facebook, X, TikTok, LinkedIn) and online job portals are commonly used to distribute these fake job listings. The recruitment process may involve simulated formal interviews and contracts, which create a false sense of legitimacy around the fraudulent offers and companies. While the advertised positions span various industries, they usually present as white-collar or skilled roles, particularly in tech or customer-facing fields, to attract individuals with digital proficiency and language skills, often in English or Mandarin.

Common characteristics of TIP victims include young adults, typically between the ages of 18 and 35, who possess strong English or Mandarin language skills and basic digital proficiency. TIP victims often come from countries with high unemployment rates, economic instability, or large numbers of labor migrants, such as Indonesia, Vietnam, the Philippines, Nepal, Myanmar, and Cambodia.

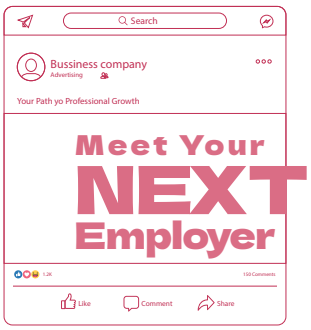
01 Recruitment

Trafficking In Persons **TIP**

POTENTIAL TIP VICTIMS

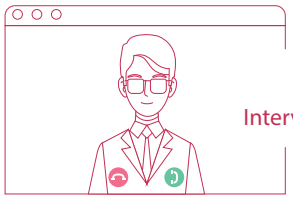
TIP targets

Contact: Fake job offers



TIP targets express interest

Create trust and legitimacy



Job acceptance

A. Sign employment contract
B. Pay recruitment fee
C. Submit requested documents

TIP VICTIMS

A. Red Flags

Too-good-to-be-true job offers

Promises of high salaries, free travel, luxury accommodation, and visa support for entry-level or unskilled work (e.g., data entry, customer service) with no required experience should raise immediate suspicion.

Use of social media & informal channels

Recruiters are increasingly leverage legitimate platforms rather than just informal channels. Recruitment is often conducted through Facebook groups, TikTok videos, WhatsApp, and other informal platforms rather than official company websites or vetted recruitment agencies. Ads may look professional but lack verifiable contact information.

Fake formality

Scammers often replicate legitimate hiring processes— conducting virtual interviews, issuing professionally-crafted contracts, and providing seemingly official company documents via legitimate platforms such as Facebook, TikTok, Indeed, X etc. . However, a closer examination reveals red flags, such as nonexistent or inconsistent company websites, unverifiable business registrations, and fake or unreachable HR personnel.

Request for personal documents & fees

Applicants are asked to submit copies of passports, national IDs, or other sensitive documents early in the process, along with upfront payments via bank transfers, money service businesses or mobile money services especially in regions where banking access is limited for "*visa processing*," "*training*," or "*security deposits*," which are signs of potential exploitation or identity theft.

Recruiter pressure and urgency tactics

Recruiters pressure TIP victims to make quick decisions, reading job offers—often telling them that slots are limited or that delays will cost them the opportunity. These urgency tactics are designed to bypass critical thinking and prevent proper back-ground checks.

B. Questions and Actions for Legitimate Social Media Companies and Job Portals

01 Are job advertisements hosted or promoted on legitimate platforms such as Facebook, X or TikTok verified for authenticity?

- High Priority Action: Platforms should implement systems to vet employers, especially those offering high-salary, remote, or low-entry job opportunities in tech or customer service.

Good Practice: As a good practice example, Meta has piloted AI-based systems to detect misleading job ads before they spread.

02 Does the platform track accounts or pages that post repetitive or suspicious job offers?

- High Priority Action: Look for patterns like repeated postings across regions, identical job descriptions, or promises of unrealistic pay with minimal qualifications at legitimate platforms. LinkedIn uses automated systems to detect and flag accounts engaging in suspicious or automated activity in addition to repeated postings.

03 Are there proactive mechanisms to detect and remove fake employer profiles or job scams?

- High Priority Action: The use of machine learning would enable job portals to identify and remove fake recruiter accounts before they contact job seekers. Platforms can use AI and keyword analysis to flag potentially fraudulent recruiters or misleading job descriptions

04 Does the platform have reporting mechanisms for users to flag suspicious recruitment behavior?

> Good Practice: Ensure users can easily report suspicious job posts or recruiter behavior and receive timely feedback or action. Some platform show offers one-click reporting buttons on job ad pages for review.

05 Is there a process to collaborate with law enforcement or NGOs if trafficking-related recruitment is suspected?

> Good Practice: Social media companies can have a protocol to share data responsibly when there is credible suspicion of human trafficking activity.

06 Are there educational resources on the platform warning users about common recruitment scams?

> Good Practice: Provide pop-ups, ads, or informational links for users browsing job content, especially in high-risk regions.

C. Case Study: The Deceptive Job Offer

Victim A, a 23-year-old recent college from Business Administration department from Indonesia, is facing increasing financial pressure as he struggles to find stable employment in a highly competitive job market. With limited local job prospects, he begins actively searching for employment opportunities abroad, particularly in Southeast Asia, where entry-level positions in marketing, IT, and administrative roles are commonly advertised.

One evening, while scrolling through Facebook, Victim A notices a compelling job advertisement posted in a popular public group dedicated to international job seekers. The listing promises a twelve-month contract in Cambodia, working as a call center operator. It offers a generous salary, free housing, meals, health insurance, and full assistance with visa processing. The company behind the ad has an impressive digital footprint such as a polished website, active social media presence, and positive reviews. Motivated by the prospect of financial stability and international experience, Victim A applies for the job and is contacted by the company's recruiter. The recruiter seems professional and attentive, responding promptly to inquiries and offering reassurances about the job's legitimacy.

Over the next few days, Victim A is guided through what appears to be a standard recruitment process. He is asked to complete an application form and attend a virtual interview via Zoom with someone introducing themselves as a Senior HR Manager. The interview is brief but formal, with questions about Victim A's background, skills, and willingness to relocate.

Within 48 hours of the interview, Victim A receives a professionally designed offer letter and employment contract via email. The recruiter congratulates him and explains the next steps, which includes submitting a copy of his passport, academic credentials, and personal ID documents for visa processing and a recruitment fee.

Victim A submits the documents, pays the fee, and eagerly waits for his visa to arrive.

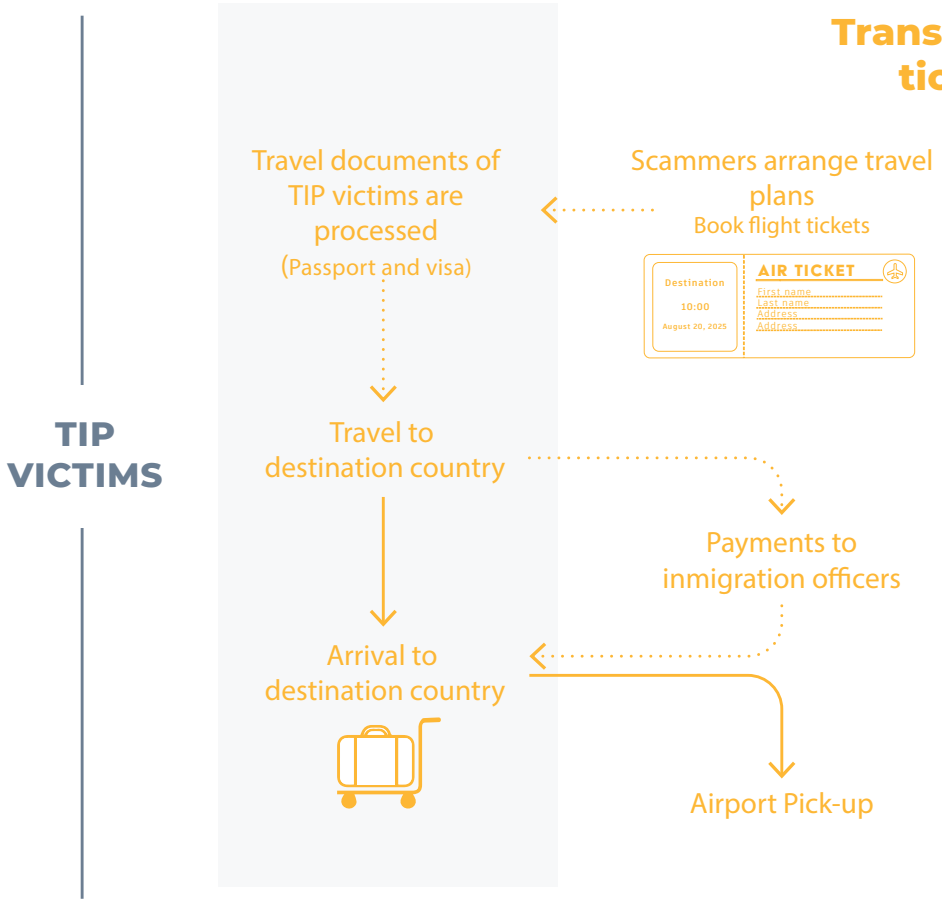
VI. Transportation

Once recruited, TIP victims must relocate from their home countries to the destination countries where they are expected to work. They are typically required to obtain travel documents, such as passports and visas, often with the help or supervision of criminal networks. Criminal network representative may also provide fraudulent or fake supporting documents, such as invitation letters or work permits, to bypass immigration regulations.

Criminal networks operating these scam centers frequently leverage commercial air and sea travel to transport TIP victims across borders, leveraging the accessibility and relative ease of both modes. They manage travel logistics, including passport processing, visa applications, flight or ferry bookings, and port arrivals, to ensure the TIP victim's seamless transit to the destination country.

When traveling, TIP victims present the travel documents requested or provided by criminal networks during immigration checks. They respond to questions from immigration officers, airline staff, or port authorities according to the criminal network representative's instructions. Criminal networks often collude with corrupt immigration or port officials to circumvent security protocols, enabling the undetected transport of TIP victims. In some cases, criminal networks move TIP victims through transit hubs with looser visa requirements before transferring them to the destination country by land or sea, where they are picked up at airports, bus terminals, or seaports and transported to scam centers.

Transportation and 02



A. Red Flags

Travel documents appear suspicious or inconsistent

Passports, visas, or supporting documents (e.g., invitation letters or work permits) may be forged, recently issued with limited history, or not verifiable with consular or immigration databases.

Travelers show visible control or lack of autonomy

Travelers appear to give scripted responses to immigration staff, show visible anxiety, or, if they are traveling with someone from the criminal network, they defer to someone else to speak on their behalf.

Complex travel routes through visa-lenient transit hubs

TIP victims are often routed through the same third countries such as Indonesia, Vietnam or the Philippines, where the immigration controls are less stringent. Different facilitators may be involved at each stage to obscure the TIP victim's final destination and evade detection by authorities.

One-way flight tickets to scam center hotspots

TIP victims often travel on one-way flights to countries such as Cambodia, Myanmar, Laos, or Thailand, regions known for hosting scam centers without clear return plans.

Third-party payment and booking of travels

Flights and sea travel are frequently booked and paid for by unrelated individuals or entities such as fake recruiting companies, shell companies or corrupt travel agencies on behalf of the travelers, often with limited transparency about the sponsor's identity or relationship to the traveler.

Group travel with uniform documentation

Travelers arrive in groups carrying nearly identical paperwork such as work permits or invitation letters, which may indicate mass recruitment or coordinated trafficking operations.

Use of secondary airports

Secondary airports which serve a metropolitan area but are not the primary or largest airports in that region are exploited by human traffickers to transport TIP victims by using the airports lower security and oversight to conceal their operations.

B. Questions and Actions for Airlines/Port Controls

01 Are airline and seaport staff trained to recognize signs of trafficking or exploitation during check-in and boarding?

- High Priority Action: Training should include behavioral red flags such as passengers avoiding eye contact, reading from the scrip or appearing confused about their destination or itinerary.

02 Do airlines and seaport operators have a protocol for reporting suspicious passenger behavior discreetly?

- High Priority Action: Airlines and seaport authorities should establish clear protocols that enable cabin crew, port personnel, and ground staff to discreetly escalate concerns to security or law enforcement, ensuring swift response without alerting the potential TIP victim or criminal network representative traveling with the TIP victim (if applicable).

03 Are group bookings for unrelated individuals flagged for review?

Good Practice: Unusual bookings such as multiple unrelated individuals on the same reservation or paid by a third party should trigger additional scrutiny with clear instructions.

04 Is there coordination with immigration and customs officials on high-risk routes?

Good Practice: Airlines and seaport operators should work with authorities to identify patterns on routes frequently misused for trafficking, particularly those involving stopovers in visa-lenient countries.

05 Do airlines and seaport operators verify the authenticity of travel documents beyond basic checks?

Good Practice: Carriers can enhance document verification using technology or by flagging inconsistencies like last-minute one-way bookings, mismatched identification, or unusual visa types for the routes.

C. Case Study: A Journey into Deception

Victim A received his visa documentation and was surprised to find it was a 30-day tourist visa, not a work visa as he had expected. When he questioned the recruiter, he was reassured that the work permit would be arranged upon arrival at the job site. The explanation seemed suspicious but temporarily allayed his concerns.

The recruiter sent Victim A his travel itinerary and covered all travel costs, including the flight and airport pickup. He was also instructed to take a clear photo of himself and maintain the same appearance throughout the trip. In preparation for possible questioning, the recruiter told him exactly what to say to immigration officers, emphasizing that he should present himself as a tourist visiting friends.

When Victim A landed at the airport in Cambodia, he proceeded to the immigration counter. A police officer stood there, holding a copy of his photo. Without asking questions, the officer stamped his passport and gestured toward the exit.

Outside the terminal, a driver arranged by the recruiter waited in a parked car. Using a translation app, the driver informed him that the trip would take around three hours. This conflicted with the recruiter's earlier assurance that the company was just a short drive from the airport.

As the drive continued, his concerns grew. Victim A began to suspect that the job might not be what was promised. He realized he had no working phone service in Cambodia, leaving him unable to contact anyone for help. Isolated and afraid, he had no choice but to wait and see where he was being taken.

VII. Harboring and Receipt

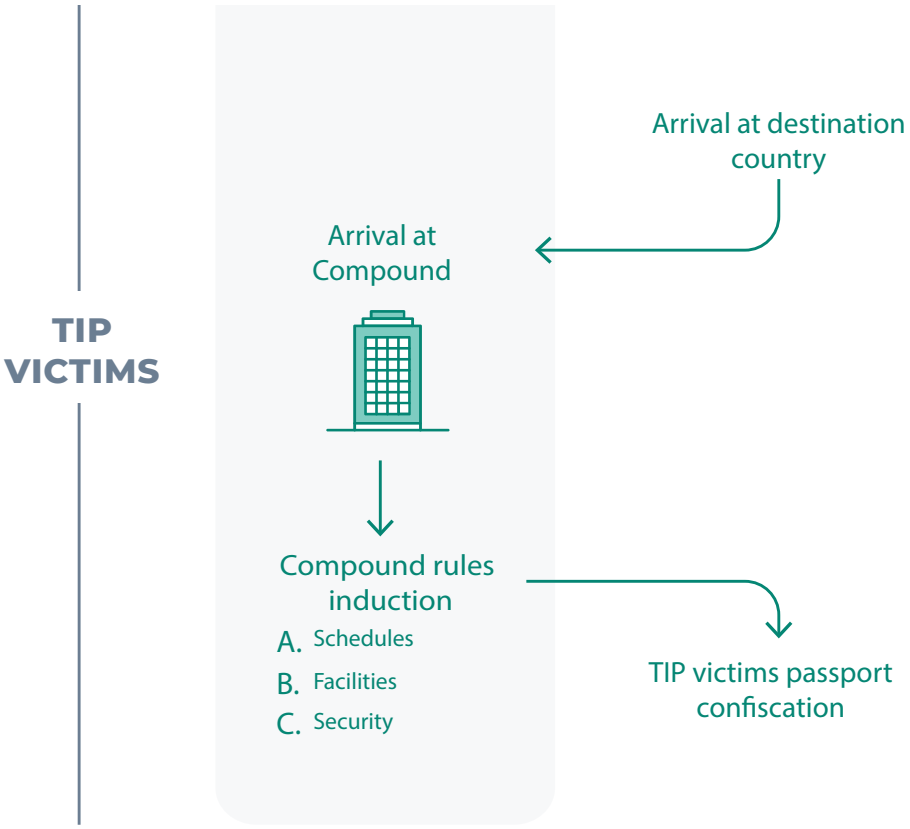
Upon arriving at the scam center, TIP victims begin to sense something is amiss, though they remain unaware of its true nature. They are stripped of their passports, confined against their will, and closely monitored to prevent escape or contact with family or authorities. At this stage, TIP victims understand they are trapped and have no means of leaving voluntarily. Some TIP victims may be subjected to threats, intimidation, or even physical violence to enforce obedience and compliance.

Scam centers function as containment sites where criminal networks tighten their control over TIP victims. These facilities are typically multi-story commercial buildings located in Special Economic Zones (SEZs) with limited regulatory oversight. A SEZ is a geographically defined area within a country that operates under unique economic laws and regulations. The primary purpose of an SEZ is to foster a business-friendly environment and attract investment to achieve specific economic objectives. SEZs are areas where business and trade laws differ from the rest of the country, designed to attract foreign investment through reduced taxes and relaxed regulations. This autonomy and weak oversight create a permissive environment that transnational criminal groups can exploit. SEZs have been exploited by criminal organizations to set up scam centers that rely on human trafficking and forced labor.

Exploiting weak governance and limited law enforcement in these regions, criminal syndicates run large-scale online scam operations, they are often fortified with high walls, locked rooms, and, in some cases, armed guards to prevent escape. TIP victims are frequently monitored through surveillance systems and may be forced to share rooms with others tasked with reporting suspicious behavior. This controlled environment fosters fear, confusion, and isolation—intensifying both the physical and psychological grip criminal networks maintain over their TIP victims. Scam centers often operate with official sanction within the criminal enabling environment of SEZs, highlighting their links to the wider ecosystem of transnational organized crime driven by factors like corruption and cross-border impunity.

MEKONG CLUB

03 Harboring and Receipt



A. Red Flags

Confiscation of personal documents upon arrival

TIP victims are stripped of their passports and identification documents to limit autonomy and prevent escape or contact with outside help.

Physical confinement and movement restrictions

Scam centers often feature locked rooms, high walls, or guards-physical barriers used to harbor victims and prevent them from leaving voluntarily.

Constant surveillance and peer monitoring

TIP victims are closely watched through security cameras or placed in rooms with other TIP victims instructed to report disobedience or escape attempts, reinforcing an environment of distrust and control.

Induction with strict scam center rules and schedules

Upon arrival, TIP victims undergo detailed orientations outlining behavioral expectations, punishments, and operational protocols used to assert psychological control.

Intimidation, threats, or physical violence

Criminal networks maintain control by instilling fear. TIP victims may be subjected to verbal abuse, intimidation, or physical harm if they disobey orders or attempt to escape.

B. Questions and Actions for Local Authorities and Regulatory Agencies

01 Do local authorities inspect high-risk facilities with reports of confinement or coercion?

- ☑ High Priority Action: Regular site visits or unannounced inspections can help uncover conditions such as locked doors, lack of personal belongings, or surveillance equipment consistent with trafficking operations.

02 Is there monitoring of buildings with high electricity usage, restricted access, or modified layouts?

- ☑ High Priority Action: Unusual building patterns such as blackout windows, physical barriers, or excessive power consumption can be red flags for trafficking centers requiring further investigation.

03 Are there consistent reports of officials ignoring or obstructing investigations near known scam centers?

Good Practice: Establish a monitoring and reporting mechanism to track dismissed cases, follow-up on credible victim reports, and investigate delays by local authorities. Escalate findings of potential complicity or corruption to oversight bodies and ensure independent review.

04 Do local records show multiple overseas individuals registered at the same address?

Good Practice: An unusually high number of individuals residing at a single address, according to local housing or registration records, may indicate a potential harboring location. This could suggest the business is using overseas workers recruited through informal or unlicensed third-party agencies, raising concerns about legality and possible exploitation.

C. Case Study: From Opportunity to Captivity

After several hours on the road, the car pulls up to a heavily guarded center surrounded by high walls and metal gates. As the gates open, the driver instructs Victim A to leave his belongings in the car. He is quickly escorted by a group of armed guards. They lead him through a corridor to a small office, where he is introduced to a Chinese manager.

His recruiter instructs him to hand over his passport and phone. When Victim A hesitates, one of the guards threatens to beat him if he refuses. Intimidated, he complies. He is then forced to sign a stack of documents, including what appears to be a contract, all written in Chinese, a language he does not understand. The recruiter explains that because the company paid for his travel expenses, his salary will be reduced to an amount far less than what was originally promised. When Victim A objects, he is warned that bad things will happen if he refuses to cooperate. With no other option, he signs the contract.

Victim A is then taken to a crowded dormitory filled with four sets of bunk beds. As the night shift ends, the room quickly fills with other workers. One of the workers tells Victim A that if he makes enough money, maybe they will let him go home.

IX. Forced Criminality in Scam Operations

At this stage, TIP victims are assigned to roles within the scamming operation by a designated supervisor. They are introduced to strict performance expectations, including key performance indicators (KPIs), and are given detailed manuals outlining how to manipulate and defraud targets—primarily through romance or investment scams. TIP victims are issued work tools such as mobile phones, SIM cards, and laptops, all tightly controlled and monitored to prevent outside communication or escape attempts.

Control is maintained through a deliberate mix of physical violence, psychological coercion, and financial manipulation. TIP victims who fail to meet daily targets may face threats, beatings, humiliation, or punishments intended to break their will. Compensation is minimal or non-existent—salaries are often withheld or reduced through arbitrary fines, such as being charged for "poor attitude" or for not responding to scam targets quickly enough, keeping TIP victims in a cycle of dependency and fear.

Many TIP victims are forced to participate in scams, where they assume fake online personas to target individuals through social media, messaging apps, or dating platforms. After gaining trust, they persuade targets to invest in fake cryptocurrency schemes, often guiding them to open digital wallets at legitimate cryptocurrency platforms and transfer funds. Once the target sends money, the funds are moved to scam-controlled crypto wallets and all communication is cut off, leading the target to suffer significant financial losses.

Exploitation 04

Forced Labour A

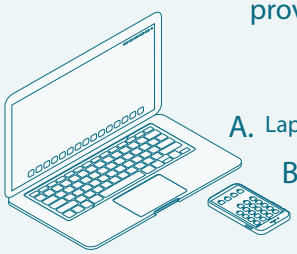
TIP VICTIMS

Introduction to the scam compound

A. Asign employment roles
B. KPIs stablishment
C. Scamming manual provision

↓

Scamming equipment provision



A. Laptop
B. Mobile Phone
C. SIM Card

TIP victims received training

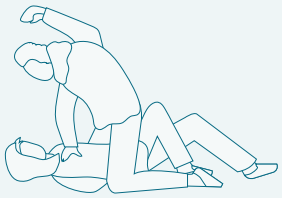
↓

TIP victims receive scam targets

FORCED TO ACT AS SCAMMERS

TIP victims are forced to carry out scams

A. Threats and violence
B. Wage withholding and fines



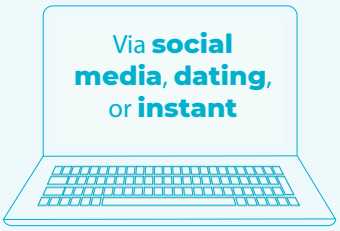
Scam operations B

TIP VICTIMS TURN INTO SCAMMERS

Scammer creates a fake persona

↓

Scammer reaches out to the victim



↓

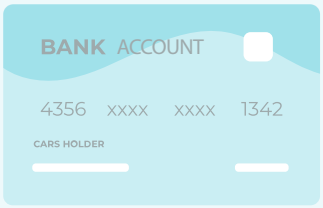
Scammer establishes trust with the victim → Scammer casually mentions cryptocurrency investments and create fake investment success stories.

↓

Scammer creates a sense of urgency by presenting exclusive investment opportunities or limited-time offers.

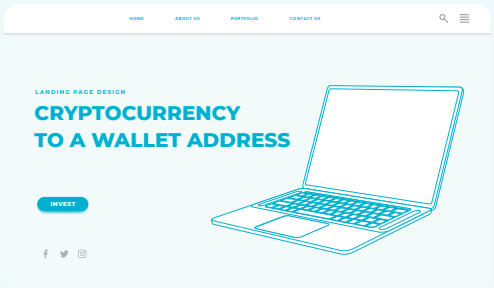
↓

Victim creates a crypto account at a crypto exchange and transfer funds from their bank account to their crypto account.



↓

Scammer asks the victim to send cryptocurrency to a crypto wallet address for investment



↓

Victim transfers funds to the scammer's wallet.

↓

Scammer steals the victim's funds and cuts off all communication leading to financial losses.

A. Red Flags

Forced to work unusual hours with performance quotas tied to threats

TIP Victims report working 12–18-hour days with KPIs tied to the number of scams executed. Failure to meet daily targets results in punishments ranging from food deprivation to public humiliation or beatings.

Communication monitored and payment withheld or arbitrarily deducted

TIP victims are denied access to independent communication channels and paid little or nothing for their labor. Salaries may be withheld entirely or deducted through fabricated fines for minor infractions, ensuring financial dependency on criminal networks.

Scripted online personas with identical scam narratives

TIP victims often use pre-written scripts to impersonate romantic partners or financial advisors, repeating highly coordinated messages across platforms (e.g., WhatsApp, Telegram) and dating apps.

Provided with tools and scripts for scamming but denied freedom of movements

TIP victims are issued phones, laptops, and manuals instructing them on how to defraud targets. However, their movement is heavily restricted, and any deviation from protocol is met with harsh consequences, signaling their lack of autonomy.

False job ads for industries not supported in the job-ad country

TIP victims are recruited through online ads promising employment in industries that lack local infrastructure (e.g., web developers or digital marketing specialists in countries with little or no tech sector). These fabricated opportunities lure job seekers into trafficking schemes, where they are later coerced into scam operations or forced labor.

B. Questions and Actions for Legitimate Social Media Companies and Job Portals

01 Did the person work excessively long hours with little or no compensation?

- ☑ High Priority Action: Long, unpaid shifts, especially when paired with threats, confinement, or abuse, are indicators of forced labor within scam operations and require urgent attention.

02 Was the person monitored by guards, surveillance systems, or restricted in communication with others?

- ☑ High Priority Action: Exploitation schemes often involve isolation, surveillance, or movement restrictions to control TIP victims and prevent outside contact. These are key signs of trafficking.

03 Was the person told they owed a "debt" for recruitment, travel, or training, and forced to work it off?

- ☑ High Priority Action: Debt bondage is a common tactic used by criminal networks to entrap TIP victims in exploitative labor situations. This is unlawful and a serious red flag for modern slavery.

04 Did the person face punishments or threats for failing to meet unrealistic performance targets?

- ☑ High Priority Action: When individuals are penalized through food deprivation, abuse, or threats of being "sold" for failing to achieve quotas, it reflects coercive control and exploitation consistent with trafficking.

05 Was the person forced to follow scripted communications or use fake online identities to deceive others?

Good Practice: Scam centers often coerce TIP victims into using pre-written scripts and false personas to defraud targets. This manipulation, combined with a lack of autonomy, is a hallmark of forced criminality.

06 Was the person required to use pre-written scripts that show coordinated messaging across platforms?

Good Practice: When individuals are forced to rely on identical phrases, tone, or copy-paste responses often combined with stock images or AI-generated photos, it reflects control and points to organized scam operations consistent with trafficking

C. Case Study: Forced to Defraud

Early morning, Victim A is brought to a large room filled with rows of desks, each equipped with a laptop and a mobile phone. A supervisor hands him a thick manual written in English and Chinese and instructs him to start reaching out to international clients. Initially, Victim A believes this might be related to a legitimate call center operator role, as promised. However, as he reads through the manual, he notices detailed scripts for creating fake social media profiles and messaging templates that encourage people to invest in cryptocurrency. The instructions emphasize building trust with targets over weeks, using specific phrases to manipulate them into transferring money.

Over the next few days, Victim A is assigned daily targets for messaging potential clients, in other words "*targets*". He is told to follow the scripts exactly, posing as a romantic interest or a financial advisor. The supervisor monitors his progress closely, and when Victim A fails to get responses on the first day, he is denied food for the evening as punishment. A fellow worker quietly confides in him that everyone in the scam center is engaged in the same deceptive task which is crafting fake personas to trick targets into believing they're genuine, ultimately defrauding them of their money. Slowly, the reality dawns on Victim A that he is not working as a call center operator as advertised but is instead being forced to scam people for money, trapped in a cycle of coercion with no way out.

Over the next few days, Victim A is assigned to connect with wealthy American and Canadian women as targets through dating apps and develop a romantic relationship. His role is to follow the scripts exactly, posing as an attractive man with a charming persona.

After a 17-hour shift, another worker whispers to him that everyone here is doing the same thing—tricking people into sending money into crypto wallets managed by scammers.

The supervisor monitors his progress closely. When Victim A fails to get responses in his first week, he is beaten and kept in a dark room for hours as a punishment. The supervisor warns him that if he does not perform well, he will be sold to another company known for even harsher treatment.

Once a target agrees to move the conversation to text and shares her phone number, Victim A is instructed to take screenshots of the conversations and pass them off to a senior-level scammer, Victim B.

Over the next several days or weeks, Victim B carefully nurtures the relationship, following a meticulously crafted script. He uses affectionate language and consistent engagement to earn the target's trust. Once the emotional bond is strong enough, Victim B pivots the conversation toward financial topics, casually introducing cryptocurrency as his area of expertise. He claims to have insider access to a high-performing, exclusive investment opportunity with guaranteed returns. The target, now emotionally invested and eager to impress or support their romantic interest, expresses interest in participating.

Victim B then provides detailed instructions to the target on how to proceed by opening a cryptocurrency account with a reputable exchange, then transferring funds from their traditional bank account into it. Once the money is in the reputable exchange, the target is told to send the crypto to a specific wallet address that is controlled by scammers for "*investment*".

The target follows Victim B's instructions and transfers cryptocurrency to the wallet address he provides. As soon as the funds reach the scam-controlled wallet, Victim B cuts off all contact, leaving the target with significant financial losses.

X. Money Laundering of Criminal Proceeds

After the funds are moved to the scam-controlled crypto wallets, criminals who are operating scam centers and exploit TIP victims often deploy advanced money laundering techniques to obscure the origin of stolen funds.

Money laundering is a sophisticated criminal process used to disguise the illegal origins of funds, making them appear legitimate and enabling their integration into the formal financial system. According to the UNODC estimates, the spread of sophisticated criminal networks into regions with weak governance has attracted new actors, fueled corruption, and enabled the illicit industry to scale and consolidate—culminating in hundreds of industrial-scale scam centers generating nearly US $40 billion in annual profits. Criminals aim to obscure the trail of illicit money through various methods including the use of privacy coins, crypto mixers, and structured transactions. These techniques allow offenders to evade detection by authorities, complicating efforts to trace and seize the proceeds of crime. Cryptocurrency, with its pseudo-anonymous nature, has become a favored tool among criminals to launder the proceeds of illicit activities, particularly through tactics like mixing services and layered transactions. By blending illicit funds with legitimate ones, criminals misuse blockchain technology to create a complex web that challenges law enforcement and anti-money laundering (AML) measures, making it critical to understand these methods to combat financial crime effectively.

A prevalent tactic employed by criminals involves leveraging privacy coins which offer enhanced anonymity and reduced traceability compared to traditional cryptocurrencies to conceal their illicit transactions. After acquiring illicit funds in commonly used cryptocurrencies such as Bitcoin (BTC) or Ethereum (ETH), scammers convert them into privacy-focused cryptocurrencies designed to conceal transaction details. To further complicate tracking, they repeatedly swap between different privacy coins, severing any direct link to the original source. Eventually, they convert the obfuscated funds back into high-liquidity cryptocurrencies like BTC or ETH, which can then be easily exchanged for fiat currency. The process culminates in

transferring the fiat to bank accounts that is commonly referred to as the fiat securing stage.

Criminals also manipulate crypto mixers (or tumblers) to launder stolen funds. These services blend illicit crypto with legitimate transactions, redistributing them in small, randomized amounts across multiple crypto wallet addresses. This fragmented output makes it exceedingly difficult for blockchain analysts to trace the money trail, adding a critical layer of obfuscation.

Another laundering method involves smurfing or structured transactions, where criminals split stolen crypto funds into smaller amounts and transfer them to multiple cryptocurrency exchanges to evade detection. Once inside the exchanges, they convert the crypto to fiat, consolidate the funds, and then transfer the fiat to bank accounts, effectively integrating the illicit proceeds into the legitimate financial system. This technique makes it harder to trace the money trail, adding a critical layer of difficulty for blockchain analysts to unravel.

Advanced laundering techniques also allow criminals to bypass traditional AML measures, making it challenging for authorities to track and recover the funds. By leveraging these sophisticated methods, offenders can obscure the origins of their illicit gains, posing significant hurdles to law enforcement efforts.

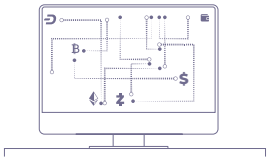
05 Money laundering

STAGE 1

Stolen funds are placed into a crypto-currency wallet to distance them from the source.

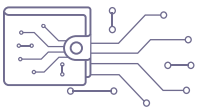
STAGE 2

The funds are sent through a crypto mixer to obscure their transaction history.



STAGE 3

Funds are received back from the mixer in small amounts at random intervals to a new wallet address.



STAGE 3

The "mixed" funds are sent to a cryptocurrency exchange and swapped for widely accepted crypto-currencies like Bitcoin or Ethereum.

STAGE 4

Funds are converted fiat currency.

STAGE 5

Transfer fiat currency (USD, EUR etc.) from cryptocurrency exchange into bank account(s)

STAGE 3

At this stage, funds can be withdrawn, spent, or reinvested without raising red flags.

A. Red Flags

Newly created wallets with high transaction volumes

Wallets that are recently created (e.g., within days or weeks) but show unusually high transaction volumes, especially if they involve multiple small deposits followed by large withdrawals, may indicate scam activity.

Transactions associated with reported scam wallets

TIP victims are denied access to independent communication channels and paid little or nothing for their labor. Salaries may be withheld entirely or deducted through fabricated fines for minor infractions, ensuring financial dependency on criminal networks.

Unusual geographic patterns of cryptocurrency transactions

Transactions originating from regions known for scam centers (e.g., Cambodia, Myanmar) or involving IPs linked to high-risk areas for scam centers, especially if the recipient wallet is in a different jurisdiction, raise suspicion.

Frequent transfers to privacy-focused cryptocurrencies

Wallets that regularly convert assets into privacy coins such as Monero (XMR), Zcash (ZEC), or Dash, especially after receiving large sums of crypto, may be attempting to obscure the transaction trail.

Involvement with known mixing services

Transactions that pass-through wallets or platforms associated with mixing services (e.g., Tornado Cash, ChipMixer) can be a red flag for laundering activities aimed at obfuscating fund origin.

Multiple low-value deposits across exchange

Evidence of multiple small crypto deposits that are often just under Know Your Customer (KYC) or AML reporting thresholds across different exchanges or wallets, especially when linked to the same original source.

Fast crypto-to-fiat transactions

Transactions that convert cryptocurrency to fiat currency at a high speed should be closely monitored, particularly when they involve large sums of money that do not align with the account's typical activity.

Reactivation of dormant bank accounts via cryptocurrency transfers

Bank accounts that have been inactive for long periods and suddenly see significant transactions or transfers could be being used to launder funds after being reactivated for this purpose.

Large and immediate withdrawals

Sudden withdrawals of large sums following deposits, especially from a crypto exchange, can indicate an effort to quickly cash out illicitly obtained funds.

B. Questions and Actions for Banks and Cryptocurrency Companies

01 Are the funds being sent to wallets previously flagged for fraud, romance scams, or investment fraud?

- ☑ High Priority Action: Cryptocurrency companies should monitor and block transactions to wallets associated with scam typologies. Blockchain analytics can help identify destination wallets linked to illicit activity. Scam targets often unknowingly send funds to criminal-controlled addresses.

02 Are new customer accounts funded with multiple small transactions from unrelated parties?

- ☑ High Priority Action: This may indicate smurfing which is a common money laundering tactic often used by scam centers to mask illicit origins of funds. Financial service providers and crypto platforms should apply transaction monitoring rules to detect and investigate such patterns.

03 Has the customer engaged in suspicious peer-to-peer transactions inconsistent with their profile or location?

Good Practice: Transactions that don't align with a user's behavior, employment, or transaction history should trigger enhanced due diligence and potentially account review or freezing.

04 Are there visible signs of distress or physical abuse on customers who come into a branch?

Good Practice: Criminal networks may force TIP victims to act as money mules by conducting final cash withdrawals or face-to-face transactions. TIP victims used in this way may show signs of physical abuse, fear, or confusion. Frontline staff—such as bank tellers or customer service representatives—should be trained to recognize and discreetly report these red flags to internal security or compliance teams. Institutions should establish clear escalation protocols to intervene without endangering the individual.

C. Case Study: Covering the Trail

Once the stolen cryptocurrency lands in the scam-controlled wallets via the efforts of Victim B, the laundering phase begins. From this point, criminal network representative steps in to handle the transfer, obscure the origin of the funds and make them appear legitimate. To do this, the scam operation follows a multi-layered approach.

Criminal network representative first convert the stolen assets—often Ethereum or Bitcoin—into privacy-focused cryptocurrencies such as Monero (XMR), Zcash (ZEC), or Dash. These coins are designed to mask wallet addresses, transaction amounts, and counterparties, offering enhanced anonymity over traditional tokens.

Once the funds are in privacy coins, they are often moved between multiple privacy cryptocurrencies, making the trail even harder to follow. This stage is crucial for severing any traceable link between the scam-controlled wallets and the original theft.

Criminal network representative then deposits the anonymized funds into crypto mixers-also known as tumblers. These services pool together thousands of transactions from various sources and redistribute them in randomized amounts across many wallet addresses. The result is a fragmented money trail that is very difficult for blockchain forensic experts to reconstruct.

In this case, criminal network representative uses several mixers in succession, bouncing small amounts of crypto between wallets controlled by the scam center and others used temporarily. This tactic injects additional complexity, further reducing the traceability of the transactions.

To avoid detection by cryptocurrency exchanges' AML systems, criminal network representative splits the laundered funds into dozens of smaller amounts and send them to multiple cryptocurrency exchanges. Each transaction is just small enough to avoid triggering suspicious activity alerts.

Once inside the exchanges, criminal network representative:

1. Converts the privacy coins back into high-liquidity tokens like BTC or ETH.
2. Sells the crypto for fiat currency (e.g., USD, CAD).
3. Distributes the fiat into numerous bank accounts, often registered under fake or stolen identities

This stage, known as fiat integration, is the final step in laundering, as it injects the illicit funds into the formal financial system, where they can be withdrawn, spent, or reinvested without raising red flags.

By the end of this process, criminal network representative is able to access the money through local bank accounts, often cashing out through shell companies or accomplices in different countries.

D. Additional Resource: How Bank Accounts Are Leveraged in Crypto-Related Scams

In addition to the misuse of cryptocurrency platforms, scammers often rely on traditional bank accounts as the first step in their laundering schemes. Recent investigations reveal that criminal networks obtain access to legitimate U.S. bank accounts—frequently opened under stolen or synthetic identities—via online black markets. These accounts are then used as temporary collection points to receive funds from scam targets before being quickly converted to cryptocurrency.

There are two primary tactics used to access these accounts:

1. Impersonation or identity fraud: Scammers open online accounts in other people's names without proper identification, using them to receive payments from scam targets.

2 Creation of front companies: Criminal groups recruit individuals to establish fake businesses and open accounts under the guise of legitimate operations. These accounts are then used to receive, launder, and transfer stolen funds.

Social media platforms like Telegram serve as a marketplace for this activity. Criminal networks advertise services that facilitate laundering, such as receiving wire transfers as fake business payments, making cash withdrawals from U.S. banks, and converting deposits into cryptocurrency, ultimately funneling funds to overseas scam operations.

In some scam centers described in this report, TIP victims are tasked with coordinating cyber fraud operations and are provided with account "*suppliers*" who are third-party brokers who match them with usable bank accounts to move illicit proceeds. The end goal is to collect funds into these accounts and swiftly convert them into cryptocurrency, making them harder to trace as they are funneled to scam centers, often located in Southeast Asia.

This activity highlights the large-scale misuse of the banking system. In response, many financial institutions are now strengthening their identity verification protocols, transaction monitoring systems, and inter-agency collaboration efforts to detect and disrupt these laundering networks before funds exit the formal financial system.

MEKONG CLUB

XI. An Overview of The Mekong Club

The vision of the Mekong Club is to harness the power of the private sector to change business practices in a way that will significantly reduce modern slavery. We aim to act as a catalyst for this change – engaging, inspiring and supporting the private sector to take the lead in the fight against this crime.

We have two major objectives:

A. To increase understanding and awareness of modern slavery throughout the international business community.

B. To identify practical ways to address modern slavery to meet these objectives, we use four strategic pillars:

01

Mekong Club Association:

The Mekong Club uses an association model to bring together four industry-specific working groups that meet on a quarterly basis:

- Banking and Finance
- Footwear and Apparel
- Hospitality
- Retail

02

Development of Tools:

Between working group meetings, The Mekong Club takes the recommendations made by its members and operationalizes them with the help of technical advisors/ experts in the field (toolkits, training programs, data updates, etc.). Once developed and tested, these tools are used by members to improve their response to modern slavery. The materials are also made available to our industry partners, thus increasing their reach and usefulness. Here are some of the tools that are currently offered:

A. An automated risk assessment tool to help companies assess risk of forced labor related to commodities and countries.

B. A resource guide for the banking industry.

C. A training program for relationship managers.

D. A multi-language e-learning tool comprised of videos and infographics.

E. A repository of best practices from companies in various sectors.

03 Awareness Raising and Advocacy:

Increasing awareness of the issue through the use of training has always been a core component of The Mekong Club's strategy. Our training programs have the following objectives:

A. To create a general understanding of the issue.

B. To help companies understand the potential vulnerability to their business.

C. To desensitize the private sector.

D. To encourage companies to join the fight to solve the problem.

04 Leadership:

Using ambassadors from the business world, The Mekong Club aims to increase the influence of the private sector in stepping up and taking a leadership role in the fight against modern slavery.

These individuals, who are leaders in their respective fields, are made available to mentor individual companies. They aim to identify gaps in knowledge and actions related to modern slavery, offer useful recommendations and then encourage private sector partners to take a more active role.

XII. Glossary of Terms

Advance Fee Scam

A type of fraud where someone is tricked into paying money upfront in exchange for a promised service or reward (like a loan, job, or investment) that never happens.

AML (Anti-Money Laundering)

Laws and systems used by banks and governments to stop criminals from hiding or cleaning ("laundering") money made through illegal activity.

Bitcoin (BTC)

A well-known cryptocurrency used in both legal and illegal transactions. It allows people to send and receive digital money without using a bank.

Blockchain

A digital record book that permanently keeps track of all cryptocurrency transactions. It is public and permanent, but people involved in each transaction are not always easily identified.

Scam Center

A building or facility where TIP victims are forced to work in illegal operations, often running scams online. These are often guarded and located in countries with weak law enforcement.

Cryptocurrency (Crypto)

A digital form of money (like Bitcoin or Ethereum) that is not issued by any government or bank. It's commonly used in online scams because it can be harder to trace.

Crypto Exchange

A website or platform where people buy, sell, or trade cryptocurrencies. Scammers often create fake versions to steal people's money.

Crypto Mixers

A crypto mixer is a service that jumble together many people's crypto to hide where the money came from or where it's going. It is also known as tumbler or blender and is a service that aims to obscure the transaction trail of cryptocurrency

Dash (DASH)

A cryptocurrency focused on fast and cheap transactions. Dash offers more privacy than Bitcoin, making it attractive for scammers.

Debt Bondage

When someone is forced to work to pay off a debt, often under false promises. It's commonly used in scam centers to trap TIP victims.

Digital Wallet / Crypto Wallet

A software app or device that stores cryptocurrencies. Scammers often use digital wallets to receive and move stolen funds.

Ethereum (ETH)

A popular cryptocurrency and blockchain platform that supports "*smart contracts*"—automated agreements without banks. Scammers often promote fake Ethereum investments.

Fiat Currency

Traditional government-issued money like US Dollars and Euros. Unlike crypto, fiat currency is regulated by central banks.

KYC (Know Your Customer)

A process banks and other services use to verify someone's identity. Proper KYC checks can help stop scammers from opening accounts.

Monero (XMR)

A cryptocurrency designed for complete privacy—transactions are hidden and untraceable. It's often used in illegal markets and scams.

Money Mule

A person who transfers money for criminals. Sometimes they know what they're doing; other times, they're tricked into it through fake job offers.

NFT (Non-Fungible Token)

A unique digital item (like art or music) stored on a blockchain. These are sometimes used in scams to fake investments or steal money.

Red Flag Indicator

A warning sign that something may be suspicious like a person sending money overseas for unknown reasons or receiving high amounts of crypto suddenly.

Romance Scam

A fraud where someone builds a fake romantic relationship online to emotionally manipulate and financially exploit the individual who is a scam target

Smart Contract

A computer program on a blockchain that runs automatically when conditions are met.

Technical detail

These are self-executing codes stored on the blockchain; scammers sometimes create fake smart contracts to steal funds.

Smurfing:

Smurfing is a technique where funds are divided into smaller amounts to bypass reporting thresholds, launder money and evade detection by regulators. Breaking up large amounts of money into many smaller transactions to avoid getting caught.

Spoofing

Faking caller IDs, websites, or email addresses to make messages look like they're from a trusted person or company.

Trafficking (Human)

The illegal movement of people—often through deception or force—for exploitation. In scam centers, this means forcing people to run scams against their will.

Zcash (ZEC)

A cryptocurrency that lets people send money without easily revealing who is involved. It has built-in privacy features and ,ike Monero, it's designed to hide who is sending and receiving funds —making it attractive for illegal use.

XIII. References

BBC News. (2024, January 23). Surrey family scammed in crypto fraud linked to trafficking. BBC. https://www.bbc.com/news/uk-england-surrey-68110626

California Department of Financial Protection and Innovation. (2025, March). Pig butchering scam playbook. https://dfpi.ca.gov/wp-content/uploads/2025/03/Pig-Butchering-Scam-Playbook.pdf

Center for Strategic and International Studies (CSIS). (2023, October 31). Cyber scamming goes global: Sourcing forced labor for fraud factories. https://www.csis.org/analysis/cyber-scamming-goes-global-sourcing-forced-labor-fraud-factories

Federal Trade Commission. (2023a, August). Scammers impersonate well-known companies to recruit for fake jobs on LinkedIn and other job platforms. https://consumer.ftc.gov/consumer-alerts/2023/08/scammers-impersonate-well-known-companies-recruit-fake-jobs-linkedin-and-other-job-platforms

Federal Trade Commission. (2023b). What to know about cryptocurrency and scams. https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

FBI. (n.d.). Cryptocurrency investment fraud. Federal Bureau of Investigation. https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud

International Justice Mission. (n.d.). Forced scamming. IJM. https://www.ijm.org/our-work/trafficking-slavery/forced-scamming

International Labour Organization. (2012). ILO global estimate of forced labour: Results and methodology. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_norm/@declaration/documents/publication/wcms_203832.pdf

International Air Transport Association. (n.d.). Human trafficking. IATA. https://www.iata.org/human-trafficking

Office of the High Commissioner for Human Rights. (2023, August 29). Hundreds of thousands trafficked to work as online scammers in Southeast Asia, says UN report. https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report?utm

ProPublica. (2023, December 22). How pig butchering scam networks launder billions through U.S. banks. https://www.propublica.org/article/pig-butchering-scam-cybercrime-us-banks-money-laundering

TRM Labs. (2023, September 19). Unmasking pig butchering scams: The $4 billion crypto scheme preying on vulnerable investors. https://www.trmlabs.com/resources/blog/unmasking-pig-butchering-scams-the-4-billion-crypto-scheme-preying-on-vulnerable-investors

United Nations Office on Drugs and Crime. (2008). Toolkit to combat trafficking in persons: Global programme against trafficking in human beings (Tool 1.1). https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_1-1.pdf

United Nations Office on Drugs and Crime. (2023, September). Key indicators of trafficking in persons for forced criminality. UNODC. https://www.unodc.org/roseap/uploads/documents/Publications/2023/UNODC_Key_Indicators_of_TIP_for_Forced_Criminality_FINAL_September_2023.pdf

United Nations Office on Drugs and Crime. (2025, April). Cyberfraud at an inflection point in the Mekong region. UNODC. https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html

United States Institute of Peace. (2024, May 14). Transnational crime in Southeast Asia: A growing threat to global peace and security. https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

Human Rights Council. (2024, May). Cyber-slavery in the scamming compounds: Briefing note. https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66447ab0da3cd25e7614a192_HRC-Briefing_Cyber-Slavery-in-the-Scamming-Compounds-ENGLISH.pdf

New York Times. (2024, September 10). Scammers, trafficking and cybercrime in Southeast Asia. The New York Times. https://www.nytimes.com/2024/09/10/business/scammers-trafficking-cybercrime.html


MEKONG
CLUB