THAMMASAT UNIVERSITY
FACULTY OF SOCIAL ADMINISTRATION

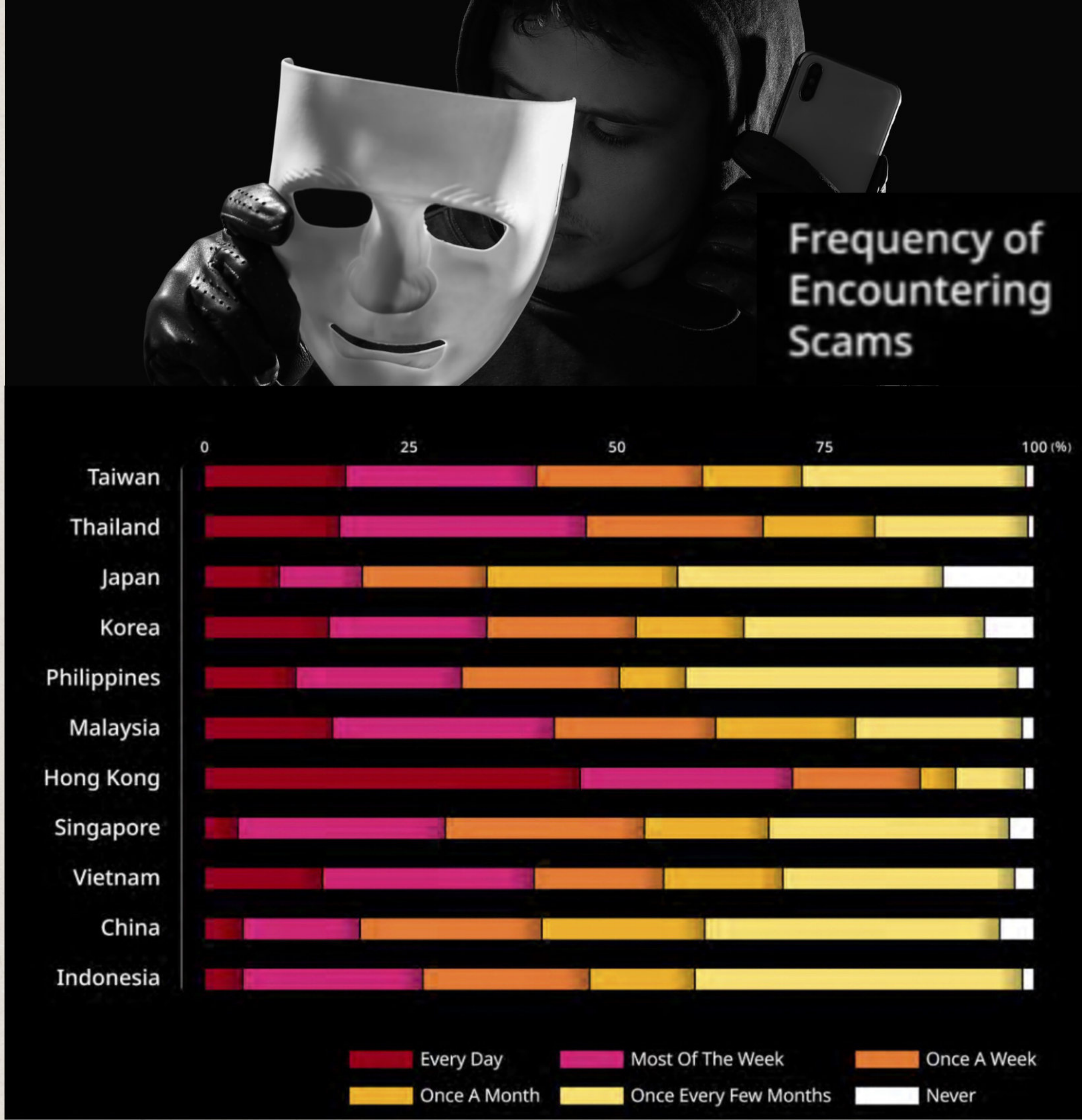
ECONOMIC CRIMES THROUGH TELE-SCAMMING OPERATIONS IN SOUTHEAST ASIA

Presented by
Tonnam Rattaorapin, Social Policy & Development Program

WHAT'S GOING ON?

- Tele scam is a operation done online by roaring in vulnerable people
- the scam networks adapt quickly: relocate, shift online, change cash-out methods

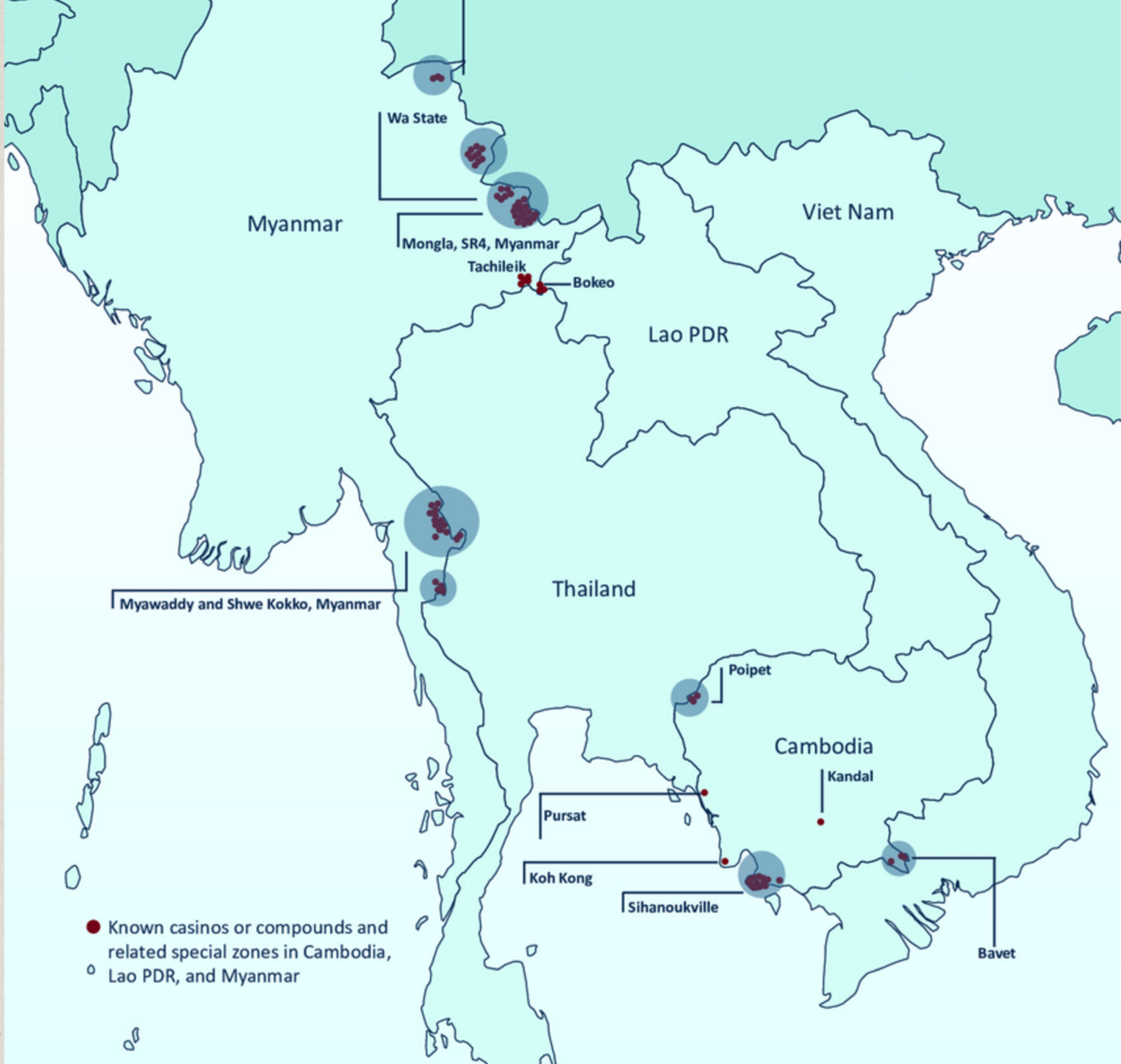
Especially in 2023 Countries in Southeast Asia including Thailand, Vietnam and The Philippines encounters nearly **20% of tele scamming everyday**



SCAM LOCATIONS

Base #1 Cambodia, Poi Pet, O Smach, Sihanoukville

Base #2 Myanmar, Tachileik, Payathonzu, Myawaddy

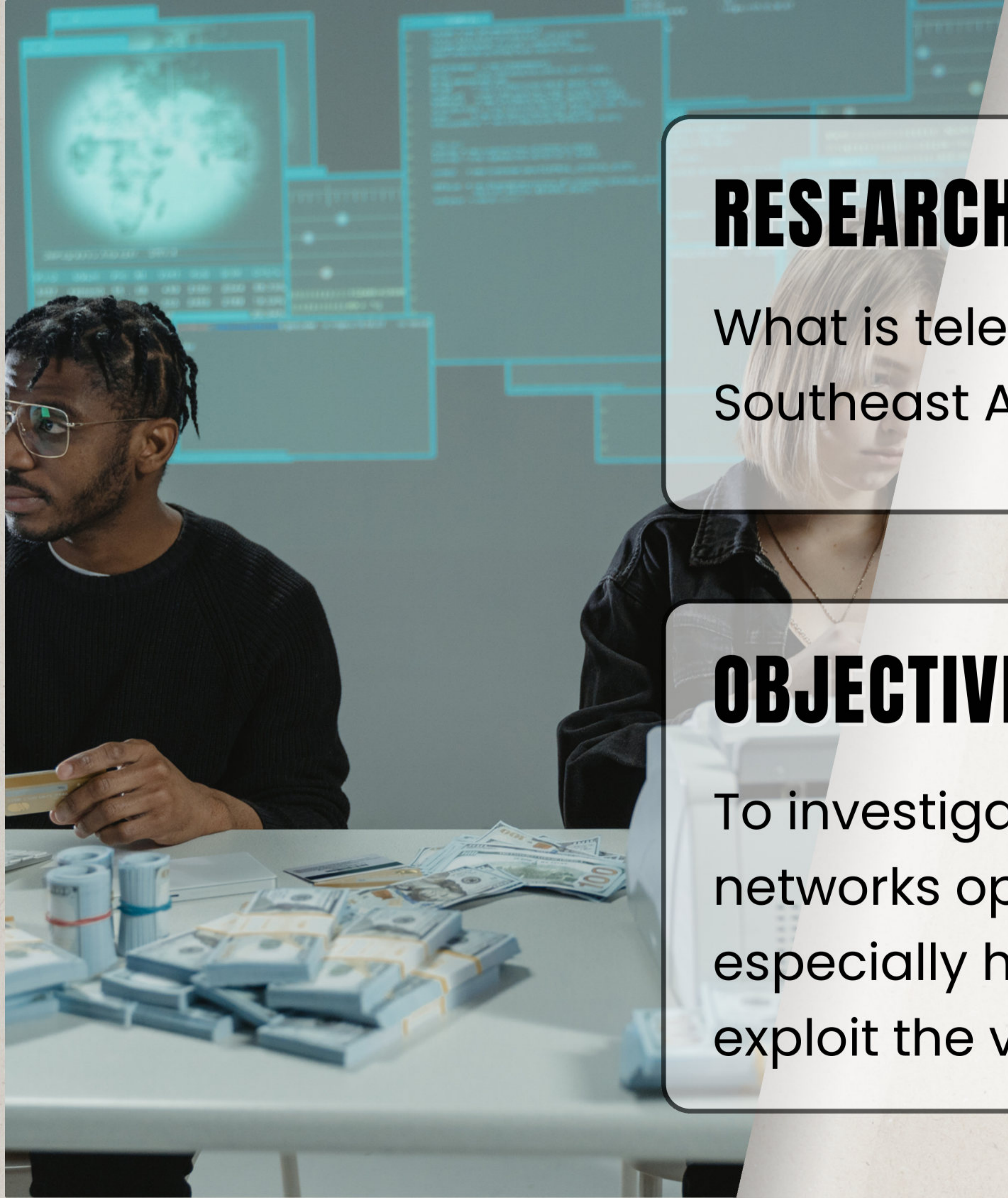


THE EFFECTS ON ECONOMY

- In 2024, an estimated total loss was, $23.6 billion from Southeast Asians, with nearly one in four adults reporting financial losses. Scams are being executed rapidly, with two-thirds occurring within 24 hours of initial contact.
- In Singapore specifically, scam losses are very high: average of US$2,132 lost per victim in 2024 per that same report.
- In Thailand, losses from online fraud including telephone / SMS scamshit 60 billion baht (~US$1.76 billion) in 2024.

RESEARCH GAPS

- The network being unexplored results in lower level of awareness to be exploited from scam organizations
- Results lead to losing asset, digital currency, and escalating crimes



RESEARCH QUESTION

What is tele-scamming patterns in Southeast Asia ?

OBJECTIVE

To investigate patterns of tele-scamming networks operate across Southeast Asia, especially how they develop strategies to exploit the vulnerable people

SCOPE OF WORK

- The study focuses on scam operation in Myanmar and Cambodia

DATA COLLECTION

- Data collected from offical documents, news, and academic papers from 2020-2025

ANALYTICAL FRAME

- To analyze the Economic Impact Scam center have made and how scam operations works through each process

How scam operations works through each process	To analyse the role of each stakeholder	To analyze the economic wage cut within the organization	Policy against tele scamming

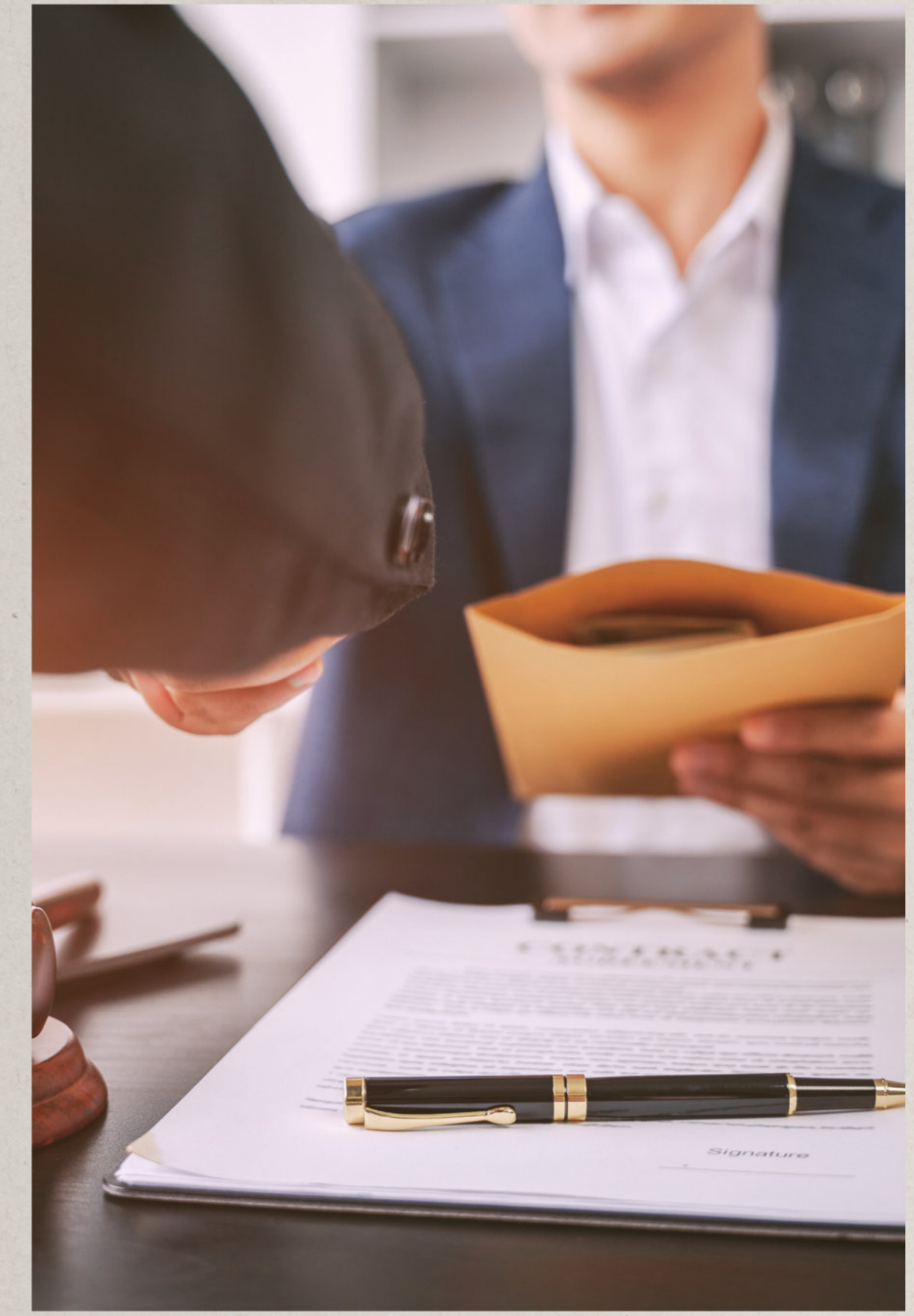
Stage of scamming operation

Recruitment

Control

Transportation

Exploitation



TELE SCAM STRATEGIES

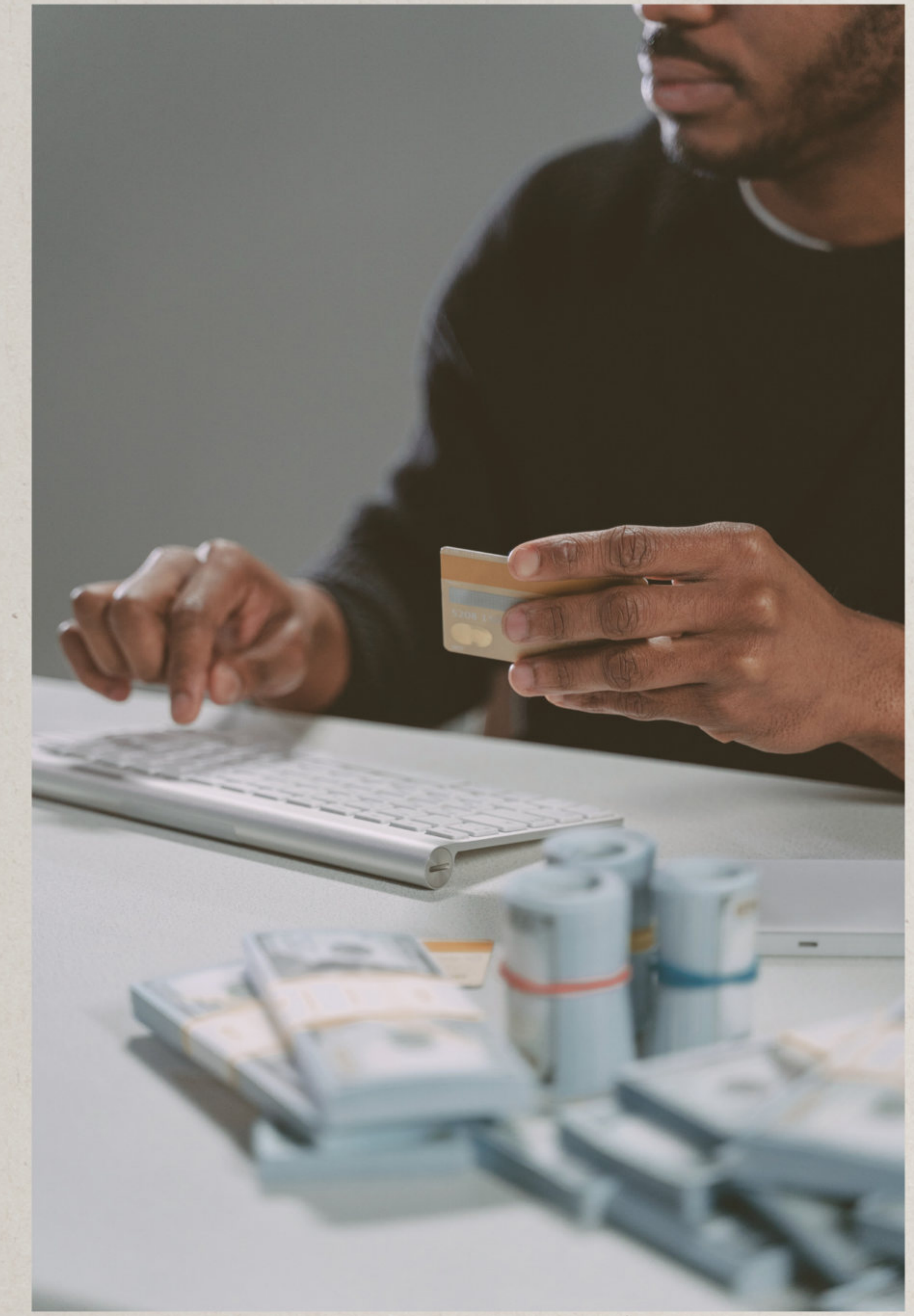
Recruitment

- Starting by employing a fake job advertisements online/Hired a front agent to help with the reputation of business
- Set up a team with A fake agent that had connections with the official in order to gain access to the personal information in order to have connections with vulnerable group
- Have the agent arrange a meet up with the victim somewhere safe and assessable for the victim to make them feels unharmed then convince them to sign a contract or make them agree to travel to the borderlands

TELE SCAM STRATEGIES

Transportation

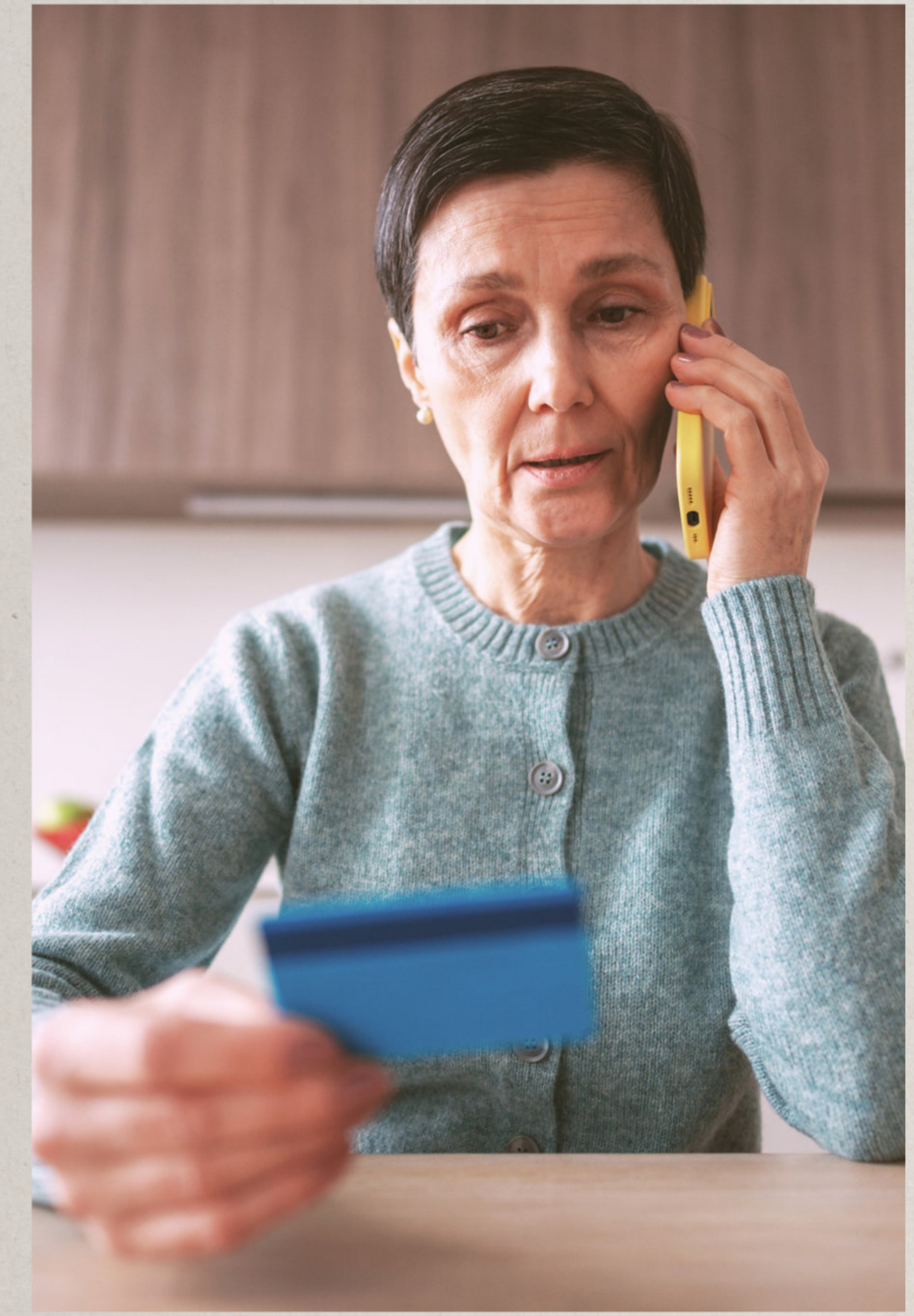
- The agent would arrange a meeting day to travel to the job site often in borderland, whether the agent might sponsor the transportation cost or have the victims be dropped off by themselves.
- Victims are then sneaked through the border by the Corrie through natural pass with the support from their network who lives around the border.
- Victim are then getting through the registration stage by the people in charge. At this rate there might be physical harm involved



TELE SCAM STRATEGIES

Exploitation

- Victims are made to work long hours, sometimes 12–18 hours per day, 7 days a week.
- In “cyber scam” centers, they are forced to chat online, run investment scams, romance scams, or cryptocurrency frauds, often under supervision.
- Refusal to meet quotas or mistakes may result in beatings, torture, or fines.

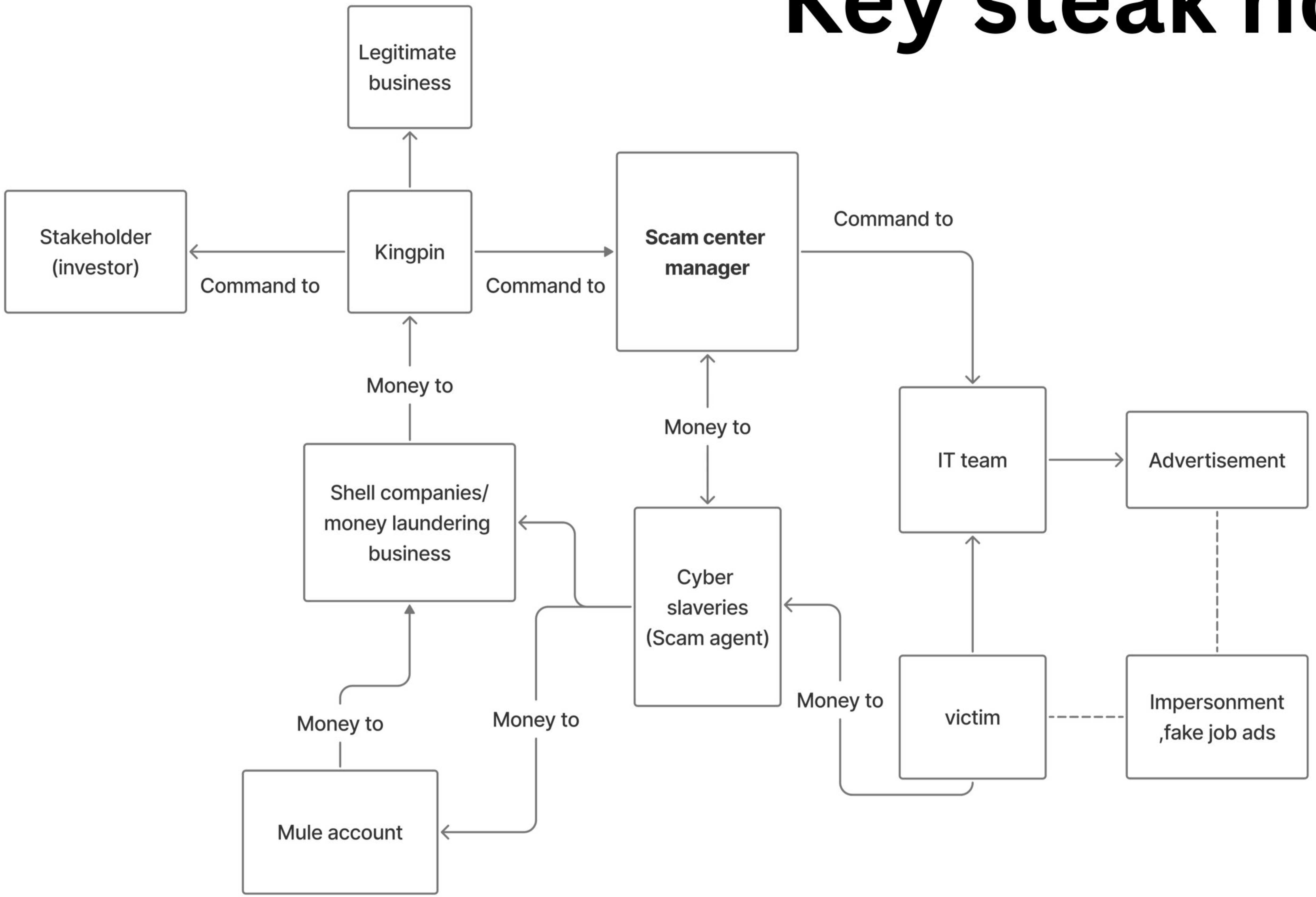


TELE SCAM STRATEGIES

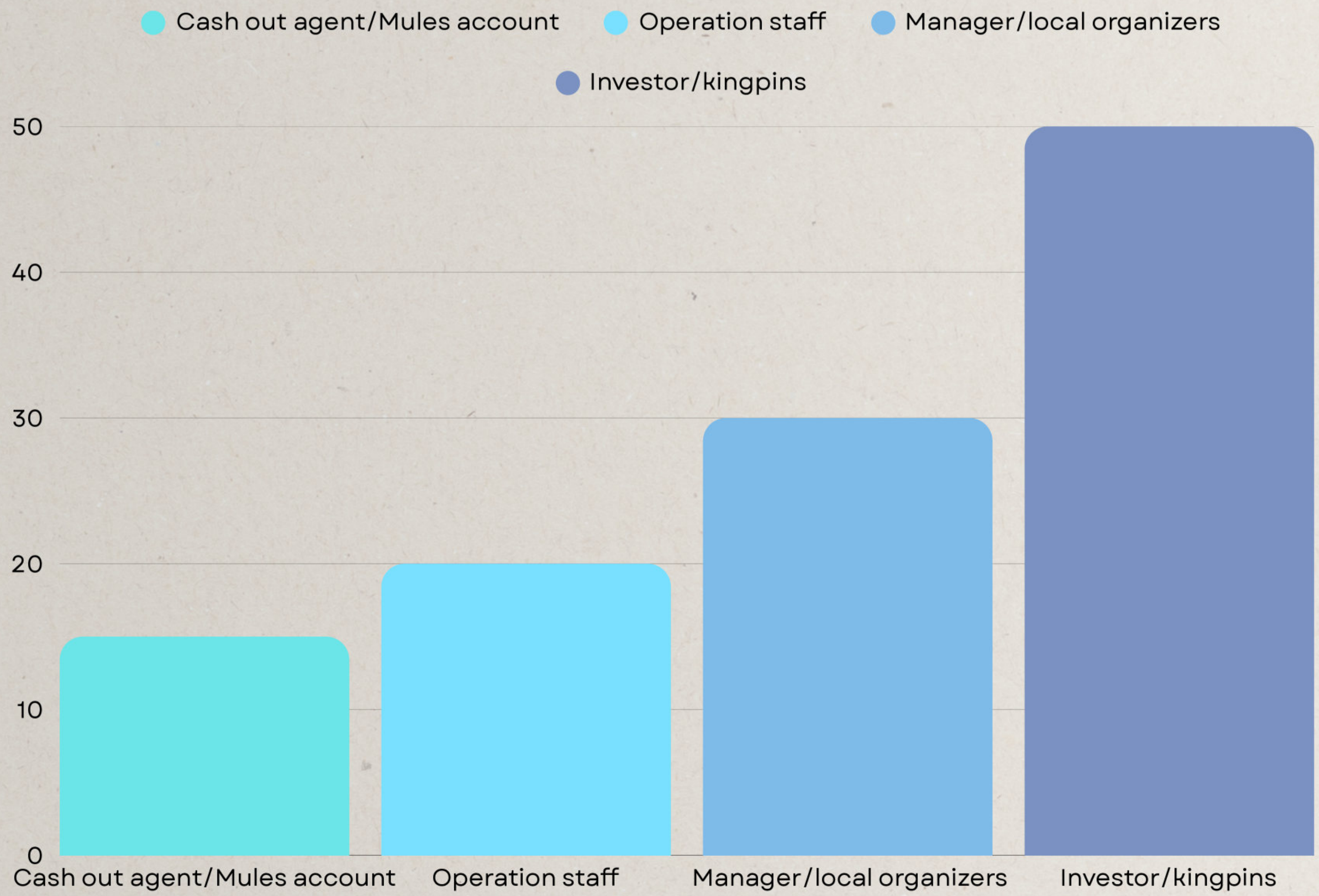
Control

- they use official-sounding rules (lockdown, “control period”) to justify keeping people confined, isolating them from help, and preventing escape.
- passports, ID, phones, or permits are taken to stop victims leaving or contacting others.
- victims may be restricted of food, sleep or movement to weaken resistance.

Key steak holder



Money laundering system and the pay cut to each stakeholder



Exact splits vary enormously by scheme, geography, and level of risk. Public reports and prosecutions indicate wide variability; below are illustrative ranges often reported in investigations

- Top-level organizers / investors / kingpins: 20–50%+

- Call/centre managers and local organizers: 10–30%

- Front-line scammers / operation staff (agents): 10–50% of net take

- Money-mules/cash-out agents: 1–15%(

Cash flow within the organization

Victim Payments
|
Front-End Accounts (bank, crypto, payment apps)
|
Money Mules -------> Gift Cards -------> Resellers
| |
Shell Companies------ -------------> Crypto Mixing Services
| |
Final Beneficiaries / Scam Operators

Fraud Revenue from Victims Scam centers don't cold-call completely at random — they get leads from affiliate marketers. Either from shady website or victim who

→

Money Laundering Infrastructure
Local casinos are often used to launder cash. Since casinos deal in large volumes, illicit funds can be mingled with legitimate gambling money

↓

Reinvestment & Funding Other Crimes
Some of this money is also reinvested in infrastructure — real estate, more compounds, or even legitimate-seeming businesses (e.g., casinos) that help to launder further.

- **According to UN-linked reporting, scam operations in Southeast Asia may rake in tens of billions of dollars annually.**

Conclusion and Recommendations

Protect & Rescue Victims

- Create cross-border victim protection programs (for trafficked workers in scam centers).
- Provide repatriation, legal aid, and rehabilitation for those coerced into scamming.

Financial Controls

- Use anti-money laundering (AML) tools to trace and freeze illicit proceeds from scam operations.
- Work with banks, crypto exchanges, and payment platforms to identify and block funds linked to scam-centre networks.

Public Awareness & Education

- Conduct large-scale digital trust campaigns (e.g., via GSMA, national regulators) to educate citizens about tele-scams.
- Promote awareness about emerging AI-powered scams (deepfakes, voice cloning).

Damage to economy	Prevention
Tele-scamming is a major regional economic crime with growing financial and social impacts.	Operations exploit technology, weak regulation, and cross-border enforcement gaps.
Because tourism is a big part of many Southeast Asian economies, loss of trust can have ripple effects on foreign investment and travel.	Public awareness and early-detection tools remain key preventive measures.
In Thailand, scam losses reached 110 billion baht (~US$3.39 billion) in a year	A multi-layered, coordinated strategy is needed to protect people and financial systems.
High scam losses reduce trust in digital financial systems. For example, as scam frequency increases, people may be more reluctant to engage in digital investment or payments.	Regulatory and Enforcement Burden • Governments must spend more on law enforcement, cross-border cooperation, and telecom regulation.