Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Scam Compounds and Virtual-Asset Laundering: A Structured Case Analysis of the Alleged Chen Zhi/Prince Group Network

Raymond L.M. Tang

rlmtang@hku.hk

University of Hong Kong

Bo Wen

University of Macau

Research Article

Keywords: scam compounds, transnational organised crime, forced criminality, virtual-asset laundering, corporate embedding, regulatory arbitrage

Posted Date: September 8th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10917505/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

This article presents a documentary case analysis of the alleged Chen Zhi/Prince Group network, examining how scam compounds combine coerced labour, industrialised fraud, virtual-asset laundering, corporate vehicles, and cross-border protection. The corpus comprises 59 cited public sources available through 30 June 2026, including legal and regulatory materials, United Nations and Financial Action Task Force publications, scholarship, blockchain analysis, denial statements, reporting, and non-governmental organisation investigations. Directed content analysis, negative-case analysis, and source-status coding distinguish allegations, administrative findings, corroborated observations, contested claims, and contextual evidence. The record alleges layered laundering through wallet fragmentation, underground remittance, gambling infrastructure, companies, and conventional assets. Rather than a new general theory, the Scam-Compound Organisational Matrix is presented as a bounded comparative heuristic assessing whether five functions are internalised or coordinated: labour control, fraud production, financial concealment, corporate embedding, and protection or regulatory arbitrage. It distinguishes integrated organisations from fraud networks that outsource functions and generates testable expectations about resilience and substitution. The analysis shows why indictment claims cannot be treated as independently verified facts, why asset provenance matters for restitution, and why disruption requires victim-safety assessment.

1 Introduction

Cyber-enabled investment fraud has shifted from opportunistic deception to industrialised cross-border enterprises that combine scripted social engineering, cryptocurrency settlement, and coerced labour (OHCHR, 2023; UNODC, 2023). ‘Pig butchering’ (*sha zhu pan*) often involves enticing individuals using stories of romance, friendship, or investment, eventually leading them to transfer money to fake platforms. Studies reveal a pattern that includes attracting victims, building trust, showing fake profits, increasing the amount of money deposited, and then preventing withdrawals, occasionally carried out by trafficked individuals forced into these activities (Gujarathi et al., 2026; Nocella, 2025; Oak & Shafiq, 2025).

Building on this general pattern, the Southeast Asian scam-compound phenomenon is distinctive because it fuses two victim populations: remote fraud victims who lose money and trafficked workers coerced into committing fraud under conditions that may include confinement, debt bondage, and violence. The Office of the United Nations High Commissioner for Human Rights (OHCHR) estimated in 2023 that at least 120,000 people in Myanmar and approximately 100,000 in Cambodia may have been held in situations forcing them to carry out online scams, and the United Nations Office on Drugs and Crime (UNODC) identified casino and special economic zone infrastructure as central to the emergence of secure compounds across Cambodia, Lao PDR, Myanmar, and elsewhere, where trafficked persons were forced to run romance, brokerage, cryptocurrency, and illegal-gambling scams under violent discipline (OHCHR, 2023; UNODC, 2023). Consistent with these findings, the Global Initiative Against Transnational Organised Crime describes this ecosystem as a “compound crime” model in which repurposed hotels, casinos, and private compounds become global fraud centres protected by corruption, local elites, and money-laundering networks (Global Initiative Against Transnational Organized Crime, 2025).

Within this broader landscape, the alleged Chen Zhi case is a critical study because it links the regional scam-compound economy to a distributed laundering architecture and a record United States (U.S.) cryptocurrency forfeiture action (Nocella, 2025; Office of Public Affairs, 2025). The indictment describes Chen, also known as Vincent, as the founder and chairman of Prince Holding Group, a Cambodian conglomerate with more than 100 entities in over 30 countries. Authorities allege that, from approximately 2015, the group operated forced-labour

scam compounds and laundered proceeds through gambling, mining, shell companies, and conventional assets; the Prince Group denies wrongdoing (Davies & Zhao, 2024; Lin, 2025).

Against this background, this study addresses three research questions: (1) what chronological pattern of alleged criminal conduct and enforcement action is visible from open-source documents between 2015 and 2026; (2) what laundering typology is alleged, and how does it correspond to known virtual-asset, casino, shell-company, and real-estate money-laundering patterns; and (3) what does the case reveal about cross-border anti-money laundering and counter-financing of terrorism (AML/CFT) cooperation, sanctions, asset freezing, victim restitution, and the governance of scam-compound economies? These questions were addressed through a qualitative case study design that treats the alleged Chen Zhi matter as an ongoing, legally unresolved case, rather than an adjudicated account of criminal liability.

The article makes a deliberately bounded contribution. It does not claim that coerced labour, fraud industrialisation, laundering, corporate embedding, or political protection are newly discovered features. Prior work on compound capitalism, compound crime, and scam cities has already established those elements (Franceschini et al., 2023; Global Initiative Against Transnational Organized Crime, 2025; Lilli & Zucca, 2025). The present contribution is instead an evidence-disciplined case analysis and a structured comparative matrix for assessing the degree to which these functions are internalised within one organisational architecture. This reframing yields two empirical questions that descriptive accounts alone do not resolve: whether functional integration is associated with greater resilience after node-specific enforcement, and whether interventions directed at one pillar produce substitution, relocation, or contraction in the others. Scam-Compound Organisational Matrix (SCOM) is therefore used as a sensitising and comparison-enabling heuristic, not as a universal theory or a claim to conceptual priority.

2 Methods

This article uses a qualitative, single-case documentary design. The case was selected purposively because it is unusually information-rich and brings together cyber-enabled fraud, alleged trafficking for forced criminality, virtual assets, casinos, corporate structures, sanctions, forfeiture, extradition, and insolvency across several jurisdictions. The design reconstructs claims and institutional responses; it does not determine criminal liability, test intervention effects, or estimate the total number of victims or losses.

The final corpus contains 59 unique cited sources available through 30 June 2026. A retrospective search and source audit was conducted using Google Scholar, Crossref, and publisher searches for academic work, and Google and targeted site searches for official and grey literature. Search strings combined ‘Chen Zhi’, ‘Prince Group’, ‘Prince Holding Group’, ‘scam compound’, ‘pig butchering’, ‘forced criminality’, ‘Huione’, ‘virtual asset laundering’, ‘OJBK wallet’, ‘LuBian’, ‘sanctions’, ‘forfeiture’, ‘extradition’, ‘Prince Bank’, and ‘Chapter 15’. Citation chaining was used from the indictment, sanctions notices, United Nations (UN) reports, and core academic studies. The temporal scope was 2015 to 30 June 2026, while earlier theoretical literature was retained where necessary.

Documents were included when they (a) concerned the named case or a directly linked enforcement, corporate, financial, or insolvency action; (b) supplied regional evidence relevant to the alleged organisational functions; or (c) provided an established theoretical or AML/CFT framework used in analysis. Duplicated wire-service reproductions, unattributed social-media posts, promotional material without evidentiary content, and reports that merely repeated an earlier source without adding facts were excluded. English-language sources were analysed directly. Chinese-language court reporting and Cambodian or Taiwanese developments were included only where

an identifiable judgment, official release, or reputable translated report was available. This language restriction is a material limitation.

Each retained item was logged by date, jurisdiction, source type, legal status, principal claim, named entities, and relationship to the research questions. Directed coding began with predicate fraud, labour coercion, organisational control, virtual-asset flows, underground remittance, gambling, corporate vehicles, real estate and luxury assets, corruption or protection, sanctions, asset restraint, extradition, insolvency, and victim protection. Inductive refinements added contested provenance, successor infrastructure, dual victimisation, and professional-gatekeeper responses. A working codebook and claim-evidence table were maintained, and chronology entries were checked against the underlying cited source before inclusion.

Coding was undertaken by the author. Because there was no second coder, an inter-coder agreement rate cannot responsibly be reported. Reliability was addressed through two-pass coding, recoding after the inductive categories stabilised, and an audit trail linking consequential claims to specific documents. This is procedural consistency rather than independent reliability, and the absence of inter-coder testing remains a limitation. Reflexive memos recorded the risk that a financial-crime and enforcement lens could privilege state categories, especially U.S. and United Kingdom (U.K.) prosecutorial narratives.

To counter that asymmetry, the analysis used negative-case and adversarial-source procedures. Searches specifically sought Prince Group denials, defence-oriented accounts, Cambodian and Chinese reporting, court developments not favourable to prosecution narratives, independent blockchain analysis, survivor-focused non-governmental organisation (NGO) evidence, and discrepancies within official materials. Claims were classified as: (1) adjudicated fact; (2) administrative or regulatory finding; (3) prosecutorial allegation; (4) independently corroborated observation; (5) contested or contradictory claim; or (6) contextual typology. Where sources conflicted, the text reports the conflict and avoids collapsing different evidentiary standards. The LuBian attribution and the questioned indictment images are retained precisely because they complicate, rather than confirm, the prosecution account.

Official documents are therefore evidence that an allegation, designation, seizure, or procedural act occurred, not proof that the underlying conduct occurred as alleged. Journalistic and NGO materials are not treated as automatically corroborative merely because they are consistent with an indictment. Corroboration is claimed only where a source contributes independently derived evidence, such as a separate court record, asset action, first-hand investigation, or blockchain attribution. Otherwise, the source is described as contextual or derivative.

The approach is limited by sealed evidence, incomplete language coverage, uncertain blockchain attribution, selective disclosure, and evolving proceedings. These constraints limit causal inference and generalisation, while source-status coding clarifies what the public record establishes.

3 Theoretical Framework

The analysis uses four established lenses, not as competing theories but as tools addressing different levels of the case: money-laundering stages organise alleged fund movement; routine activity theory addresses victim access and guardianship; state-organised crime scholarship addresses possible protection; and transnational network theory addresses dispersed coordination and resilience. SCOM, introduced in Section 5.1, does not replace these theories. It converts their case-relevant organisational implications into a common observation matrix.

First, the classic money-laundering stage model – placement, layering, and integration – organises Section 4.2 and Fig. 1, conceptualising laundering as a sequential transformation of illicit proceeds through successive financial vehicles designed to sever the link between funds and their criminal origin (Levi & Reuter, 2006). The case extends this model into the virtual-asset domain, where “spraying and funnelling” across wallets substitutes for the layering historically performed by shell banks and correspondent accounts, showing that cryptocurrency has accelerated and disaggregated the stage model rather than replaced it.

Second, routine activity theory explains the pre-crime mechanism: crime emerges from the convergence of a motivated offender, suitable target, and absence of a capable guardian (Cohen & Felson, 1979). Cyberspace extensions argue that digital environments multiply offender-target convergence by removing spatial and temporal constraints on victim contact (Leukfeldt & Yar, 2016). “Pig butchering” operationalises the scam at scale: scripted social engineering and always-available messaging create a low-guardianship environment in which a small workforce can victimise large and dispersed populations. The theory also illuminates the case’s dual-victim structure, since the same conditions exposing remote investors to fraud also expose trafficked compound workers to coercion.

Third, the state-organised crime framework explains the alleged durability and jurisdictional reach of the enterprise: criminal enterprises are sometimes best understood not as clandestine actors evading the state but as entities operating with tacit or active state toleration, where elites and criminal operators exchange protection for revenue or political capital (Chamblis, 1989). This situation is consistent with the case’s reported “neak oknha” honourific ties, the elite-linked Crown-casino network implicated alongside the Prince Group, and Cambodia’s subsequent liquidation of Prince Bank, suggesting that formal institutions were allegedly co-opted rather than merely circumvented.

Fourth, transnational criminal network theory accounts for the enterprise’s dispersed, multi-node structure, treating transnational criminal enterprises as loosely coupled networks of specialised nodes – recruiters, launderers, technology providers, and corporate facilitators – that can reconstitute quickly after individual nodes are disrupted (Williams, 2001). This lens accommodates the case’s “role shifter” logic (Global Initiative Against Transnational Organized Crime, 2025) and explains why enforcement in one jurisdiction did not immediately halt operations elsewhere (“#8 Park” reportedly still operating per Amnesty International in June 2026).

Taken together, these lenses frame scam compounds not merely as cyberfraud operations or trafficking sites but as criminal ecosystems in which opportunity structures, organisational networks, laundering mechanisms, and political protection interact – an organisational adaptation of transnational organised crime rather than a purely technological evolution of fraud.

4 Results

4.1 Chronological case narrative, 2015–2026

The U.S. indictment alleges that Chen Zhi served as chairman of Prince Holding Group from approximately 2015, operating over 100 entities in more than 30 countries while publicly describing legitimate businesses in real estate, financial services, and consumer services (Nocella, 2025). Prosecutors allege that the enterprise built and operated at least ten scam compounds across Cambodia, including the Jinbei Compound, Golden Fortune Science and Technology Park, and Mango Park/Jinhong Park, where trafficked workers were forced to execute cryptocurrency

investment fraud using internal ledgers, scripted chat operations, and phone farms, allegedly including two facilities with 1,250 phones controlling 76,000 accounts (Nocella, 2025).

Building on this operational base, the alleged model combines high-volume victim acquisition with transfers between virtual and conventional assets. 'Money houses' allegedly received Bitcoin and stablecoins, off-ramped them into fiat, and repurchased 'clean' cryptocurrency; Chen allegedly discussed 'BTC washing' and controlled unhosted wallets holding approximately 127,271 Bitcoin by 2020 (Nocella, 2025).

Notably, Chinese law enforcement attention reportedly preceded the 2025 U.S. action: Radio Free Asia reported Chinese criminal court judgements from 2020 to 2022 describing Prince Group as a "notorious transnational online gambling criminal group," alleging at least 5 billion yuan (approximately US$700 million) in illicit revenue and a Beijing task force formed in May 2020, although Chen and senior executives were absent from the judgements reviewed, and Prince Group denied the allegations as impersonation (Davies & Zhao, 2024). East Asia Forum also linked Chinese probes back to 2020, detailing how a task force discovered bank-card networks that circumvented capital restrictions (Lin, 2025).

Enforcement then accelerated markedly: on October 14, 2025, the U.S. and U.K. authorities launched a coordinated enforcement package (see Tables 1 and 2). The U.S. indictment charged Chen with wire fraud and money-laundering conspiracy, with forfeiture allegations seeking approximately 127,271 Bitcoin, which the U.S. Department of Justice valued at roughly US$15 billion and described as the largest forfeiture action in U.S. Department of Justice history (Nocella, 2025; Office of Public Affairs, 2025). Office of Foreign Assets Control (OFAC) designated the Prince Group Transnational Criminal Organisation and 146 associated targets, while Financial Crimes Enforcement Network (FinCEN) issued a Section 311 final rule cutting Huione Group off from the U.S. financial system as a primary money-laundering concern (FinCEN, 2025; U.S. Department of the Treasury, 2025).

Table 1
Timeline of key events

Date	Event	Source
2014–2015	Chen Zhi obtained Cambodian citizenship (2014); the indictment alleges he founded/chaired Prince Group from ~ 2015.	Davies and Zhao (2024); Nocella (2025)
Approx. 2015 onwards	Alleged construction/operation of forced-labour scam compounds across Cambodia used to launder proceeds.	Nocella (2025)
2018	Alleged procurement of millions of phone numbers/passwords; phone-farm and scripted-chat infrastructure.	Nocella (2025)
2019	Cambodia has banned online gambling; the Prince Group allegedly continued to operate through mirror websites.	Nocella (2025)
Jul. 2020	Chen was awarded the “neak oknha” honourific after reportedly donating over US$18 million and was named personal counsellor to PM Hun Sen.	Tower and Amerhauser (2026)
By approx. 2020	Chen allegedly controlled ~ 127,271 Bitcoin in unhosted wallets; Elliptic traced this to a Dec. 2020 LuBian theft, and it remained dormant until it was consolidated into U.S.-custody wallets by mid-2024.	Elliptic (2025); Nocella (2025)
2020–2022	RFA: ≥7 Chinese provincial judgements against low-level employees; alleged 5 billion yuan in illicit revenue.	Davies and Zhao (2024)
May 2021–Aug. 2022	The alleged Brooklyn network laundered over US$18 million from more than 250 victims.	Nocella (2025)
Aug. 2023	OHCHR/UNODC reports have contextualised regional scam compounds, trafficking, and forced criminality.	OHCHR (2023); UNODC (2023)
2024	The Singapore Police received intelligence on Chen and associates; investigations began.	Public Affairs Department (2025)
October 14, 2025	U.S. indictment/forfeiture unsealed; OFAC designated 146 targets; FinCEN rule on Huione; U.K. sanctions announced.	FinCEN (2025); Foreign Commonwealth & Development Office et al. (2025); Office of Public Affairs (2025); U.S. Department of the Treasury (2025)
Oct. 30–31, 2025	Singapore seized/restrained over S$150 million in assets.	Public Affairs Department (2025)
Nov. 2025	Hong Kong froze HK$2.75 billion; Taiwan detained 25 and seized ~ US$150 million.	Lam and Zhuang (2025); Reuters (2025)
Jan. 6–9, 2026	Cambodia arrested/extradited Chen to China, NBC ordered Prince Bank’s liquidation (Morisonkak MKA), and the Eastern Caribbean Supreme Court appointed Interpath JPLs over 30 British Virgin Islands (BVI) entities.	Agence France-Presse (2026); Broomhead (2026); Tabahriti (2025); U.S. Department of the Treasury (2026a)
March 4, 2026	Focus Taiwan: Prosecutors indicted 62 people/13 companies over alleged NT$10.79 billion “OJBK wallet” scheme; NT$5.5 billion seized.	Lin and Lee (2026)

Date	Event	Source
April 8, 2026	Interpath JPLs, via Sullivan & Cromwell, filed a Chap. 15 petition in SDNY; the emergency motion was found to contain AI-fabricated citations, prompting a firm apology to Judge Glenn.	Basu and Church (2026); Jakubowski (2026)
Mar.–Jun. 2026	Singapore restrained over S$500 million; Prince Bank depositor compensation began; U.S. Department of the Treasury sanctioned Kok An's Crown-branded casinos; a ~ US$760 million loan book moved to Cambodia Post Bank; Amnesty reported "#8 Park" still operating.	Amnesty International (2026); Cambodia Investment Review (2026); Morisonkak MKA Audit-Accounting Co. Ltd. (2026); Public Affairs Department (2026); U.S. Department of the Treasury (2026b)
Apr. 2026	Li Xiong, an alleged Chen/Huione-associated figure, was extradited from Cambodia to China.	Davies and Young (2026); Reuters (2026b)
Jun. 11–18, 2026	Judge Glenn granted Chap. 15 recognition of the BVI liquidation as a foreign main proceeding.	Basu and Church (2026); Jakubowski (2026)
June 23, 2026	U.S. Department of the Treasury sanctioned 9 more individuals/26 entities linked to Prince Group TCO, including Hu Xiaowei.	U.S. Department of the Treasury (2026a)

Table 2
Sanctions, asset seizures, and restraints by jurisdiction

Jurisdiction	Date(s)	Action	Amounts/assets reported	Source
United States	Oct. 2025–Jun. 2026	The Department of Justice unsealed the indictment/forfeiture; OFAC designated the Prince Group TCO and 146 targets; FinCEN severed the Huione Group.	~ 127,271 Bitcoin (~ US$14–15 billion at seizure, ~US$9 billion after price declines); Huione allegedly laundered ≥ US$4 billion.	FinCEN (2025); Nocella (2025); U.S. Department of the Treasury (2025, 2026a, 2026b); Woodman (2026)
United Kingdom	Oct. 2025	The U.K. sanctioned Chen, Prince Group, Jin Bei Group, Golden Fortune Resorts World, and Byex Exchange.	Frozen: £12 million Avenue Road mansion; Fenchurch Street office (~£94–100 million); and 17 flats.	Foreign Commonwealth & Development Office et al. (2025); GOV.UK (2025)
Singapore	Oct. 2025–Jun. 2026	Police seized assets, issued prohibition orders, arrested three Singaporeans, and investigated Hu Xiaowei/Qiu Wei Ren.	S$150 million+ (Oct. 2025), rising to S$600 million+ (Jun. 2026); six properties, a yacht, and 11 cars.	Public Affairs Department (2025, 2026)
Hong Kong	Nov. 2025	The police froze the assets after a fund-flow analysis of the linked accounts.	HK$2.75 billion (~ US$352 million) in cash, stocks, and funds.	Lam and Zhuang (2025)
Taiwan	Nov. 2025–Mar. 2026	Prosecutors detained suspects over an alleged "OJBK wallet" scheme and later indicted 62 people/13 companies.	Approximately NT$4.5 billion was seized in Nov. 2025; Mar. 2026 indictment cites NT$10.79 billion laundered, with NT$5.5 billion, 24 properties, and 35 vehicles seized.	Lin and Lee (2026); Reuters (2025)
Cambodia/China	Jan.–May 2026	Cambodia arrested and extradited Chen Zhi, and later Li Xiong, to China; NBC ordered Prince Bank's liquidation; and a ~ US$760 million loan portfolio was transferred to Cambodia Post Bank.	Individual Prince Bank asset amounts are not stated in the cited sources.	Agence France-Presse (2026); Cambodia Investment Review (2026); Morisonkak MKA Audit-Accounting Co. Ltd. (2026); Tabahriti (2025)
BVI/U.S. (insolvency)	Jan. 2026–Jun. 2026	Eastern Caribbean Supreme Court-appointed Interpath JPLs. The U.S. counsel filed a Chap. 15 petition in SDNY; Judge Glenn granted recognition after an AI-fabricated-citation episode delayed proceedings.	Not applicable (insolvency, no seizure).	Basu and Church (2026); Broomhead (2026); Jakubowski (2026)

Independent blockchain analysis creates a material chronological problem for the forfeiture narrative. Elliptic traced the 127,271 Bitcoin identified in the complaint to the December 29 2020 theft of approximately 127,426 Bitcoin from LuBian, a China- and Iran-linked mining pool; the cache reportedly remained dormant until consolidation into wallets attributed to U.S. custody in June–July 2024 (Elliptic, 2025). If that attribution is correct, these coins could not have circulated through the charged 2021–2022 Brooklyn fraud period. This does not resolve control, ownership, other alleged laundering, or the legal basis for forfeiture, but it distinguishes possession from use as a layering pool. International Consortium of Investigative Journalists reports that the evidentiary gap has already affected recovery claims because investors have struggled to connect particular losses to the seized coins (Woodman, 2026). The seizure must therefore be analysed as a contested-provenance and restitution problem, not uncomplicated proof of the laundering sequence.

In parallel, the October 2025 U.K. action sanctioned Chen, Prince Group, Jin Bei Group, Golden Fortune Resorts World, and Byex Exchange and froze London property interests, including a £12 million mansion, a Fenchurch Street office valued at approximately £94–100 million, and 17 flats (Foreign Commonwealth & Development Office et al., 2025). The sanctions-list entry recorded reasonable grounds to suspect involvement in Cambodian scam centres and associated forced labour and degrading treatment (GOV.UK, 2025).

Taiwanese prosecutors reportedly detained 25 people and seized approximately NT$4.5 billion in November 2025, later indicting 62 individuals and 13 companies over an alleged NT$10.79 billion laundering scheme (Lin & Lee, 2026; Reuters, 2025). The alleged OJBK system is analytically important because it appears to have been bespoke infrastructure: reporting describes a proprietary cold-wallet arrangement developed by Taiwan-based Cheng Wei Tech, using physical-device signing outside routine exchange custody. A client reportedly uploaded a banknote serial number that an underground-remittance courier verified upon cash delivery (blockcast.it, 2026). If established, this mechanism shows vertical integration between on-chain custody and off-chain settlement rather than mere exploitation of a weak virtual asset service provider (VASP).

The enforcement track then shifted to Cambodia and China. Cambodia arrested and extradited Chen Zhi to China in January 2026 after a joint investigation and later revoked his titles and citizenship (Reuters, 2026a; U.S. Department of the Treasury, 2026a). Li Xiong, an alleged Chen- or Huione-associated figure, was extradited to China in April (Davies & Young, 2026; Reuters, 2026b). On January 8 2026, the National Bank of Cambodia ordered Prince Bank's liquidation and appointed Morisonkak MKA Audit-Accounting Co., Ltd.; its approximately US$760 million loan portfolio was transferred to Cambodia Post Bank on May 5 2026 (Agence France-Presse, 2026; Cambodia Investment Review, 2026; Morisonkak MKA Audit-Accounting Co. Ltd., 2026).

Enforcement continued to widen. Between March and June 2026, Singapore announced three arrests, a warrant for Chen Xiuling (Karen Chen), investigations involving Hu Xiaowei and Qiu Wei Ren, and restrained or seized assets exceeding S$600 million (Lim, 2026; Public Affairs Department, 2026). On June 23, the U.S. Department of the Treasury sanctioned nine additional individuals and 26 entities linked to Prince Group, including Hu Xiaowei, and alleged that Huione Group had transferred and consolidated scam-derived assets (U.S. Department of the Treasury, 2026a).

4.2 Alleged money-laundering typology

Having traced the chronology, this section examines the laundering mechanics in detail. The alleged laundering architecture was layered rather than channel-specific: at placement, scam proceeds were allegedly received as Bitcoin, USDT, USDC, and other virtual assets from fabricated investment platforms; at layering, funds moved

through laundering houses, underground money shops, shell companies, and exchange accounts, with some converted to fiat and used to repurchase cleaner cryptocurrency; and at integration, proceeds were allegedly placed into casinos, online gambling, real estate, mining companies, yachts, watches, and luxury goods (Foreign Commonwealth & Development Office et al., 2025; Nocella, 2025; U.S. Department of the Treasury, 2026a).

Within this layered architecture, cryptocurrency "spraying and funnelling" is the signature alleged virtual-asset typology: large volumes are repeatedly split across scores of wallets, then consolidated under Chen's alleged personal monitoring of fund-flow diagrams (Nocella, 2025), matching Financial Action Task Force (FATF) red-flag indicators for multiple accounts lacking logical business explanation, rapid conversion from unrelated wallets, immediate withdrawals to private wallets, weakly regulated VASPs, and links to online gambling or fraud (FATF, 2020). It also illustrates the broader operational challenge identified by the FATF in 2024: many jurisdictions remain non-compliant with Recommendation 15, Travel Rule implementation is uneven, and offshore VASPs remain difficult to supervise (FATF, 2024).

Beyond the virtual-asset layer, shell and holding companies allegedly enabled concealment, financial access, and integration. More than a hundred entities have been designated internationally, and among them were companies that did not have any real business transactions and other accounts that were opened under false pretences of trading or investment management services (Nocella, 2025; U.S. Department of the Treasury, 2025). These designations made in June 2026 were based on locations like the BVI, Hong Kong, Singapore, the U.K., Cambodia, and Thailand, which also included the firms listed in the Hong Kong Stock Exchange, Geotech Holdings, and Khoon Group (U.S. Department of the Treasury, 2026a). This is analytically important because listed securities, auditors, and other professional gatekeepers can confer market legitimacy and transactional access even where the underlying control structure is opaque. Geotech's subsequent auditor resignation illustrates a delayed de-risking response rather than proof that ordinary corporate controls identified the alleged network ex ante. The same integration logic reportedly extended to luxury-cigar interests linked through Allied Cigar and Habanos-related structures, followed by auditor and distributor-level restructuring. These episodes strengthen Scam-Compound Organisational Model's fourth pillar: corporate-institutional integration can involve not only shells but also listed issuers, professional services, branded goods, and cross-border distribution chains.

It has been claimed that the casinos and the online gambling offered cover and avenues for settling and laundering money. Government officials referred to the defunct casinos and specially constructed complexes, while the charges have it that even after the ban in 2019 in Cambodia, the online gambling activities went on through mirror sites, and the instructions issued were regarding using "clean money." UNODC also mentions the use of casinos and special economic zones for facilitating cyber fraud and coerced crime. In April 2026, the U.S. Treasury Department imposed sanctions on Senator Kok An and Crown casinos, stating that such places are used for scamming and extortion (U.S. Department of the Treasury, 2026b). His status illustrates how office-holding may raise the political and procedural cost of investigation and why elite-linked infrastructure should be analysed as shared capacity rather than a firm-specific channel.

Real estate and luxury goods were apparently used as part of the core storage of value. Property, accounts, securities, money, a yacht, cars, and watches were either seized or frozen by authorities in the U.K., Singapore, and Hong Kong; the indictment also mentions that bribes were paid using luxury goods and receipts (Foreign Commonwealth & Development Office et al., 2025; Lam & Zhuang, 2025; Nocella, 2025; Public Affairs Department, 2025). Sumi Zhi is among those named in the U.K. case, and it highlights how family members may act as storage of value during the integration phase (TRM Labs, 2025).

Huione Group reportedly operated as a central laundering hub. FinCEN attributed at least US$4 billion in proceeds from North Korean cyber heists and Southeast Asian virtual-currency investment scams to the group between August 2021 and January 2025; U.S. Department of the Treasury later alleged that Prince Group used Huione to move and consolidate scam-derived assets (FinCEN, 2025; U.S. Department of the Treasury, 2025, 2026a). The example reveals the case of disruption of infrastructural facilities and speedy replacement. In June 2026, FinCEN considered imposing sanctions on H-Pay Service PLC and other presumed successor organisations, while the Department of Justice moved to seize cloud computing infrastructure utilised by Huione Guarantee, the Telegram-based marketplace that is believed to be associated with theft of data, malware, trafficking and money laundering (FinCEN, 2026; Office of Public Affairs, 2026). Thus, technological and monetary flows can be addressed.

Figure 1 maps the alleged placement–layering–integration structure, connecting scam compounds and victims to money houses, the OJBK system, LuBian-linked wallets, shell companies, the Huione Group, casinos, property, luxury assets, bribery, and mining. It also locates the principal 2025–2026 enforcement responses. All depicted relationships are allegations and remain unadjudicated (Foreign Commonwealth & Development Office et al., 2025; Nocella, 2025; U.S. Department of the Treasury, 2025, 2026a).

Note

Schematic representation of publicly alleged relationships. All relationships depicted are allegations that remain unadjudicated; arrows indicate alleged fund flows or laundering-node involvement.

5 Discussion

5.1 From descriptive elements to a comparative organisational matrix

The case does not establish a previously unknown list of scam-compound features. Coerced labour, industrialised fraud, casinos, laundering, corruption, and elite protection are central to compound capitalism, compound crime, and scam-city scholarship (Franceschini et al., 2023; Global Initiative Against Transnational Organized Crime, 2025; Lilli & Zucca, 2025). The analytical problem is narrower: how can researchers compare organisations that display similar features but differ in the extent to which they internalise, coordinate, or outsource them?

To address that problem, this article recasts SCOM as the Scam-Compound Organisational Matrix rather than a new general theory. The matrix records five functions: labour control; fraud production; virtual-financial concealment; corporate-institutional embedding; and protection or regulatory arbitrage. Each function may be absent, externally purchased, loosely affiliated, or internally controlled. The unit of analysis is therefore the organisational configuration, not the physical compound alone.

The first function concerns labour control: recruitment, confinement, debt, discipline, movement, and compelled participation in fraud (Jesperson et al., 2023; Luong, 2025; OHCHR, 2023). The second concerns industrialised fraud production through scripts, account farms, fabricated interfaces, performance targets, and specialised roles (Cross, 2024; Oak & Shafiq, 2025). These functions distinguish, for example, a coercive production site from a voluntary online fraud group that recruits autonomous participants.

The third function concerns whether receipt, conversion, layering, and off-ramping are embedded in the organisation or obtained episodically from outside brokers. The fourth concerns sustained access to companies,

property, financial institutions, casinos, listed or private vehicles, and professional interfaces that provide infrastructure, legitimacy, or wealth storage. Inclusion in this category does not imply that every employee or gatekeeper knew of alleged offending.

The fifth function concerns continuity through political protection, jurisdictional fragmentation, weak supervision, and regulatory arbitrage. It is analytically distinct from corporate embedding because a group may possess legitimate companies without reliable protection, or protection without extensive corporate ownership. The distinction permits closer comparison across state-tolerated, militia-protected, casino-linked, special-economic-zone, and mobile operations.

Figure 2 depicts the five functions as potentially reinforcing, but the arrows are hypotheses rather than established causal effects. SCOM predicts that organisations controlling more functions will be less dependent on arm's-length facilitators and may therefore withstand the removal of a single node. It also predicts substitution: disruption of one function may shift activity to successor payment services, replacement compounds, alternate companies, or new protection arrangements rather than end the enterprise.

These expectations distinguish the matrix from a checklist. Evidence inconsistent with SCOM would include durable operations lacking labour control, corporate embedding, or protection; rapid organisational collapse after a single financial or leadership intervention despite high apparent integration; or cases in which the five functions vary independently without observable coordination. Comparative testing could score the degree of control over each function and examine whether integration predicts longevity, geographic relocation, victim volume, or enforcement displacement.

Applied to the present case, public sources allege unusually close coordination across all five functions, but the strength of evidence varies. Prosecutorial filings provide most detail on labour, fraud, and wallet management; sanctions and corporate records document official action against companies and assets; NGO and UN materials establish the regional pattern; and independent blockchain analysis contests parts of the forfeiture narrative. The matrix makes these evidentiary differences visible rather than treating each pillar as equally proven.

SCOM consequently adds no claim that its ingredients are original. Its contribution is operational and comparative: it specifies the unit of analysis, separates functions from indicators, permits degrees of organisational control, identifies rival configurations, and generates falsifiable expectations about resilience and substitution. It should be treated as a provisional heuristic to be tested across cases, not as a universal model of transnational organised crime.

This bounded formulation also clarifies the relation to transnational network theory. Network analysis identifies specialised nodes and ties; SCOM asks which critical functions are brought within a common governance architecture and which remain external. Compound capitalism and compound crime explain the political economy and convergence of harms; SCOM provides a case-coding structure for comparing how that convergence is organised.

5.2 Layered victimisation and organised financial crime

Having established SCOM as an organisational framework, this section turns to its victimisation dimension. This case supports treating pig butchering as organised financial crime rather than consumer fraud. Psychological manipulation is sustained by scripts, phone farms, fabricated interfaces, shell accounts, money houses, and exchange or off-ramp pathways (Cross, 2023, 2024; Nocella, 2025; Oak & Shafiq, 2025). The estimated annual

suspicious flows of US$27.8 billion to exchange deposit accounts during 2021–2023 indicate the scale such infrastructure may support (Griffin & Mei, 2024).

Forced labour blurs the line between perpetrator and victim because an employee at the frontline could be tricking investors while himself being trafficked, held captive, and under the threat of his supervisors. “OHCHR notes that the need to provide justice for financial victims should not preclude the exploitation of coerced workers” (OHCHR, 2023). Several empirical research studies show misleading recruitment, passport confiscation, debt, violence, arrest, deportation, social stigma, and danger of re-trafficking (Jesperson et al., 2023; Luong, 2025; Sarkar & Shukla, 2024). Rather than a simple concept of victimisation, a layered approach would be more appropriate because the investor suffers financially and psychologically, the worker is trafficked and forced into committing crimes, and the family faces expenses related to ransom, debt, and repatriation.

5.3 Regulatory arbitrage and fragmented enforcement

Turning from victimisation to enforcement, this section examines the AML/CFT response and its limitations. From an AML/CFT perspective, the alleged money laundering pattern reflects the persistent supervisory gaps noted in Section 4.2: as of 2024, three-quarters of the assessed jurisdictions remained only partially compliant or non-compliant with FATF Recommendation 15, and Travel Rule implementation remained uneven (FATF, 2024).

These discrepancies are further exacerbated by the existence of differing thresholds, conflicting timetables for implementation, and varying degrees of enforcement, creating a “sunrise issue,” where transactions and their counterparts can avoid standard due diligence (Steves, 2026).

In this context, the international response is characterised by both a great deal of scope and certain differences. Various jurisdictions have engaged in prosecuting, forfeiting, sanctioning, Section 311, restricting property, arresting, extradition, liquidation, and regulating banks, among others, in countries such as the U.S., the U.K., Singapore, Hong Kong, Taiwan, Cambodia, China, and BVI (Foreign Commonwealth & Development Office et al., 2025; Lam & Zhuang, 2025; Lin & Lee, 2026; Office of Public Affairs, 2025; Public Affairs Department, 2026; Reuters, 2026a). However, different jurisdictions focus on different priorities: prosecution, sanctions, deportation, maintenance of financial stability, recovery of creditors, or repayment, whereas employees, victims of the fraud, defendants, wallets, and evidence are scattered around various jurisdictions.

Cross-border insolvency is an additional recovery mechanism. In January 2026, the Eastern Caribbean Supreme Court appointed joint provisional liquidators for 30 BVI-incorporated Prince Group entities; a Chap. 15 petition followed in New York on April 8, and recognition was granted in June (Broomhead, 2026; Jakubowski, 2026; Winerman & Berte, 2026). A filing in that proceeding reportedly contained fabricated or incorrect AI-generated authorities (Basu & Church, 2026). Because this is a single procedural incident and not evidence about scam-compound organisation, it does not support a general policy prescription here. Its limited relevance is methodological: complex cross-border recovery depends on verifiable records and source-level checking.

The Bitcoin forfeiture illustrates both the promise and the distributive difficulty of virtual-asset recovery. Digital assets can be immobilised quickly once keys or custodial access are obtained, yet ownership, provenance, procedure, volatility, and competing claims remain substantial obstacles (Nocella, 2025; Woodman, 2026). Here, the LuBian chronology matters directly to civil-forfeiture legitimacy and restitution: if the seized cache remained dormant before the charged 2021–2022 fraud period, claimants must establish a legally sufficient nexus between particular losses, wallets, and forfeitable property rather than relying on the cache’s association with an alleged controller. Competing narratives involving mining-pool theft, scam proceeds, and other claimants create a risk that

administratively convenient aggregation will obscure offence-specific entitlements. Transparent wallet-level tracing, published claims criteria, independent review, and ring-fenced restitution procedures are therefore essential to prevent recovered value from being absorbed by state or professional costs before victims are compensated.

Unlike ex post recovery methods, sanctions have the ability to interrupt networks prior to legal proceedings by freezing assets, alerting business partners, and focusing on key figures and enablers. Their effectiveness is demonstrated through rapid implementation and continuous expansion, as seen in the actions taken by the U.S. and U.K. against secondary participants (Foreign Commonwealth & Development Office et al., 2025; U.S. Department of the Treasury, 2025, 2026a). However, sanctions cannot substitute for adjudication, compensation, survivor protection, or reform of casino licensing, VASP supervision, beneficial ownership transparency, and anti-corruption enforcement.

5.4 Durability, limitations, and future research

Notwithstanding extensive enforcement, leadership-focused action may not dismantle compound infrastructure. Reports that Meun Chey Commercial City ('#8 Park') continued alleged forced-labour scam activity after arrests and sanctions, alongside relocation claims, are consistent with displacement, although this single-case design cannot determine whether total activity increased, declined, or moved (Amnesty International, 2026; Elliptic, 2026; Reuters, 2026c). Accordingly, this article does not claim that cutting connectivity, hosting, utilities, or payment access is demonstrably effective. Those interventions require comparative evaluation against outcomes such as victim release, reported fraud volume, relocation, re-trafficking, and harm to nearby communities.

Any place-based intervention should be lawful, targeted, reversible, and preceded by a victim-safety assessment. Indiscriminate electricity or communications shutdowns could isolate confined workers, obstruct emergency contact and evidence preservation, or harm surrounding residents. A protection-first sequence would prioritise intelligence validation, safe communication channels, coordinated labour rescue, medical and immigration support, preservation of financial and digital evidence, and only then narrowly tailored action against infrastructure demonstrably controlled by operators. Financial and hosting providers can be required to preserve data and restrict identified criminal accounts without disabling essential services for an entire locality.

The case therefore supports research and governance priorities rather than causal claims about intervention effectiveness. Promising measures include better beneficial-ownership verification, risk-based supervision of VASPs and casinos, rapid cross-border preservation requests, wallet-level tracing, and non-punishment safeguards for trafficked persons compelled to offend. Whether any combination produces durable reduction rather than displacement must be tested through comparative and longitudinal designs.

However, the available body of evidence continues to be disjointed in a manner similar to those found in other academic fields. The meta-analysis of 50 studies revealed industrial socio-technical systems, precarious migration, coercion, and the grey area between victimhood and perpetrator status, along with the underrepresentation of survivors and lack of cross-jurisdictional comparability (Lazarus et al., 2026). Hence, SCOM serves as a typology to test against, but not as a universal one.

Building on these limitations, future research should link compound locations, beneficial ownership, VASP exposure, victim complaints, enforcement, and relocation across different jurisdictions. Survivor interviews should be combined with financial and legal analyses of extradition, mutual assistance, forfeiture, insolvency, non-punishment, and restitution. Comparative work should test whether SCOM's pillars are necessary features or

dimensions that vary among state-protected, militia-protected, casino-linked, special economic zone, and mobile configurations.

6 Legal Note

This article analyses public materials for academic purposes and does not determine liability. Allegations in indictments, sanctions, regulatory actions, law-enforcement statements, and media reports have not been independently verified and may be disputed or amended. All persons and entities remain presumed innocent unless liability is established by a competent tribunal.

7 Conclusion

The alleged Chen Zhi/Prince Group case provides a detailed but legally unresolved view of how scam compounds may connect forced criminality, industrialised fraud, virtual-asset laundering, corporate infrastructure, and political or regulatory protection. The article's principal contribution is empirical and methodological: a source-status-conscious reconstruction of a multi-jurisdictional case, supplemented by the Scam-Compound Organisational Matrix as a bounded comparative heuristic. SCOM does not claim originality for its five constituent features. It specifies how researchers can measure whether those functions are internalised, outsourced, or absent, and generates testable expectations about resilience and substitution. The record also demonstrates why indictment allegations must be separated from corroborated facts and why contested wallet provenance is central to restitution. Policy implications should remain proportionate to the design. Stronger beneficial-ownership, VASP, casino, and gatekeeper supervision is warranted by established AML/CFT risks, but the effectiveness of infrastructure disruption cannot be inferred from this case. Any such intervention must be targeted and protection-first, with secure communication, rescue capacity, evidence preservation, and safeguards for surrounding communities. Comparative research should now test whether functional integration predicts survival, relocation, victimisation, and recovery outcomes across different scam-compound configurations.

Declarations

Author Contribution

All authors contributed equally to this study. The authors are listed in alphabetical order.

References

1. Agence France-Presse (2026). *Cambodia dissolves accused scam tycoon Chen Zhi's Prince Bank*. South China Morning Post. https://www.scmp.com/news/asia/southeast-asia/article/3339137/cambodia-dissolves-accused-scam-tycoon-chen-zhis-prince-bank
2. Amnesty International (2026). *Cambodia: Evidence suggests scamming compounds bypassed despite high-profile 'crackdown'*. https://www.amnesty.org/en/latest/news/2026/06/cambodia-evidence-suggests-scamming-compounds-bypassed-despite-high-profile-crackdown/
3. Basu, R., & Church, S. (2026). *Top Law Firm Apologizes to Bankruptcy Judge for AI Hallucination*. Bloomberg. https://www.bloomberg.com/news/articles/2026-04-21/top-law-firm-apologizes-to-bankruptcy-judge-for-ai-hallucination

4. blockcast.it (2026). *Prince Group launders NT$10.7 billion in Taiwan: Self-developed 'OJBK wallet' linked to underground remittance*. blockcast.it. https://blockcast.it/2026/03/05/prince-group-launders-107m-in-taiwan-uses-ojbk-wallet-linked-to-underground-banking/
5. Broomhead, K. (2026). *Liquidators from Interpath appointed to companies within Prince Group*. Interpath. https://interpath.com/media-hub/articles/liquidators-from-interpath-appointed-to-companies-within-prince-group/
6. Cambodia Investment Review (2026). *Prince Bank's Estimated US$760 Million Loan Book Fully Transferred to Cambodia Post Bank Following 2025 Closure*. https://cambodiainvestmentreview.com/2026/05/14/prince-banks-estimated-us760-million-loan-book-fully-transferred-to-cambodia-post-bank-following-2025-closure/
7. Chamblis, W. J. (1989). State-Organized Crime. *Criminology*, *27*(2), 183–208. https://doi.org/10.1111/j.1745-9125.1989.tb01028.x
8. Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American sociological review*, *44*(4), 588–608. https://doi.org/10.2307/2094589
9. Cross, C. (2023). I knew it was a scam: Understanding the triggers for recognizing romance fraud. *Criminology & public policy*, *22*(4), 613–637. https://doi.org/10.1111/1745-9133.12645
10. Cross, C. (2024). Romance baiting, cryptorom and 'pig butchering': An evolutionary step in romance fraud. *Current issues in criminal justice*, *36*(3), 334–346. https://doi.org/10.1080/10345329.2023.2248670
11. Davies, J. A., & Young, M. (2026). *Cambodia Extradites Another Associate of Alleged 'Criminal' Conglomerate to China*. Organized Crime and Corruption Reporting Project. https://www.occrp.org/en/news/cambodia-extradites-another-executive-from-alleged-criminal-conglomerate-to-china
12. Davies, J. A., & Zhao, M. (2024). *Part I: Chinese courts go after 'notorious' Cambodian conglomerate*. *Radio Free Asia*. https://www.rfa.org/english/special-reports/prince-group/assets/p1-prince-group-investigation.html
13. Elliptic (2025). *$15 billion seized by US originates from Iran/China bitcoin miner theft*. Elliptic. https://www.elliptic.co/blog/15-billion-us-seizure-reveals-prince-groups-connection-to-iran-china-bitcoin-mining-theft
14. *#8 Park: Prince and Huione's role in a scam compound still operating amid crackdowns*. Elliptic, & Eliptic (2026). https://www.elliptic.co/blog/8-park-prince-and-huiones-role-in-a-scam-compound-still-operating-amid-crackdowns
15. FATF (2020). *Virtual assets red flag indicators of money laundering and terrorist financing*. FATF. https://www.fatf-gafı.org/content/dam/fatf-gafı/reports/Virtual-Assets-Red-Flag-Indicators.pdf
16. FATF (2024). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. FATF. https://www.fatf-gafı.org/content/dam/fatf-gafı/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf
17. FinCEN (2025). *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System*. Financial Crimes Enforcement Network. https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system
18. FinCEN (2026). *FinCEN Proposes to Sever H-Pay Service PLC and Other Huione Group Successor Entities from the U.S. Financial System*. *Financial Crimes Enforcement Network*. https://www.fincen.gov/news/news-releases/fincen-proposes-sever-h-pay-service-plc-and-other-huione-group-successor
19. Foreign, C., & The Rt Hon Lord Hanson of Flint. (2025). & Development Office, Home Office, The Rt Hon Yvette Cooper MP, &. *UK and US take joint action to disrupt major online fraud network*. GOV.UK.

https://www.gov.uk/government/news/uk-and-us-take-joint-action-to-disrupt-major-online-fraud-network

20. Franceschini, I., Li, L., & Bo, M. (2023). Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations. *Critical Asian studies*, *55*(4), 575–603. https://doi.org/10.1080/14672715.2023.2268104
21. Global Initiative Against Transnational Organized Crime (2025). *Compound crime: Cyber scam operations in Southeast Asia*. Global Initiative. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf
22. GOV.UK (2025). *UK Sanctions List: CHEN Zhi*. GOV.UK. https://search-uk-sanctions-list.service.gov.uk/designations/GHR0179/Individual
23. Griffin, J. M., & Mei, K. (2024). How do crypto flows finance slavery? The economics of pig butchering. *The Economics of Pig Butchering*. https://doi.org/10.2139/ssrn.4742235
24. Gujarathi, P., Verma, S., & Nair, V. V. (2026). Pig Butchering Scams as Cyber-Enabled Financial Crime: A Scoping Review of Dimensions, Modus Operandi, and Victim-Offender Dynamics. *Deviant behavior*, 1–16. https://doi.org/10.1080/01639625.2026.2677691
25. Jakubowski, S. (2026). *In re Prince Global Holdings Limited, No. 26-10769 (MG): Memorandum opinion recognizing the BVI proceedings as foreign main proceedings and granting related relief*. Bankruptcy Litigation Blog 2.0. https://www.bankruptcylitigation.blog/
26. Jesperson, S., Alffram, H., Denney, L., & Domingo, P. (2023). *Trafficking for Forced Criminality: The Rise of Exploitation in Scam Centres in Southeast Asia*. ODI Global. https://media.odi.org/documents/The_rise_of_exploitation_in_scam_centres_in_southeast_asia.pdf
27. Lam, K., & Zhuang, S. ((2025).). *Hong Kong police freeze HK$2.75 billion in assets linked to accused scammer Chen Zhi*. South China Morning Post. https://www.scmp.com/news/hong-kong/law-and-crime/article/3331498/hong-kong-police-freeze-hk275-billion-assets-linked-accused-scammer-chen-zhi?module=perpetual_scroll_0&pgtype=article
28. Lazarus, S., Chiang, M., Dimitrova, R. S., Thu, T. T., & Essien, E. (2026). What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises. *Deviant behavior*, *47*(6), 1091–1123. https://doi.org/10.1080/01639625.2025.2604138
29. Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409
30. Levi, M., & Reuter, P. (2006). Money Laundering. *Crime and justice (Chicago, Ill.)*, *34*(1), 289–375. https://doi.org/10.1086/501508
31. Lilli, S., & Zucca, M. V. (2025). Scam cities: criminal hubs in transnational cybercrime networks. *Journal of Criminal Investigation and Criminology*, *76*(4), 332–345.
32. Lim, R. (2026). *Two men linked to Cambodia-based scam syndicate Prince Group investigated for money laundering offences*. *CNA*. https://www.channelnewsasia.com/singapore/cambodia-scam-prince-holding-group-foreigners-arrested-money-laundering-6204136
33. Lin, C., & Lee, H. Y. (2026). *Taiwan indicts dozens in NT$10.7 billion money laundering case*. *Focus Taiwan*. https://focustaiwan.tw/society/202603040017
34. Lin, L. S. F. (2025). *Unravelling Prince Group's criminal networks*. *East Asia Forum*. https://eastasiaforum.org/2025/11/29/unravelling-prince-groups-criminal-networks-2/
35. Luong, H. T. (2025). Simple job, high salary: unveiling the complexity of scam-forced criminality in Southeast Asia. *Humanities and Social Sciences Communications*, *12*(1), 1305. https://doi.org/10.1057/s41599-025-

05605-1

36. Morisonkak, M. K. A., & Audit-Accounting Co. Ltd.. (2026). *Notice on compensation for depositors of Prince bank*. *Open Development Cambodia*. https://opendevelopmentcambodia.net/announcements/notice-on-compensation-for-depositors-of-prince-bank/
37. Nocella, J. (2025). *Indictment: Cr. No. 25-CR-312* U.S. Department of Justice. https://www.justice.gov/usao-edny/media/1416286/dl
38. Oak, R., & Shafiq, Z. (2025). Hello, is this Anna? Unpacking the Lifecycle of Pig-Butchering Scams. *USENIX SOUPS 2025*. https://doi.org/10.48550/arxiv.2503.20821
39. Office of Public Affairs (2025). *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes*. U.S. Department of Justice. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged
40. Office of Public Affairs (2026). *Justice Department Seizes Backend Infrastructure Used by the Huione Group for Money Laundering Services*. U.S. Department of Justice. https://www.justice.gov/opa/pr/justice-department-seizes-backend-infrastructure-used-huione-group-money-laundering-services
41. OHCHR (2023). *Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report*. United Nations. https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report
42. Public Affairs Department (2025). *Police Seize Assets And Issue Prohibition Of Disposal Orders In Money Laundering Investigation Relating To Transnational Scam Syndicate Prince Holding Group*. Singapore Police Force. https://www.police.gov.sg/media-hub/news/2025/10/20251031_police_seize_assets_and_issue_prohibition_of_disposal_orders
43. Public Affairs Department (2026). *Police Arrest Three Singaporeans In Money Laundering Investigation Relating To Transnational Scam Syndicate Prince Holding Group*. Singapore Police Force. https://www.police.gov.sg/Media-Hub/News/2026/03/20260303_police_arrest_three_singaporeans_in_money_laundering_investigation
44. Reuters (2025). *Taiwan detains 25, seizes $150 mln tied to suspected scam centre operator*. Reuters. https://www.reuters.com/world/asia-pacific/taiwan-detains-25-seizes-150-mln-tied-suspected-scam-centre-operator-2025-11-04/
45. *Cambodia extradites Chen Zhi to China amid scrutiny of 'scam centres'*. Reuters, & Reuters (2026a). https://www.reuters.com/world/china/cambodia-says-chen-zhi-among-3-extradited-china-after-transnational-crime-probe-2026-01-07/
46. *Cambodia says it extradited accused money laundering leader to China*. Reuters, & Reuters (2026b). https://www.reuters.com/sustainability/climate-energy/alleged-chen-zhi-associate-li-xiong-extradited-cambodia-china-cctv-says-2026-04-01/
47. Reuters (2026c). *Cambodia says it has closed almost 200 scam centers in fraud crackdown*. Reuters. https://www.reuters.com/world/china/cambodia-says-it-has-closed-almost-200-scam-centers-fraud-crackdown-2026-02-11/
48. Sarkar, G., & Shukla, S. K. (2024). Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime. *Journal of Human Trafficking*, 1–22. https://doi.org/10.1080/23322705.2024.2353015

49. Steves, R. (2026). *Why the FATF Travel Rule still splits VASP compliance in 2026*. The Industry Spread. https://theindustryspread.com/fatf-travel-rule-vasp-compliance-split-2026/
50. Tabahriti, S. (2025). *UK, US sanction Southeast Asian scam networks exploiting trafficked workers*. Reuters. https://www.reuters.com/world/uk/uk-us-sanction-southeast-asian-scam-networks-exploiting-trafficked-workers-2025-10-14/
51. Tower, J. G., & Amerhauser, K. (2026). *The fall of a cyber scam kingpin: Will Chen Zhi's arrest and extradition be a wake-up call for scam bosses in the Mekong?* Global Initiative. https://globalinitiative.net/analysis/will-chen-zhis-arrest-and-extradition-be-a-wake-up-call-for-scam-bosses-in-the-mekong/
52. TRM Labs ((2025).). *Historic U.S.–U.K. operation targets Southeast Asia's scam compounds with record $15 billion Bitcoin seizure*. TRM Labs Insights. https://www.trmlabs.com/resources/blog/historic-u-s--u-k-operation-targets-southeast-asias-scam-compounds-with-record-15-billion-bitcoin-seizure
53. U.S. Department of the Treasury. (2025). *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sb0278
54. U.S. Department of the Treasury. (2026a). *Treasury Further Dismantles Overseas Scam Operations Targeting Americans*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sb0538
55. U.S. Department of the Treasury. (2026b). *Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sb0469
56. UNODC. (2023). *Casinos, cyber fraud and trafficking in persons for forced criminality in Southeast Asia: Policy Brief – Summary Overview*. United Nations Office on Drugs and Crime. https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Summary_Policy_Brief.pdf
57. Williams, P. (2001). Translational Criminal Networks. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and Netwars* (pp. 61–97). RAND Corporation.
58. Winerman, J., & Berte, S. (2026). *Provisional relief — Another tool in the Chap. 15 toolbox*. Reuters. https://www.reuters.com/legal/litigation/provisional-relief-another-tool-chapter-15-toolbox--pracin-2026-06-22/.
59. Woodman, S. (2026). *Questions swirl around US plans for record $15B Prince Group crypto seizure*. International Consortium of Investigative Journalists. https://www.icij.org/investigations/coin-laundry/questions-swirl-around-us-plans-for-record-15b-prince-group-crypto-seizure/

Figures

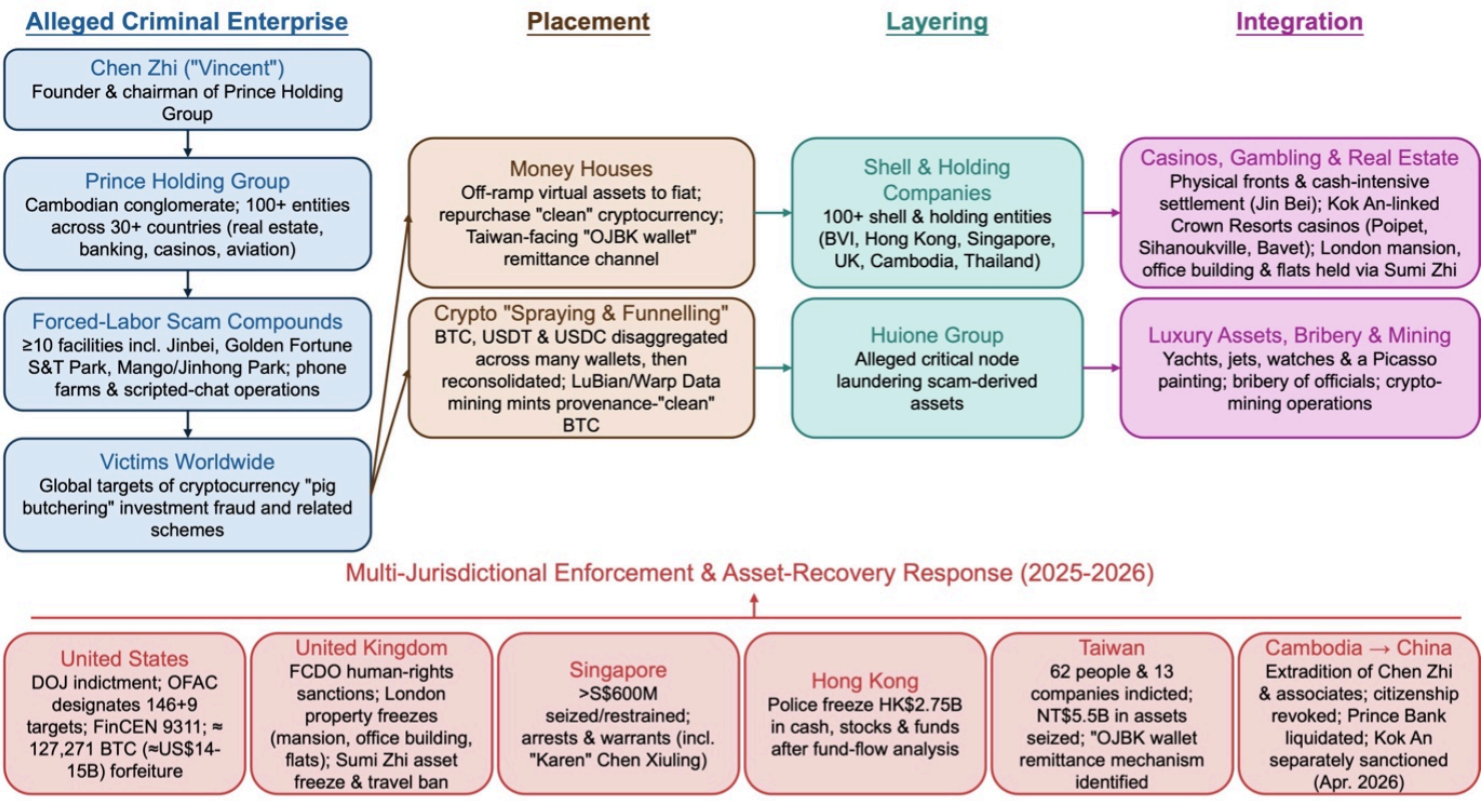


Figure 1

Schematic of Prince Group's alleged transnational laundering network structure

Note: Schematic representation of publicly alleged relationships. All relationships depicted are allegations that remain unadjudicated; arrows indicate alleged fund flows or laundering-node involvement.

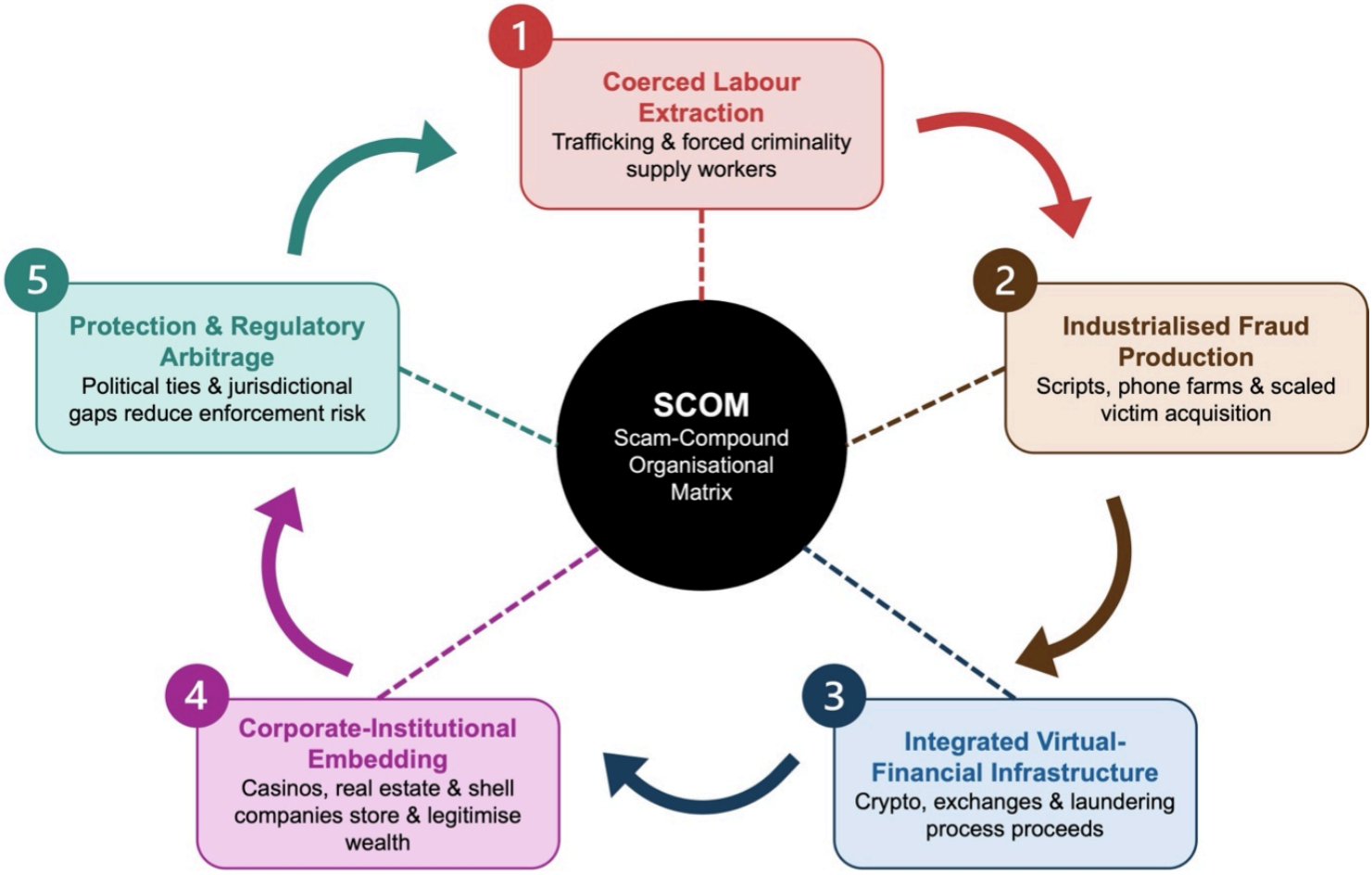


Figure 2

The Scam-Compound Organisational Matrix (SCOM)