UNODC
United Nations Office on Drugs and Crime

Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat

January 2024

Technical Policy Brief

Acknowledgements

Preparation of this report would not have been possible without data, information and intelligence shared by governments of East and Southeast Asia, international partners, and other organizations. This study was conducted by the UNODC Regional Office for Southeast Asia and the Pacific (ROSEAP) with the support of several experts in the field.

Supervision and conceptualization
Jeremy Douglas, Regional Representative, Southeast Asia and the Pacific (Conceptualization and review)

Core team
Inshik Sim, Programme Officer (Coordination, analysis and drafting)
John Wojcik, Associate Programme Officer (Analysis and drafting)
Lili Sang, Programme Officer (Drafting and review)
Seong Jae Shin, Associate Programme Officer (Drafting and review)
David Spence, Associate Programme Officer (Review)
Akara Umapornsakula (Graphic design)

This report has also benefited from the valuable input of many UNODC staff members and external experts and organisations who reviewed or contributed to various sections of the report including Peter German, Rebecca Miller, Fabrizio Fioroni, Sylwia Gawronska, Lorenzo Piacientini, Kirbee Tibayan, Woody Tan, and Vickram Ragunath.

Disclaimer

This report has not been formally edited.

The contents of this publication do not necessarily reflect the views or policies of UNODC, Member States, or contributory organizations, and neither do they imply any endorsement.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of UNODC or the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Explanatory note

Reference to dollars ($) are to United States dollars, unless otherwise stated. Reference to tons are to metric tons, unless otherwise stated. Conversions and statistics presented in this report are current as of the time of printing.

UNITED NATIONS OFFICE ON DRUGS AND CRIME

Southeast Asia and the Pacific

Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat

January 2024

Technical Policy Brief

Foreword

Transnational organized crime in Southeast Asia has evolved rapidly in recent years. This change was first and most profoundly marked by growth in cross-border trafficking of synthetic drugs and other commodities, but the landscape has changed. Major transnational organized crime groups have embraced technology and revolutionized the crime environment in the region.

This transformation follows years of progressive enforcement and regulatory efforts targeting cross-border cash movement, the casino industry, and related money laundering, and has been led in part by casino and junket operators who have effectively become bankers for organized crime. At the same time, many casinos and connected businesses like junkets have physically relocated into autonomous areas and Special Economic Zones or SEZs across the region that, in some instances, have become safe havens and breeding grounds for criminal networks.

Online casinos and cyberfraud have also recently mushroomed across Southeast Asia, particularly in the Mekong since the onset of the COVID-19 pandemic. Alarmingly, organized crime groups running many of these operations have done so with growing sophistication, through the use of data mining and processing, blockchain technology and, increasingly, generative artificial intelligence.

The acceleration of globalized crime networks centred in the Mekong aided by technology has dramatically expanded criminal revenue streams. This has necessitated a revolution in the regional underground banking architecture, resulting in the development of systems and infrastructure capable of moving and laundering massive volumes of state-backed fiat and cryptocurrencies.

While casinos and junkets have for years served as vehicles for regional underground banking and money laundering, the proliferation of online gambling platforms, e-junkets, and both illegal and underregulated cryptocurrency exchanges in Southeast Asia has changed the game, allowing for faster anonymized movement of funds. At the same time, the creation and success of these systems has helped expand the region's broader, booming illicit economy, in turn attracting new networks, innovators, and service providers to the criminal ecosystem of Southeast Asia and the Mekong.

The development of this report has required analysis of lengthy law enforcement investigations and prosecutions which have provided insights into the methods used by the underground banking industry in Asia. More specifically, it uses selected excerpts of prior UNODC analysis of criminal indictments, case records and court filings, intelligence documents, and corporate records, as well as consultation with both international and regional law enforcement and criminal intelligence partners.

Expanding on UNODC's past reporting on casinos, money laundering, and transnational organized crime in Southeast Asia, this technical policy brief have been developed in an effort to further improve understanding of the region's criminal landscape. Failure to address this landscape will have consequences for Southeast Asia and other regions as organized crime reinvest to further innovate, professionalize, and consolidate operations. Importantly, the report provides recommendations to improve knowledge, awareness, policy, capacity, and coordination, and should serve as a foundation for further work and solutions. We also trust it will prove a useful reference for deeper engagement between countries in Southeast Asia, UNODC, and international partners.

Jeremy Douglas
Regional Representative
Southeast Asia and the Pacific

Table of Contents

Abbreviations and Acronyms

AMLC	Anti-Money Laundering Council (Philippines)
AUSTRAC	Australian Transaction Reports and Analysis Centre
BGF	Border Guard Force
CEZA	Cagayan Economic Zone Authority (Philippines)
DNFBPs	Designated Non-Financial Businesses and Professions
DNS	Domain Name System
DRG	Dragon Coin
FATF	Financial Action Task Force
FCLRC	First Cagayan Leisure and Resort Corporation
FDI	Foreign Direct Investment
FLG	Fully Light Group
GCNP	General Commissariat of National Police of the Ministry of Interior (Cambodia)
GGRs	Gross Gaming Revenues
GTSEZ	Golden Triangle Special Economic Zone
ICO	Initial Coin Offering
IRCs	Integrated Resort Casinos
KNLA	Karen National Liberation Army
KNU	Karen National Union
KYC	Know Your Customer
MERs	Mutual Evaluation Reports
MIC	Myanmar Investment Commission
MNDAA	Myanmar National Democratic Alliance Army
NACD	National Authority for Combating Drugs of (Cambodia)
NCA	Nationwide Ceasefire Agreement
NFTs	Nonfungible Tokens
OFAC	Office of Foreign Assets Control
PAGCOR	Philippine Amusement and Gaming Corporation
PEZA	Philippine Economic Zone Authority
PoC	Province of China
POGO	Philippine Offshore Gaming Operator
RCBC	Rizal Commercial Banking Corporation
RMB	Renminbi
SAR	Special Administrative Region
SEC	Securities and Exchange Commission (Philippines)
SEZ	Special Economic Zone
SR	Special Region
STRs	Suspicious Transaction Reports
TOC	Transnational Organized Crime
UNODC	United Nations Office on Drugs and Crime
USDT	Tether Stable Coin
UWSA	United Wa State Army
VASPs	Virtual Asset Service Providers

List of Figures, Tables and Maps

Figures

Regional Overview

Alvin Chau Cheok-wa (周焯华) and Suncity junket

Tables

Regional Overview

Taiwan PoC, Money Laundering Networks, and Organized Crime in the Mekong

Maps

Regional Overview

Executive Summary

Executive Summary

Southeast Asia faces unprecedented challenges posed by transnational organized crime and illicit economies, and in recent years has become a testing ground for new technologies. This was first and most observed in the shift to synthetic drug production, and particularly methamphetamine, with the supply expanding to record levels year after year in the Golden Triangle and particularly Shan State, Myanmar. However, a less visible, parallel shift was taking place in the regional underground banking[1] and money laundering business.

Fundamentally, the expansion of the illicit economy has necessitated a revolution in the underground banking systems of the region. Southeast Asia's booming casino industry, followed by connected junkets,[2] then online casinos, e-junkets, and increasingly illegal and underregulated cryptocurrency exchanges have become foundational pieces of the banking architecture used by organized crime. Casinos and related businesses have proven both capable and efficient in moving and laundering massive volumes of state-backed fiat as well as cryptocurrencies undetected; creating channels for effectively integrating billions in criminal proceeds into the formal financial system.

At the same time, the development of scalable and digitized solutions has supercharged the criminal business environment across Southeast Asia, particularly in the Mekong, creating opportunities for those who have made the region their base of operations. This has in turn attracted criminal networks, innovators, and service providers to circle around, support, and benefit from the various illicit markets in the region while simultaneously driving the need for underground banking.

Concerningly, as law enforcement and regulators stepped up their efforts against casinos, illegal online gambling, and cyberfraud in Southeast Asia, organized crime have started migrating operations into inaccessible and autonomous armed group territories and other pockets of criminality in and around the Golden Triangle. Ongoing pressure is likely to motivate criminal groups to innovate and move further into the shadows.

This report has been developed through extensive examination and analysis of criminal indictments,

1 Underpinning transnational organized crime in the region are sophisticated and increasingly digitized underground banking systems. Underground banking refers to banking activities that run parallel to, and operate outside of, the formal banking system, commonly in the form of informal value transfer. These informal value transfer systems involve dealers who facilitate the transfer of value to a third party in another jurisdiction without having to physically move the items. In East and Southeast Asia, this has increasingly involved the use of unregulated or illegal casino operations. The final settlement between brokers occurs through the exchange of cash, cryptocurrency, real estate, trade, or by other means.

2 A junket is an arrangement between a hosting casino and a junket operator to facilitate gambling by an individual or group of high-wealth players for a period of time through VIP programmes or tours. Through their relationships with casinos, junket operators can offer incentives and perks to their VIP club members and other prospective VIP gamblers. Most critically, recent law enforcement action has demonstrated the scale at which some junket operators have been able to serve as international bank-like entities, providing a variety of underground financial services including credit issuance, currency exchange and multi-currency payment and settlement solutions, remittances, and extra-legal debt collection mechanisms which have been exploited by organized crime.

case records, financial intelligence, court filings, and related public disclosure, as well as consultation with both international and regional law enforcement and criminal intelligence partners over more than a year. It represents a unique attempt to understand the mechanics, intricacies, and drivers of underground banking in the region.

Evolution of cross-border gambling and displacement into Southeast Asia

In recent years, the casino industry in Southeast Asia, and in particular the Mekong, has experienced exponential growth, totaling 340+ licensed and unlicensed land-based casinos by early 2022. This follows a series of enforcement and regulatory developments in the Macau Special Administrative Region (SAR) which were driven, in part, by efforts to address on illegal capital outflows, corruption, and money laundering. Between 2019 and 2023, these measures culminated in the arrests and subsequent convictions of Macau SAR junket tycoons, Alvin Chau of Suncity and Levo Chan of Tak Chun, two of the world's largest junket operators. While they were sentenced to 18 years and 14 years in prison on hundreds of charges relating to organized crime and illegal betting, the industry is far larger than these two men and their businesses, and many operators and players have been gradually relocating to areas in and around loosely regulated Special Economic Zones (SEZs) in Southeast Asia.[3] This is demonstrated by the sizable decrease in licensed junkets in Macau SAR which dropped off from a high of 235 in 2014 to just 36 in 2023, with approximately 12 currently in operation.[4]

Prior to this decline, Macau SAR's biggest junket operators made enormous profits compared to licensed casinos. Because of the historically close links between junkets, which served as credit providers for customers seeking to evade capital controls and quotas, and organized crime, which have traditionally provided corresponding debt collection services, these profits supported a range of other criminal enterprises requiring money laundering or money transfer services, as well as seemingly legitimate investments. In the mid-2000s, forward-thinking junket operators began diversifying into online gambling, expanding the market and increasing revenues and profits.

The displacement into, and subsequent growth of, the casino industry in Southeast Asia is particularly noticeable in the Mekong region, where environmental factors that are attractive for casinos and organized crime converge. Among others, this includes the existence of autonomous Special Regions (SRs) in Myanmar, characterized by an absence of government control and rule of law, as well as many underregulated SEZs, and remote and porous borders that allow ease of cross-border movements of people and commodities, rapid digitization, and large illicit economies.

Proliferation of online casinos and infiltration of organized crime

According to latest available projections, the formal online gambling market is projected to grow to more than US $205 billion by 2030,[5] with the Asia Pacific region representing the largest share of market growth between 2022 to 2026 at a projected 37 per cent.[6] Concerningly, the rise of the 'offshore' online casino industry (including online sports betting) in several high-risk jurisdictions in Southeast Asia, and particularly the Mekong region, has been reported as a major and growing challenge faced by authorities in and beyond the region. Macau SAR junket operators and their close criminal associates have been key drivers of this trend.

Unregulated and underregulated online casino platforms run by junket operators, while profitable in and of themselves, also serve as a useful channel of credit settlement between junkets and their clients, and have been observed to be misused extensively to comingle and disguise proceeds of crime as legitimate online gambling profits. Most, if not all, of the largest junket operators have established these operations, with smaller junkets and online platforms acting as customer referral agents where further money laundering and layering can take place. At the same time, many illegal online casino in Southeast Asia have diversified their business lines into cyberfraud operations, with extensive evidence of infiltration of organized crime within casinos and SEZs for the purposes of concealing various illicit activities.

3 Centre for Gaming and Tourism Studies, Macao Polytechnic University, 2023.

4 Ibid.

5 Polaris Market Research, Online Gambling Segment Forecast, 2022 – 2030. Accessed at: https://www.polarismarketresearch.com/industry-analysis/online-gambling-market.

6 Technavio market research report on online gambling: forecast and analysis 2022 – 2026. Accessed at: https://www.prnewswire.com/news-releases/online-gambling-market-size-to-grow-by-usd-142-38-billion--37-of-the-growth-will-originate-from-apac--17-000-technavio-reports-301539695.html.

Due to limited access to SRs, SEZs, and casino and cyberfraud compounds, it is not possible to determine the full extent of these operations. However, recent cases relating to the dismantling of illegal online gambling and cyberfraud operations, rescues of victims of human trafficking, seizures of bulk cash and virtual assets, as well as arrests of known organized crime figures, demonstrate that the scale of the industry is massive.

Complicating matters further, the integration of technologies including mirror websites,[7] cryptocurrency, and third-party betting software or so-called 'white-label'[8] service providers in Southeast Asia has meant that it has never been easier to set up an online casino operation with limited technical expertise and overhead capital, irrespective of gambling laws within a given jurisdiction. The development and advancement in internet payment technologies has also assisted in supporting the online casino market with a rise in the number of third-party payment providers, e-wallets, and other payment solutions to support online transactions and in-app purchases. The massive, growing scale of the industry has also drawn in an unprecedented number of young people seeking work in the sector, with opportunities for some and risks for others linked to recruitment fraud and trafficking for forced criminality.

7 The vast majority of online gambling platforms operating in Southeast Asia exploit what are known as 'mirror websites'; exact replicas of primary betting websites housed under different URLs which are often algorithmically generated and used to evade regulatory attention, effectively staying several steps ahead of authorities by running hundreds of mirror websites on the same server to ensure services remain uninterrupted in the event that a URL is shut down.

8 White-labels have proliferated rapidly in recent years and are among the driving forces behind developments in the online gambling industry. They are similar to franchises, with betting operators being able to outsource every component of the business including sophisticated and secure betting technology, offshore licensing schemes, website design, customer data and management, branding and marketing materials, and operating license from third-party service providers. In this model, a white label may be a specific product or solution (for example a live-dealer casino platform) created with the intention of leasing or selling it to other businesses or agents, which will then re-brand it and market as their own. White-label providers may also specialize in facilitating sub-licenses to online gambling operators in certain jurisdictions in order to enable expansion of business operations. For instance, Asian-facing online gambling operators wishing to advertise on the jerseys of sports clubs in the United Kingdom require a local license to do so. This is commonly facilitated through white-label companies based in the offshore jurisdictions of the British Virgin Islands or Isle of Man, among others.

Casino and junket-based underground banking and money laundering

As demonstrated by cases analyzed for this report, casinos and junkets represent a critical piece of the underground banking and money laundering infrastructure, serving the needs of transnational organized crime groups operating in the region and globally.

Money laundering is typically understood to occur in three phases:

- Placement, when funds are integrated into the financial system or into a legal business;
- Layering, which is the process through which money is distanced from its illegal source – the idea is to make it difficult for investigators to follow the money trail; and
- Integration, when money enters the legal economy – after integration, the money appears clean and investigators can no longer tell where it originated from.

All three phases of the money laundering process are at play in land-based and online casino and junket based methods, offering a dynamic end-to-end solution that organized crime groups have perfected and continue to exploit to move massive volumes of money without exposure to the formal financial system. Money laundering and underground money transfers using casinos, junkets, and increasingly online gambling platforms, can be conducted using a variety of methods including cash-in cash-out,[9] collusion between gamblers,[10] junket financing[11]

9 Cash-in cash-out: This is the simplest, most typical method of laundering money at a casino. A criminal simply exchanges their money for playing chips and then converts them back into cash. This way, dirty money can get mistaken for money won at a casino. Some players may even divide money into several different betting accounts, which will make them appear less suspicious.

10 Collusion between players (intentional gambling losses): Under this strategy, proceeds of crime are brought into either physical or online casinos and deliberately lost – in a poker game for example – in a way that benefits an accomplice who acts as another player in the same game. An unfortunate 'advantage' of this method is that it allows launderers to dodge any AML detection policies that are only triggered by successful bets against the casino itself, not other players.

11 Junket financing: gambler/client deposits money into junket account in one country or stakes other assets, then accesses this credit at another jurisdiction to gamble – system of debits and credits used to offset wins and losses against the original amount deposited, allowing the operator to move money/value quickly and informally below the radar of tax and law enforcement agencies. Junkets may also provide a high interest rate to individuals willing to store their money with the junket to be used for offsetting.

and so-called 'offsetting' arrangements,[12] and misuse of casino 'VIP cash' accounts,[13] among others.[14] Casinos and junket operators in East and Southeast Asia and the Pacific have also been found to provide so-called 'safekeeping' transactions in which players, including those with clear links to organized crime, are permitted to deposit casino chips for safekeeping with respective casino treasury divisions and cash-out later. This system has evolved into so-called 'investment' arrangements with major junket operators in which 'investors' can earn between 5 to 7 per cent per month on the funds deposited with the junket.

Attractiveness of online gambling for underground banking and money laundering

Due to the various anonymous payment methods available, and the fact that authorities have a very limited view of what goes on in an online gambling account, it is difficult to verify the source of funds and whether an online gambling account is used for legitimate gambling or underground banking and money laundering. The online gambling sector is also characterized by a non-face-to-face element, minimal, if any, compliance staff, and huge and complex volumes of transactions and financial flows, which are often international in nature. The various jurisdictions involved and the limited extent to which the legislation between these jurisdictions is harmonized further complicate investigations while creating large enforcement gaps and grey zones that organized crime capitalized on. As designated non-financial businesses and professions[15] (DNFBPs), the sophistication of the compliance regimes instituted by online casinos lag far behind those of banks, making online casinos attractive targets for criminals while enabling what continues to be a 'heads-down' approach by operators.

Rise of 'points running' syndicates, 'motorcades', and cryptocurrency

A key characteristic of online casino operations are the ever-evolving efforts of operators to hide flows of illicit funds from authorities. Together with enforcement of capital controls in some countries in East and Southeast Asia, these efforts have been accelerated by recent COVID-19 pandemic restrictions on the cross-border movement of goods and people. These restrictions limited the ability for cash to be smuggled across borders and into casinos in the region, in turn driving up the need for organized crime to innovate the methods used to transfer funds.

Authorities in the region have reported a growing number of methods being used by organized crime to facilitate the movement of illicit funds both through and into gambling platforms. Common modalities include online casinos utilizing underground money laundering and banking

12 Offsetting arrangements (also known as mirror transactions): Similar to traditional Hawala networks; used as a means of transferring value between jurisdictions via financial credit and debit relationship between entities in different countries. Organizations facilitating offsetting arrange for money debited from an entity in one jurisdiction to be credited to (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both. Offsetting through the use of casinos and junkets as well as more traditional trade-based arrangements has been reported as a method increasingly employed by money laundering organizations based in the Asia Pacific connected to drug production and trafficking, arrangement of precursor chemical shipments, and cybercrime, among other crime types.

13 Misuse of gambling accounts for illegal transactions between players: In this case, for example, buyers and sellers of illegal items could use their respective gambling accounts as traditional bank accounts to make and receive payments. Once the seller's gambling account is credited, the money can be cashed out, claiming it was a successful gamble. It can also be used for hiding purposes on holding accounts or for wagering at casinos.

14 'Dummy' room transactions: arrangement for international VIP customers to use a credit or debit card at the resort hotel to authorize a transfer of funds to be made available to the same customers casino and/or junket. The hotel issues a room charge bill to the patron, falsely asserting that the hotel had provided services to the person. Patron will pay the bill and be given a voucher acknowledging the receipt of funds, escorted to the casino cage and able to exchange it for cash or chips as part of the transaction. 'Incidental' charges: when the patron had not stayed at the resort hotel but arrange to pay an incidental charge through their credit or debit card. The money for the incidental charge is then made available to the patron.

15 DNFBPs represent an attractive channel for money laundering and financial crime, consisting of reporting entities including casinos; real estate agents; dealers in precious metals and precious stones; lawyers; notaries; other independent legal professionals and accountants; and trust company service providers. DNFBPs are acknowledged as a global vulnerability and have historically enjoyed weaker levels of implementation and enforcement of national anti-money laundering measures. This challenge is particularly acute in Southeast Asia and especially the five lower Mekong countries of Cambodia, Lao PDR, Myanmar, Thailand, and Viet Nam.

networks including so-called 'points running'[16] or 'score running' (跑分) syndicates, money mule 'motorcade'[17] (車隊) teams, and third- and fourth-party payment providers, sometimes referred to as running points platforms and syndicates.[18] As of 2020, the Government of China estimated at least 5 million participants in this underground industry, totaling an estimated US $157 billion in capital outflows from China, and have attributed it to the rise in illegal online gambling and telecommunications fraud.[19]

As third- and fourth-party payments have become better understood by authorities and more widely reported following 'Operation Chain Break'[20] and other measures in China, organized crime groups have responded by accelerating the integration of cryptocurrencies into their illegal betting operations, creating significant challenges for investigators. In recent years, law enforcement and financial intelligence authorities have reported the growing use of sophisticated, high-speed money laundering 'motorcade' teams specializing in underground USDT – fiat currency exchanges (卡接回U) across East and Southeast Asia. This has also included the mass recruitment of mule bank accounts across virtually all jurisdictions in the Asia Pacific region which can be purchased for as little as US $30.

Due to the rise of cryptocurrency-integrated motorcades, points running syndicates, and other challenges, in 2021 the Government of China banned cryptocurrency transactions, trading, and mining. The industry subsequently migrated to various jurisdictions, particularly driving up already rising cryptocurrency adoption in several countries in Southeast Asia, together with the establishment of high-risk and underground cryptocurrency exchanges.[21] At the same time, it is worth noting that cryptocurrency flows connected to organized crime have been cited as being vastly underestimated by industry experts[22] as well as law enforcement and regulatory authorities in the region. Experts have pointed to a number of shortcomings related to existing analyses including massive gaps in crime attribution on the blockchain, fabricated reporting by crypto exchanges, and the prevalence of wash trading[23] which inflates crypto transaction volumes, thereby shrinking the portion of illicit transactions identified. This has been echoed by authorities in

16 Criminals in East and Southeast Asia often use points running syndicates, sometimes referred to as 'moving ants', to transfer stolen money between multiple bank or cryptocurrency exchange accounts, as well as online casinos, to obfuscate the source and destination of funds. This informal and often cross-border money transfer modality can involve groups of hundreds and sometimes thousands of individuals and has grown incredibly popular among youth due to underemployment in East and Southeast Asia who will provide their bank account(s) and set up front companies for use by points running syndicates for the purpose of account and company pass-through activities (collecting and transferring funds of an unknown origin) in exchange for a commission. These systems are frequently used to collect money for criminal activities such as traditional predicate offences including drug trafficking as well as cyberfraud and illegal gambling. Running points has been largely used to facilitate illegal online gambling 'and provide another layer of money laundering in which funds are routed through online gambling platforms and subsequently 'white-washed' by cashing in and cashing out through the platform to justify the source of funds as casino winnings. This strategy is commonly mixed with transaction miscoding to obfuscate use of the casino platform and depends on third- and fourth-party payment providers to help obscure the nature of transactions.

17 This term can be found on many major platforms where criminals advertise 'services' for one another, including Facebook groups and Telegram groups. Motorcades are an extension of points running syndicates who offer sophisticated layering schemes by routing money through multiple bank accounts for a percentage of the total laundered and transferred funds. Those individuals at the 'front of the car' who bear the most risk of detection have been seen advertising commission fees of between 20 to 40 per cent online. UNODC has also observed a common practice of large motorcade teams working with others when processing very large contracts in order to improve concealment and effectiveness. According to conversations with authorities in the region, smaller online casinos are used down the money laundering chain by organized crime groups and illegal betting syndicates to further 'white-wash' funds.

18 Among the most common modalities today appear to be so-called fourth-party payments and running points platforms. Fourth-party payments are an evolution of third-party payments which, until recently, exploited gaps in transaction reporting in popular third-party payment apps. While both platforms have since enhanced reporting of suspected gambling transactions at the request of Chinese authorities, fourth-party payment providers now typically install an additional intermediary between bookmaker, bettor, and third-party payment application in order to circumvent these measures and further obscure the nature of transactions.

19 Anhui Provincial People's Government, Press conference for crackdown on cross-border gambling operations, April 2021. Available at https://www.ah.gov.cn/zmhd/xwfbhx/553972891.html.

20 In response to large-scale underground banking utilizing third- and fourth-party payment platforms and the casino industry, the Chinese government initiated 'Operation Chain Break' in 2019 and has intensified its effort in subsequent years. The country's efforts to try to disrupt the flow of money from mainland China and Macau SAR to countries in Southeast Asia has included an August 2020 'blacklist' of casino destinations. For more details see below box story on the operation.

21 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.

22 Association of Certified Anti-Money Laundering Specialists, 2023. Accessed at: https://www.moneylaundering.com/news/cryptocurrency-research-firms-vastly-underestimate-illicit-payments-critics-claim/.

23 Wash trading is a form of market manipulation in which an entity simultaneously sells and buys the same financial instruments, creating a false impression of market activity without incurring market risk or changing the entity's market position.

the region who have reported major challenges in blockchain investigation capacity alongside rapidly growing use of high risk and underground cryptocurrency exchanges by organized crime.[24]

Money laundering using cryptocurrencies follows the general pattern of placement-layering-integration but with some specific features:

- Cryptocurrencies are anonymous at their point of creation therefore the placement stage of the money laundering process is often absent.
- It only takes a few seconds to create an account (address) and this is free of cost.
- It is possible to create a large money laundering scheme with thousands of transfers at a low cost and to execute it using a computer script.
- Due to rapid increases in exchange rates, with some cryptocurrencies showing very high growth, it is very easy to justify unexpected wealth through cryptocurrencies, or alternatively losses.

Online gambling platforms, and especially those that are operating illegally, have emerged as among the most popular vehicles for cryptocurrency-based money launderers, particularly for those using Tether or USDT on the TRON[25] blockchain,[26] while also fueling the intensification of Southeast Asia's rapidly growing illicit digital economy, and particularly the regional cyberfraud industry. Using this method, funds are paid into an online gambling platform or an affiliate agent who may be part of a money laundering network and arranges the transfer of in-game points online through some combination of identifiable or anonymous accounts. They are either cashed out or placed in bets, often in collusion with affiliates. Once the money in the gambling account is paid out in a desired currency and jurisdiction, it can effectively be given legal status and integrated into the formal financial system and economy.

24 Meetings with regional law enforcement and financial intelligence officials, 2023.

25 As of June 2023, TRON had over 165.5 million total user accounts, more than 5.81 billion total transactions, and over US $11.79 billion in total value locked (TVL), hosting the largest circulating supply of Tether (USDT) globally since April 2021.

26 USDT on the TRON blockchain has become a preferred choice for crypto money launderers in East and Southeast Asia due to its stability and the ease, anonymity, and low fees of its transactions. Law enforcement and financial intelligence authorities in the region have reported USDT among the most popular cryptocurrencies used by organized crime groups in the region, particularly those involved in the regional cyberfraud industry, demonstrated by a surging volume of cases and unauthorized online gambling and cryptocurrency exchange platforms offering undergroud USDT-based services.

Convergence between online gambling, cyberfraud, and human trafficking

In recent years, a growing number of organized crime groups have diversified extensively into criminal cyberfraud operations in several countries in Southeast Asia. Together with enhanced law enforcement and regulatory pressures on the regional online casino industry, criminal groups were forced to innovate, digitize, and diversify their business model following the outbreak of COVID-19 to maintain revenue streams for the region's sprawling casino industry. More specifically, casino operators have moved bases of operation deeper into loosely regulated and highly vulnerable jurisdictions including Cambodia, Lao PDR, and the Philippines, as well as several border areas controlled by armed groups in Myanmar, in turn expanding their business lines to include cyberfraud among other illicit activities.[27] Others have moved operations outside Asia including to the United Arab Emirates (UAE), Africa, Eastern Europe, and the Pacific, and have also attempted to legitimize operations by investing into licensed but underregulated offshore gambling companies and other technology-related businesses and other illicit activities.

In doing so, these groups have taken advantage of the region's casino and SEZ infrastructure alongside advances in information technology and rising youth unemployment. They have recruited hundreds of thousands of workers using the promise of lucrative employment and professionalized recruitment schemes, often using social media platforms such as Telegram, WeChat, TikTok, and Facebook. At the same time, victims of cyberfraud have been targeted using data bought and sold on various online data markets and lured to invest into professionally designed fraudulent investment platforms.

Growing indication of generative AI use, deepfake fraud, and other malicious technology

Concerningly, recent advances in large language model-based chatbots, deepfake technology, and automation, have given rise to more sophisticated and damaging cyber fraud schemes, posing a major threat to individuals and the formal banking industry. By using artificial intelligence (AI) to

27 Consultations with regional law enforcement and financial intelligence authorities.

create computer-generated images and voices that are virtually indistinguishable from real ones, scammers can execute social engineering scams with alarming success rates, exploiting people's trust and emotions. Among others, this includes sophisticated investment fraud and financial grooming including 'pig butchering'[28] and, increasingly, task scams,[29] sextortion, and schemes impersonating law enforcement officers and other government officials. Criminals also exploit stolen obtained from various sources including the dark web and so-called 'grey and black market' Telegram groups to profile and identify potential targets, and use profile photos harvested from social media platforms to create fake profiles and 'masks' that can bypass digital face verification systems and know-your-customer (KYC) measures, adding to challenges related to money-muling, money laundering, and underground banking. Additionally, it is worth noting that authorities in the region have also reported indication of cyberfraud operations based in Southeast Asia rapidly diversifying their business model by expanding into the development of malicious mobile and web applications or malware, the broader blockchain gaming industry, online bank fraud schemes, high-risk and und cryptocurrency exchange and payment services, and offering a range of cybercrimes as a service.[30]

Recommendations

The following broad recommendations are intended to help countries in the region address the findings and vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. Fundamentally, it is important that the region more effectively understand, monitor, prevent, and respond to transnational organized crime challenges related to casinos, underground banking, and technological innovation.

28 Pig butchering is a type of investment fraud in which criminals lure victims into digital relationships to build trust before convincing them to invest in cryptocurrency using fraudulent cryptocurrency platforms.

29 Task scams involve the online recruitment of victims for what appears to be a remote work scheme. Victims are ordered to carry out various online tasks including content engagement (liking social media posts, leaving automated reviews, etc.) in exchange for commission, however 'earning' more money requires layers of 'investment' into the tiered operation via cryptocurrency which is subsequently stolen.

30 Consultations with regional law enforcement and financial intelligence authorities, 2023.

Knowledge and awareness

- In-depth analysis is undertaken on online gambling platforms, junkets, cyberfraud, and the connection to money laundering, underground banking, and other forms of organized crime, as well as on the infiltration of organized crime in legitimate business sectors, in particular real estate, construction, and travel tour operators.
- Collaborative research is done with governments in Southeast Asia to understand illicit financial flows within the region, with an emphasis on gatekeepers and facilitators, offshore jurisdictions, and methods.
- Monitoring of organized crime involvement in casinos, junkets, and cyberfraud operations in border areas and SEZs is conducted.
- Forums where organized crime are discussed are used to expand awareness of, and build momentum to address, underground banking and money laundering.
- Advocacy is undertaken to expand public awareness about the connection of the casino industry to organized crime.

Legislation and policy

- National action plans and a regional strategy to deal with organized crime, underground banking, money laundering, and related criminality, in casinos, junkets, and SEZs, are developed.
- Legislation related to money laundering, asset forfeiture, casino supervision and management, and SEZs, is revised and strengthened.
- Mechanisms are established and enforced to review profiles of investors in casinos, including online platforms and junket operations, and SEZs, to determine beneficial ownership and associations with organized crime.
- Legislation related to offshore online casino operations fall in line with emerging industry best practices in moving away from the Point of Establishment ('POE') model to the Point of Consumption ('POC').

Enforcement and regulatory responses

- A regional inter-agency forum to share information and intelligence on the use of casinos for money laundering is created with

participation of regulatory bodies, financial intelligence units, and law enforcement authorities. Unlicensed and unregulated casinos, including online platforms, are identified and prevented from operating.

- Digital forensic evidence is recovered, preserved, analyzed and shared.
- A mechanism is established with social network service providers to monitor job recruitment advertisements.
- Authorities are trained on online gambling operations and money laundering methods enabled by sophisticated technologies.
- Filing of suspicious transaction reports (STRs) is mandatory for casinos and related financial service providers.
- Regulators improve capacity for land-based and online casino management and supervision, particularly in the areas of integrating suspicious transaction reporting software and surveillance technologies, and enforcing anti-money laundering measures including enhanced beneficial ownership requirements, and KYC and customer due diligence (CDD) policies and procedures, particularly in the case of junket and associated VIP rooms.
- Specialized training on money laundering investigations and asset forfeiture, is offered to police, prosecutors, and regulators.
- Funds entering land-based and online casinos over a prescribed threshold should be verified as to their origin, and sufficient information should be provided to allow for cross-checking.
- Licensing regimes for money transfer services are reviewed and strengthened, making it a criminal offence for a business to be engaged in related activity without a license, including cryptocurrency exchanges.

Report Development and Analysis

Report Development and Analysis

In 2019, UNODC published the 'Transnational Organized Crime in Southeast Asia: Evolution, Growth, and Impact' threat assessment, which described the characteristics and evolution of organized crime and the mechanics of different forms of trafficking over a five-year period. The report also highlighted several related crimes and important vulnerabilities facing the region, including drug and other forms of trafficking and related money laundering in border areas that have attracted the development of casinos and SEZs.

UNODC presented the findings of the report to policymakers, relevant law enforcement authorities, and international partner countries, as well as to academics and other experts, with the objective of advancing discussions and debate related to organized crime and supporting the region to better address related challenges. Following this, in November 2019 UNODC met with Ministers and senior officials from six Mekong countries – Cambodia, China, Lao PDR, Myanmar, Thailand, and Viet Nam – under the framework of the Mekong MOU on Drug Control, where discussions and negotiations on a new political agreement and plan to address the deteriorating drug situation took place. Using a spin-off policy brief on casinos and money laundering as a basis for discussion during the meeting, UNODC and the six governments agreed that a deeper understanding was needed of the connections between organized crime, drug trafficking, money laundering, casinos, and SEZs in the region.

Other partner countries in the region also expressed support and acknowledged that a study exploring the relationship between the casino industry, money laundering, drug trafficking, and transnational organized crime was a necessary first step to assist countries in the region to better understand the various threats posed by organized crime, and to facilitate multilateral cooperation and strategies.

In what followed, UNODC initiated the development of an internal assessment on casinos, money laundering, and transnational organized crime in Southeast Asia, and a separate internal analysis of illicit financial flows, with a mix of in house analysts and international experts. Ongoing research has involved consultation with extensive networks of regional public security, law enforcement, and criminal and financial intelligence agencies, providing an in-depth analysis of major threats, risks, and red flags associated with the rapid proliferation of casinos and associated money laundering methods utilized by organized crime in the region. Among the most striking findings, however, was the ways in which COVID-19 and various enforcement and regulatory pressures had rapidly accelerated the rate at which organized crime groups have innovated and shifted operations online. This was most clearly demonstrated by the surge in online gambling and e-junket platforms that fundamentally revolutionized underground banking, money laundering, and the broader criminal business environment in Southeast Asia.

In expanding on this work, UNODC began conducting a series of bilateral and multilateral meetings with law enforcement, criminal and financial intelligence, and casino regulatory authorities, to develop information on the evolving situation and specifically online casinos, junkets, and previously identified organized criminal actors. Due to the sensitive nature of this work, meetings were mostly conducted in private settings across the region over more than a year. UNODC also initiated a comprehensive review of criminal indictments, case records, financial intelligence, court filings, and related public disclosure. This included an analysis of investigation, indictment, and court decision documents relating to the convictions of Macau SAR junket bosses, Alvin Chau of Suncity, and Levo Chan of Tak Chun.

Extensive data and information produced by national and regional authorities as well as international organizations was also reviewed alongside a variety of corporate records related to casinos and junket operators in the region. This includes information originating within East and Southeast Asia, Australia, Canada, Europe, United Kingdom, the United States, and elsewhere. UNODC has also conducted an extensive mapping and analysis of thousands of so-called 'grey and black business' Telegram groups as well as other clear web and dark web platforms, forums, and marketplaces used for a wide range of illicit activity relating to underground banking, money laundering, cyberfraud, drug trafficking, and human trafficking and migrant smuggling.

This report presents information and data points that have never been pieced together in an effort to raise awareness of the scale of the challenge and to help countries in the region consider how to address it. Importantly, the report helps set the stage for the consideration of priorities to improve knowledge, awareness, policy, coordination, and capacity in the region, while providing an analysis of key vulnerabilities, threats, and risks associated with the rapid proliferation of casinos, cryptocurrency, and technological innovation. It also contains a series of recommendations intended to assist governments and international partners to better deal with the fast-evolving issues involving casinos and organized crime in Southeast Asia.

The findings should serve as a foundation for further information development, and drive solutions-oriented dialogue about the connection of organized crime, casinos, money laundering, and underground banking in Southeast Asia, and will be used as a basis for discussions and development of responses with authorities in the region.

Regional Overview

Regional Overview

Introduction

Southeast Asia, and particularly the Mekong region, faces unprecedented challenges posed by organized crime and illicit economies, which have grown rapidly in recent years. Transnational organized crime groups in the region are remarkably open, appearing in public and presenting themselves as legitimate business entities while making investments in sectors that can be useful for their illicit businesses. Leaders of these groups have also proven highly effective in forming alliances with influential local figures, with the intent of leveraging these relationships to advance their criminal activities.

The most significant of these challenges can be observed in the case of casinos and Special Economic Zones (SEZs)[1] which have proliferated across Southeast Asia to facilitate economic development, but have also inadvertently enabled organized crime groups to traffic illicit goods, operate illegal casinos and recently cyberfraud compounds, and facilitate industrial-scale money laundering and underground banking. These risks are of particular concern in the five lower Mekong countries which have a long and well-documented history of organized crime and illicit economies, in part due to geopolitical circumstances beyond their control, but also as a result of the social and political environment within the region. The below section examines vulnerabilities that enable organized crime in the region, and why the proliferation of largely unregulated casinos, SEZs, and increasingly high-risk and underground cryptocurrency exchanges, should be recognized as a serious, evolving security concern.

Growing power of organized crime and the scale of illicit economies in Southeast Asia

Organized crime groups operating in Southeast Asia have become increasingly sophisticated and agile in recent years, demonstrating the ability to adapt to, and use, changes in political and business environments. There was an initial disruption in the supply of illicit drugs following the onset of the COVID-19 pandemic, but the market quickly rebounded, particularly with the surging supply of synthetic drugs in the region.[2] Porous borders and the availability of a growing number of precursors and non-controlled chemicals have been major factors, and organized crime demonstrated an ability to exploit related vulnerabilities. At the same time, a parallel evolution was taking place within the regional underground banking and money laundering architecture using the casino industry and innovations in online gaming.

So-called 'high-rollers' increased activity in Southeast Asia following the tightening of controls over casino and junket businesses in Macau SAR starting in 2014, but the industry accelerated its use of technology in the wake of COVID-19. Organized crime groups have managed to integrate developments in information, financial,

1 According to the United Nations Conference on Trade and Development (UNCTAD), SEZs are defined as geographically delimited areas within which governments facilitate industrial activity through fiscal and regulatory incentives and infrastructure support.

2 UNODC, Synthetic Drugs in East and Southeast Asia: Latest Developments and Challenges 2021.

and blockchain technology, with thousands of sophisticated online casinos and so-called 'e-junkets' operating alongside high-tech white-label[3] and underground banking service providers in the region. The growing use of cryptocurrency and largely unregulated virtual asset service providers (VASPs) operating in certain parts of the region by actors within these underground systems have compounded the challenges faced by law enforcement. Complicating matters further, many of these networks have been found to be deeply connected to online cyberfraud operations and trafficking for forced criminality across the region.

Proceeds of these innovative crimes together with the continued expansion of the synthetic drug trade are generating billions of dollars in revenue for organized crime in the region. This, in turn, has necessitated a revolution in underground banking and money laundering solutions capable of moving high volumes of state-backed fiat and cryptocurrencies undetected.

Criminal and financial intelligence officials consulted for the development of this study have shared a similar assessment of the characteristics of transnational organized crime operating in the Mekong region. At the same time, the traditional hierarchical structures of Asian crime syndicates have adapted, and they now appear to be to enterprises more modern in structure. Collaboration and cooperation among a growing number of crime groups, particularly in relation to underground banking, money laundering, and online crime has become the norm. Cases examined in this report also make it clear that transnational organized crime groups in East and Southeast Asia have infiltrated licit economies and, concerningly, elements of the formal financial system, as a strategy to diversify their business portfolios, launder money, and cover their criminal activities.

Overview of casino industries and SEZs in Southeast Asia

In recent years, the casino industry in Southeast Asia, and in particular the Mekong, has experienced exponential growth. By the beginning of 2022, UNODC estimated that there were 340+ licensed and non-licensed casinos in the region, alongside 45 casinos in Macau SAR.[4] This number changed following the COVID-19 pandemic and associated mobility restrictions, having a profound impact on the casino industry as numbers increased in some jurisdictions while dropping off in others. For instance, the number of licensed casinos in Cambodia increased from 101 in 2021 to 174 in 2023 following an all-time high of 193 in 2019,[5] while the number decreased in Macau SAR to just 30 by the end of 2022.[6]

At the same time, the online casino industry expanded rapidly as a reaction to these restrictions, effectively forcing the industry to innovate and accelerate the shift online to reach its client base remotely while developing new revenue streams. According to industry experts in the Philippines, for instance, gross gaming revenue (GGR) from online operators for 2023 is projected to reach over US $438 million, up from US $109.2 million prior to the COVID-19 pandemic in 2019.[7]

A growing number of licensed and unlicensed land-based and online casinos and junket operators have also been established in the region in recent years. Growth in these industries has been driven by several factors including recent policy changes in parts of East Asia that have caused a displacement, increased controls over junkets operating in Macau SAR, a loose or altogether non-existent regulatory environment in certain parts of Southeast Asia, and new technologies that have enabled illegal online casinos to proliferate.

The displacement and subsequent growth of the casino industry in Southeast Asia is particularly noticeable in the Mekong region, where environmental factors that are attractive for casinos and organized crime converge. These factors include the existence of autonomous Special Regions (SRs) in Myanmar that are characterized by an absence of government control and rule of law, large number of SEZs, remote and porous borders that allow ease of cross-border movements of people and commodities, rapid digitization, and illicit economies of scale.

3 White-label gambling websites are similar to franchises, with betting operators being able to outsource every component of the business including sophisticated and secure betting technology, offshore licensing schemes, website design, customer data and management, branding and marketing materials, and operating license from third-party service providers.

4 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.

5 General Secretariat of the Cambodian Gambling Management Commission.

6 'Statista Market Research, 2023. Accessed at: https://www.statista.com/statistics/253763/number-of-casinos-in-macao/.

7 Asia Gaming Brief, 2023. Accessed at: https://agbrief.com/news/philippines/24/07/2023/pogo-tax-payments-rise-127-percentyearly-in-2022/.

As shown in Map 1 below, most casinos in lower Mekong countries are located in border towns neighbouring China and Thailand where most forms of gambling is illegal and patrons can easily travel to visit. At the same time, casinos located on the eastern and western Cambodian borders and on the coast in Sihanoukville were established to attract people from neighbouring Thailand, Viet Nam, and tourists from mainland China.

A unique feature of the casino industry in the region is the large number of unauthorized online operators, particularly in Cambodia, Myanmar, the Philippines and, increasingly, Lao PDR.[8] Due to limited access to SRs, SEZs, and casino compounds, it is not possible for authorities to determine the extent of these operations. However, recent cases relating to the dismantling of illegal online gambling and cyberfraud[9] operations, rescues of victims of human trafficking, seizures of bulk cash and virtual assets, as well as arrests of known organized crime figures, demonstrate that the scale of the industry is massive and associated challenges and threats are severe.

Similar to the region's casino industry, there has also been a marked increase in the number of SEZs established in the Mekong region in recent years. This expansion has been driven by governments seeking to accelerate economic growth, particularly in key border and coastal areas attractive to foreign investors. At the same time, several SEZs are located in key areas close to drug and precursor production and trafficking in the Mekong region, while high-profile criminals and organized crime syndicates are also known to be involved in SEZs as owners, developers and investors.

The desire and need for development in areas that have historically been considered remote has contributed to the increasing support of governments in Southeast Asia, and particularly the Mekong, for the establishment of development in border areas using SEZs, including casinos and so-called 'smart city' SEZs. During the March 2018 6th Greater Mekong Subregion (GMS) Summit, several Mekong countries emphasized smart cities as part of their new vision for the region's next stage of cooperation, particularly targeting the improvement of economic connectivity and competitiveness by way of cross-border SEZ developments in key economic corridors and border cities.[10] While exactly what is meant by 'smart city' remains undefined, several countries have already approved or tacitly accepted several of the region's first smart city projects to be developed despite growing risks posed by organized crime. They have also started licensing cryptocurrency mining operations, exchanges, and other VASPs which, together with the growing number that are unlicensed and operating underground, risk becoming fronts for organized crime groups involved in illegal online betting, cyberfraud, money laundering, and underground banking.

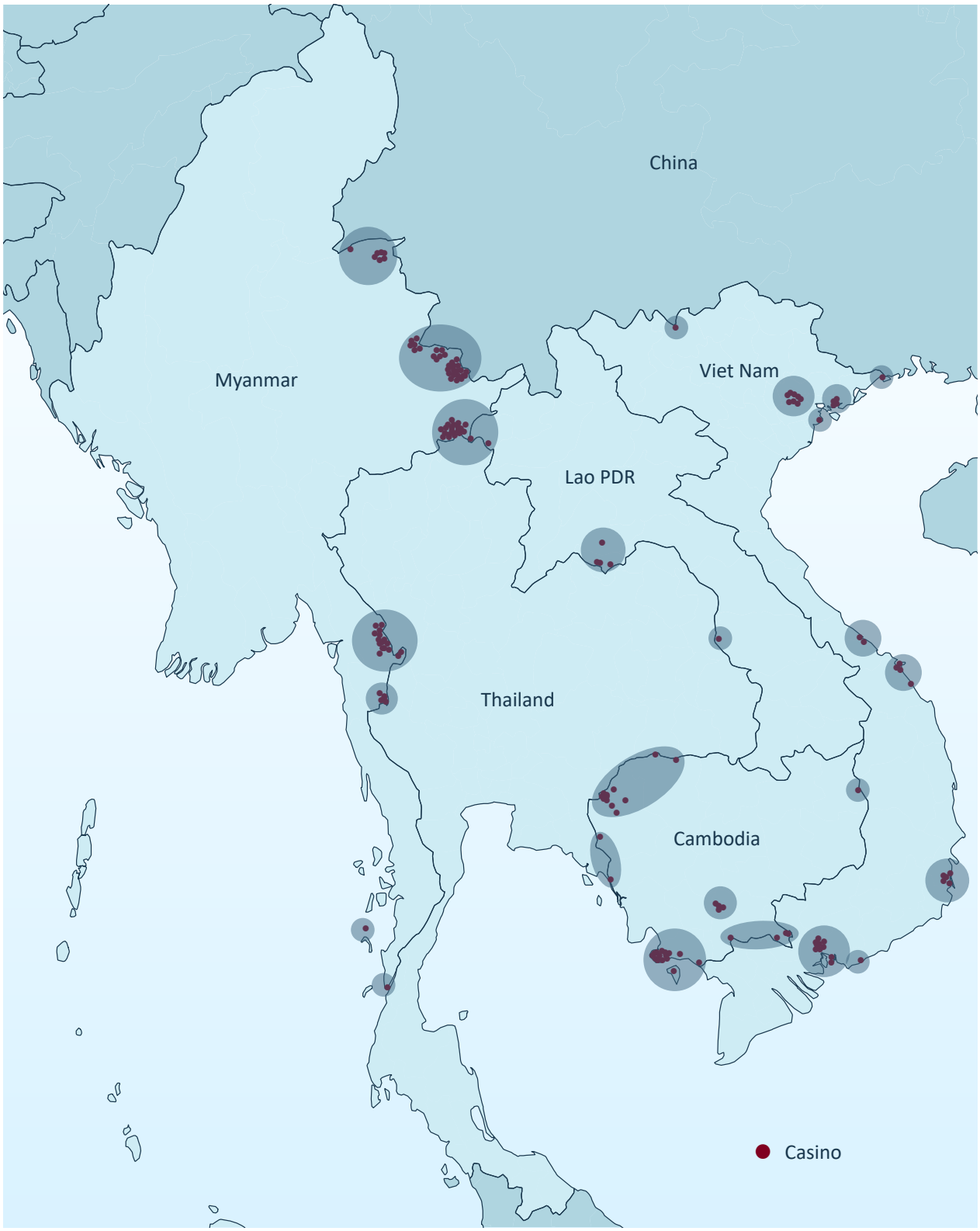
Among the best-known examples of infiltration of organized crime into 'smart city' SEZs is that in and around Myanmar's Myawaddy township in Karen State, and specifically the Shwe Kokko (also known as Yatai New City), Huanya International City, Saixigang Industrial Zone, and KK Park cyberfraud compounds. Targeting grey and illicit businesses hedging beyond Cambodia following joint Chinese and Cambodian law enforcement operations beginning in 2017, the companies involved in these developments share several characteristics including clear, documented links to criminal networks or actors engaged in casinos, junkets, cryptocurrencies, and cyberfraud. These particular smart city developments have also attracted gambling operations looking to relocate from Macau SAR, the Philippines, and elsewhere in Asia due to a range of law enforcement crackdowns targeting criminality within the casino industry, and have evolved to become a haven for organized crime and cyberfraud operations (see below section).

8 While the Philippines have developed a robust regulatory framework for online casino operators under the Philippine Offshore Gambling Operator (POGO) licensing scheme, Philippine authorities have noted severe challenges in regulatory enforcement as well as significant gaps in regulatory frameworks. For instance, several cases have emerged in recent years of licensed POGO operators acting as 'master license holders' which subsequently provide 'sub-licenses' to other operators, allowing these entities to present themselves as licensed POGOs. In fact, these entities are commonly licensed as 'POGO service providers' which have no authority to operate online casino operations. Law enforcement authorities in the Philippines have uncovered multiple entities using this scheme to have been involved in large-scale cyberfraud activities in addition to human trafficking, illegal online gambling, and money laundering.

9 As demonstrated by several cases throughout this report, online casino compounds in Southeast Asia have diversified their business lines and are regularly found to include cyberfraud operations. Licensed land-based and online casino operators in the region often serve as a legitimate business front for organized crime groups engaged in cyberfraud activities. As high cash volume business, casinos are also used to justify the source of stolen funds.

10 Asian Development Bank, Greater Mekong Subregion: Capacity Development for Economic Zones in Border Areas, 2018.

Map 1. Locations of casinos in lower Mekong countries, 2022



Note: Boundaries, names and designations used do not imply official endorsement or acceptance by the United Nations; The number of casinos for each country is an estimate based on information received from various channels, yet the actual number of casinos in operation might be different, and a few may have been closed down due to COVID-19. It is also important to note that unlicensed casinos are also included.
Source(s): UNODC elaboration based on information obtained through various channels, including its Country Offices in Southeast Asia and field researchers.

4. The proposed amount of the investment (in Kyat and US$) — US$ 22.50 million (including Kyat 5940 million)
5. A description of the plan for the implementation of the Investment including expected timetable:
   (a) Construction or Preparatory Period (Describe MM/YY) — 36 months
   (b) Commercial Operation Date (Describe MM/YY) — 2021 July
6. Number of employees to be appointed — 70 person
   (a) Local — 66 person
   (b) Foreign (Expert/Technician) — 4 person
7. Please specify the detailed list of foreign capital (Capital in-Cash and Capital in-Kinds) in K and US$:
   (a) Capital in-cash to be brought in — US$ 9.94 mn (kyat 13116.14 mn)
   (b) Capital in-kind to be brought in — US$ 8.06 mn (kyat 10643.86 mn)

Note: The investor may request the Commission to refrain from publishing commercial-in-confidential information of its investment.

KAI

Mr. Tang Kriang Kai
Managing Director
Myanmar Yatai International Holding Group Co., Ltd.

Billboard advertisement of Karen State Border Guard Force Commander Chit Thu and She Zhijiang as well as purchase agreement of Shwe Kokko, Myanmar, signed by Zhijiang under alias, Tang Kriang Kai. Source: Myanmar Investment Committee 2018.

Convergence of organized crime and armed groups in Myanmar

Located in armed group-controlled territory in Karen State, Myanmar, an area along the western border with Thailand, several so-called 'smart city' projects including the Shwe Kokko, Huanya International City, Saixigang Industrial Zone, and KK Park, have drawn international attention for their housing of industrial-scale cyberfraud operations, engaging in human trafficking, and clear links to organized crime figureheads Wan (Broken Tooth) Kuok Koi and She Zhijiang.[11] In 2018, the Myanmar Investment Commission (MIC) approved an investment proposal of US $22.5 million in cash for the Shwe Kokko project in Myawaddy Township, which planned for the construction of several dozen villas (59 villas) on about 25.5 acres of land within three years. The developer would be known as Myanmar Yatai, a joint venture between Chit Lin Myaing Company (or Chit Linn Myaing) - a construction and mining company owned and managed by Colonel Saw Chit Thu, who was sanctioned under U.K. Global Human Rights Sanctions on December 2023,[12] and the Karen Border Guard Force which owns 20 per cent, and Yatai International Holding Group, a company owned by She Zhijiang, who was also designated under the U.K. sanctions.[13]

Similarly, Wan Kuok Koi, a longtime senior 14K triad member, is also a key investor in and around Karen State. Through his Hong Kong SAR-registered Dongmei Group, Wan injected millions of dollars into the local casino industry and is believed to be a key player behind the proliferation of Myawaddy cyberfraud compounds.[14] He is also understood to be involved in several related projects in Cambodia and elsewhere in Southeast Asia and the Pacific. In December 2020, Wan was designated by the U.S. Treasury OFAC as a triad leader and his companies as engaging in various criminal activities. Myawaddy has also attracted the attention of other armed groups including the United Wa State Army (UWSA) through one of its agricultural conglomerates, which is said to have opened an office at Shwe Kokko. In addition, the Kokang BGF has heavily invested in the Karen BGF-controlled areas and significant investments in Chit Thu's enterprises, including a joint business in Myawaddy that was launched in 2018 between the business units of the two BGF militias.[15] This includes casino investments around Laukkaing in SR 1 and appears to have large-scale underground banking operations linked to cyberfraud in Myawaddy as well as Sihanoukville, Cambodia (see below case study on Kokang SR 1 of Myanmar).

11 She Zhijiang is a Chinese-born naturalized Cambodian citizen who had been wanted by Chinese authorities for illegal gambling charges since 2014. He was arrested by Thai authorities in 2022 and is known to have a robust business and investment portfolio across Southeast Asia, and particularly Cambodia, Myanmar, Thailand, and the Philippines, spanning across industries including real estate, construction, entertainment, and blockchain technology technology.

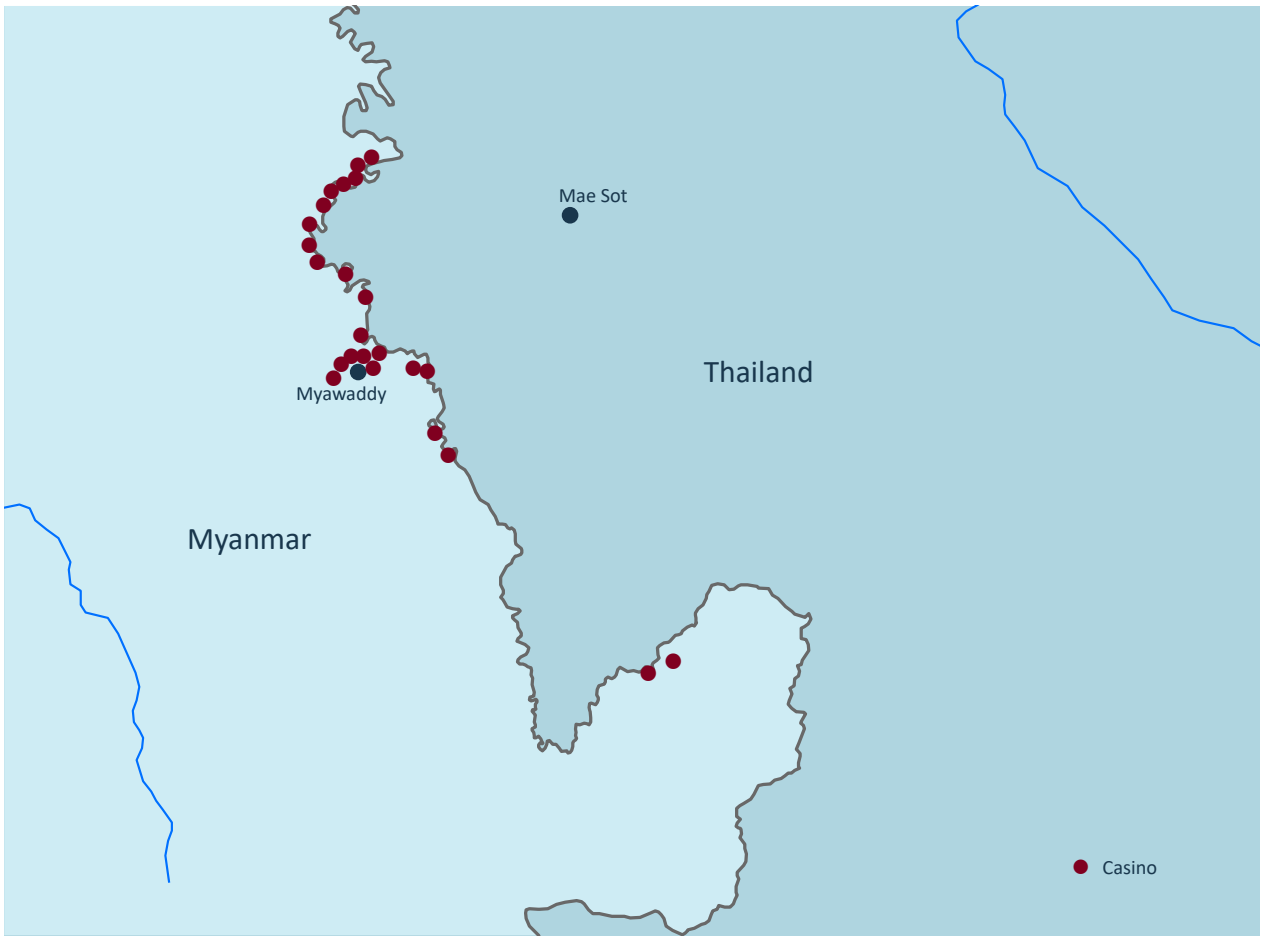
12 Office of Financial Sanctions Implementation HM Treasury, Global Human Rights Sanctions, Financial Sanctions Notice, December 2023. Accessed at: https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf

13 Consultations with regional law enforcement and financial intelligence officials, 2023.

14 Ibid.

15 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.

Map 2. Locations of land-based casinos in and around Myawaddy, Kayin State, Myanmar, 2023



Note: Boundaries, names and designations used do not imply official endorsement or acceptance by the United Nations.
Source: UNODC elaboration based on information provided by regional law enforcement and intelligence officials, 2023.

Displacement and evolution of cross-border gambling

A major driver behind the initial displacement of cross-border gambling out of Macau SAR in recent years was a stronger emphasis placed by the Government of China on enforcing currency transfer quotas and controls.[16] Prior to the various law enforcement actions that followed, it was not uncommon for individuals to transfer large amounts of currency by pooling quotas of relatives, friends, and even employees, however China now prohibits anyone from transferring money on behalf of someone else. While the new currency policies began to slow the rapid currency outflows, many innovative workarounds still exist, often involving Chinese companies doing business overseas. The methods used to evade currency controls are many and often highly sophisticated and creative, and they can be facilitated by underground banks and exchanges as well as cross-border gambling and tourism groups, junket operators and, increasingly, online casinos and e-junket operators.

For this reason, the Government of China has formally expressed the view that "cross-border gambling groups have fundamental characteristics of organized crime, featuring highly organized structures, and open crime systems with the main purpose of procuring economic interests."[17] Chinese public security officials have also noted the rising use of cryptocurrencies, the dark web, and other technologies by organized crime groups, noting that the country has experienced growing concern over rampant cross-border and online gambling in

16 Several countries in Asia restrict the amount of fiat currency which can leave their jurisdiction and enforce transfer quotas. Following an anti-corruption and money laundering campaign beginning 2014 China set a limit of approximately US $50,000 per individual which could be transferred out from the country to Hong Kong SAR, Macau SAR, Taiwan PoC, or other foreign destinations annually. While this is not new, what has changed in recent years is a greater emphasis placed by China on enforcing currency transfer controls. Moreover, prior to 2017, it was not uncommon for individuals to transfer large amounts of currency by pooling quotas of relatives, friends, and even employees. China now prohibits citizens from transferring money on behalf of other parties.

17 Official communication with the Ministry of Public Security of China, October 12, 2020.

Southeast Asia linked to criminal activities including drug trafficking, money laundering, kidnapping, and unlawful detention.[18]

One major challenge in the region relates to underground banking which has become more widespread and sophisticated, in part due to regulations and controls meant to reduce cross-border gambling. According to industry estimates, cross-border illegal gambling resulted in at least US $145 billion of illegal capital outflows from China alone through offshore gambling websites and casinos in 2020.[19] Much of these outflows are understood to be facilitated through casino junkets and sophisticated offsetting arrangements[20] as well as offshore online casino websites utilizing other underground money laundering and banking networks including so-called 'points running'[21] (跑分) syndicates, money mule 'motorcades'[22] (車隊) and third- and fourth-party payment providers[23] (see below section on the rise of 'points running' syndicates, 'motorcades', and cryptocurrency. As of 2020, the Government of China estimated at least 5 million participants in these various underground industries.[24]

In response, the Chinese government initiated 'Operation Chain Break' in 2019 and has intensified its effort to clamp down on online casinos in subsequent years. For instance, in addition to several operational achievements, the government's efforts to disrupt capital outflows from mainland China and Macau SAR to countries in Southeast Asia has notably included an August 2020 'blacklist' of overseas casino destinations. The list also applies to junket operators, private jet travel operators, and water charters,[25] and is understood to include travel to various gambling hubs in Southeast Asia.

Several high-profile arrests and subsequent convictions have taken place in recent years following the initial crackdown on illegal gambling, corruption, and money laundering in China, offering insights into related underground banking operations controlled by organized crime together with the evolution of the industry. Among the best known cases relate to purported triad members, Macau SAR junket bosses, Alvin Chau Cheok-wa (周焯華) and Levo Chan Weng Lian (陈荣炼), who ran the Suncity and Tak Chun junkets, respectively – two of the world's largest junket tour operators (full details described in below case study chapter).

In July 2020, the Wenzhou Public Security Bureau of China initiated an investigation into Alvin Chau, and several associates for establishing and managing casino related business operations in

18 Ibid.

19 Asian Racing Federation, How China's Crackdown on Illegal Betting Impacts Global Betting, September 2021.

20 As described in detail in later sections of this report, junket-based offsetting arrangements, also referred to as mirror transactions, are ultimately a means of junket financing in which the gambler deposits money into a junket account or stakes their local assets in one jurisdiction, and in turn may access this credit minus a fee at another. While this model should be limited to gambling, in practice it has become a favoured typology for underground banking and money laundering as a system of debits and credits allowing operators to move money quickly and informally below the radar of tax and law enforcement agencies. In short, offsetting is used as a means of transferring value between jurisdictions through a junket-gambler credit and debit relationship between entities in different countries. Organizations facilitating offsetting arrange for money debited from an entity in one jurisdiction to be credited to (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both.

21 Criminals in Southeast Asia often use points running syndicates to transfer stolen money between multiple bank accounts as well as online casinos to obfuscate the source and destination of funds, regularly using personal accounts to collect and transfer money on behalf of others to earn commissions. These systems are frequently used to collect money for illegal and criminal activities such as telecommunications scams, fraud and illegal gambling which can also be used to launder money by cashing in and cashing out through the platform to justify the source of funds as casino winnings.

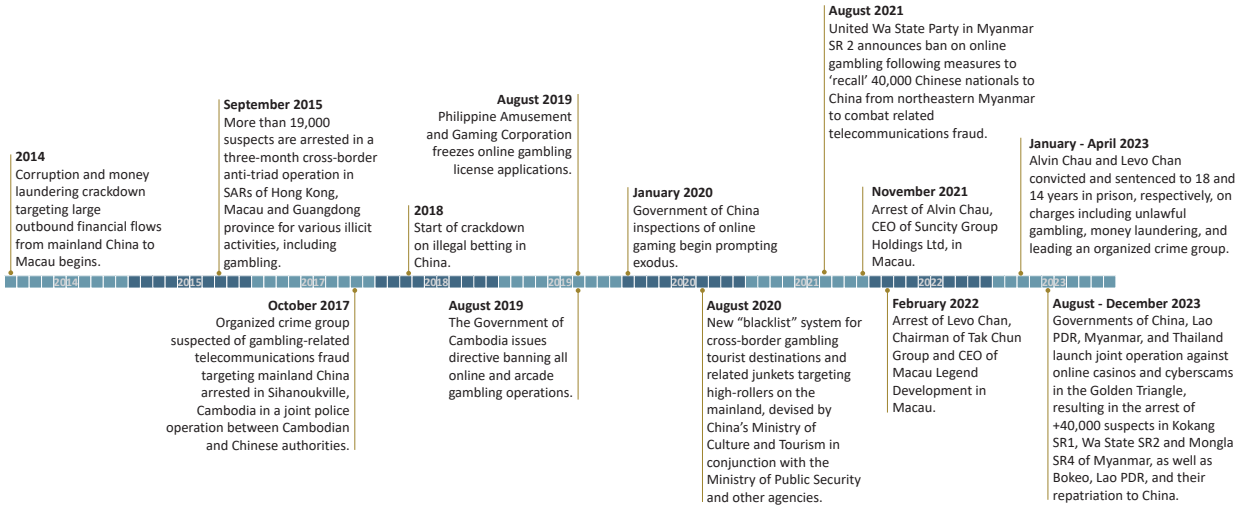
22 This keyword can be found on many major platforms where criminals advertise "services" for one another, including Facebook groups and Telegram groups. Motorcades are an extension of points running syndicates who offer sophisticated layering schemes by routing money through multiple bank accounts for a percentage of the total laundered and transferred funds. Those individuals at the 'front of the car' bear who bear the most risk of detection have been seen advertising commission fees of between 20 to 40 per cent online. UNODC has also observed a common practice of large motorcade teams working with others when processing very large contracts in order to improve concealment and effectiveness. According to conversations with authorities in the region, smaller online casinos are used down the money laundering chain by organized crime groups and illegal betting syndicates to further 'white-wash' funds.

23 Among the most common modalities today appear to be so-called fourth-party payments and running points platforms. Fourth-party payments are an evolution of third-party payments which, until recently, exploited gaps in transaction reporting in popular third-party payment apps. While both platforms have since enhanced reporting of suspected gambling transactions at the request of Chinese authorities, fourth-party payment providers now typically install an additional intermediary between bookmaker, bettor and third-party payment application in order to circumvent these measures and further obscure the nature of transactions.

24 Ministry of Public Security of China, 2020.

25 Ibid.

Figure 1. Significant developments in combating cross-border gambling and cyberfraud in Cambodia, China, Lao PDR, Myanmar, and the Philippines



Source: UNODC consolidated timeline based on documents issued by Ministry of Public Security of China, Macau Judicial Police, and related reports.

China to facilitate cross-border gambling.[26] The Wenzhou People's Procuratorate issued an arrest warrant for Alvin Chau on 26 November following a request from the Bureau,[27] and he was arrested in Macau SAR the next day together with 10 others for using the company's VIP junket business to recruit Chinese residents to engage in illegal online gambling. Police also seized numerous computers, servers, and electronic storage devices as well as more than HK $3 million (about US $385,000) in cash.[28] It was reported that illegal proceeds were laundered and transferred through the junket accounts of Macau SAR casinos using various illegal channels including underground banks.[29] With the arrest of Alvin Chau, the Suncity Group announced the termination of its junket operation in Macau SAR on 10 December 2021.

Chau was convicted in January 2023 and sentenced to 18 years in prison on over 100 charges relating to operations facilitating illegal bets exceeding US $105 billion between March 2013 and March 2021.[30] Data seized by authorities also show that between 2015 - 2019, Chau and Suncity had processed an estimated +300 billion yuan (US $42 billion) bet by online gamblers in China through the group's illegal offshore operations.[31] In a related case handled in separate proceedings in mainland China, the Wenzhou Intermediate People's Court convicted 36 individuals connected to the Chau-led syndicate, finding that the group provided cross-border currency exchange and settlement services and collected gambling debts through asset management companies and underground banks it had established on the mainland.[32] Between 2016 and 2021, the Suncity-linked consortium had expanded to more than 280 mainland Chinese shareholder-level agents, more than 38,000 gambling agents/promoters, and more than 80,000 players, totaling at least US $160 million in illegal cross-border payments and transactions facilitated through Suncity's regional network of VIP rooms and associated online gambling and phone betting platforms operating within offshore casinos in jurisdictions including Cambodia, the Philippines, and Viet Nam, among others.[33] This was further substantiated in Chau's indictment[34] and conviction decision.[35]

26 Official announcement issued by the Wenzhou People's Procuratorate, 29 November 2021. Available at: https://www.12309.gov.cn/12309/gj/zj/wzs/zdajxx/202111/t20211129_11120587.shtml).

27 Official announcement issued by the Macau SAR Judiciary Police, "Eleven persons arrested in the crackdown of a criminalsyndicate involving in illegal gambling operation and money laundering", November 2021. Available at https://www.pj.gov.mo/Web//Policia/202111/20211129/12920.html?lang=en).

28 Ibid.

29 Macau SAR Judiciary Police, Two local men arrested for criminal syndicate, illegal operation of gambling and money laundering, November 2021. Available at: https://www.pj.gov.mo/Web//Policia/202201/20220131/13182.html?lang=en.

30 Acusação do Ministério Público n.º: 1345/2022. Accessed at: https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.

31 China Central Television, Government of the People's Republic of China, January 2024.

32 Wenzhou City Public Security Bureau, 26 November 2021.

33 Ibid.

34 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.

35 Acusação do Ministério Público n.º: 1345/2022. https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.

Arrest of Alvin Chau and related associates, November 2021. Source: Chinese state-owned media.

Similarly, in January 2022, Levo Chan Weng Lian, a purported triad leader and CEO of the Tak Chun Group, the second largest junket operator in Macau SAR, was charged with operating illegal gambling businesses for the purpose of money laundering.[36] More specifically, Chan was charged for running offshore proxy and side-betting businesses across a total of 39 VIP rooms and gaming venues in East and Southeast Asia. Macau SAR authorities found that under-the-table bets totaling US $4.46 billion generated profits of HK $1.5 billion for the junket, facilitated by two local companies established by Chan named Grupo Levo Lda and Weng Chun. Chan was sentenced to 14 years in prison upon being found guilty on all counts including 24 counts of illegal gambling in a licensed area, seven counts of substantial fraud, one count of illegal gambling and aggravated money laundering. Documents found at the time of his arrest also showed Chan had recently applied to obtain residency in Taiwan PoC, with investigators also reporting he had wired a large sum of money to Taiwan PoC in the days leading up to his arrest.

Concerningly, both junket operators, among many others in the region with documented criminal association, have expanded across Southeast Asia in recent years, establishing operations in countries including Cambodia, Lao PDR, the Philippines, and Viet Nam, and potentially elsewhere in the region.

Responses by governments in East and Southeast Asia

Following the surge in criminality together with official requests from China for countries in the region to take a tougher stance against Chinese-facing operators targeting bettors on the mainland, in August 2019 the Bank of Cambodia announced the decision to ban all new online gambling operations in the country. In the same month, the Philippine regulator, PAGCOR, announced a similar decision to freeze all new licenses issued for Philippine offshore gambling operators (POGOs), resulting in tens of thousands of foreign industry workers returning home from both countries. This outflow was accelerated further by a series of return notices issued by law enforcement in China to curtail cross-border gambling in Shan State, Myanmar, particularly in Kokang SR 1, Wa SR 2, and Mongla SR 4 where many land-based and online casinos, unregulated fiat and cryptocurrency exchanges, and cyberfraud centres targeting mainland China, Southeast Asia, and other regions, are located.

According to latest available data released by the Ministry of Public Security of China, between January to November 2023, authorities in the country successfully resolved 391,000 cases related to telecommunications and network fraud, totaling the arrest of 79,000 suspects including 263 'backbone members or paymasters' of cyberfraud groups by task forces dispatched in Cambodia, Indonesia, Lao PDR, the Philippines, Thailand, and Viet Nam.[37] This also included the interception of 2.75 billion fraud calls and 2.28 billion fraud messages, the removal of 8.36 million fraud-related domain names, and 328.8 billion yuan (US $46 billion) in funds related to fraud cases.[38] In 2022, Chinese police also solved more than 37,000 cases involving cross-border gambling, with operations nationwide cracking down on 2,600 online gambling platforms, more than 1,100 casinos, as well as in excess of 2,500 illegal payment platforms and underground banks, 1,200 technical support teams, and 1,600 platforms promoting illegal gambling.[39]

In August 2023, police in China, Lao PDR, Myanmar, and Thailand jointly launched a 'special regional campaign' against organized crime groups involved in online gambling, telecommunications and

36 Macau SAR Criminal Court Case No. CR1-22-0166-PCC. Accessed at: Accessed at: https://www.court.gov.mo/sentence/zh-27669220ca401221.pdf.

37 Ministry of Public Security of the People's Republic of China, 2023.

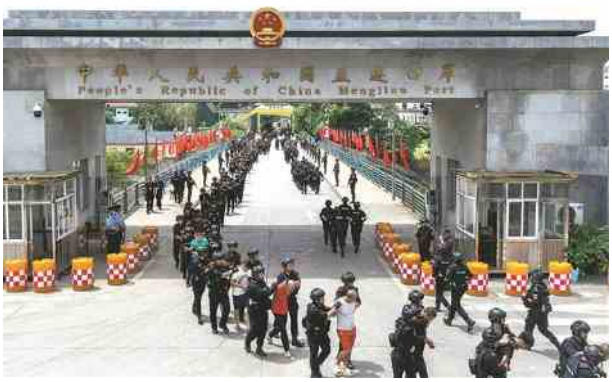
38 Ibid.

39 State Council of the People's Republic of China, 2022. Accessed at: https://english.www.gov.cn/statecouncil/ministries/202212/29/content_WS63ad52a3c6d0a757729e4e37.html#:~:text=China%20cracks%20over%2037%2C000%20cross%2Dborder%20gambling%20cases%20in%202022&text=BEIJING%2C%20Dec.,in%20a%20statement%20on%20Thursday.

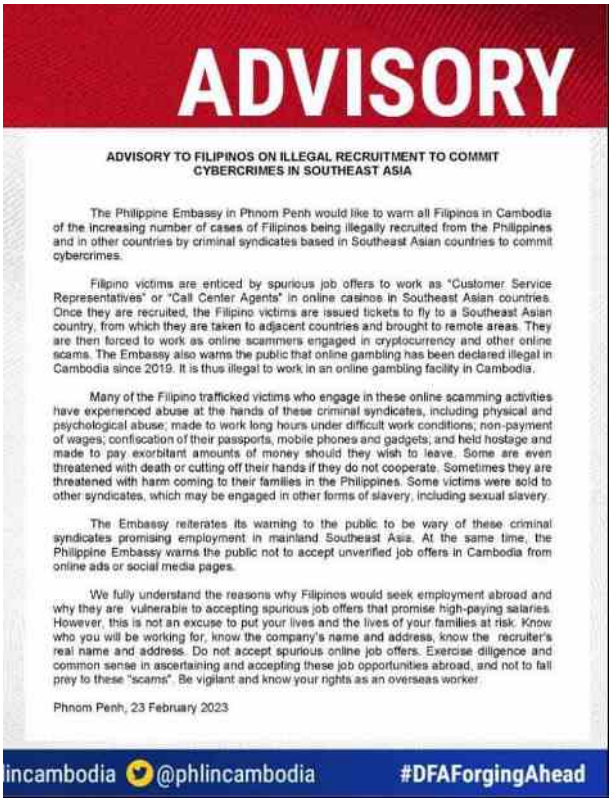
cyberfraud, and human trafficking, kidnapping, and illegal confinement.[40] Within the following month authorities reported the arrest of more than 1,350 suspected criminals in Wa State SR 2 and Mongla SR 4 of Myanmar, and Bokeo, Lao PDR.[41] By November 2023, the Ministry of Public Security of China had reported a total of 31,000 suspects transferred from Myanmar to Chinese custody following the crackdown on telecommunication fraud originating from northern Myanmar, totaling 63 alleged masterminds, organizers, or key members, as well as 1,531 fugitives.[42]

Beyond responses by governments, another key development in the SRs of Myanmar took place in October 2023 under Operation 1027 following the announcement of the Three Brotherhood Alliance between the Myanmar National Democratic Alliance Army (MNDAA), Ta'ang National Liberation Army (TNLA), and the Arakan Army (AA) armed groups. In addition to the objective of eradicating the 'oppressive military dictatorship', the offensives also ostensibly targeted online fraud in Kokang SR 1 along the China – Myanmar border.

In what followed, several cyberfraud centres in Kokang were forced to relocate operations to safer territory while the MNDAA also released many Chinese human trafficking victims back to China. In December 2023, the Criminal Investigation Bureau of the Ministry of Public Security of China issued ten arrest warrants for high-ranking members of the Kokang BGF leadership on charges relating to their roles in leading multiple violent criminal groups engaged in telecommunications and network fraud against Chinese citizens (more information available in below case study chapter on Kokang SR 1 of Myanmar).[43]



More than 1,200 cyberfraud suspects are handed over to Chinese law enforcement officials in Pu'er, Yunnan province, on Sept 6, 2023.


ADVISORY

ADVISORY TO FILIPINOS ON ILLEGAL RECRUITMENT TO COMMIT CYBERCRIMES IN SOUTHEAST ASIA

The Philippine Embassy in Phnom Penh would like to warn all Filipinos in Cambodia of the increasing number of cases of Filipinos being illegally recruited from the Philippines and in other countries by criminal syndicates based in Southeast Asian countries to commit cybercrimes.

Filipino victims are enticed by spurious job offers to work as "Customer Service Representatives" or "Call Center Agents" in online casinos in Southeast Asian countries. Once they are recruited, the Filipino victims are issued tickets to fly to a Southeast Asian country, from which they are taken to adjacent countries and brought to remote areas. They are then forced to work as online scammers engaged in cryptocurrency and other online scams. The Embassy also warns the public that online gambling has been declared illegal in Cambodia since 2019. It is thus illegal to work in an online gambling facility in Cambodia.

Many of the Filipino trafficked victims who engage in these online scamming activities have experienced abuse at the hands of these criminal syndicates, including physical and psychological abuse; made to work long hours under difficult work conditions; non-payment of wages; confiscation of their passports, mobile phones and gadgets; and held hostage and made to pay exorbitant amounts of money should they wish to leave. Some are even threatened with death or cutting off their hands if they do not cooperate. Sometimes they are threatened with harm coming to their families in the Philippines. Some victims were sold to other syndicates, which may be engaged in other forms of slavery, including sexual slavery.

The Embassy reiterates its warning to the public to be wary of these criminal syndicates promising employment in mainland Southeast Asia. At the same time, the Philippine Embassy warns the public not to accept unverified job offers in Cambodia from online ads or social media pages.

We fully understand the reasons why Filipinos would seek employment abroad and why they are vulnerable to accepting spurious job offers that promise high-paying salaries. However, this is not an excuse to put your lives and the lives of your families at risk. Know who you will be working for, know the company's name and address, know the recruiter's real name and address. Do not accept spurious online job offers. Exercise diligence and common sense in ascertaining and accepting these job opportunities abroad, and not to fall prey to these "scams". Be vigilant and know your rights as an overseas worker.

Phnom Penh, 23 February 2023

incambodia @phlincambodia #DFAForgingAhead

Warning advisory issued by the Embassy of the Philippines in Cambodia related to illegal gambling and cyberfraud recruitment, 2023.

As demonstrated by recent law enforcement action across Southeast Asia, in recent years the situation has diversified beyond illegal online gambling, with many land-based casinos and SEZs housing cyberfraud operations utilizing casino-related businesses for cover. Together with tens of thousands of rescued victims, this trend has been evidenced by countless warnings issued by embassies in the region, and particularly in the Mekong, detailing risks including kidnapping, extortion, and human trafficking by criminal groups operating within the expanding online casino and cyberfraud industry.

40 Ministry of Foreign Affairs of China, Press Release, August 2023. Accessed at: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/202308/t20230824_11132299.html.

41 Ministry of Public Security of China, 2023.

42 Ministry of Public Security of the People's Republic of China, Press Release, November 2023. Accessed at: 31,000 Telecom Scam Suspects Handed over to China by Myanmar (mps.gov.cn)

43 Official WeChat of the Criminal Investigation Bureau of the Ministry of Public Security, December 2023. Accessed at: https://mp.weixin.qq.com/s/sm3wSWuxPSFcuSg4zlEfsQ.

Great Wall Park compound where Cambodian authorities reported evidence of human trafficking, kidnapping and torture during September 2022 raids in Sihanoukville, Cambodia.

Demonstrating this concerning development further, in May 2023, Philippine police executed the first of a series of operations against licensed Philippine offshore gambling operators (POGOs) in the Clark Freeport Zone in Pampanga, rescuing 1,090 individuals including 919 foreign nationals and 171 Filipinos at the Colorful and Leap Group Company in the Clark Sun Valley Hub. The syndicate, concealing its criminal activities using its POGO license, was found to be forcing victims to carry out cyberfraud and cryptocurrency investment fraud, with authorities citing a wide-scale intelligence failure that permitted the compound to remain operational for as long as it did.

Weeks later in June, police executed another operation at the Hong Tai compound in Las Pinas, Manila, rescuing more than 2,800 reported victims of forced labour consisting of more than 1,500 Philippine nationals and 1,300 foreign nationals from 17 other countries. The raids have intensified calls by certain local officials to ban online offshore gambling operators following a senate inquiry in October 2022 to investigate the situation and allegations of widespread criminality, resulting in a new licensing scheme being imposed by PAGCOR to reduce unauthorized sub-licensing and reveal beneficial ownership of online operators (see below section on convergence of casinos, cyberfraud, and human trafficking). In 2023, the regulator placed all existing POGOs on a probationary 1-year license status to provide a grace period to operators for complying with the new licensing scheme. PAGCOR also sued 33 POGOs, including some who have left the country, for non-payment of fees amounting to US $39 million.[44]

Similarly to the experience of authorities in the Philippines, in September 2022, Cambodian law enforcement authorities executed a series of sweeping raids across multiple suspected illegal online gambling and cyberfraud compounds in Sihanoukville and Phnom Penh, confirming evidence relating to illegal gambling, money laundering, human trafficking and illegal confinement, torture, and prostitution. According to officials, victims included many skilled workers with information technology expertise, among others, who had been lured into the country through social media advertisements promising high-paying jobs at casinos and hotels who were ultimately deceived and trafficked into heavily guarded compounds for forced criminality – namely perpetrating cryptocurrency-based romance and investment scams. Thousands of victims rescued under the operation included nationals of Bangladesh, China, India, Lao PDR, Malaysia, Myanmar, Taiwan PoC, Thailand, Russia, and Viet Nam. Authorities also seized more than 8,000 mobile phones, 804 computers, and confiscated numerous passports and weapons.[45]

The sustained measures initially taken to address online gambling and cyberfraud operations in Cambodia and the Philippines, as well as countries including Malaysia, Thailand, and Viet Nam, have caused a partial subsequent displacement into countries including Lao PDR and various parts of Myanmar. This has been particularly observable through ongoing developments in Karen State and north and south Shan, especially in the SRs of Myanmar, as well as through the recent establishment of the Laos Offshore Gaming Authority (LOGA) in August 2022.

44 Philippine Amusement and Gaming Corporation, 2023. Accessed at: https://www.pagcor.ph/press-releases/pagcor-taking-legal-action-vs-33-pogos-with-unpaid-fees.php#:~:text=The%20Philippine%20Amusement%20and%20Gaming,Chairman%20and%20CEO%20Alejandro%20Tengco.

45 Cambodian National Police, 2022.

Images of Cambodia- and Myanmar-based hybrid and online casino mobile application and live-dealers, 2022.

The announcement of LOGA,[46] which was being modelled on the Philippine system currently being reformed, is particularly concerning as Lao PDR possesses very low levels of regulatory enforcement capacity with respect to addressing the risks posed within its casino sector. This is demonstrated by its issuance of zero suspicious transaction reports within the sector.[47] Yet, the country has proceeded with a pilot project as of 2022 which saw the licensing of an undisclosed number of several foreign-owned offshore online operators.[48] More than this, the country's casino sector, which has virtually no functioning regulatory system for casino supervision,[49] has shown clear connections to transnational organized crime groups, evidenced most famously by the Kings Romans Casino within the Golden Triangle SEZ (see below). The severity of associated risks of money laundering within the casino industry in Lao PDR is also reflected in the latest Mutual Evaluation Report (MER) by the Asia Pacific Group (APG) for Money Laundering which designated the sector among the highest-level money laundering risks in the country in 2023.[50] These developments demonstrate how exerting pressure in one jurisdiction in the regiona tends to displace operations to another.

At the same time, the Government of Lao PDR has stated its intent to attract as many as 750 new companies into its SEZs and smart city projects, particularly within new developments of Siphandone SEZ and the revitalized Boten SEZ which is already largely developed.[51] Between 2016-2020, 743 companies invested over US $12 billion in registered capital into SEZs and included foreign investors from 18 jurisdictions.[52, 53] A further US $2.5 billion was invested in 2021.[54]

Concerns over control of SEZs in Lao PDR are pronounced. As mentioned, one of the largest and most visible SEZ and casino complexes in the Mekong region is the Kings Romans casino complex, which is strategically located inside the Golden Triangle SEZ on the east bank of the Mekong River, in Bokeo, Lao PDR. Located adjacent to the porous border with Myanmar and Thailand, Kings Romans also has various connections to the drug trade in Shan State and other parts of Asia,

46 LOGA is a private company working in cooperation with the Ministry of Public Security of Lao PDR presently tasked with regulating the emerging online casino industry in the country and providing a range of traditional security and cybersecurity services.

47 Asia Pacific Group on Money Laundering. Lao PDR Mutual Evaluation Report, 2023. Accessed at: https://apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162.

48 Meetings with national casino regulators and financial intelligence officials, 2023.

49 Ibid.

50 Asia Pacific Group on Money Laundering. Lao PDR Mutual Evaluation Report, 2023. Accessed at: https://apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162.

51 Conversations with national law enforcement officials, 2023. Sources also indicated that the newly developed high-speed railway station is based within the Boten SEZ together with the customs check point, posing a significant possible trade security risk should the zone ultimately be operated by the Zhao Wei transnational organized crime network.

52 Asia Pacific Group on Money Laundering. Lao PDR Mutual Evaluation Report, 2023. Accessed at: https://apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162.

53 Investment Promotion Department, All Approved Investment Projects by Country (1 January 2016 to 31 December 2020), 12 September 2022. From: https://investlaos.gov.la/resources/statistics/.

54 Ibid.

and has been identified as a key drug trafficking and money laundering hub connected to other criminally implicated casinos and junkets in the region.[55] Regional law enforcement and financial intelligence officials have also confirmed the use of affiliate gold traders and money exchange networks across the Thailand and Myanmar border area.[56]

Zhao Wei (赵伟) is the owner of the Dok Ngiew Kham Group and co-owner of Hong Kong SAR-listed Kings Romans International (HK) which operates the casino. He was a timber trader before entering the casino business in Macau SAR, and later opened one of the biggest casinos in Mongla SR 4 before investing in the Golden Triangle SEZ.

Zhao Wei's network of criminal connections in Asia has been solidified through his close association as a purported member of the 14K triad. In January 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Kings Romans and Zhao Wei, declaring his network a 'transnational criminal organization' and imposing sanctions on him and three associates as well as three of his companies based in Lao PDR, Thailand, and Hong Kong SAR. In addition to drug trafficking, the U.S. Treasury also alleges that Zhao's network engages in human trafficking, wildlife trafficking, money laundering, and bribery, much of which is facilitated through Kings Romans.[57] In 2015, following an extensive on-site investigation, the Environmental Investigation Agency reported that several Lao SEZs, and particularly Kings Romans, are a growing hub for illegal wildlife trade including tiger skins and body parts, rhino horns and ivory.[58]

Despite the sanctions, the importance of Kings Romans as a storage, trafficking, deal-making, and laundering hub is likely to expand now that Zhao Wei has made his Osiano Trading Sole Co. the major investor in a nearby port development project, buying out the shares of other investors in October 2020. Osiano is an affiliate of the Dok Ngiew Kham Group and is reported to have invested some US $50 million to purchase the port, which once developed will handle cargo into the SEZ, and include a hotel and office complexes. The group is also understood to be in control of a new airport located approximately five kilometers to the east of the Golden Triangle SEZ, which is a joint venture between the Dok Ngiew Kham Group and the Government of Lao PDR. Kings Romans and the area around it are a key transit hub for drugs smuggled across the Mekong River into Lao PDR from Shan State. There is also transportation of drugs and other contraband between the ports of Sop Lwe, Ban Mom, and other ports.

More recently, in December 2023, authorities in China and Lao PDR executed a joint operation targeting confirmed cyberfraud operations, raiding seven business offices and arresting 462 suspects in the Golden Triangle SEZ.[59] In January 2024, the Government of the Republic of Korea announced a Level 4 travel alert for the Golden Triangle region of Lao PDR, citing a rise in criminality targeting its nationals and prohibiting travel into the area.[60]

Images released following the joint operation within the Golden Triangle SEZ. Source: Ministry of Public Security of Lao PDR, December 2023.

Designated non-financial businesses and professions and the evolution of money laundering

DNFBPs represent a highly attractive channel for money laundering and financial crime, consisting of reporting entities including casinos; real estate agents; dealers in precious metals and precious stones; lawyers; notaries; other independent legal professionals and accountants; and trust company service providers (TCSPs).

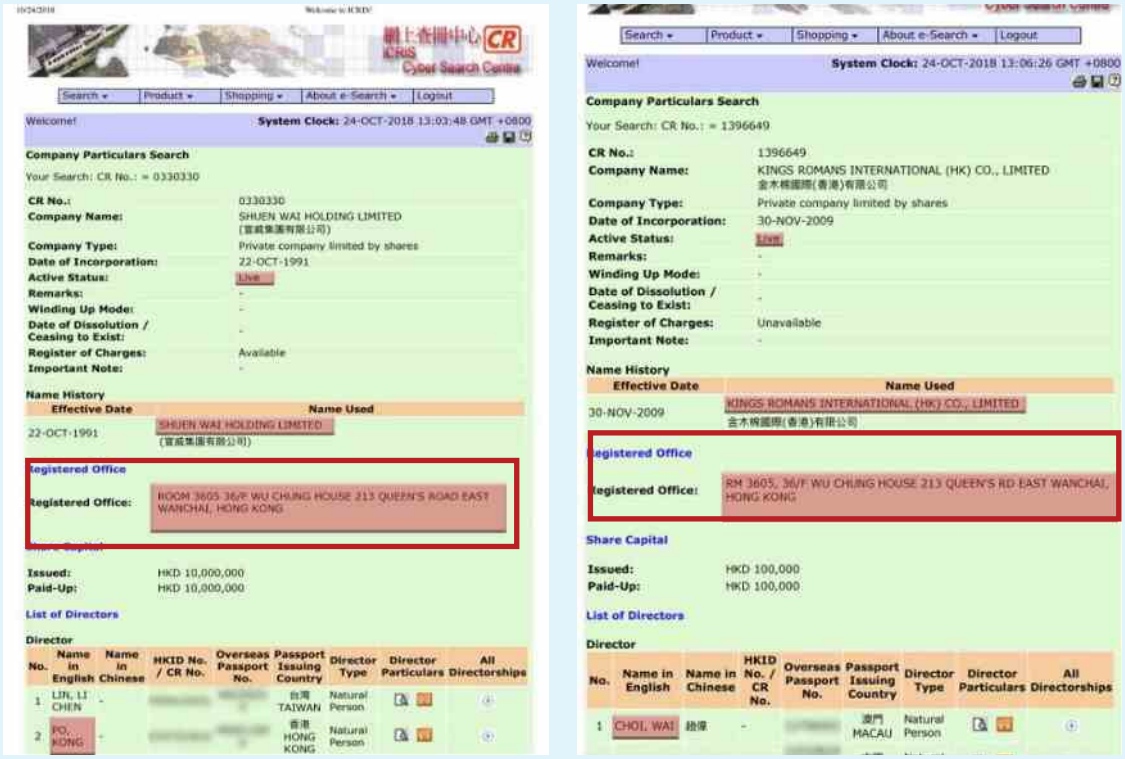
While DNFBPs are acknowledged as a global vulnerability and have historically enjoyed weaker levels of implementation and enforcement of national anti-money laundering measures, this

55 Meetings with regional law enforcement and financial intelligence officials in East and Southeast Asia, 2023.
56 Ibid.
57 U.S. Department of the Treasury, Treasury Sanctions the Zhao Wei Transnational Criminal Organization, Press Releases, 30 January 2018. Available at: https://home.treasury.gov/news/press-releases/sm0272.
58 UNODC threat analysis on casinos, money laundering and transnational organized crime in Southeast Asia, 2022.
59 Minister of Public Security of Lao PDR, December 2023.
60 Ministry of Foreign Affairs of the Republic of Korea, 2024.

Strong ties between armed groups in Myanmar and the Zhao Wei criminal syndicate

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has designated several individuals and entities in the Mekong region in connection to drug trafficking and money laundering. Most notably, sanctions were announced against the UWSA in 2008 and the Zhao Wei criminal network in 2018.

Recognizing the UWSA as the largest and most powerful drug trafficking organization in Southeast Asia, the 2008 OFAC measures listed 26 individuals and 17 companies tied to the UWSA and sanctioned them as Specially Designated Narcotics Traffickers pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act). The 17 companies were located across several countries in Southeast Asia, including Myanmar, Thailand, and Singapore, as well as China and Hong Kong SAR. One of these entities was Shuen Wai Holding, registered in Hong Kong SAR. The exact same address was used for registration of Kings Romans International in 2009 by alleged 14K triad leader, Zhao Wei, who was sanctioned by OFAC in 2018 and is known to possess business interests in the Special Regions of Myanmar. The fact that the two companies were registered at the exact same address is more than a coincidence, and demonstrates the convergence of armed groups and organized crime in the Mekong region.



Hong Kong Registration records for Shuen Wai Holdings Ltd. (left) and Kings Romans International Co. Ltd. (right)

challenge is particularly acute in Southeast Asia and especially in several lower Mekong countries.[61] Consultations with various governments in the region indicate that their present understanding is largely limited to obligations addressing money laundering through traditional mechanisms, with very little effort given to DNFBPs despite the same anti-money laundering measures applying to related reporting entities.[62] This has driven significant weaknesses in the implementation of risk-based anti-money laundering measures for DNFBPs in Southeast Asia, including most importantly casinos, real estate agents, and dealers in precious metals and stones (DPMS).[63]

61 See respective Financial Action Task Force Mutual Evaluation Reports.

62 Reporting entities may differ within each country and may exclude some DNFBPs. For instance, casinos were not designated as 'covered persons/entities' under the anti-money laundering framework in the Philippines until 2017 following a senate inquiry into casinos in 2016 (Blue Ribbon Committee).

63 See respective Financial Action Task Force Mutual Evaluation Reports.

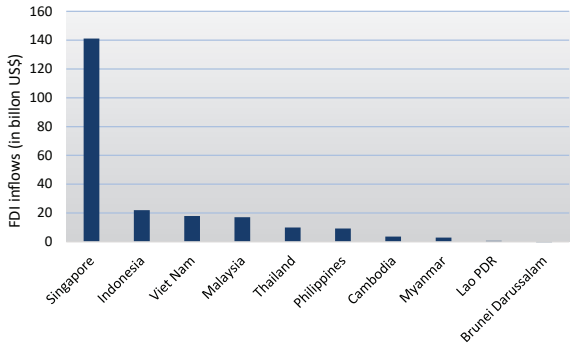
This is particularly concerning in the case of casinos which have been found to be functioning as banks for organized criminal groups operating in the region and globally. As documented across a growing number of cases in multiple jurisdictions, casinos in Southeast Asia have demonstrated extreme and accelerating levels of infiltration of organized crime in the five lower Mekong countries and the Philippines, with most countries not possessing a functioning, enforceable casino regulatory management and supervision system.[64] Severe gaps have also been observed in transaction monitoring and reporting software integration and utilization by casino operators in countries including Cambodia, Lao PDR, and Myanmar. At the same time, most countries in the region pay virtually no attention to casino junket operators and other VIP tour companies, which is problematic given that a growing number of authorities in East and Southeast Asia have reported widespread misuse of these businesses for large-scale money laundering and underground banking by transnational organized crime groups.[65]

One reason behind the apparent lack of prioritization of DNFBPs by countries in the Mekong region relates to large disparities in foreign direct investment (FDI) and economic development. This, alongside the rapid growth of the casino industry, has largely been the result of policies designed to boost tourism and attract both foreign and local investment for economic development. Despite decades of foreign investment and rapid and sustained growth, Southeast Asia continues to be constrained by economic disparities within the region, which includes Singapore, a city-state with one of the highest GDPs in the world, and three so-called least developed countries, for which foreign aid is sometimes known to exceed foreign investment. The imbalance can be observed in the inward flows of FDI among countries in Southeast Asia.

The stark difference in the amounts of FDI inflows among countries is due to a variety of factors, and discussing the causes is not a focus of this report. However, those countries with smaller FDI inflow have been actively seeking opportunities to attract FDI, including granting licenses to investors for casinos. Countries with less strict standards for vetting FDI are also vulnerable to exploitation by organized crime seeking to mask illicit proceeds as genuine investments.

64 Meetings with regional casino regulatory authorities, 2023.
65 Meetings with regional financial intelligence officials, 2023.

Figure 2. Total FDI Inflows into Southeast Asia by country, 2023



Source: Statista, 2023.

The situation is understood to have been exacerbated by the economic challenges associated with the COVID-19 pandemic which have driven countries in the region with high money laundering risk deeper into the development of grossly underregulated SEZs and both land-based and online casino operations. This particularly includes the SRs of northeastern Myanmar which are heavily rooted in illicit economies and experiencing an intensification of technologically advanced casino developments and cyberfraud compounds and are virtually exempted from any law enforcement and regulatory frameworks altogether (see below case study chapter on Kokang SR 1 of Myanmar). In turn, it is highly likely that DNFBPs in high-risk jurisdictions of the Mekong will increasingly serve as a dangerous loophole and point of least resistance in national AML systems, with recent cases showing clear connectivity between major transnational organized crime groups and casino and junket-based underground banking networks in the region.

Casino- and junket-based money laundering

The establishment of casinos and junkets has surged across East and Southeast Asia and the Pacific over the past decade, representing a critical piece of the underground banking and money laundering infrastructure serving transnational organized crime groups operating in the region and globally.

Fundamentally, money laundering occurs in three phases:

- Placement, when funds are integrated into the financial system or into a legal business;
- Layering, which is the process through which money is distanced from its illegal source – the

idea is to make it difficult for investigators to follow the money trail; and
- Integration, when money enters the legal economy – after integration, the money appears clean and investigators can no longer tell where it originated from.

All three phases of the money laundering process are at play in casino- and junket-based methods, offering a dynamic end-to-end solution that organized crime groups have perfected and continue to exploit to move massive volumes of money without exposure to the formal financial system.

Money laundering and underground money transfers using casinos, junkets, and increasingly online casinos (see below section) can be conducted using a variety of typologies including cash-in cash-out,[66] collusion between gamblers,[67] junket financing[68] or so-called 'offsetting' arrangements,[69] misuse of gambling 'VIP cash' accounts,[70] buying another player's winnings, mixing gambling and non-gambling laundering methods, among others.[71] Casinos and junket operators in East and Southeast Asia and the Pacific have also been found to provide so-called 'safekeeping' transactions in which players, including those with clear links to organized crime, are permitted to deposit casino chips for safekeeping with respective casino treasury divisions and cash-out later. This system has evolved into so-called 'investment' arrangements with major junket operators in which 'investors' can earn between 5 to 7 per cent per month on the funds deposited into the junket, leading authorities including the Philippines Security Exchange Commission to issue a warning about the trend in 2019.[72]

Extensive misuse of the junket industry

Junkets are an extension of casino operators and represent the driving force behind VIP gambling as they connect high-roller gamblers with casinos. A junket is an arrangement between a hosting casino and a junket operator to facilitate gambling by an individual or a group of high-wealth players for a period of time through VIP programmes or tours. Through their relationships with casinos, junket operators can offer incentives and perks to their VIP club members and other prospective VIP gamblers. Most critically, recent law enforcement action has demonstrated the scale at which some junket operators have been able to serve as international bank-like entities, providing a variety of underground financial services including credit issuance, currency exchange and multi-currency payment and settlement solutions, remittances, and extra-legal debt collection mechanisms which have been exploited by organized crime.

In many cases, the partner casino will itself pay some or all of the gambler's travel and accommodation costs, while the junket operators typically receive a

66 Cash-in cash-out: this is the simplest, most typical method of laundering money at a casino. A criminal simply exchanges their money for playing chips and then converts them back into cash. This way, dirty money can be presented as money won at a casino. Some players may even divide money into several different betting accounts, which will make them appear less suspicious.

67 Collusion between players (intentional gambling losses): under this strategy, proceeds of crime are brought into either physical or online casinos and deliberately lost – in a poker game for example – in a way that benefits an accomplice who acts as another player in the same game. An unfortunate 'advantage' of this method is that it allows launderers to dodge any AML detection policies that are only triggered by successful bets against the casino itself, not other players.

68 Junket financing: gambler/client deposits money into junket account in one country or stakes other assets, then accesses this credit at another jurisdiction to gamble. This system of debits and credits is used to 'offset' wins and losses against the original amount deposited, allowing the operator to move money/value quickly and informally below the radar of tax and law enforcement agencies. Junkets may also provide a high interest rate to individuals willing to store their money with the junket to be used for offsetting.

69 Offsetting arrangements (also known as mirror transactions): similar to traditional Hawala networks; used as a means of transferring value between jurisdictions via financial credit and debit relationship between entities in different countries. Organizations facilitating offsetting arrange for money debited from an entity in one jurisdiction to be credited to (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both. Offsetting through the use of casinos and junkets as well as more traditional trade-based arrangements has been reported as a method increasingly employed by money laundering organizations based in the Asia Pacific connected to drug production and trafficking, arrangement of precursor chemical shipments, and cybercrime, among other crime types.

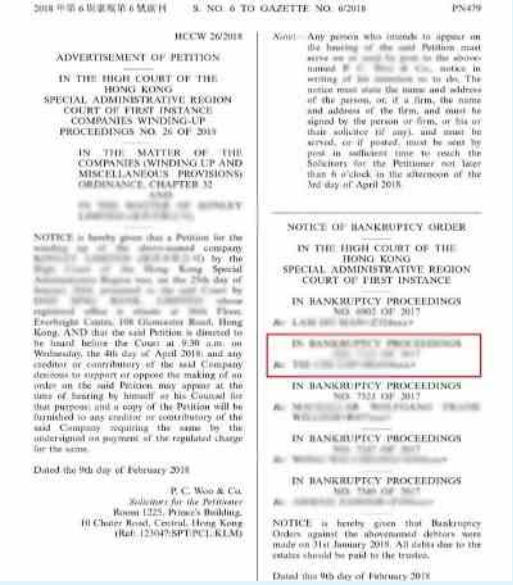
70 Misuse of gambling accounts for illegal transactions between players: in this case, for example, buyers and sellers of illegal items could use their respective gambling accounts as traditional bank accounts to make and receive payments. Once the seller's gambling account is credited, the money can be cashed out, claiming it was a successful gamble. It can also be used for hiding purposes on holding accounts or for wagering at casinos.

71 For instance, 'dummy' room transactions: arrangement for international VIP customers to use a credit or debit card at the resort hotel to authorize a transfer of funds to be made available to the same customers casino and/or junket. The hotel issues a room charge bill to the patron, falsely asserting that the hotel had provided services to the person. Patron will pay the bill and be given a voucher acknowledging the receipt of funds, escorted to the casino cage and able to exchange it for cash or chips as part of the transaction. 'Incidental' charges: when the patron had not stayed at the resort hotel but arrange to pay an incidental charge through their credit or debit card. The money for the incidental charge is then made available to the patron.

72 Meetings with regional law enforcement and financial intelligence officials in East and Southeast Asia, 2023.

Sam Gor (三哥) or 'The Company' and casinos

Sam Gor, also known as 'The Company', is a multi-billion-dollar transnational organized crime syndicate that has had a dominant role in the Asia Pacific drug trade. Money laundering has been essential for Sam Gor, although there is limited official public information disseminated about the methods used by the group. However, the New South Wales *Report of the Inquiry under section 143 of the Casino Control Act 1992 (NSW)*, which recently examined Crown Casino, found that Roy Moo, who was imprisoned in 2013, laundered the illicit proceeds of the Sam Gor syndicate through Crown Casino Melbourne. The same report also concluded that a leading member of the Sam Gor Syndicate was a suspected business partner of the Hot Pot Junket until 2015 at Crown Casino Melbourne and was also involved in money laundering.



HCCW 26/2018

ADVERTISEMENT OF PETITION

IN THE HIGH COURT OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION COURT OF FIRST INSTANCE COMPANIES WINDING-UP PROCEEDINGS NO. 26 OF 2018

IN THE MATTER OF THE COMPANIES (WINDING UP AND MISCELLANEOUS PROVISIONS) ORDINANCE, CHAPTER 32

NOTICE is hereby given that a Petition for the winding up of the above-named company [illegible] by the High Court of the Hong Kong Special Administrative Region was on the 25th day of January 2018 presented to the said Court by [illegible] whose registered office is situate at 36th Floor, Everbright Centre, 108 Gloucester Road, Hong Kong, AND that the said Petition is directed to be heard before the Court at 9:30 a.m. on Wednesday, the 4th day of April 2018; and any creditor or contributory of the said Company desirous to support or oppose the making of an order on the said Petition may appear at the time of hearing by himself or his Counsel for that purpose; and a copy of the Petition will be furnished to any creditor or contributory of the said Company requiring the same by the undersigned on payment of the regulated charge for the same.

Dated the 9th day of February 2018

P. C. Woo & Co.
Solicitors for the Petitioner
Room 1225, Prince's Building,
10 Chater Road, Central, Hong Kong
(Ref: 123047/SPT/PC1/KLM)

Note: Any person who intends to appear on the hearing of the said Petition must serve on or send by post to the above-named [illegible], notice in writing of his intention so to do. The notice must state the name and address of the person, or, if a firm, the name and address of the firm, and must be signed by the person or firm, or his or their solicitor (if any), and must be served, or if posted, must be sent by post in sufficient time to reach the Solicitors for the Petitioner not later than 6 o'clock in the afternoon of the 3rd day of April 2018.

NOTICE OF BANKRUPTCY ORDER

IN THE HIGH COURT OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION COURT OF FIRST INSTANCE

IN BANKRUPTCY PROCEEDINGS NO. 6002 OF 2017

IN BANKRUPTCY PROCEEDINGS NO. 7123 OF 2017

IN BANKRUPTCY PROCEEDINGS

IN BANKRUPTCY PROCEEDINGS

NOTICE is hereby given that Bankruptcy Orders against the abovenamed debtors were made on 31st January 2018. All debts due to the estates should be paid to the trustee.

Dated this 9th day of February 2018

Hong Kong court bankruptcy proceedings No.7123 re: 9 February 2018.

Several other documented cases of Sam Gor activity also indicate their known associates using casinos in the region. For instance, reports discussed with law enforcement state that a leading Sam Gor member spent US $66 million in one day in a Macau casino, and was sued for around US $1.4 million by a casino in Singapore in November 2017 for failing to settle a debt. Law enforcement sources also confirmed that the same syndicate member had previously made visits to a major casino in Cambodia.

Another member of the Sam Gor syndicate that frequented casinos in the past is Hsieh Tsung Lun, who was arrested in 2018 and extradited from Cambodia to Myanmar. According to regional enforcement officials, Hsieh organized shipments of large quantities of methamphetamine as well as heroin for the syndicate while he was working out of a casino in the Golden Triangle. The same sources have confirmed that Hsieh frequently visited the same major Cambodian casino prior to his arrest.

commission from casinos derived from the amount of money gambled by the players within VIP gaming rooms that are unavailable to mass market gamblers. A growing number of junket operators also now run online and proxy gambling platforms.

Although junket operators began as recruiters of high net worth gamblers, they quickly diversified into credit providers to satisfy the need of customers wishing to evade capital controls, and as a result also had to become debt collectors when loans were not repaid. Since both of these key business lines are illegal in mainland China, junket operators relied on other means, and particularly connections to organized crime, to collect such debts. In the early 2000s, forward-thinking junkets began to diversify into online gambling, first for their core clients in Asia, then globally. This vastly expanded their potential market and increased revenues exponentially (see below).

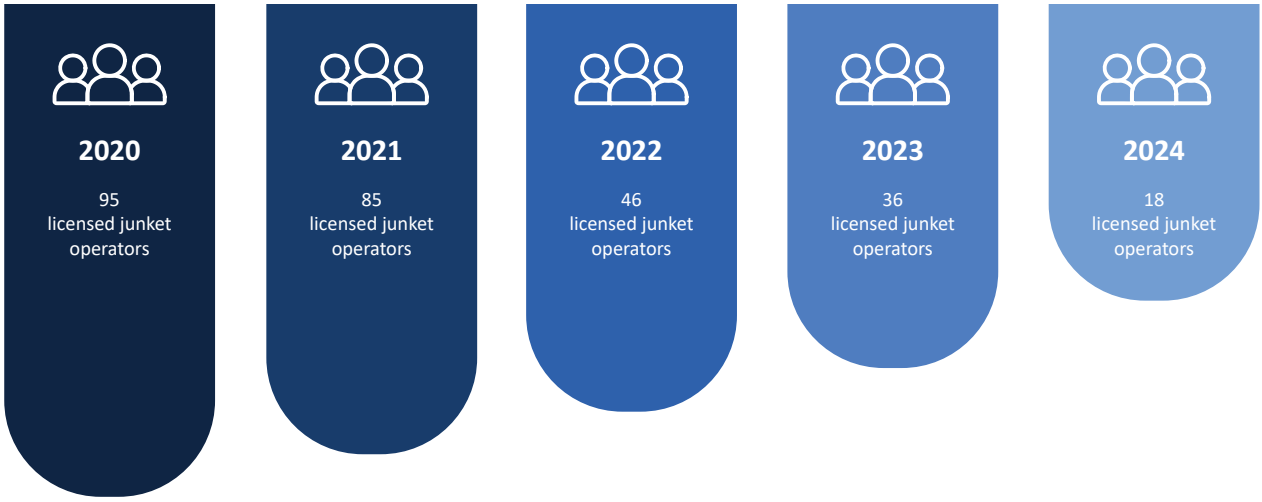
In recent years, junket operators have been gradually relocating their business operations and players to small-scale casinos in Southeast Asia after regulatory reforms transformed the gaming market in Macau SAR.[73] While the Macau SAR gaming industry once had 235 junket promoters and a multitude of VIP rooms spread throughout the local casinos, only 18 licensed junket operators remain active as of January 2024.[74] This has resulted in a profound shift in the industry's entire landscape throughout Southeast Asia.

This displacement has been accompanied by an intensification in a wide range of criminality in vulnerable parts of Southeast Asia, and particularly the Mekong region. More specifically, the junket sector in the region has been exposed for its heavy

73 Centre for Gaming and Tourism Studies, Macao Polytechnic University, 2023.

74 Ibid.

Figure 3. Change in licensed junket operators in Macau SAR, 2020-2024



Source: Gaming Inspection and Coordination Bureau (DICJ) of Macau SAR.

infiltration by organized crime for industrial-scale money laundering and underground banking operations, as well as increasingly clear links to drug trafficking and cyberfraud. These connections to transnational organized crime have become strikingly apparent in recent years, stemming largely from wide-scale deficiencies in casino supervision and enforcement of related anti-money laundering measures including customer due diligence (CDD) and know-your-customer (KYC) principles, source and distribution of funds analysis, beneficial owner requirements, and financial reporting by operators which are particularly prevalent in several high-risk jurisdictions.[75]

Recent law enforcement action targeting junket operators and organized crime figures has demonstrated that many junkets operating in East and Southeast Asia and the Pacific have been extensively infiltrated by organized crime groups (see case study chapters below for more detailed analysis). In Australia, for instance, major Asian transnational organized crime groups including the Sam Gor drug trafficking network and 14K triad have been identified as using junkets to move money through Australian casinos. In March 2022, the Australian Transaction Reports and Analysis Centre (AUSTRAC) issued a Statement of Claim filed in Federal Court in relation to money laundering activities at Crown Casinos.[76] According to the document, Crown Melbourne and Crown Perth casinos had partnerships with several junket operators, including the Suncity, Neptune (later renamed Guangdong), Meg-Star, Song, Chinatown, Tak Chun, Jimei, and Oriental Group junkets, which were used as conduits for money laundering and other illicit activities. The document also shed light on the significant scale of revenues generated by junket operations at the Crown casinos.

Between July 2015 and June 2020, Crown Melbourne's reported turnover (cross-table transactions or rollings) from its VIP program was AU $220.8 billion (equivalent to US $162 billion), and a substantial proportion of that amount was from Asian gamblers. During the same period, Crown Melbourne made over AU $1 billion in junket revenues (equivalent to US $732 million), while Crown Perth's revenue from junket operations exceed AU $320 million (equivalent to US $234 million).[77] In 2023, AUSTRAC and Crown jointly agreed that the casino operator should pay AU $450 million penalty for 546 breaches of anti-money laundering laws revealed during the country's inquiry into casinos and junkets.[78] In 2020, AUSTRAC also assessed that the general risk profile of persons involved in junkets is high, further pointing out that, under current arrangements, it is not possible to clearly determine beneficial ownership and control of the funds.[79]

75 Government of New South Wales, inquiry under section 143 of the Casino Control Act 1992, February 2021 at p. 67.

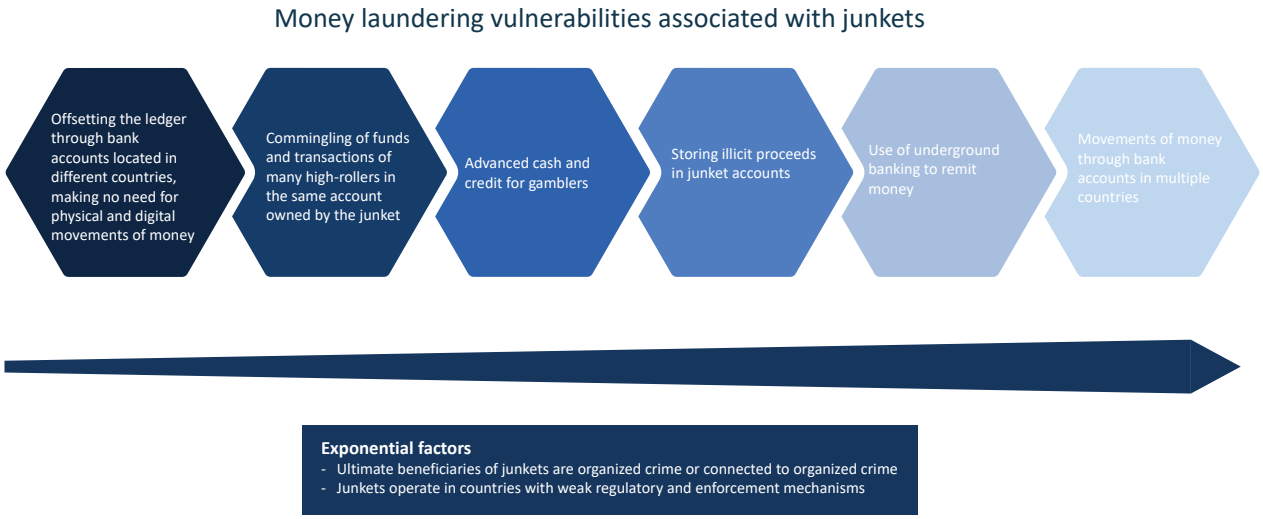
76 Statement of Claim, Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, March 2022. Available at: https://www.austrac.gov.au/sites/ default/files/2022-03/20220301_Statement_of_Claim_ stamped_0.pdf).

77 Ibid.

78 Australian Transaction Reports and Analysis Centre, 2023. Accessed at: https://www.austrac.gov.au/news-and-media/media-release/austrac-and-crown-agree-proposed-450-million-penalty.

79 Australian Transaction Reports and Analysis Centre, Money Laundering and terrorism Financing Risk Assessment: Junket Tour Operations in Australia, 2020. Accessed at: https://www.austrac.gov.au/sites/default/files/2020-12/JTO_2020_FINAL.pdf.

Figure 4. Money laundering vulnerabilities associated with junket operators



Source(s): UNODC elaboration based on consultations with regional authorities and international experts.

Another example occurred in the Philippines, where a number of licensed casinos and junket operators and representatives were found to have played an important role in laundering approximately US $81 million stolen in a cyberattack attributed to the Lazarus Group[80] from the Bangladesh Central Bank in 2016. While the money initially passed through banks and remittance companies, the paper trail disappeared after the money was transferred to casino junket operators, agents and players including Bloomberry Hotel and Resort's Solaire Casino, Eastern Hawaii Leisure Company, Suncity junket, and Goldmoon junket (see below breakdown chart).

CCTV surveillance image presented during 2016 senate inquiry into the Bangladesh bank heist showing tranches of cash being exchanged for casino chips and cash returned by a Philippines-based junket operator following the inquiry.

According to filings by the Bangladesh Central Bank with the New York Southern District Court in January 2019 as well as records in the Philippines, Alvin Chau was the direct recipient of a large portion of the stolen funds that were laundered through the Suncity junket in the Solaire Hotel and Casino.[81]

More specifically, the documents confirm that the money launderers had exchanged Solaire Casino chips worth 903.7 million pesos or US $20 million for an equal amount of non-negotiable Suncity junket chips which were then systematically transmitted through the junket operator as VIP rollings over several weeks and ultimately ended up in casinos in jurisdictions outside of the Philippines. This was later confirmed by Solaire's lawyer during the associated Senate Committee on Accountability of Public Officers and Investigations (Blue Ribbon Committee) hearings.[82]

Beyond the Bangladesh bank case, a 2023 study conducted by the Philippines' Anti-Money Laundering Council (AMLC) into suspicious transactions associated with casino junkets found multiple instances of junket operators failing to report on covered transactions, in breach of junket

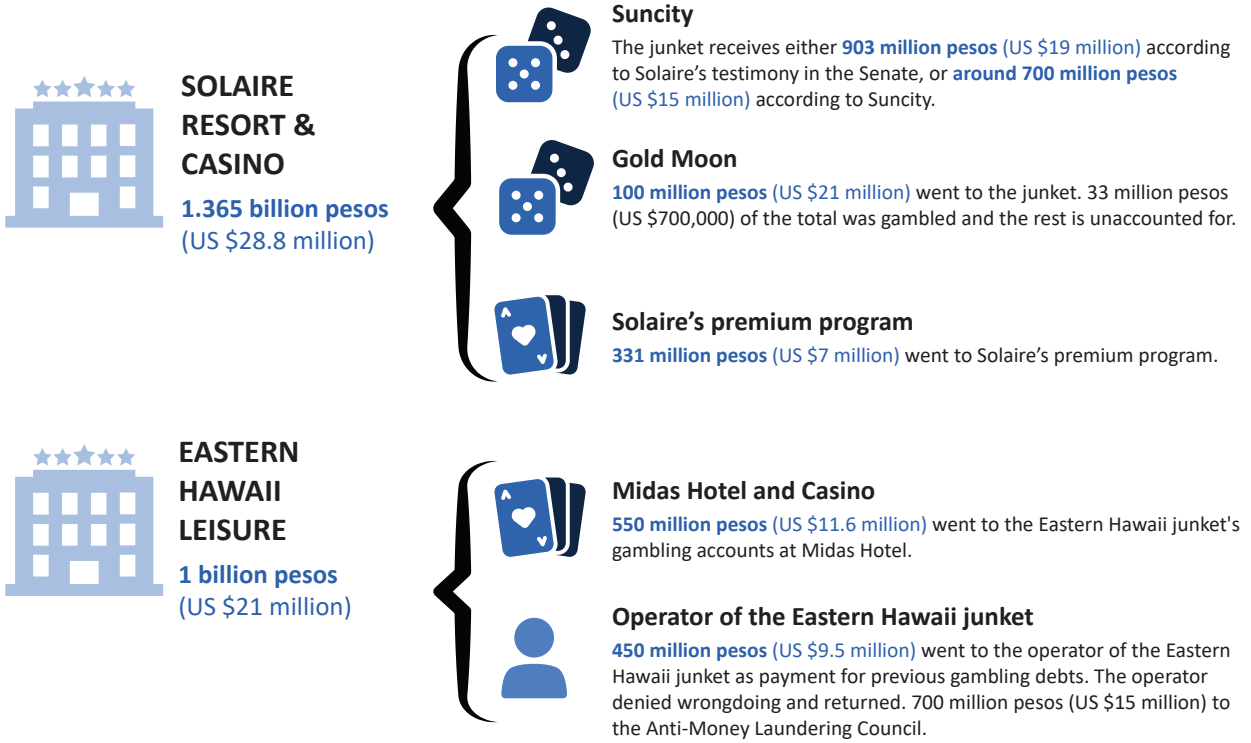
80 Lazarus, also known as APT38, is a notorious Advanced Persistent Threat (APT) actor best known for conducting high-profile financial cyberattacks and engaging in cyber espionage. Their operations often involve the deployment of sophisticated malware and more recently have been attributed to billions of dollars in stolen cryptocurrency.

81 Philippines Ministry of Justice, 2020. Accessed at: https://elibrary.judiciary.gov.ph/assets/dtSearch/dtSearch_system_files/dtisapi6.dll?cmd=getdoc&DocId=93584&Index=*47d2af93eea3c41eede94fa5db1eb960&HitCount=16&hits=b2+d6+f5+13e+185+194+227+48f+699+784+7af+80b+845+9b7+b03+b16+-&SearchForm=C:%5celibrev2%5csearch%5csearch_form.

82 Senate Committee on Accountability of Public Officers and Investigations (Blue Ribbon Committee), 2016.

Figure 5. Distribution of stolen funds in the Bangladesh bank heist through Philippine casinos and junkets

Cash stolen from the Bangladesh central bank was routed and laundered through casino and junket operators which were exempt from anti-money laundering laws in the Philippines until 2017.



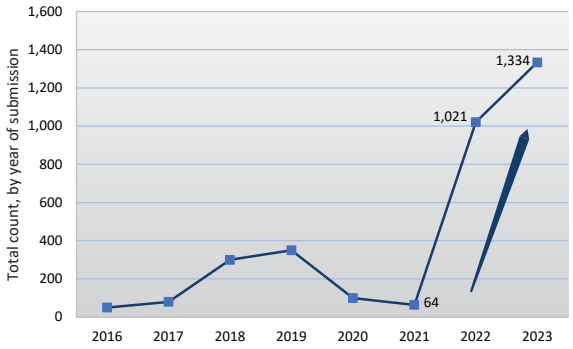
Note: Pesos converted at $1 = 47.4 pesos, the rate at the time of senate hearings. *These junkets operated inside and had accounts at Solaire.
Source: UNODC elaboration based on Philippine senate inquiry testimony.

agreements.[83] The study also observed a dramatic rise in the volume of suspicious transaction reports (STRs) which increased from 64 to 1,021 between 2021 and 2022, together with growth in the value of STRs which rose from US $16 million to more than US $170 million during the same period.[84] According to discussions with regulatory authorities in the Philippines, the sudden increase is in part attributable to enhanced enforcement measures and reporting requirements as well as the crackdown on Macau SAR junket operators and developments in the e-junket space. Notably, several STRs examined in the study relate to predicate offences including drug trafficking as well as a criminal scam syndicate that was under investigation.[85]

These findings are consistent with reports by law enforcement authorities which have confirmed the use of junkets by drug traffickers for payment disbursement and money laundering, as well as by kidnappers in the Philippines for ransom payments.[86] For instance, in 2018, Philippine authorities dismantled a synthetic drug manufacturing facility in Malabon City and arresting 9 suspects.[87] According to law enforcement and criminal intelligence officials involved in the case, shipments of precursor chemicals sourced by the drug syndicate were arranged at a VIP room in Macau SAR while payments were subsequently arranged through a junket operator and disbursed using casino chips. Concerningly, as reported by law enforcement, those arrested were known to have frequented integrated casino resorts in the Philippines, namely the Solaire Hotel & Casino, where Suncity VIP rooms were operating at the time. It is also worth noting that Philippine regulatory authorities have cited a high level of non-compliance and non-cooperation during inspections of casino junkets operating in the country.[88]

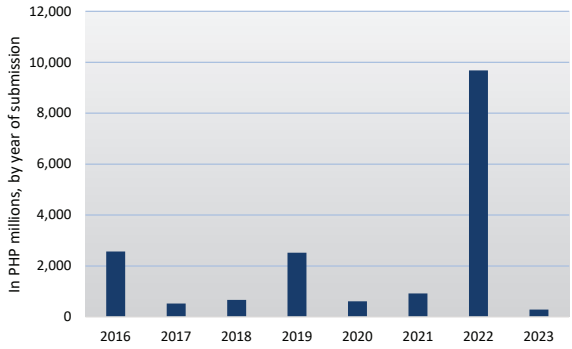
83 Anti-Money Laundering Council of the Philippine, Analysis of Suspicious Transactions Associated with Casino Junkets, 2023. Accessed at: http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf.
84 Ibid.
85 Ibid.
86 Meetings with national law enforcement and financial intelligence officials in East and Southeast Asia, 2023.
87 Ibid.
88 Consultations with regional casino regulatory authorities, 2023.

Figure 6. Volume of STRs related to junkets in the Philippines, 2016-2023



Source: Anti-Money Laundering Council of the Philippines, 2023.

Figure 7. Value of STRs related to junkets in the Philippines, 2016-2023



Source: Anti-Money Laundering Council of the Philippines, 2023.

Junket-based money laundering and underground banking methods

Recent law enforcement action has exposed several sophisticated methods devised and exploited by transnational organized crime groups to facilitate money laundering using casino junkets. Primary among them are offsetting arrangements which were first developed for cross-border gambling in Macau SAR and have since evolved as a solution for underground banking and money laundering utilized by organized crime. Fundamentally, these transactions are made outside the formal banking sector and pose a high level of risk in the case of casino junkets as they circumvent international funds transfer reporting requirements and facilitate the laundering of domestically generated proceeds of crime.[89]

Offsetting is used as a means of transferring value between jurisdictions via financial credit and debit relationships between entities in different countries. Organizations facilitating offsetting arrange for money to be debited from an entity in one jurisdiction to be credited to a corresponding (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both. In the case of casino junkets, a gambler (high-roller) deposits money into a junket account or stakes using credit issued by the junket or other assets in one country and is subsequently issued a corresponding amount of value in another. While the funds are theoretically transferred for the purpose of gambling, misuse of this mechanism has enabled organized crime to move vast amounts of cash and increasingly cryptocurrency while bypassing the formal financial system.

As demonstrated by cases in the region, it is common for funds held in junket representative-controlled casino accounts to offset against money in accounts held overseas partially derived from onshore individuals known as 'cash collectors' who move money from domestic organized crime groups to junket operator casino accounts.[90] This can include proceeds of crimes including drug trafficking, cybercrime, fraud, and scams, and human trafficking, among others. Notably, while more complex and less prevalent, authorities have also reported the use of an offsetting method whereby money to fund players' junket activity is raised by directing the player to purchase shares in a foreign company, rather than simply depositing the money into an offshore bank account.[91]

Compounding the challenge further, several industry-wide deficiencies in casino and junket management and supervision that have been uncovered across the region in recent years have clearly exacerbated the situation and the level of infiltration of organized crime. This includes the following:

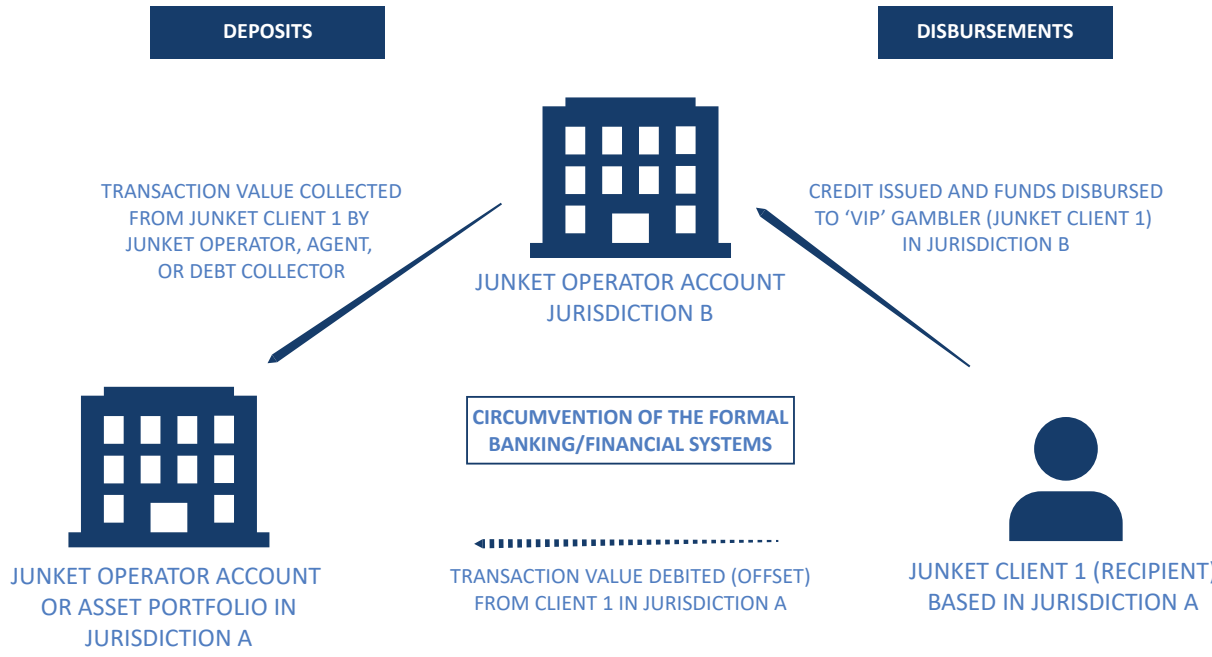
- **Prevalence of multi-party transactions and cash deposits:** loosely regulated junket accounts can receive large cash deposits from a multitude (tens to hundreds) of individuals over a given reporting period, with only some depositors registered with the junket (individuals who are neither operator nor agent) – thereby violating most casinos' practice of only allowing junket operators

89 Australian Transaction Reports and Analysis Centre Money Laundering and terrorism Financing Risk Assessment: Junket Tour Operations in Australia, 2020. Accessed at: https://www.austrac.gov.au/sites/default/files/2020-12/JTO_2020_FINAL.pdf.

90 Ibid.

91 Ibid.

Figure 8. Simplified informal money transfer model via casino junket offsetting arrangement



Source: UNODC elaboration based on extensive consultations with regional law enforcement and financial intelligence officials, 2023.

or agents to transact on junket accounts. At the same time, too many agents allowed to transact on a junket's accounts may diminish effective control over transactors, resulting in authorities having limited view of gambling account behaviour and banks unable to isolate junket-related transactions from other casino transactions. This presents obvious transaction monitoring and analysis challenges.

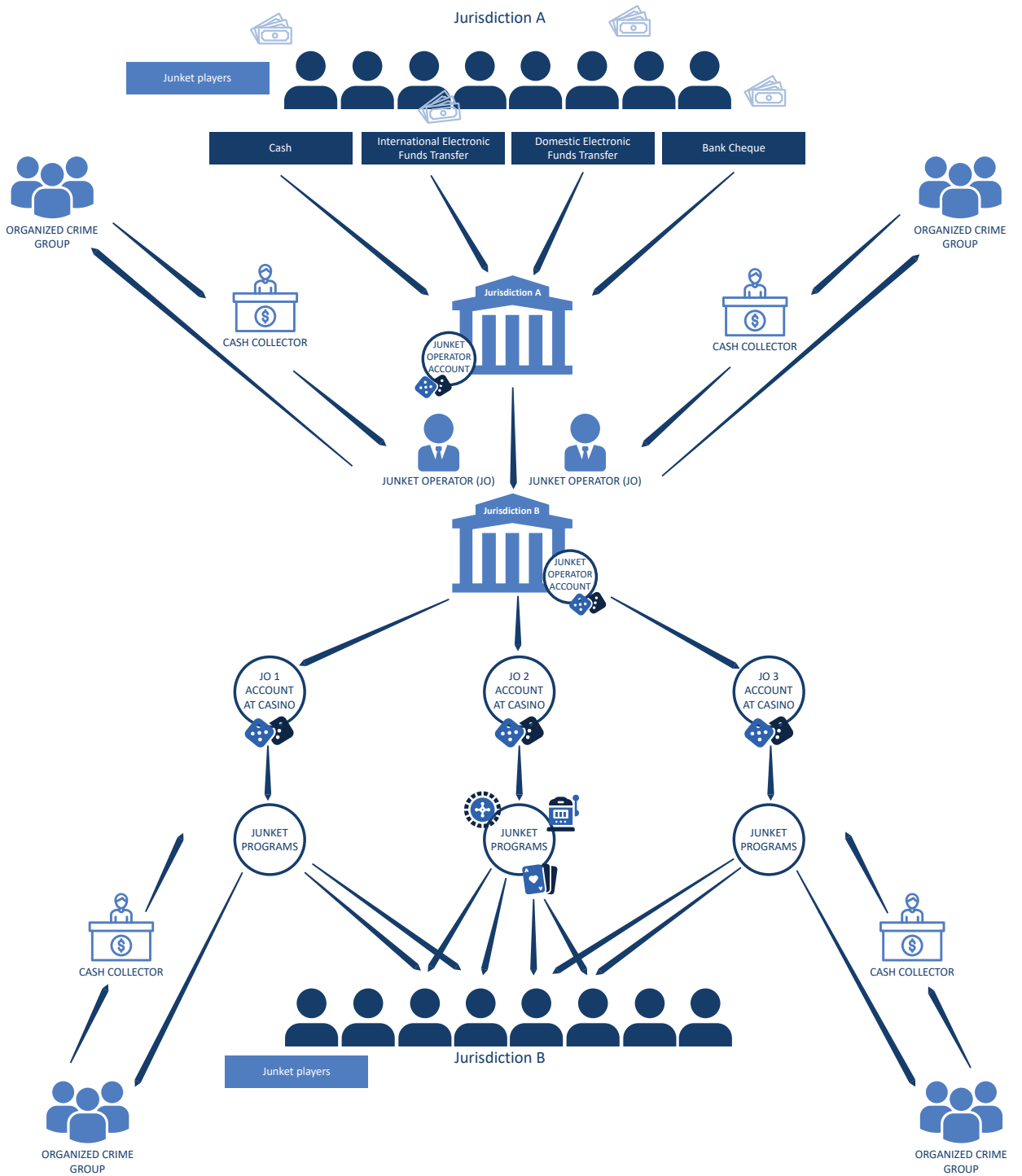
- **Misuse of VIP cash accounts**[92]**:** casino operators across the region often open bank accounts under their business for their junket partners which have been observed to facilitate the storage and movement of significant amounts of money, both domestically and internationally, by transnational organized crime. On a per-transaction and per-customer basis, the junket sector is also significantly exposed to the risks associated with high-value cash activity. The destination of large cash withdrawals from junket accounts represents a key intelligence gap throughout East and Southeast Asia and the Pacific.

- **Treating junket operators as individuals rather than corporate entities:** discussions with casino regulators and financial intelligence authorities indicate that casino operators often consider junkets to be individuals and transact with them on that basis. However, it is clear that some junkets operate as part of large international businesses. This grey area has been found to lead to different levels of application of due diligence which subsequently increases the vulnerability associated with understanding of beneficial ownership and control. At the same time, diversification of junket tour operations into a range of different business lines increases opportunities for commingling, and presents difficulties for banks in understanding the origin of funds.

- **Prevalence of multiplier betting in the junket industry:** multiplier betting refers to a form of 'under-the-table' gambling in which a bet formally denominated at the casino gambling tables only represents a fraction of the total amount of a private bet made between gamblers and junket operators to avoid gaming revenue levies. It allows clients to pre-negotiate their preferred payment method, betting currency, and cash-out method while increasing the commissions received by the junket promoter, and can be used as a tactic to conceal the total amount of money transmitted through the casino or junket by an individual bettor and obfuscate the source and destination of funds. Such arrangements are understood to have grown in popularity due to most junket

92 See below case studies on Alvin Chau of Suncity Junket and Levo Chan of Tak Chun Junket.

Figure 9. Model of simplified junket lifecycle and misuse by organized crime



Note: Both junket players and cash collectors seeking underground banking and/or money laundering services through junket operators may transfer funds directly into junket operator-held accounts which have been set up by partner casinos. Junket operators will 'offset' the debited amount received in one jurisdiction and credit the corresponding amount in another.
Source: Extensive consultations with regional law enforcement and financial intelligence officials, 2023.

customers in Macau SAR originating from mainland China. These customers do not—and in any case cannot—bring money with them to play due to strict capital controls and a nation-wide gambling ban in mainland China, and instead rely on credit issued by junket agents. For instance, should a customer request a HK $1 million credit, the junket agent can request the casino to provide HK $100,000 worth of chips, with the understanding between the junket agent and customer that a ten times multiplier is in effect.

- **Use of unlicenced money service businesses (MSBs):** in several markets, use of unlicenced money transfer businesses lending gambling patrons, often from East and Southeast Asia, funds to gamble have been identified in numerous criminal cases to play a key facilitation role in money laundering. The origin of the funds is often unknown and can potentially related to criminal activity. The funds from the unlicenced MSB are loaned to the gambler, and the gambler will repay the funds within another jurisdiction where only a domestic transaction will occur. This method also assists in circumventing strict currency controls in some jurisdictions and allows access to capital to gamble in different countries. It also allows the money operator to convert cash from one jurisdiction into a bank deposit within another.
- **Growing use of cryptocurrency by major online casino and junket operators:** while use of cryptocurrencies by online casino and junket operators is not authorized by any casino regulators in Southeast Asia, UNODC has observed widespread advertising of cryptocurrency exchange and payment services being provided by both licensed and unlicensed operators across the region.

Daily currency exchange rate table including Tether cryptocurrency advertised by a licensed junket operator in the Philippines, August 2023. Source: official social media business accounts.

As depicted in figure 9 above, the resulting conditions have resulted in a complex and vulnerable casino junket lifecycle easily exploited by transnational organized crime and junkets facilitating offsetting arrangement.

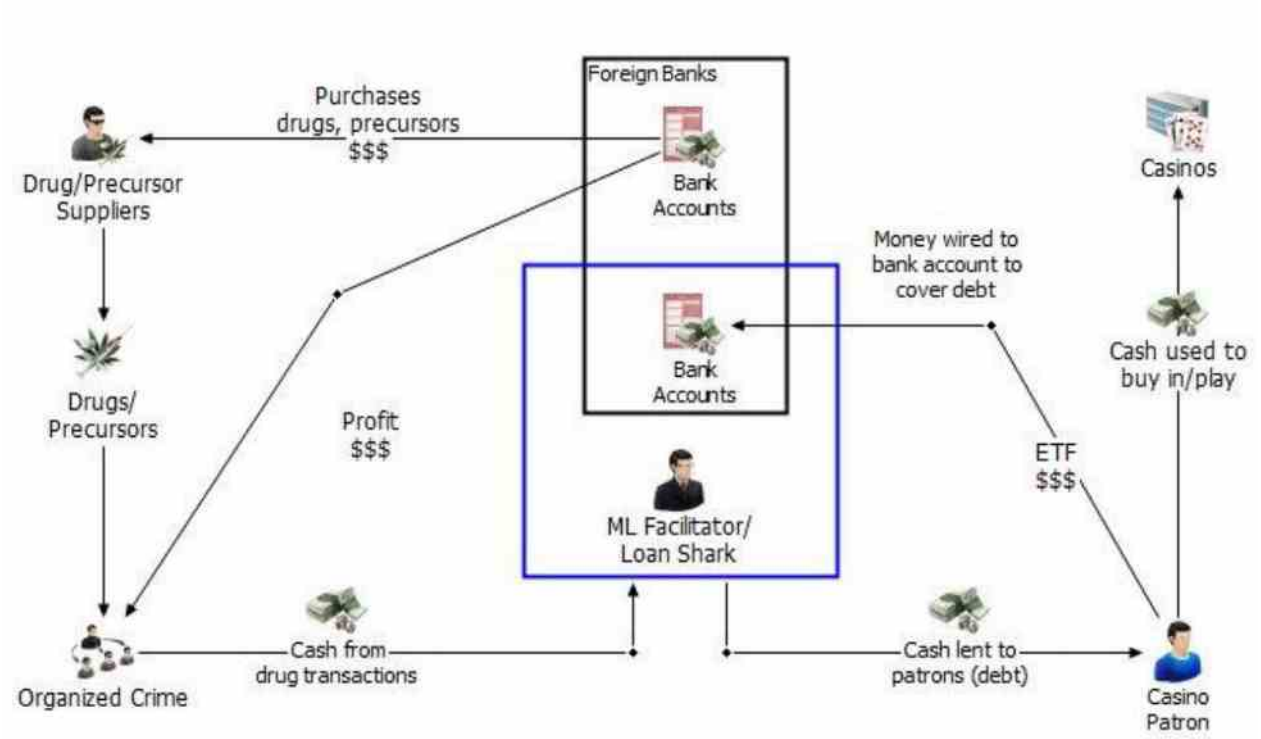
The 'Vancouver Model'

Among the best-documented examples of misuse of casinos and junkets (licensed and unlicensed) by organized crime relates to what has been coined by law enforcement and industry experts as the 'Vancouver model' for money laundering and underground banking. While the model was initially uncovered through the Cullen Commission money laundering inquiry[93] in Canada, authorities and experts have identified similar methods exploited by organized crime networks operating though casinos in Australia, Macau SAR, and several countries including Cambodia, Lao PDR, Myanmar, and the Philippines.[94] According to the inquiry, the model, which was devised by Asian transnational organized crime groups despite junkets not being formally permitted in Canada, successfully laundered millions of dollars through casinos in British Columbia between 2008 and 2018, including proceeds generated by drug cartels based in Mexico and countries in South America. The inquiry also cited surveillance footage in which bags of cash were brought into casinos to convert to casino chips, play a few games and cash out as clean money (sometimes known as short play).

93 Commission of Inquiry into Money Laundering in British Columbia. Accessed at: https://cullencommission.ca/com-rep/.

94 Meetings with regional law enforcement and financial intelligence officials, 2023.

Figure 10. 'Vancouver model' for money laundering through British Columbia's casinos



Source: Cullen Commission of Inquiry into Money Laundering in British Columbia.

The Vancouver model combines elements of traditional hawala money laundering methods and mixes them with cash-in, cash-out strategies. It can be understood through the following process:

1. A person in Jurisdiction X (who may or may not have been involved in a crime) attempts to transfer substantial funds out of that jurisdiction and may circumvent cash export control laws.
2. The person transfers funds to a criminal group in Jurisdiction X and then travels to Jurisdiction Y.
3. A criminal gang in Jurisdiction X arranges for its associates in Jurisdiction Y to transfer an equivalent amount of the original transfer amount to someone now in Jurisdiction Y (mostly in the form of cash derived from criminal activity which needs to be laundered).
4. The person enters the casino, converts the money into chips, then makes several low value bets and cashes out.
5. This person traded the chips for clean cash or cash checks, and now has both laundered funds for the criminal group through the original transfer and bypassed the cash exit control laws in Jurisdiction X for their own benefit.

While this phenomenon has occurred in countries with robust regulatory capacity such as Australia and Canada, many of the world's largest junket operators remain active in casinos located in higher-risk jurisdictions of Southeast Asia. Considering the relatively minimal regulation and enforcement to counter money laundering in the region, the availability of junket operators should be seen as a serious money laundering risk likely to be accompanied by other criminal activity. It is also important to note the role of junket representatives (often referred to as agents), who work on behalf of junkets in return for commissions. Some of these representatives open accounts with junket operators and store large amounts of cash which can be advanced to gamblers. For instance, in December 2020, the People's Procuratorate of Jiangsu Province of China indicted five people for running casino rooms in China while acting as representatives for major junkets. They opened junket accounts with Suncity, Tak Chun and others from which advanced credits were sent to gamblers. In addition, they opened and managed casino rooms in China where screens of gambling tables from the Tak Chun VIP room in Manila were live streamed. A minimum of RMB 170 million (approximately US $27 million) was transacted

through the indicted operators since 2016 before the indictment.[95]

Law enforcement authorities have also reported the extensive misuse of the Suncity VIP room network together with multiple land-based casinos across the region including Golden Triangle-based casinos for money laundering and underground banking by organized crime. More specifically, analysis of financial intelligence by both international and regional law enforcement confirms the use of these establishments for facilitating payments to drug traffickers and arranging the production of synthetic and other drugs in and around the Golden Triangle.

Proliferation of online casinos and their misuse for money laundering and underground banking

In recent years, the rapid proliferation of the 'offshore' online casino industry (including online sports betting) in several high-risk jurisdictions in Southeast Asia, and particularly the Mekong, has been reported as a growing concern by authorities in and beyond the region. Macau SAR junket operators and their close criminal associates have been key drivers behind this trend, pushing for its acceleration following enhanced law enforcement and regulatory pressures in mainland China together with mobility restrictions brought on by the COVID-19 pandemic which curbed travel for VIP gamblers. Both unregulated and under-regulated online casinos run by junket operators (sometimes referred to as e-junkets), while themselves highly profitable, also served as a useful channel of credit settlement between junkets and their clients, providing additional utility in being able to effectively disguise proceeds of organized crime as legitimate online betting profits. Most, if not all, of the largest junket operators had such operations, with smaller junkets acting as customer referral agents.[96]

The shift into online casinos has been exhibited by both a major increase in online betting and associated gambling platforms as well as the expansion of online betting products and payment methods.[97,98] More specifically, the rapid emergence of technology including mirror websites,[99] cryptocurrency, and third-party betting software or so-called 'white-label' service providers[100] in Southeast Asia has meant that it has never been easier to set up an online casino operation with limited technical expertise and overhead capital, irrespective of gambling laws within a given jurisdiction. Developments in internet payment technologies have also assisted in supporting the regional online casino industry with the rise in the number of third-party payment providers, e-wallets, and other digital payment solutions to support online transactions and in-app purchases. Additionally, the massive, growing scale of the industry has drawn in an unprecedented number of young employees into the sector, posing opportunities for some and risks for others given the surge in related recruitment fraud and human trafficking.

Advances in internet speed and technology have also helped to facilitate more sophisticated online games and gambling including live-dealer casino streaming which can essentially replicate the same experience for a gambler as land-based casinos. With the introduction of mobile apps, the proliferation of online betting and online casinos has also increasingly become available to mass markets. Online gaming and the rise of social gaming[101] has also been changing the industry and its associated money laundering risks as so-called 'crypto casinos' and non-fungible token (NFT) play-to-earn games become more popular.[102]

According to latest segment forecasts, the formal online gambling market is projected to grow to

95 People's Procuratorate of Xinwu District, Wixi City, Jiangsu Province, Indictment, December 2020, Available at: https://www.12309.gov.cn/12309/gj/js/wxs/wxskfq/zjxflws/202109/t20210923_10584144.shtml.

96 Asian Racing Federation, 2023.

97 Asian Racing Federation, How China's Crackdown on Illegal Betting Impacts Global Betting Markets. September 2021.

98 International Center for Gaming Regulation. An assessment of AML risks linked to accepting crypto-payments in the gambling sector (A regulator's guide), May 2023.

99 The vast majority of online gambling platforms operating in Southeast Asia exploit what are known as 'mirror websites'; exact replicas of primary betting websites housed under different URLs which are often algorithmically generated and used to evade regulatory attention, effectively staying several steps ahead of authorities by running hundreds of mirror websites on the same server to ensure services remain uninterrupted in the event that a URL is shut down.

100 White-label gambling websites are similar to franchises, with betting operators being able to outsource every component of the business including sophisticated and secure betting technology, offshore licensing schemes, website design, customer data and management, branding and marketing materials, and operating license from third-party service providers.

101 The term 'social gaming' refers to online video games accessed mainly through social media platforms. In addition to being entertained while playing, users share the gaming experience with their network on the platform they're on. By integrating into commonly used platforms, these types of games can attract audiences that aren't typically interested in video games.

102 International Center for Gaming Regulation. Online Casinos, Alternative Payment Mechanisms and the Associated Financial Crime Risks, 2022. Accessed at: https://www.unlv.edu/sites/default/files/media/document/2022-02/IGCR-OnlineCasinos-AlterPaymentMechanisms-FinanceCrimeRisks.pdf.

Live-dealer casino employees in Kokang, SR1 of Myanmar.
Source: Criminally implicated New Jinjiang Hotel and Werner International hybrid casino, 2022.

more than US $205 billion by 2030,[103] with the Asia Pacific region representing the bulk share of market growth between 2022 to 2026 at a projected 37 per cent.[104] In the Philippines alone, there are currently 34 licensed offshore operators (POGOs), each of which is permitted to operate up to 10 online gaming platforms and sub-license 10 service providers. At the time of writing, industry experts in the Philippines project gross gaming revenue (GGR) for 2023 to reach over US $438 million, up from US $109.2 million prior to the COVID-19 pandemic in 2019 and more than double the amount generated in 2022.[105] It is worth noting however that these projections do not take into account illegal, unlicensed online casino operators, and that the offshore online casino industry is also highly prevalent in countries including Cambodia, Lao PDR, and Myanmar, although very little data is available due to the industry operating in a grey space due to lack of formal, functioning, and enforced regulatory frameworks.

The growth of online gambling in Southeast Asia is not a new phenomenon and in fact has been taking place for years. It is part of the broader changing model of the region's casino and junket industry – one that has steadily pivoted away from identifying high-rollers and facilitating their luxury gambling tourism, and towards the broader targeting of the premium mass market population online. With that said, surging law enforcement action reported throughout East and Southeast Asia has highlighted the fact that, like land-based casinos, online casinos can be misused to serve as integral components of the regional underground banking and money laundering infrastructure (see detailed analysis in below case study section). It has also provided more channels for commingling recreational gambling flows with proceeds of crime.

For instance, following a surge in criminality related to incidents of murder, kidnapping, money laundering and growing influence of organized crime, in 2022 Philippine authorities ordered the shutdown of 175 offshore gambling firms and deportation of approximately 40,000 foreign workers.[106] That same year, a total of 461 individuals were arrested in Thailand for involvement in illegal online gambling websites, with authorities blocking more than 6,000 website URLs involved.[107] Thai authorities have noted that illegal gambling flows within the country have totaled billions of dollars in the first half of 2023, reporting that one of the largest networks operating in Thailand under investigation was found to have generated illegal gambling revenues totaling more than US $500 million per month.[108] Similarly, in Malaysia, online gambling-related STRs have nearly doubled between 2019 - 2022, totaling more than 42,000 reports, with the value of related STRs also increasing dramatically to more than MYR 26 billion or US $5.5 billion in transaction volume during the same period, representing a 273 per cent increase.[109] Authorities in China additionally reported more than 37,000 cases involving cross-border and online gambling, with operations nationwide cracking down on 2,600 online gambling platforms, more than 1,100 casinos, as well as in excess of 2,500 illegal payment platforms and underground banks, 1,200 technical

103 Polaris Market Research, Online Gambling Segment Forecast, 2022 – 2030. Accessed at: https://www.polarismarketresearch.com/industry-analysis/online-gambling-market.

104 Technavio market research report on online gambling: forecast and analysis 2022 – 2026. Accessed at: https://www.prnewswire.com/news-releases/online-gambling-market-size-to-grow-by-usd-142-38-billion--37-of-the-growth-will-originate-from-apac--17-000-technavio-reports-301539695.html.

105 Asia Gaming Brief, 2023. Accessed at: https://agbrief.com/news/philippines/24/07/2023/pogo-tax-payments-rise-127-percent-yearly-in-2022/.

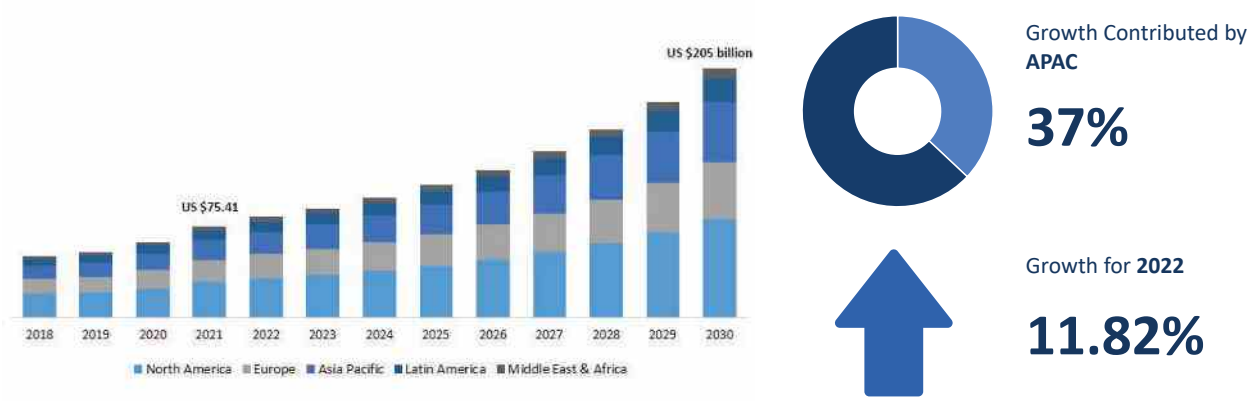
106 Ministry of Justice of the Philippines, 2022.

107 Ministry of Digital Economy and Society of Thailand, 2023.

108 Meetings with national law enforcement and financial intelligence officials, 2023.

109 Ibid.

Figure 11. Online gambling market size by region 2018-2030 (US $ billion)



Source: Polaris Market Research Analysis, 2023.

support teams, and 1,600 platforms promoting illegal gambling.[110]

Associated challenges and risks

Despite intensifying regulatory and enforcement efforts across East and Southeast Asia, it is clear that millions of new online betting customers have emerged following the COVID-19 pandemic.[111,112] This has in turn broadened the customer base for licensed and unlicensed betting operators based in countries including Cambodia, Lao PDR, Myanmar, the Philippines, and Viet Nam, while boosting illegal betting revenues and creating new outlets for money laundering and underground banking. At the same time, as the Asia-facing junket industry has longstanding connections to various Macau SAR-based triad groups, the continued geographic diversification by junket operators, together with the advent of the e-junket model an dispersion of online gambling operations across vulnerable parts of the Mekong, risks providing huge new revenue streams for organized crime and their partners while fueling further consolidation and expansion of syndicates already operating in te region.

By their nature, illegal online betting operations function similarly to most organized crime syndicates. This is reflected by the common structure that both share aspects of, where illegal street bookmakers have traditionally operated.[113] Illegal online betting operators in East and Southeast Asia have emulated this structure, albeit with a greater volume of smaller regional online operators acting as mid-level agents for the biggest grey market Asian bookmakers.

Under this traditional pyramid structure, illegal betting syndicate organizers issue credit down the chain through a roster of ranked agents and middlemen to brokers at the bottom who ultimately acquire customers by assessing creditworthiness and taking bets. Once a bet is placed, the transaction is passed upwards to hedge liability and aggregate risk, with each level of the network taking a commission along the way to the organizer. In the case of online betting markets, however, while bets are still taken at street level, customers can increasingly place bets directly on the illegal websites by themselves. Similarly, so-called super and master-agents to whom brokers report will often run their own online betting sites, purchasing access to syndicate 'materials' complete with premade web design, content, and a registered domain. This network of regional and national level sites hedge liability between one another as well as with the larger ones up the pyramid. At the top, the biggest grey-market betting sites in the region accept billions of dollars in bets annually, with their liquidity being so high that major global sports betting sites hedge with them.[114]

110 State Council of the People's Republic of China, 2022. Accessed at: https://english.www.gov.cn/statecouncil/ministries/202212/29/content_WS63ad52a3c6d0a757729e4e37.html#:~:text=China%20cracks%20over%2037%2C000%20cross%2Dborder%20gambling%20cases%20in%202022&text=BEIJING%2C%20Dec.,in%20a%20statement%20on%20Thursday.

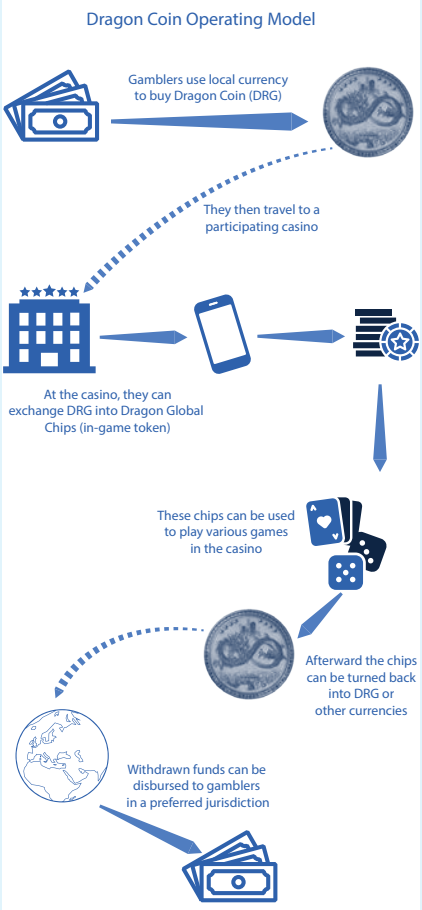
111 UNODC consultations with industry experts and academics in Southeast Asia, 2022.

112 Asian Racing Federation, A Report of Illegal Betting Growth During the COVID-19 Pandemic, May 2021.

113 Koleman Strumpf, 'Illegal Sports Bookmakers', 2003. Available at: https://www.unc.edu/~cigar/papers/Bookie4b.pdf.

114 David Forrest, 'Understanding the Impact of Asian Betting Markets', International Association of Gaming Regulators Webinars, June 2017. Available at: www.iagr.org/membership/webinars.

Wan (Broken Tooth) Kuok Koi and cryptocurrency-integrated 'e-junkets'



Source: Elaboration based on DRG white paper.

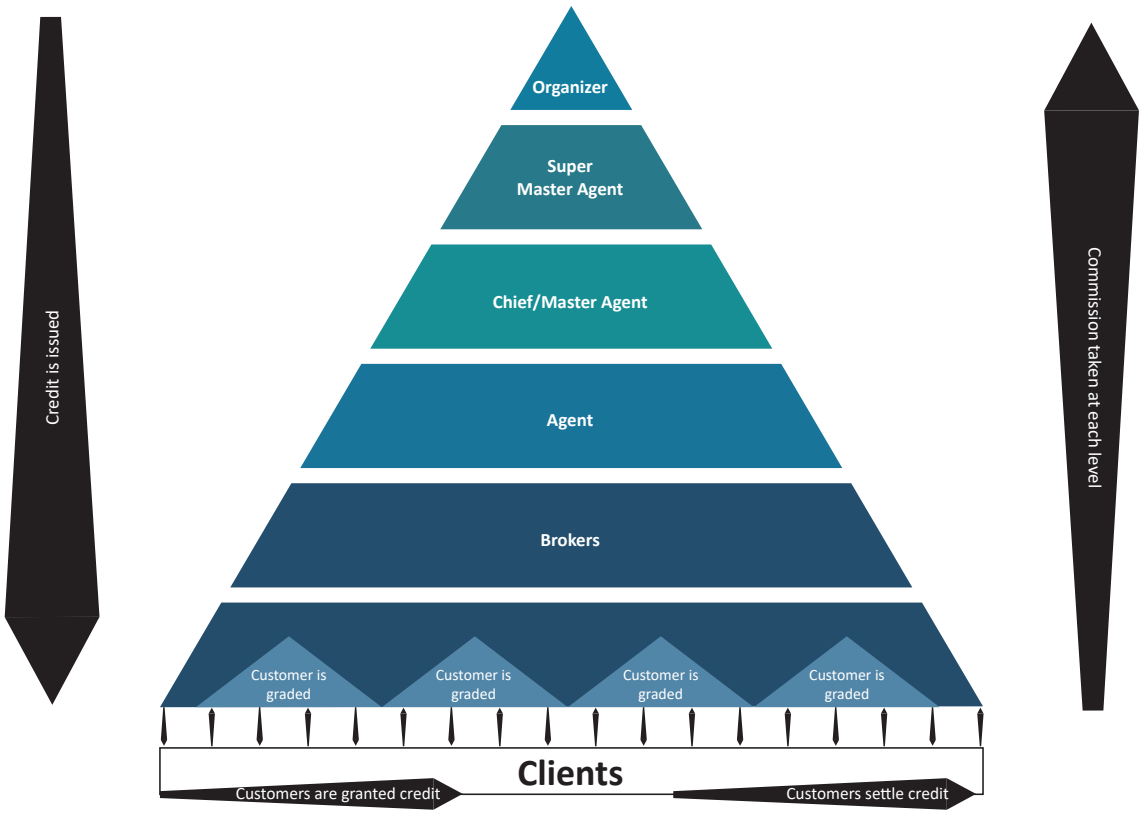
Among the best-known examples of criminal convergence around online casinos, e-junkets, and cryptocurrency relates to longtime senior member of the 14K triad, Wan Kuok-Koi, and the announcement of his 2017 Initial Coin Offering (ICO) for the 'HB Token' cryptocurrency, also known as 'Triad Coin', as well as his involvement in at least two other related projects, 'Dragon Coin' (DRG) and the Saixigang 'smart city' Industrial Park in Karen State, Myanmar. The Triad Coin ICO was reported to have generated the sale of 450 million tokens, raising US $750 million through Koi's company, World Hongmen Investment, in partnership with Internet Technology Company 1, which would develop and operate affiliated online poker tournaments.[110] Triad Coin traded exclusively on A.Top, an exchange launched by All In Group, a Hong Kong-based company registered in April 2018.[111] The group's sole shareholder was reported to be 3658 Investment and Management, a business partner of Internet Technology Company 1.

In practice, clients could purchase Triad Coin with another crypto or fiat currency, transferring it to the casino operator in exchange for casino credits logged on A.Top's 'Allchain' ledger. In turn, clients could effectively wager online, drawing down on the ledger for losses.[112] Similarly, Koi was associated with Macau Dragon, a company which launched the joint Dragon Coin (DRG) ICO with Thailand-based Holding Company 1 in 2018. The project, which has since been shut down, had planned to integrate cryptocurrency into high stakes international gambling via partnerships with various Macau SAR-based junket operators. According to the whitepaper issued by Macau Dragon,[113] the project aimed to reduce the 5-7 per cent fee historically incurred by VIP gamblers using junket-based offsetting arrangements, using blockchain technology to increase efficiency. The whitepaper states that players would exchange fiat into DRG which would then be converted into Dragon Chip non-fungible tokens which could later be exchanged back into DRG and cashed out for fiat and luxury prizes using their smartphone wallet, and does not include any information concerning measures to address related money laundering concerns.

Both Triad Coin and Dragon Coin exhibited similar market activity characterized by rapid price increases and equally dramatic decreases, culminating in a stoppage in trading activity. This indicates possibility of the crypto's use in a money laundering and/or so-called 'pump and dump' investor fraud scheme. Additionally, on 9 December 2020, the U.S. Treasury OFAC designated Koi as "a leader of the 14K triad, one of the largest Chinese organized crime organizations in the world that engages in drug trafficking, illegal gambling, racketeering, human trafficking, and a range of other criminal activities, including bribery, corruption, and graft."[114] The U.S. Treasury also alleges that the Hongmen Association "has managed to co-opt elite figures in Malaysia and Cambodia" while establishing "a powerful business network involved in the development and launching of crypto currencies, real estate, and … a security company."[115]

115 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.
116 Ibid.
117 HB Token (Triad Coin) whitepaper. Accessed at: https://www.yibencezi.com/notes/79352.
118 Dragon Coin whitepaper. Accessed at: https://s3.amazonaws.com/drg-token/Whitepaper-Dragon.pdf.
119 U.S. Department of the Treasury, 2020. Available at: https://home.treasury.gov/news/press-releases/sm1206.
120 Ibid.

Figure 12. Traditional pyramid nature of illegal betting



Source: Elaboration based on Asian Racing Federation State of Illegal Betting Report, 2022 and UNODC internal threat analysis on casinos, money laundering and transnational organized crime in Southeast Asia, 2022.

Attractiveness of online gambling as a money laundering and underground banking method

Because of the various anonymous payment methods available and the fact that authorities have a very limited view of what goes on in an online gambling account, it is difficult to verify whether the gambling account is used for actual gambling or for laundering money and underground banking. The online gambling sector is also characterized by a non-face-to-face element, minimal compliance staff, and huge and complex volumes of transactions and financial flows, which are often international in nature.[121] The various jurisdictions involved and the limited extent to which the legislation between these jurisdictions is harmonized further complicate investigations. As DNFBPs, the sophistication of the compliance regimes instituted by online casino operators lags considerably behind those at banks, making online casinos attractive targets for criminals while enabling a 'heads-down' approach by operators.[122]

Based on an examination[123] of recent cases in multiple jurisdictions, the most significant AML vulnerabilities identified within the online casino sector in East and Southeast Asia and the Pacific include but are not limited to:

- **Non-face-to-face transactions (anonymity):** non-face-to-face business relationships can present unique AML risks around identification and verification of the customer registering for the online gambling account. While stolen identities have been frequently used for online gambling purposes, another vulnerability includes player profiles being set up with stolen IDs or given to a third party to access the account for the facilitation of transactions of high-risk clients including criminals, politically exposed persons (PEPs), or those subject to sanctions without the appropriate enhanced customer due diligence (CDD) procedures.[124]

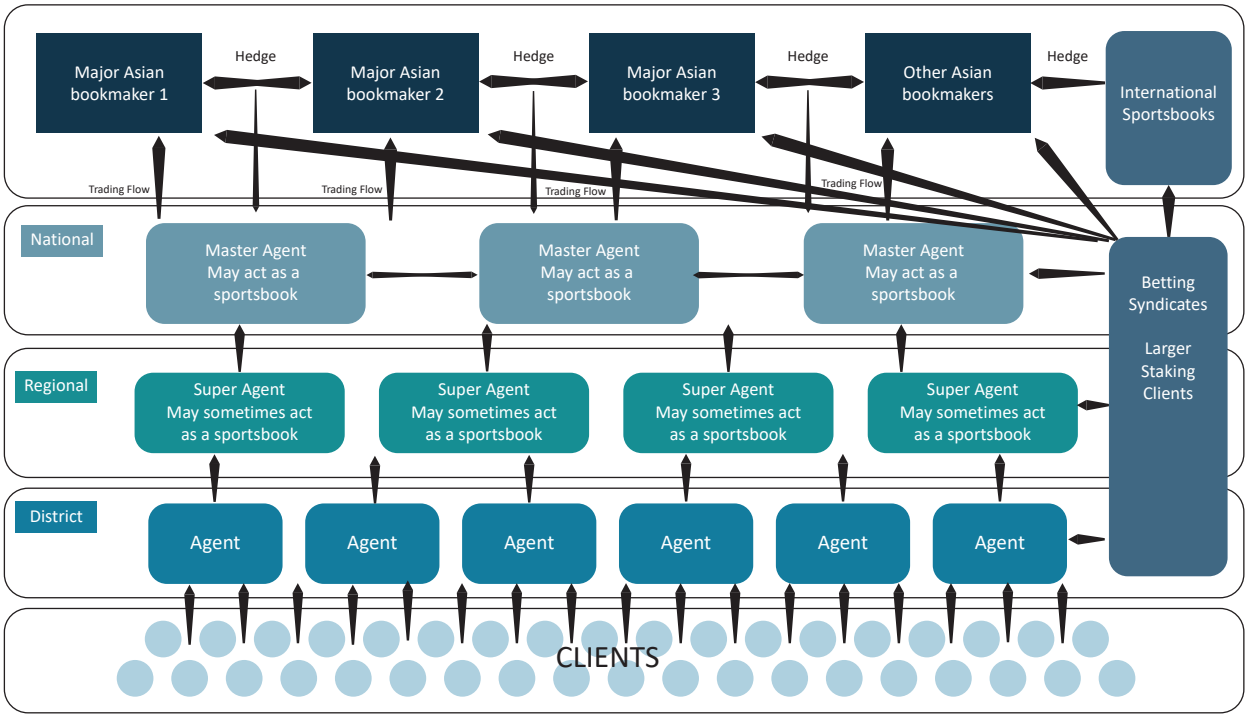
121 Online gambling as a money laundering method, Anti-Money Laundering Council of the Netherlands. Accessed at: https://www.amlc.eu/online-gambling-as-a-money-laundering-method/.

122 Ibid.

123 Findings based on series of UNODC meetings with law enforcement, financial intelligence, and regulatory authorities in Southeast Asia, 2023.

124 International Center for Gaming Regulation, Online Casinos, Alternative Payment Mechanisms and Associated Financial Crime Risks, 2023. Accessed at: https://www.unlv.edu/sites/default/files/media/document/2022-02/IGCR-OnlineCasinos-AlterPaymentMechanisms-FinanceCrimeRisks.pdf.

Figure 13. Pyramid nature of online betting markets in East and Southeast Asia



Source: Elaboration based on Asian Racing Federation State of Illegal Betting Report, 2022, and UNODC internal threat analysis on casinos, money laundering and transnational organized crime in Southeast Asia, 2022.

- **Third party transactions:** representing a vulnerability linked to the non-face to face nature of online casinos, third party transactions are among the biggest vulnerabilities where money deposited by one player could be withdrawn and deposited into another party's account. If Player A deposits via an e-wallet, they can then potentially withdraw to a crypto address that is owned by another party – this transaction could take place as payment for drugs, for example.
- **Miscoding transactions:** miscoding transactions have been relatively commonplace in the online gambling industry in East and Southeast Asia, used to avoid government scrutiny. For instance, a charge may appear on a gambler's credit card as 'flower shop' rather than 'online casino', making it difficult to identify the gambling transaction.
- **Gambling in exchange for luxury goods using in-game online gambling points:** a common service provided by e-junket operators in East and Southeast Asia in which in-game credit can be redeemed online and exchanged for high-value items including luxury watches, handbags, vehicles, vacations, and more.
- **Gambling in exchange for illicit goods using online gambling account[125]:** a money laundering scheme that has been observed being advertised by several land-based and online casino operators in high-risk jurisdictions in Southeast Asia. In this scenario, a buyer and a seller of illegal goods participate in the same game. Through a game or bet, the buyer will transfer funds to the seller, who then collects the funds from their payment account in exchange for the goods. The gambling account essentially acts like a bank account. Since the money technically came to the seller through betting, it cannot be easily traced to illicit activity. This typology has notably been attributed to major organized crime groups operating in the region and their use of junkets for disbursement of large payments.
- **Safe-keeping transactions using online gambling account[126]:** a gambling account held with an illegal, unregulated, or underregulated provider can be used exclusively for storing money and hiding it from the authorities. In this method, the money is being concealed and retrieved from the gambling account using either the same payment method or underground channels.

125 Ibid.

126 Online gambling as a money laundering method, Anti-Money Laundering Council of the Netherlands. Accessed at: https://www.amlc.eu/online-gambling-as-a-money-laundering-method/.

- **Widespread unregulated live-dealer proxy betting**[127]**:** authorities in Southeast Asia have reported widespread unregulated and unauthorized live-dealer proxy betting taking place within junket VIP rooms and online casino operations.[128] This betting modality, which poses high levels of money laundering risk due to challenges with customer identification verification, appears most common in countries including Cambodia, Lao PDR, Myanmar, and the Philippines, with many large operators in the industry possessing clear connections to known criminal networks (see below case study section). Coupled with offsetting arrangements through e-junkets and a loose regulatory environment, this can (and has) allowed unidentified individuals to transfer and launder vast amounts of funds from one jurisdiction into another with a click of a button or phone call.
- **Challenges of funds verification and commingling of proceeds of crime:** authorities in the region have reported one of the major challenges associated with online casinos to be difficulties in source of funds verification and misuse of online gambling platforms for commingling proceeds of crime with recreational gambling flows by organized crime groups.[129] This challenge is largely the result of the variety of available payment providers, including unregulated payment methods and financial intermediaries that are not subject to adequate AML controls, the proliferation of underground (unlicensed and/or unregulated) online gambling platforms, and general lack of customer due diligence underregulated operators within the regional industry. Authorities have also reported the use of smaller online casino platforms by larger operators affiliated with organized crime groups to further obfuscate the source of funds by funneling gross gaming revenues through smaller platforms at a fee of 1 to 2 per cent to add additional layers of commingling.[130]
- **Beneficial ownership:** the risks associated with criminal elements owning or infiltrating an online casino has been demonstrated by numerous cases and is deemed high by many authorities consulted during the development of this report (see below case study section). Moreover, recent cases and information shared by authorities indicate that numerous payment providers including VASPs have also been infiltrated by organized crime, providing an even higher risk for potential money laundering. The risks around criminal elements owning, controlling and/or infiltrating the casino along with criminal elements owning and/or controlling the payment provider should be actively managed and monitored.
- **Inadequate AML/CDD policy implementation:** discussions with law enforcement, financial intelligence, and regulatory authorities in Southeast Asia have revealed clear and growing concerns around the implementation of AML due diligence policies and procedures by online casino operators. The lack of understanding and lack of prioritization of risk management, internal controls, reporting, and anti-money laundering measures has been flagged to UNODC on several occasions.
- **Considerable gaps in awareness, regulatory enforcement and investigative capacity:** discussions with authorities in Southeast Asia, and particularly those in the Mekong region, indicate severely low levels of understanding and both investigative and regulatory enforcement capacity. Low levels of AML awareness in the context of online casinos and potential risks and vulnerabilities have also been observed.
- **Difficulties in prosecuting predicate offences:** while the use of casinos for money laundering is not new, the rapid proliferation of online casinos has made the method more widespread and caused significant challenges for law enforcement in both tracing proceeds of crime and subsequently prosecuting offenders. Authorities in the region have confirmed that their inability to trace funds laundered

127 Proxy betting has been seen as a 'competitive edge' for the casino industry in Southeast Asia. It involves one person somewhere outside a casino giving betting instructions to an accomplice (the proxy), inside. The proxy buys chips, places bets per instruction, and cashes in the winnings on their behalf. In more sophisticated operations, casinos can provide a live video feed of table games, meaning gamblers can watch the game played out from another jurisdiction using a computer or mobile device while instructing the proxy via mobile phone.

128 Meetings with law enforcement and casino regulators in Southeast Asia, 2023.

129 Meetings with law enforcement and financial intelligence authorities in Southeast Asia, 2023.

130 Anti-Money Laundering Office of Taiwan PoC, Risk Assessment, 2021. Accessed at: https://www.amlo.moj.gov.tw/media/20211832/2021%E5%B9%B4%E5%9C%8B%E5%AE%B6%E6%B4%97%E9%8C%A2%E8%B3%87%E6%81%90%E5%8F%8A%E8%B3%87%E6%AD%A6%E6%93%B4%E9%A2%A8%E9%9A%AA%E8%A9%95-%E4%BC%B0%E5%A0%B1%E5%91%8A%E8%8B%B1%E6%96%87%E7%89%88.pdf?mediaDL=true.

through this method has increased use of a legal technicality in which they are unable to prove beyond a reasonable doubt in court that the gambled funds correspond to the predicate offence. Some players may even divide funds into several different betting accounts to make their activity appear less suspicious and create further difficulties for prosecutors.

- **Broadening infiltration of organized crime:** advances in information and gambling-related technologies have significantly lowered the barriers to entry for organized criminal actors looking to enter Southeast Asia's booming online casino industry. These developments, together with the advent of the 'white-label' model (see below), has attracted a large number of new actors into the space while effectively decentralizing the regional money laundering business, creating huge challenges for law enforcement and financial investigators.

White-labelling

A major challenge across both regulated and underregulated gambling jurisdictions in Southeast Asia relates to so-called 'white-label' service providers. White-label gambling websites are similar to franchises, with operators being able to outsource every component of the business including complex betting software,[131] website design, customer data and relationship management, technical support, branding and marketing materials, and often also operating licenses from third-party service providers. White-labelling enables online casino operators to set up a gambling website in a matter of weeks, requiring virtually no bookmaking experience and technical expertise.

White-label providers are commonly based in Europe for advertising and offshore licensing purposes as well as less regulated jurisdictions including the British Virgin Islands, Isle of Man, Costa Rica, Cyprus, Curaçao, Malta, and Pacific Islands including Samoa and Vanuatu, among others, but have also been identified in several Southeast Asian countries including Cambodia, Myanmar, and the Philippines for physical operations such as large-scale live-dealer streaming.[132] Some of the largest online casino operators in Southeast Asia have also been observed to have moved into the white-labelling business in recent years, providing a very high level of access for organized crime groups seeking to establish a presence in the regional online gambling industry for the purposes of money laundering and underground banking.[133]

These developments are concerning as it is understood that unlicensed and unregulated online casino operators rely almost exclusively on white-labelling for their operations, and that those based in or targeting jurisdictions where gambling is prohibited, particularly in Asia, often turn to white-labels in an effort to confer legitimacy through sub-licensing partnerships with providers.[134] This, in turn, allows white-label-based online casino operators to appear and advertise as licensed, regulated entities across the region despite not being subject to any of the oversight of their white-label providers. It also enables them to market as official betting partners of major European sports teams and leagues including those in the English Premier League and International Basketball Federation, among others, while enhancing the brand's international exposure. Most concerningly, there have been several documented incidents of white-label service providers based in Southeast Asia being implicated in criminal cases relating to human trafficking, money laundering, and cyberfraud involving triad networks and other organized crime groups in East and Southeast Asia, among other jurisdictions.[135]

Recent cases and enforcement action against online operators and white-labels by gaming regulators outside of the region

Globally, enforcement actions are becoming more common as regulators apply their powers to non-compliant online gambling operators and white-labels. A sample of recent enforcement actions are detailed below and include reference to fines for AML failures and social responsibility failings (i.e., those failing to prohibit known problem gamblers).

131 Betting websites require highly complex software, providing functionality including odds-making and risk management, live video streaming and sports data feeds, customer relationship management and technical support, and payment processing, including cryptocurrency integrated solutions. Software is commonly licensed by operators for a flat monthly fee, a percentage of bettors' losing bets, or a combination of both. In the case of a complete white-label solution, a large proportion of turnover is funneled upstream from operators to the supplier or franchiser.

132 UNODC threat analysis on casinos, money laundering and transnational organized crime in Southeast Asia, 2022.

133 Asian Racing Federation Council on Anti-Illegal Betting and Related Financial Crime, The State of Illegal Betting, 2022.

134 Ibid.

135 Consultations with regional law enforcement and financial intelligence authorities, 2023.

Table 1. Recent enforcement action against online casino operators outside of East and Southeast Asia

Date and location	Breaches and fines
2023 (various jurisdictions in UK) Social responsibility and anti-money laundering failures[136]	William Hill issued £19.2 million fine, the largest ever penalty issued by the British regulator, for "widespread and alarming" social responsibility and anti-money laundering failures.
2022 (Isle of Man, UK) Social responsibility and anti-money laundering failures[137]	LC International Ltd., which runs 13 websites fined £14 million for social responsibility and anti-money laundering failures at its online and land-based business as well as £3 million for failures at its Ladbrokes Betting & Gaming Ltd. Operation which runs 2,746 gambling premises across Britain.
2022 (Jersey, UK) Gambling Commission	Annexio (Jersey) Limited trading as Affiliate Empire was fined £612,000 for both Social Responsibility code contraventions, and breaches of the license condition put in place to combat money laundering and terrorist financing.
2022 (Malta) Anti-Money Laundering Control Failures[138]	Online Amusement Solution Limited was fined with an administrative penalty of €386,567 by the Financial Intelligence Analysis Unit for anti-money laundering failures based on a site inspection of AML controls, policies and procedures.
2021 (Malta) – Tackling illegal operators[139]	The Malta Gaming Authority issued €2.43 million in penalties between January and June 2021, as part of an effort to ramp up enforcement in the sector and tackle unlicensed gaming operators. The gaming regulator issued 11 warnings, 20 notices of breach and sanctions and nine administrative fines. It also suspended two licenses and cancelled seven.
2021 (Netherlands) Unauthorized online gambling[140]	The Dutch Gaming Authority (KSA) imposed a €440,000 fine on Curaçao-based company Raging Rhino, which offered gambling to Dutch players through their website, advertising in Dutch language and using popular local payment platform iDeal to conduct its unlicensed online gambling business.

Rise of 'points running' syndicates, 'motorcades', and cryptocurrency

A key characteristic of online casino operations are the ever-evolving efforts of operators to hide flows of illicit funds from authorities. Together with enhanced enforcement of capital controls in some countries in East and Southeast Asia, recent past restrictions on cross-border movement of goods and people at the onset of the COVID-19 pandemic which largely limited the ability for illicit cash to be smuggled across borders and into casinos in East and Southeast Asia, resulting in a need for organized crime to innovate in how these funds could be transferred.

Authorities in the region have reported a growing number of methods being used by organized crime to facilitate the movement of illicit funds both through and into illegal online gambling platforms. Beyond extensive misuse of junkets by 'high-rollers', other common modalities include online casino websites utilizing vast underground (also known as white-glove) money laundering and banking networks such as so-called 'points running' or 'score running' (跑分) syndicates or 'water houses' (水房), money mule 'motorcade' (車隊) teams, and third- and fourth-party payment providers, sometimes referred to as running points platforms.[141] As of 2020, the Government of China

136 United Kingdom Gambling Commission, 2023. Accessed at: https://www.gamblingcommission.gov.uk/news/article/william-hill-group-businesses-to-pay-record-gbp19-2m-for-failures.

137 Isle of Man Today, 2022. Accessed at: https://www.iomtoday.co.im/news/gambling-firm-fined-ps17m-560218.

138 FIAU Malta, Administrative Measure Publication Notice, January 2022 https://fiaumalta.org/wp-content/uploads/2022/01/PublicationNotice-20220114.pdf.

139 Jessica Arena, "Gaming Authority issues €2.43 million in fines in the first half of 2020", Times of Malta, February 2021 https://timesofmalta.com/articles/view/gaming-authority-issues-234-million-in-fines-in-the-first-half-of-last.851114.

140 Curacau Chronicle, 2021. https://www.curacaochronicle.com/post/main/dutch-gaming-authority-fines-local-online-gambling-company/#:~:text=THE%20HAGUE%20%2D%20The%20Dutch%20Gaming,through%20the%20website%20luckydays.com.

141 Among the most common modalities today appear to be so-called fourth-party payments and running points platforms. Fourth-party payments are an evolution of third-party payments which, until recently, exploited gaps in transaction reporting in popular third-party payment apps, such as WeChat Pay and AliPay. While both platforms have since enhanced reporting of suspected gambling transactions at the request of Chinese authorities, fourth-party payment providers now typically install an additional intermediary between bookmaker, bettor, and third-party payment application in order to circumvent these measures and further obscure the nature of transactions.

estimated at least 5 million participants in this underground industry, totaling an estimated US $157 billion in capital outflows from China and have attributed it to the rise in illegal online gambling and telecommunications fraud.[142]

- **Running points syndicates** (跑分)**:** criminals in Southeast Asia often use points running syndicates, sometimes referred to as 'moving ants', to transfer stolen money between multiple bank or cryptocurrency exchange accounts as well as online casinos to obfuscate the source and destination of funds. This informal and often cross-border money transfer modality can involve groups of hundreds and sometimes thousands of individuals and has grown incredibly popular among youth due to underemployment in East and Southeast Asia who will provide their bank account(s) for use by points running syndicates for the purpose of account pass-through activities[143] (collecting and transferring funds of an unknown origin) in exchange for a commission. These systems are frequently used to collect money for criminal activities such as traditional predicate offences such as drug trafficking as well as cyberfraud and illegal gambling. Running points has been largely used to facilitate illegal online gambling to facilitate another layer of money laundering in which funds are routed through online gambling platforms and subsequently 'white-washed' by cashing in and cashing out through the platform to justify the source of funds as casino winnings. This strategy is commonly mixed with transaction miscoding to obfuscate use of the casino platform and depends on third- and fourth-party payment providers to help obscure the nature of transactions.

As third- and fourth-party payments have become better understood by authorities and more widely reported following 'Operation Chain Break'[144] in China, organized crime groups have responded by accelerating the integration of cryptocurrencies into their illegal betting operations, creating significant challenges for investigators across East and Southeast Asia. In recent years, law enforcement and financial intelligence authorities have reported the rapidly growing use of sophisticated, high-speed money laundering 'motorcade' teams specializing in underground Tether (USDT) cryptocurrency – fiat exchanges (卡接回U) across East and Southeast Asia. This has also included the mass recruitment of mule bank accounts across virtually all jurisdictions in the Asia Pacific region which can be purchased for as low as US $30 according to regional authorities.[145]

- **Money mule 'motorcades' (車隊) and the underground USDT – fiat exchange (卡接回U)**: these keywords can be found on many major platforms where criminals advertise 'services' for one another, including Facebook, Tiktok, and Telegram groups where advertisements for motorcade formation are listed. Motorcades are an extension of points running syndicates who offer sophisticated layering schemes by routing money through multiple bank or cryptocurrency exchange accounts for a percentage of the total laundered and transferred funds. Those individuals at the 'front of the car' who bear the most risk of detection have been seen advertising commission fees of between 20 to 40 per cent online.[146] UNODC has also observed a common practice of large motorcade teams working with others when processing very large contracts in order to improve concealment and effectiveness. According to conversations with authorities in the region, smaller online casinos are used down the money laundering chain by organized crime groups and illegal betting syndicates to further 'white-wash' funds.

Due to the rise of cryptocurrency-integrated motorcades and points running syndicates, in 2021 the Government of China banned cryptocurrency transactions, trading, and mining. The industry subsequently migrated to several jurisdictions globally, driving up already rising cryptocurrency adoption in several countries Southeast Asia in recent years.[147] At the same time, it is worth noting that while leading blockchain analytics

142 Anhui Provincial People's Government, Press conference for crackdown on cross-border gambling operations, April 2021. Available at https://www.ah.gov.cn/zmhd/xwfbhx/553972891.html.

143 This presents an increased ML/TF risk as transactions passing through multiple accounts and/or jurisdictions increase the difficulty for reporting entities and law enforcement to trace illicit funds.

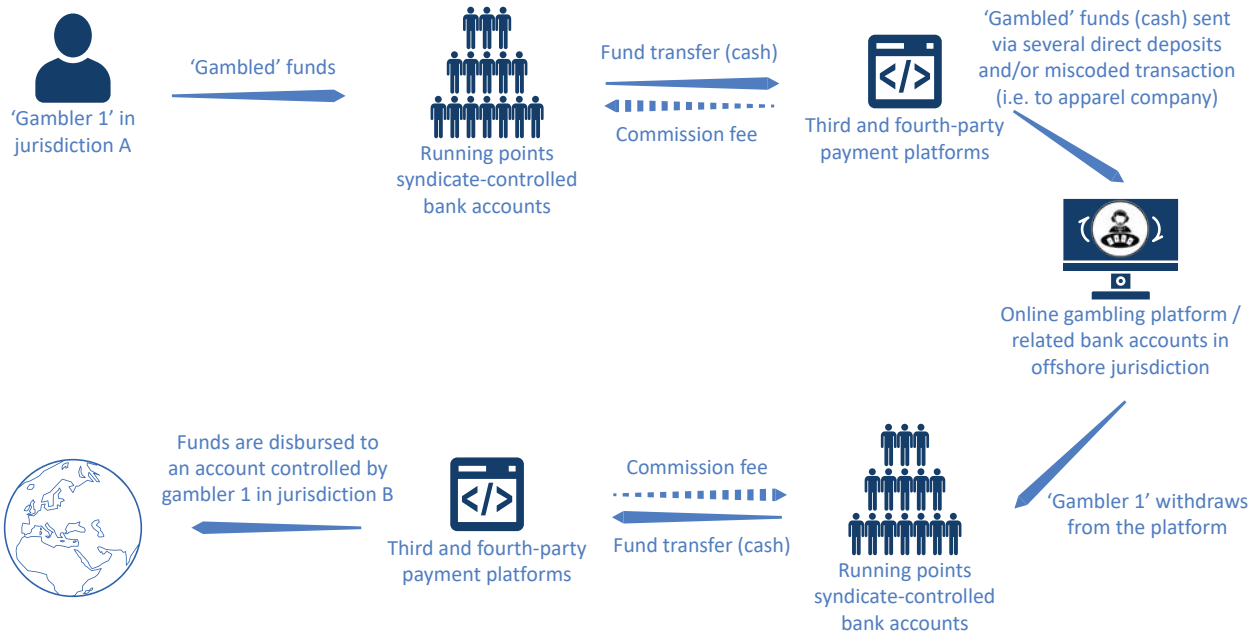
144 In response to large-scale underground banking utilizing third- and fourth-party payment platforms and the casino industry, the Chinese government initiated 'Operation Chain Break' in 2019 and has intensified its effort in subsequent years. The country's efforts to try to disrupt the flow of money from mainland China and Macau SAR to countries in Southeast Asia has included an August 2020 'blacklist' of casino destinations. For more details see below box story on the operation.

145 Meetings with regional law enforcement and financial intelligence officials, 2023.

146 Ibid.

147 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.

Figure 14. Simplified running points model for facilitating online gambling and money laundering



Source: Elaboration based on information published by law enforcement and financial intelligence authorities in China.

firms suggest that less than 1 per cent of all cryptocurrency payments are illicit,[148,149] in 2023 the Association of Certified Anti-Money Laundering Specialists (ACAMS) published an article arguing that cryptocurrency flows connected to organized crime are vastly underestimated.[150] Experts have cited a number of shortcomings related to existing analyses including massive gaps in crime attribution on the blockchain, confirmed cases of fabricated reporting by crypto exchanges, and wash trading which inflates crypto transaction volumes, thereby shrinking the portion of illicit transactions identified. This suggestion has been echoed by authorities in the region who have reported major challenges in blockchain investigation capacity alongside rapidly growing use of high-risk and underground cryptocurrency exchanges by organized crime, although successful law enforcement action remains very limited.[151]

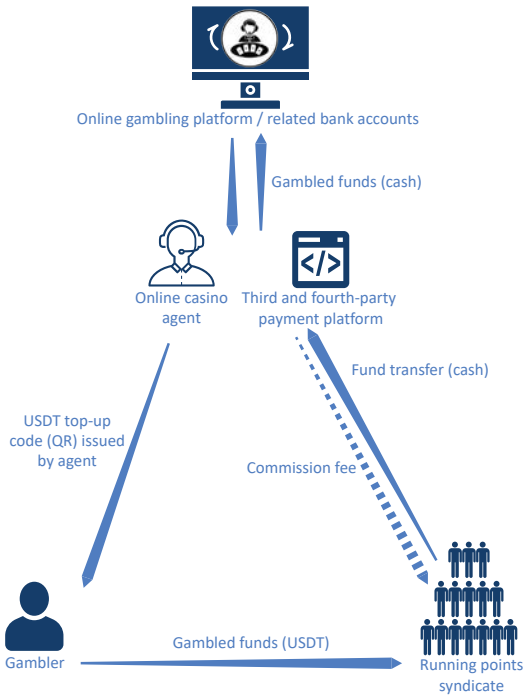
Money laundering using cryptocurrencies follows the general pattern of placement-layering-integration but with some specific features:

- Cryptocurrencies are anonymous at their point of creation therefore the placement stage of the money laundering process is often absent.
- It only takes a few seconds to create an account (address) and this is free of cost.
- It is possible to create a large money laundering scheme with thousands of transfers at a low cost and to execute it using automation.
- While stablecoins such as USDT remain the cryptocurrency of choice of organized crime in East and Southeast Asia, it can be easy to justify unexpected wealth through rapid increases in exchange rates of other virtual assets that exhibit exponential growth.

Online gambling platforms and e-junkets have emerged as among the most popular vehicles for cryptocurrency-based money launderers while also fueling the intensification of Southeast Asia's rapidly growing illicit digital economy, and particularly the regional cyberfraud[152] industry (see below). Using this method, funds are paid into an online gambling platform or an affiliate agent who arranges the transfer of in-game points online through some combination of identifiable or anonymous accounts. They are either cashed out or placed in bets, often in collusion with affiliates. Once the money in the gambling account is paid out, it can effectively be given legal status and integrated into the formal financial system and

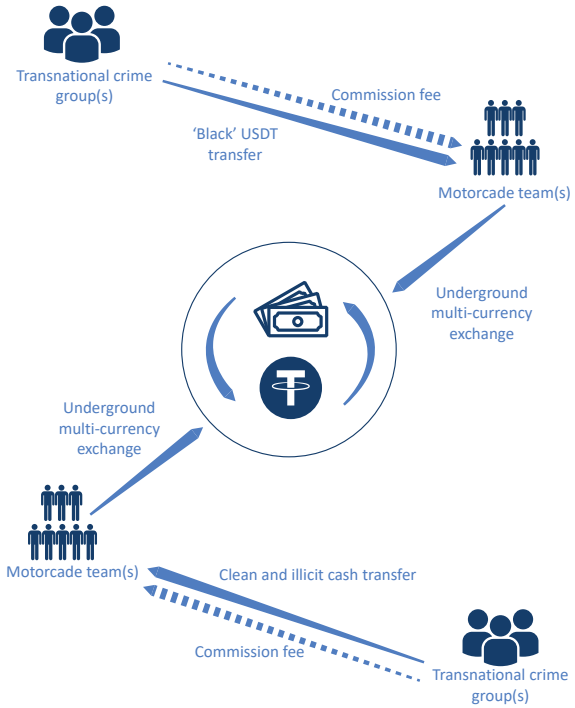
148 Chainalysis, Crypto Crime Report 2023.
149 TRM Labs, Illicit Crypto Ecosystem Report, 2023.
150 Association of Certified Anti-Money Laundering Specialists, 2023. Accessed at: https://www.moneylaundering.com/news/cryptocurrency-research-firms-vastly-underestimate-illicit-payments-critics-claim/.
151 Meetings with regional law enforcement and financial intelligence officials, 2023.
152 Concerningly, the vast majority of cyberfraud related cryptocurrency transactions are understood by regional law enforcement and financial intelligence agencies as well as industry experts to be withdrawn using major licensed exchanges.

Figure 15. Simplified USDT-based running points model for facilitating online gambling and money laundering



Source: Elaboration based on information published by law enforcement and financial intelligence authorities in China.

Figure 16. Simplified USDT to fiat 'motorcade' model for facilitating money laundering and underground banking



Note: Motorcades may also include fiat to fiat exchanges and other means of informal value transfer. They also regularly utilize online casinos in order to commingle proceeds of crime with recreational gambling flows.
Source: Elaboration based on information published by law enforcement and financial intelligence authorities in China.

economy. This growing money laundering method has been specified by the Financial Action Task Force (FATF) which has identified two situations in which online gambling platforms can be considered as a red flag: 1) funds deposited or withdrawn from a virtual asset address or wallet, with direct and indirect exposure links to known suspicious sources, including questionable gambling sites; and 2) virtual asset transactions originating from or destined to online gambling services.[153]

Proliferation of USDT-based money laundering networks

USDT, or Tether, is a popular stablecoin – a cryptocurrency pegged to and backed by fiat currencies like the U.S. dollar – which is reported as having the most liquid markets with an estimated US $20 billion daily trading volume at the time of writing.[154] USDT on the TRON[155] blockchain has become a preferred choice for regional cyberfraud operations and money launderers alike due to its stability and the ease, anonymity, and low fees of its Transactions.[156] Between September 2022 and September 2023, a recent fund audit of USDT-based transactions by one independent blockchain data analysis company found transactions totaling 17.07 billion USDT connected to underground currency exchanges, illegal commodity trades, unlawful collection and payment processes, and various criminal activities.[157] Law enforcement and financial intelligence authorities in East and Southeast Asia have also reported USDT among the most popular cryptocurrencies used by organized crime groups, demonstrated by a surging volume of cyberfraud, money laundering, and underground banking-related cases.[158,159]

153 Financial Action Task Force. Virtual Assets Red Flag of Money Laundering and Terrorist Financing, 2020. Accessed at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.
154 Coin Market Cap USDT analysis, 2023. Accessed at: https://coinmarketcap.com/currencies/tether/.
155 As of June 2023, TRON had over 165.5 million total user accounts, more than 5.81 billion total transactions, and over US $11.79 billion in total value locked (TVL), hosting the largest circulating supply of Tether (USDT) globally since April 2021.
156 Tether issues tokens on Bitcoin (Omni and Liquid Protocol), Ethereum, EOS, Tron, Algorand, SLP and OMG Network blockchains, making it easy to convert and ultimately more usable.
157 Bitrace Fund Audit, November 2023.
158 Meetings with regional law enforcement and financial intelligence officials, 2023.
159 Through ongoing analysis of case information and blockchain data, UNODC has observed several examples of regional money laundering and underground banking networks being shared between Mekong-based cyberfraud operations, drug traffickers, and more sophisticated cyber threat actors including the Lazarus Group.

Operation Chain Break

In an effort to combat the estimated RMB 1 trillion (US $157 billion)[160] in annual criminal proceed outflows from China tied to illegal cross-border gambling and related money transfer schemes facilitated by an estimated five to six million participants, in 2019 the Government of China launched a three-year campaign, codenamed 'Operation Chain Break'. While other anti-illegal betting crackdowns have taken place across China and the wider East and Southeast Asia region in recent years, 'Operation Chain Break' was broader in nature and scope than anything ever executed before. The campaign involved agencies including the People's Bank of China (PBOC), Central Cyberspace Office, and Ministries of Public Security, Tourism and Culture, and Finance, among others, which, together with local authorities in countries including Cambodia and the Philippines, as well as Macau SAR, intensified law enforcement action and regulatory pressures on casinos and junkets operating offshore.

In an effort to curb associated criminality including money laundering and kidnapping and reinforce capital controls, in 2019 authorities in China established a so-called 'blacklist' system to identify, designate, and investigate high-risk cross-border gambling tourist destinations, including specific casinos, junkets, underground banks, and especially online betting websites.[161] In tracing illicit financial flows into online gambling platforms, the PBOC cited several methods leveraged by organized crime to facilitate illegal cross-border gambling including running points syndicates, misuse of third and fourth-party payment platforms, licensed and unlicensed remittance service providers, and the use of cryptocurrency.

In connection with the operation, the PBOC publicly reported details of several associated 'funding chain' cases, highlighting the success and scale of the operation. For instance, in October 2020, the PBOC's Huizhou City branch dismantled a USDT-based cross-border online gambling operation, culminating in authorities arresting 77 suspects, shutting down three online gambling platforms, and recovering RMB 120 million (US $18.8 million).[162] In another case in April 2020, the Zhuhai Public Security Bureau of Guangdong uncovered an illegal online gambling business operated by a technology company presenting itself as a software developer. Authorities reported that the company was in fact a white-label service provider offering technical support and maintenance to at least 45 overseas operators in Southeast Asia, including in Thailand and Cambodia, with the company collecting over RMB 45 million (US $7 million)[163] in service fees.[164] The case was one of several related to a broader investigation in which authorities ultimately arrested four suspected organizers in Macau SAR in December 2020 who had attempted to cover up the sophisticated network of online casinos, including those impersonating licensed Macau gaming operators by masquerading as several technology and advertising companies in Macau SAR and Zhuhai, China.[165]

160 Anhui Provincial People's Government, Press conference for crackdown on cross-border gambling operations, April 2021. Available at https://www.ah.gov.cn/zmhd/xwfbhx/553972891.html.

161 The State Council of the People's Republic of China, official announcement, The Ministry of Culture and Tourism takes the lead in establishing a "blacklist" system for cross-border gambling tourism destinations. Available at http://www.gov.cn/xinwen/2020-08/27/content_5537828.htm.

162 Coingeek, China cracks down on extensive Tether-linked money laundering, 27 October 2020. Available at: https://coingeek.com/china-cracks-down-on-extensive-tether-linked-money-laundering/.

163 Ibid.

164 Asian Racing Federation, A Report of Blockchain and Cryptocurrencies in Illegal Betting, May 2021.

165 Inside Asian gaming, Macau's Judiciary Police arrests four over widespread "family style" online gambling operation, 14 December 2020. Available at: https://www.asgam.com/index.php/2020/12/14/macaus-judiciarypolice-arrests-four-over-widespread-family-style-online-gambling-operation/.

For instance, in 2022, police in China announced the results of a major law enforcement operation resulting in the dismantlement of a US $1.7 billion USDT-based money laundering network coordinated by the Horqin branch of the Tongliao Public Security Bureau in northeastern China.[166] Authorities dispatched more than 200 officers across 17 provinces and municipalities, arresting 63 suspects and seizing US $18 million in cash. The network was brought down over the course of the three-month operation, with the syndicate found to use USDT to launder illicit proceeds derived from illegal gambling and other crimes for domestic and foreign criminal groups. Authorities also reported that the gang had recruited individuals to participate in the money laundering network and register accounts

166 Ministry of Public Security of China, 2022. Accessed at: https://mp.weixin.qq.com/s/JO3lpwKXj66ef0wf9qo3vw.

with crypto exchanges through Telegram to facilitate pass-through activities.[167] The syndicate was further described to have a clear division of labor, with its operations stretching across China, with authorities notably reporting that two ringleaders had fled to Bangkok, Thailand prior to arrest, but eventually returned to China.[168]

Bulk cash seizure made during operation by Chinese police. Source: Ministry of Public Security, 2022.

In a similar investigation between December 2021 and July 2022, authorities in China dismantled a separate cryptocurrency-based 'points running' network that laundered a total of US $5.6 billion for criminal groups involved in telecommunication scams and illegal gambling. Police arrested a total of 93 suspects across Hainan, Guangdong, Fujian, and Gianxi in connection to the case.[169]

More recently, in November 2023 an investigation led by the United States Department of Justice in collaboration with cryptocurrency exchange OKX and Tether led to the voluntary freezing of US $225 million in USDT connected to a Southeast Asia-based human trafficking and pig butchering[170] cyberfraud ring.[171] In connection to the investigation, the Department of Justice also seized nearly US $9 million in USDT, with investigators tracing victim deposits that were laundered through chain-hopping[172] using several cryptocurrencies.[173]

167 Ibid.
168 Ibid.
169 Ministry of Public Security of China, 2022. Accessed at: https://mp.weixin.qq.com/s/1EHyqkKRd5HxPYXSaj19rg.
170 The pig butchering scam is a type of scam in which criminals lure victims into digital relationships to build trust before convincing them to invest in cryptocurrency using fraudulent cryptocurrency platforms.
171 Tether Operations Limited, November 2023. Accessed at: https://tether.to/en/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/.
172 Chain-hopping represents one of the fastest-growing money laundering typologies, involving the transfer of virtual assets from one blockchain to another, often in rapid succession, to impede the tracing of funds and make detection of illicit activity by exchanges more difficult.
173 United States Department of Justice, Press Release. November 2023. Accessed at: https://www.justice.gov/opa/pr/cyber-scam-organization-disrupted-through-seizure-nearly-9m-crypto.

Seized assets and bulk-cash reported during the Singapore raid. Source: Singapore Police Force, 2023.

In August 2023, authorities in Singapore announced the city-state's largest ever money laundering investigation, culminating in the arrest of 10 foreign nationals suspected of laundering the proceeds of overseas organized crime activities including online gambling and telecommunication scams.[174] Singapore police conducted a series of sweeping raids across the city-state consisting of more than 400 officers following analysis of suspicious transaction reports, seizing a total of US $737 million in cash and USDT, real estate, luxury cars, other assets including over 250 luxury handbags, jewelry, and watches, as well as various electronic devices and virtual asset seed phrases.[175] Authorities also noted that the suspects were in possession of a range of various passports from countries including China, Turkey, Cyprus, Cambodia, and Vanuatu, and had forged documents in order to substantiate the source of funds in Singapore bank accounts.[176] Additionally, nine of the ten suspects arrested appear to have been naturalized Cambodian citizens according to records published by Royal Decree in Cambodia,[177] with several previously investigated in China for related criminal activities.[178] Singapore authorities also brought additional charges relating to possession of criminal benefits from an unlicensed moneylending business in China as well as illegal online gambling operations in the Philippines against three of the ten suspects in the week following the operation, while at least one

174 Singapore Police Force, 2023.
175 A seed phrase is a series of 12 or 24 random words that provides the data needed to recover a lost or broken crypto wallet. It is also known as a mnemonic phrase and is best understood as a security measure for self-custodied digital assets.
176 Singapore Police Force, 2023.
177 UNODC analysis of criminal and citizenship records in China and Cambodia, 2023.
178 Boshan Branch of the Zibo Public Security Bureau, 2022.

suspect is further alleged to have been involved in operating illegal gambling websites in Myanmar using USDT.[179]

Convergence between online gambling, cyberfraud, and human trafficking

In recent years, a growing number of organized crime groups have established extensive criminal cyberfraud operations in several countries in Southeast Asia, with an estimated more than 220,000 people being held in situations where they are forced to carry out various cyberfraud and scam activities in Cambodia and Myanmar alone.[180] Together with enhanced law enforcement and regulatory pressures on the regional online casino industry, this development follows severe mobility restrictions in the wake of the COVID-19 pandemic in which criminal groups were forced to innovate, digitize, and diversify their business model in order to maintain revenues having invested hundreds of billions of dollars into the region's expanding casino industry. More specifically, both land-based and online operators have moved their bases of operation into loosely regulated and highly vulnerable jurisdictions including Cambodia, Lao PDR, the Philippines, and several border areas controlled by armed groups in Myanmar, in turn expanding their business lines into cyberfraud. Others have moved operations outside Asia including to Dubai, Africa, Eastern Europe, and the Pacific, and have also attempted to legitimize operations by investing into offshore licensed but underregulated gambling companies.[181]

These groups have taken advantage of the sprawling casino industry as well as SEZ infrastructure, advances in information technology and web design, and rising youth unemployment present in the region to set up sophisticated operations, using these venues as a legitimizing cover for their criminal activities. They lure labourers into trafficking using promise of lucrative employment and increasingly professionalized recruitment schemes, often using social media platforms such as Telegram, WeChat, TikTok, and Facebook. At the same time, victims of cyberfraud are targeted using data bought and sold on various dark web and clear web platforms

Malicious cryptocurrency trading application development advertisement targeting scam bosses 'based in major parks and special zones' stealing USDT cryptocurrency.

and lured to invest into professionally designed fraudulent investment platforms and increasingly fraudulent international banking applications. There are also growing signs of influence over local officials, as well as infiltration of key areas of the formal economy including money and virtual asset service providers, property developers, dealers in precious metals and precious stones, legal professionals and accountants, and trust and company service providers.

Underpinning and accelerating this fast-evolving and exploitative illicit digital industry, however, are the advances which have taken place in online gambling and related money laundering and underground banking systems in the region. Fundamentally, the dramatic growth and scale of the industry, demonstrated by rapid developments in new cyberfraud compound construction across the region, have required parallel developments in underground banking and money laundering capabilities, with mounting evidence pointing to casinos. The relationship between these various illicit industries and others, such as the region's highly lucrative synthetic drug trade,[182] has proven symbiotic, enabling the broader illicit economy to reach new heights.

179 Ibid.
180 United Nations Human Rights Office of the High Commissioner, Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia, 2023.
181 Asian Racing Federation, 2023.
182 UNODC Synthetic Drugs in East and Southeast Asia, 2023. Accessed at: https://www.unodc.org/roseap/2023/06/regional-synthetic-drugs-report-launch/story.html#:~:text=Released%20today%2C%20the%20report%2C%20%E2%80%9C,trafficking%20routes%20have%20shifted%20significantly.

In one Mekong country alone, estimates suggest that the cyberfraud industry generates approximately US $300 to $400 per day per worker, through approximately 500,000 workers,[183] however, other sources estimated the number to be between 80,000 and 100,000.[184] With that said, even the lower estimates would yield between US $7.5 and US $12.5 billion in raw earnings;[185] this compared to the country's GDP of just under US $27 billion in 2021.[186] In recent months, tens of thousands of cyberfraud labourers have also been identified and/or rescued in Lao PDR, Myanmar, and the Philippines following appeals from governments and crackdowns against offshore casino operators, cyberfraud compounds, and organized crime groups. In Cambodia alone, the Government of Indonesia reported repatriating +1,100 Indonesian nationals who fell victim to human trafficking and were employed by cyberfraud companies in 2023,[187] however data for the purpose of broader regional estimates remains limited. It is also worth noting that in 2022, the Federal Bureau of Investigation announced that victims had reported totaling US $3.3 billion from pig butchering, more than double the reported losses in 2021, with most that cases that have been unsealed and successfully geographically attributed linking back to cyberfraud operations based in the Mekong region.[188]

Several cases across a number of countries demonstrate the growing convergence between online gambling, cyberfraud, and human trafficking. For instance, in recent months authorities in the Philippines have conducted a series of raids across the country targeting cyberfraud operations embedded within licensed offshore gambling companies. Victims across three large and highly securitized compounds were largely found to have been lured into the country illegally and forced to work between 16 to 18 hours per day, often lacking food, and with pay withheld for failing to meet targets. Trafficked labourers were forced to engage in online game manipulation, investment scams and fraud, and romantic relationships with victim-targets from countries including Canada, the United States, and others in Europe and Asia.

Table 2. POGO raids between May – August 2023

Operator name	Date and location	Number of labourers[189]	Licensed POGO status
Xinchuang Network Technology	26 June – Hong Tai Compound, Las Pinas City	2,812	Licensed POGO
SA Rivendell Global Support	2 August – Pasay City	650	Licensed POGO customer relations service provider
CGC Technologies and Colorful and Leap Group Company	4 May– Clark Freeport Zone	1,090	Licensed POGO and licensed POGO service Provider

Source: Philippine National Police and PAGCOR, 2023.

The series of sweeping raids reveal several major issues within the Philippine offshore gambling operator (POGO) model relating to regulatory enforcement challenges including unauthorized sublicensing,[190] inspection and supervision failures,[191] and the infiltration of organized crime.

In addition to the abovementioned criminal activities, authorities identified several fugitives on site at the Hong Tai Compound in Las Pinas during the raid on Xinchuang Network Technology. More

183 UNODC, Internal Analysis on Illicit Financial Flows in the Mekong, 2023.

184 Ibid.

185 This is based on an assumption of 6-day work week, with 80,000 people at $300 per person or 100,000 people at $400 per person.

186 The World Bank, "GDP (current US$)", 2021. Available at: https://data.worldbank.org/indicator.

187 Ministry of Foreign Affairs of the Republic of Indonesia, official press conference, January 2024.

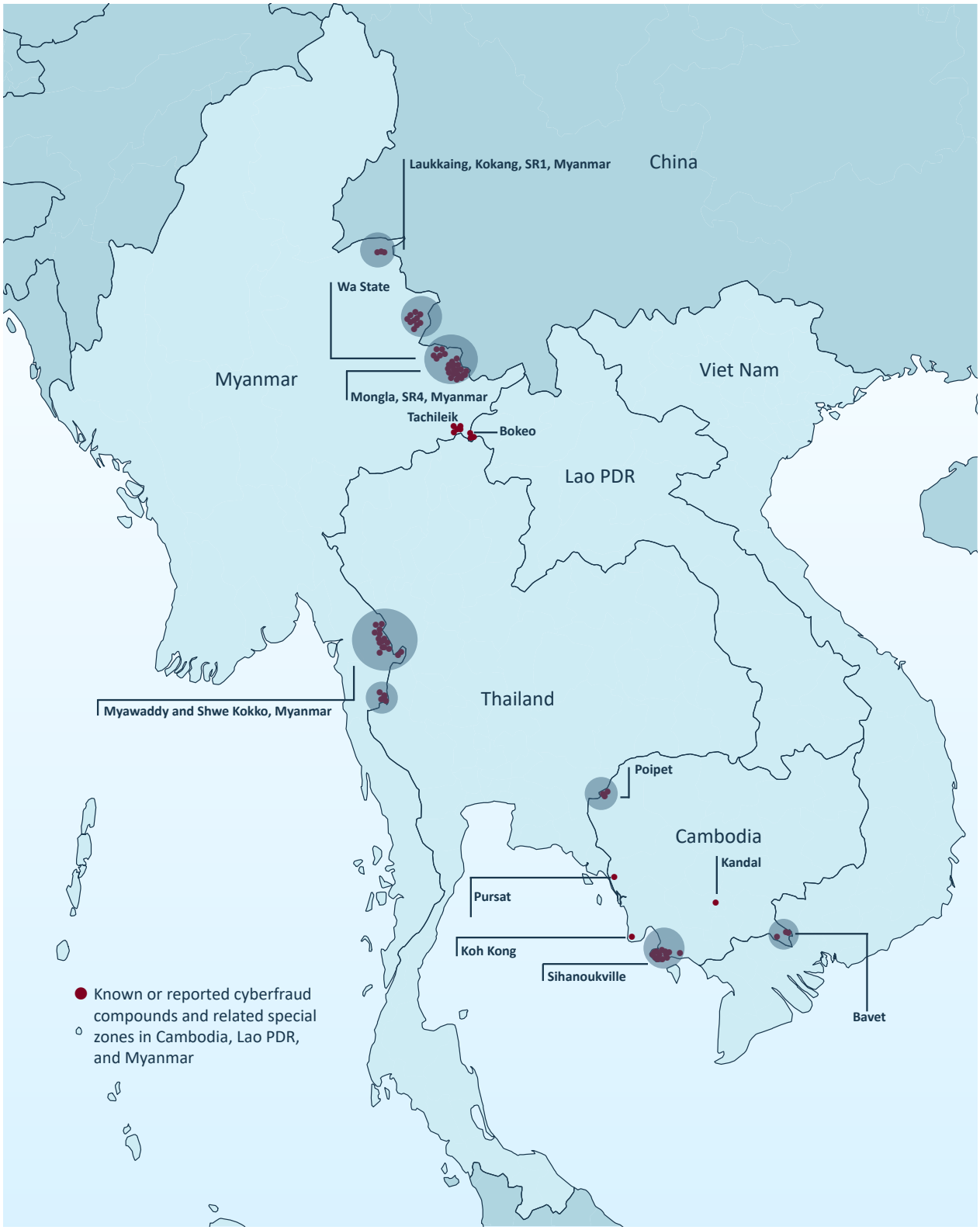
188 Federal Bureau of Investigation, Internet Crime Report, 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

189 While the vast majority of labourers identified on site during the raids were victims of trafficking for forced criminality, several individuals found in the raid of SA Rivendell Global Support were determined by authorities to be complicit in the operations, with some having previously been rescued from cyberfraud compounds in Myanmar by Philippine authorities.

190 Philippine casino regulator PAGCOR has acknowledged the common practice of sublicensing by 'master license holders' exploiting regulatory enforcement gaps relating to activities carried out by licensed service providers. In effect, licensed service providers would conduct unauthorized operations beyond their license including online gambling and cyberfraud, and other cybercrime activities, using their 'sublicense' for legal, regulatory, and fiscal cover. At the time of writing, PAGCOR has issued a freeze on all new licenses and implemented a new licensing scheme which reduces the number of service providers per 'master license holder' from 10 to 2, while placing all POGOs on a one-year probationary license until they are found compliant with new licensing and beneficial ownership requirements.

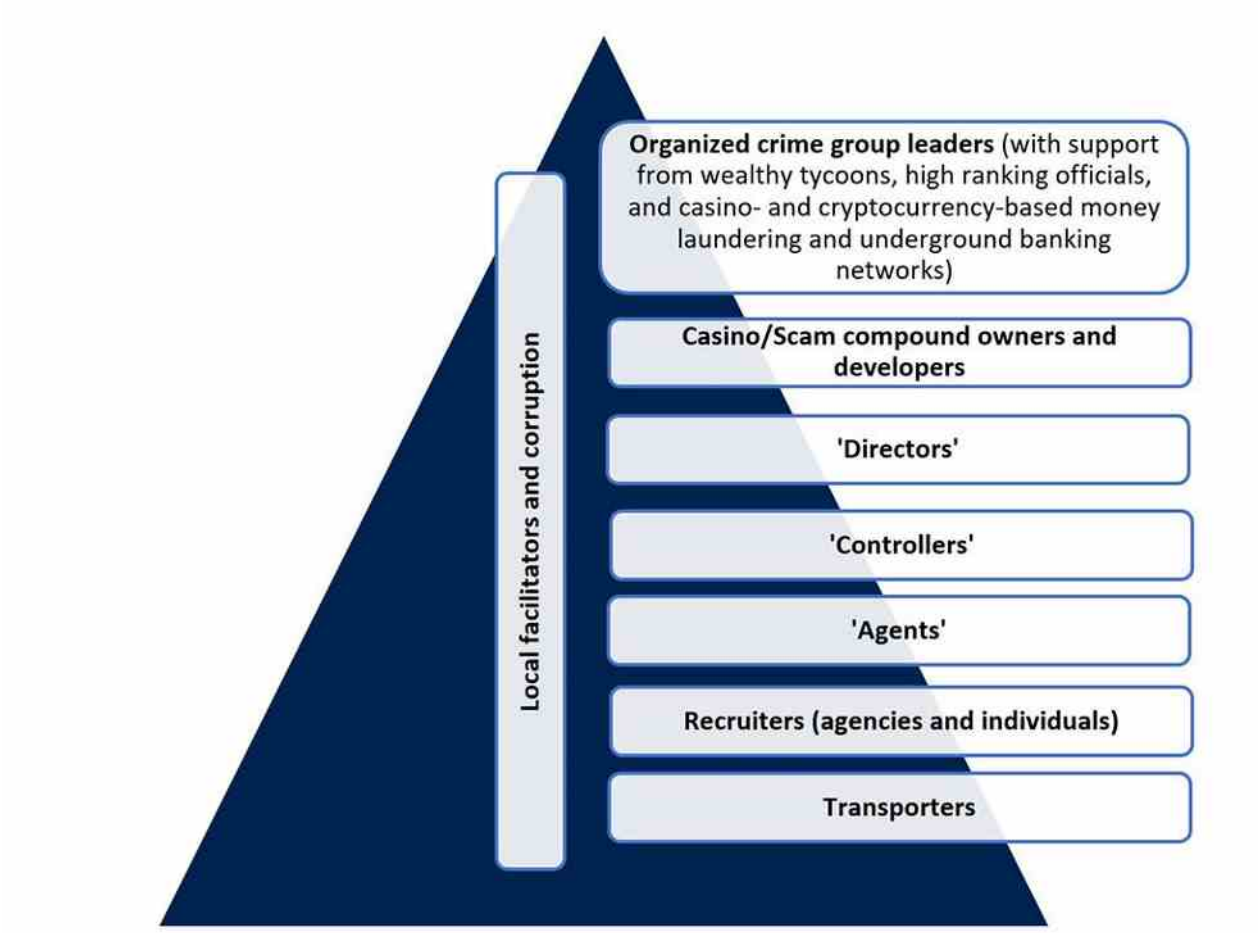
191 PAGCOR has also indicated significant difficulties in enforcing regulations and conducting inspections in licensed land-based casinos, VIP rooms, and offshore operators stemming who are regularly uncooperative and noncompliant with the regulator.

Map 3. Locations of known or reported compounds and related special zones in Cambodia, Lao PDR, and Myanmar, 2023



Note: The present map depicts locations of known or reported cyberfraud compounds and related special zones in Cambodia, Lao PDR, and Myanmar as reported by regional law enforcement authorities and may be subject to change given the evolving situation an ongoing law enforcement operations.

Figure 17. Hierarchy of offenders in trafficking for forced criminality



Source: UNODC Policy Brief on Casinos, Cyberfraud and Trafficking in Persons for Forced Criminality, 2022.

specifically, Philippine police arrested four nationals from China and three from Taiwan PoC who had allegedly worked in a fraud syndicate based within the Hong Tai online gaming compound which was used as a front to throw off authorities. According to information shared by the Ministry of Public Security of China, the individuals were wanted on detention warrants issued against them for criminal activities including contract fraud, drug trafficking, telecommunications fraud, and theft.[192] It is also worth noting that examination of another of the raided companies, SV Rivendell Global Support, using opensource IP abuse reporting database, AbuseIPDB, reveals nine malicious activity reports relating to various cyberattacks carried out by an IP address located in the Philippines and attributed to a company with the same name.[193] The reports were submitted from endpoints in Canada, the United States, the United Kingdom, Malaysia, and Viet Nam. Concerningly, SV Rivendell was inspected by the Philippine casino regulator just days before the raid according to authorities.[194]

Similar to earlier casino and cyberfraud compound displacements driven by law enforcement and regulatory pressures in Southeast Asia,[195] the ongoing crackdown in the Philippines is likely to have a profound impact on other vulnerable countries in the region. This strategy of jurisdiction shopping has proven common among high-level cyberfraud operators relocating deeper into the most vulnerable parts of the Mekong, and particularly armed group-controlled territories of northeastern Myanmar including Kokang SR 1, Wa SR 2, Mongla SR 4, as well as Tachileik and areas in and around the Golden Triangle SEZ in Lao PDR.

192 Philippine Bureau of Immigration, press release, 2023.
193 AbuseIPDB. Accessed at: https://www.abuseipdb.com/check/58.71.82.247.
194 Meetings with national law enforcement and regulatory authorities, 2023.
195 UNODC, Internal Threat Assessment on Casinos, Money Laundering, and Transnational Organized Crime, 2022.

Image of Hong Tai compound and related press release. Source: Philippine Police and Philippine Immigration Bureau, 2023.

There is already strong indication of new, large-scale cyberfraud compounds and expansions of existing infrastructure being constructed in many of these areas, with regional law enforcement reporting a growing number of cases attributed to them.[196] For instance, in July 2023, authorities in Bangkok, Thailand arrested a group of 11 mixed Chinese, Thai, and Myanmar nationals, including the leader of a scam syndicate operating from a compound inside the Golden Triangle SEZ in Bokeo, Lao PDR on charges related to telecommunications fraud and money laundering.[197] The group, which targeted would-be gold investors using the Thai Crown Property Bureau to promise returns of 10 per cent or more, generated more than US $15 million in a five-month period, converting the proceeds into USDT cryptocurrency using underground exchangers and Thai money mule accounts which were hired for between US $90 to $120.[198] According to authorities, those charged had moved operations from Sihanoukville, Cambodia to the Golden Triangle SEZ following a law enforcement crackdown in September 2022, with the leader also making several trips to the Philippines, Tachileik and Myawaddy, Myanmar, and the UAE.[199]

196 Meetings with regional law enforcement and non-governmental organizations, 2023.
197 Consultations with regional law enforcement and financial intelligence officials, 2023.
198 Ibid.
199 Ibid.

Growing indication of generative AI use, deepfake fraud, and other malicious technology

Increasingly sophisticated AI-powered chatbots and deepfake[200] technology risk becoming a favoured tool for criminals engaged in cyberfraud. In addition to the threat of accelerating the automation capabilities of cyberfraud operations based in Southeast Asia, and particularly the Mekong region, there is growing indication of deepfake fraud being deployed to both perpetrate scams and bank fraud to bypass KYC measures. This poses a significant threat to individuals as well as the formal banking industry, leading regulators, law enforcement agencies, and financial institutions to take urgent action to protect consumers and financial integrity.

While available data is limited, a recent independent identity fraud study noted a 1,530 per cent increase in deepfake incidents in the Asia Pacific region between 2022 and 2023, representing the second-highest region by incidents.[201] Among the key findings, the report noted Indonesia, Hong Kong,

200 Deepfakes are synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another through the manipulation of facial appearance via deep generative methods. While the act of creating fake content is not new, deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content that can more easily deceive the viewer.
201 Sumsub Identity Verification Service, Identity Fraud Report 2023. Accessed at: https://sumsub.com/fraud-report-2023/?utm_source=pr&utm_medium=article&utm_campaign=fraud_report2023

Screenshot of 'face-swapping' product advertisements found within Telegram 'grey and black market' groups, 2023.

and Cambodia having witnessed a more than two-fold increase in identity fraud percentages over the past two years, noting cryptocurrency industry as the main target for AI-driven deepfake fraud, representing 88 per cent of all deepfake cases detected in 2023, while Viet Nam and Japan ranked the highest for the prevalence of deepfake fraud in the same year.

Advances in deepfake technology have given rise to more sophisticated and damaging cyberfraud schemes.[202] By using AI to create computer-generated images and voices that are virtually indistinguishable from real ones, fraudsters can execute social engineering scams with alarming success rates, exploiting people's trust and emotions. Among others, this includes sophisticated investment fraud and financial grooming including, 'pig butchering' and, increasingly, task scams,[203] sextortion, and schemes impersonating law enforcement officers and other government officials. Criminals also exploit stolen personal data from various sources including the dark web and so-called 'grey and black market' Telegram groups, using data mined social media profile information and photos, among other information, to create fake identities and 'masks' that can bypass facial recognition systems and KYC measures, adding to challenges related to money-muling, money laundering, and high-risk and underground banking. It is worth noting that authorities in the region have also reported indication of cyberfraud operations based in Southeast Asia rapidly diversifying their business model by expanding into the development of malicious mobile and web applications or malware, the broader blockchain gaming industry, online

202 Bloomberg Business, 2023. Accessed at: https://www.bloomberg.com/news/articles/2023-08-21/money-scams-deepfakes-ai-will-drive-10-trillion-in-financial-fraud-and-crime?srnd=markets-vp.

203 Task scams involve the online recruitment of victims for what appears to be a remote work scheme. Victims are ordered to carry out various online tasks including content engagement (liking social media posts, leaving automated reviews, etc.) in exchange for commission, however 'earning' more money requires layers of 'investment' into the tiered operation via cryptocurrency which is subsequently stolen.

bank fraud schemes, underground cryptocurrency exchange and payment services, and offering a broad range of cybercrimes as a service.[204]

Several reports of related cyberfraud incidents have been reported in countries including Canada, China, India, the Philippines, Thailand, Viet Nam, and the United States in recent months. In April 2023, Fuzou police and Chinese state media reported the first such incident in which an individual reported that he had received a WeChat video call from a close friend and remitted US $590,000 to the other party's account within 10 minutes.[205] The victim reported the incident to local police who were able to freeze most of the funds in cooperation with counterparts in inner Mongolia where the recipient bank account was opened. That same month, police in Anhui province of eastern China also detained scammers who tricked a man into transferring a large, undisclosed amount of money to a supposed friend using AI face-swapping and voice-synthesis technology.[206] While limited information has been reported by authorities elsewhere in the region, law enforcement officials have indicated they are monitoring the situation closely and anticipate this new modus operandi to cascade across the region.[207]

Developments and vulnerabilities in the metaverse

According to recent data, the market size of the metaverse[208] was US $65.5 billion as of 2022, consisting of over 400 million active metaverse users.[209] While mass adoption has not yet occurred, research shows that the metaverse has the potential to generate up to US $5 trillion in value by 2030,[210] making it an opportunity too big to ignore and likely to attract many new participants including innovative, opportunistic, and increasingly high-tech organized crime groups.

Due to the decentralized nature of the metaverse, challenges with identity and verification, tracing the origins of virtual assets, complicated legal issues, technological advancements, and a lack of uniform legislation, the metaverse presents numerous AML compliance concerns and risks. For instance, with no intermediary such as banks, the Metaverse runs on a decentralized paradigm where users deal with one another directly. Due to the lack of a central organization in charge of monitoring and regulating transactions, this decentralized nature makes it difficult to apply AML requirements.

As the metaverse gains popularity and grows in scale, it will become increasingly challenging to ensure that in-game metaverse transactions abide by AML rules and criteria without a centralized authority. Moreover, AML compliance mechanisms within the metaverse are also difficult to monitor and enforce as a result of the lack of centralized authority. Unlike banks and other financial institutions and organizations which serve as the gatekeepers for conventional financial systems and regulatory regimes, participants in the decentralized metaverse are solely accountable for adhering to and enforcing AML policies as well as reporting suspicious activity. It is also worth noting that participants in the metaverse frequently go by aliases or remain anonymous, making it difficult to determine their true identity, resulting in substantial issues for AML compliance.

With respect to jurisdictional complexities and cross-border transactions, it is important to acknowledge that the metaverse is a worldwide network. In traditional financial systems, it is already difficult to enforce AML laws across different countries, and this problem is exacerbated by the metaverse's decentralized and international character, especially for cross-border payments. It is also challenging to develop a cohesive approach to AML compliance in the metaverse due to the lack of standardized AML legislation and different legal frameworks across jurisdictions. The metaverse is also a rapidly developing environment distinguished by technological advancement. Financial products and digital asset types are continuously developing, frequently exceeding regulatory frameworks and AML compliance procedures. At the same time, the regulatory environment in the metaverse is hugely disjointed, with various levels of AML laws and guidelines in various jurisdictions. Businesses

204 Consultations with regional law enforcement and intelligence authorities, 2023.
205 China Youth Daily, Communist Youth League of China, 2023. Accessed at: http://zqb.cyol.com/html/2023-06/06/nw.D110000zgqnb_20230606_2-05.htm.
206 Ibid.
207 Meetings with international law enforcement and regional cybercrime authorities, 2023.
208 The metaverse is the emerging 3D-enabled digital space that uses virtual reality, augmented reality, and other advanced internet and semiconductor technology to allow people to have lifelike personal and business experiences online.
209 Statista Analytics, 2023. Accessed at: https://www.statista.com/statistics/1295784/metaverse-market-size/.
210 Mckinsey & Company, 2022. Accessed at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse.

Screen capture from Decentraland's ICE Poker metaverse casino, 2023.

operating within the Metaverse have difficulties as a result of the absence of standardization since they must traverse a variety of legal obligations and compliance standards.

While the metaverse remains largely in its infancy, there is growing indication of organized crime groups targeting business projects related to the broader online gaming industry, and particularly blockchain gaming, while several metaverse casinos have already emerged. For instance, one major metaverse casino claiming to be registered in a Southeast Asian country reported generating cumulative revenue exceeding US $40 million in the first three months of 2022. At the same time, the entity demonstrates a unique regulatory challenge given that it claims to neither enable fiat nor convertible virtual currency transactions. Instead, players can buy, sell, trade, and lend NFT's using the platform's play-to-earn model. As stated within a legal opinion embedded on the company's landing page, the metaverse casino platform "would generally not contravene [local] gambling laws [as]… there is no staking or wagering of money or money's worth."[211] While the no-stake approach of this particular casino may in fact be in line with local gambling laws and regulations, there are already several other metaverse casinos which empoy a more traditional gambling model in which players can convert fiat into a number of metaverse tokens in order to place a wager.

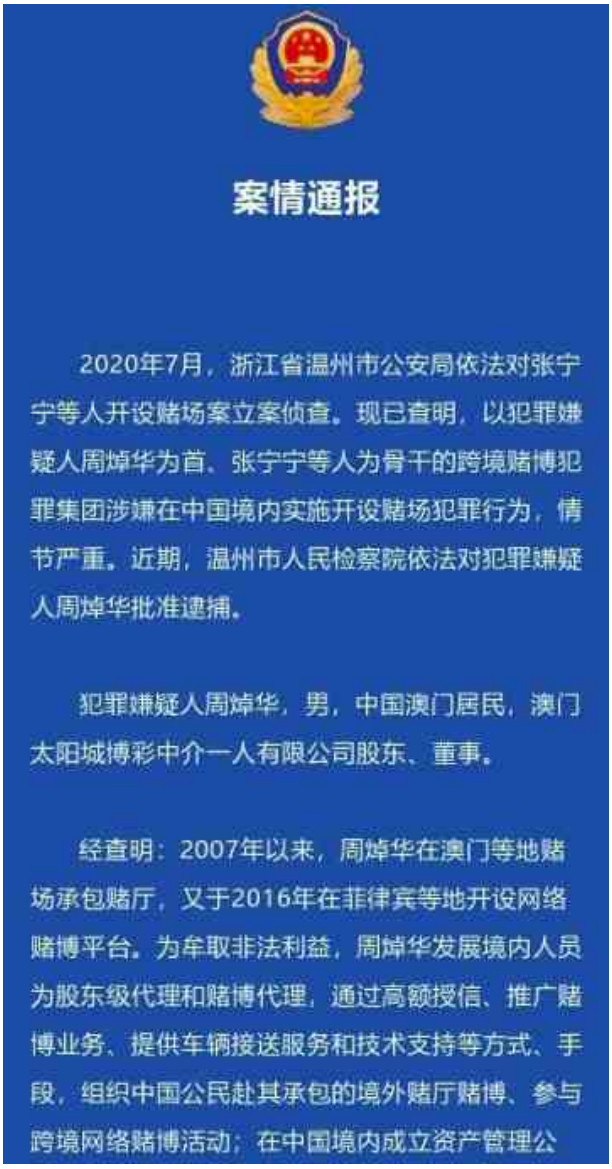
211 Official website of the metaverse casino platform, 2023.

Underground Banking and Money Laundering Methods: Case Studies

Alvin Chau Cheok-wa (周焯华) and Suncity junket

In November 2021, the Wenzhou City Public Security Bureau issued a warrant for Macau SAR-based junket mogul Alvin Chau's arrest, accused of running a massive illegal online and proxy betting operation as well as money laundering and leading an organized crime group. Following on from an investigation that started in 2019, authorities would allege that this activity was conducted through the cover provided by the Suncity junket and VIP rooms, at the time the world's biggest junket operator responsible for as much as 50 per cent of high-roller gambling turnover in Macau SAR.[1] Chau was convicted in Macau SAR in January 2023 and sentenced to 18 years in prison on over 100 charges relating to facilitating illegal bets exceeding US $105 billion between March 2013 and March 2021.[2,3] Data seized by authorities also show that between 2015 - 2019, Chau and Suncity had processed an estimated +300 billion yuan (US $42 billion) bet by online gamblers in China through the group's illegal offshore operations.[4]

In a related case, the Wenzhou Intermediate People's Court also convicted 36 individuals connected to the Chau-led syndicate, finding that the group provided cross-border currency exchange and settlement services and collected gambling debts through asset management companies and underground banks it had established on the



案情通报

2020年7月，浙江省温州市公安局依法对张宁宁等人开设赌场案立案侦查。现已查明，以犯罪嫌疑人周焯华为首、张宁宁等人为骨干的跨境赌博犯罪集团涉嫌在中国境内实施开设赌场犯罪行为，情节严重。近期，温州市人民检察院依法对犯罪嫌疑人周焯华批准逮捕。

犯罪嫌疑人周焯华，男，中国澳门居民，澳门太阳城博彩中介一人有限公司股东、董事。

经查明：2007年以来，周焯华在澳门等地赌场承包赌厅，又于2016年在菲律宾等地开设网络赌博平台。为牟取非法利益，周焯华发展境内人员为股东级代理和赌博代理，通过高额授信、推广赌博业务、提供车辆接送服务和技术支持等方式、手段，组织中国公民赴其承包的境外赌厅赌博、参与跨境网络赌博活动；在中国境内成立资产管理公

Source: Arrest Warrant Issued by Wenzhou City Public Security Bureau of China, November 2021.

1 Asian Racing Federation, 2023.
2 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.
3 Acusação do Ministério Público n.º: 1345/2022. Accessed at: https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.
4 China Central Television, Government of the People's Republic of China, January 2024.

mainland.[5] The Court determined that between 2016 and 2021, the Suncity-linked consortium had expanded to more than 280 mainland Chinese shareholder-level agents, more than 38,000 gambling agents/promoters, and more than 80,000 players, totaling at least US $160 million in illegal cross-border payments and transactions facilitated through Suncity's regional network of VIP rooms and associated online gambling and phone betting platforms operating within offshore casinos in jurisdictions including Cambodia, the Philippines, and Viet Nam, among others.[6] This was further substantiated in Chau's indictment[7] and conviction.[8]

Suncity is no longer a licensed Macau SAR junket operator, though various related entities trading under different names are still believed to be involved in the casino industry in Russia, the Isle of Man, the Philippines, and Viet Nam, among others.[9]

Mechanics

As revealed over the course of the investigation and trial, Chau was found to have led a side-betting business named 'Main Camp' which enabled large-scale underground banking, money laundering, and tax evasion. This was corroborated in testimony from Suncity executives including a former accounting director. Main Camp was based on multiplier betting,[10] also known as under-the-table betting or 'tok dai' (托底), and utilized existing Suncity corporate and technological infrastructure and resources to facilitate underground transactions concealed as legitimate gambling flows. More specifically, this included online and proxy betting facilitated through Suncity's regional network of VIP rooms and associated bank accounts and online gambling and phone betting platforms, as well as facilitating informal cross-border money transfers disguised as gambling credit issued to VIPs.[11] Illegal transactions were carried out through Suncity VIP cash cards, referred to as 'Operation Reserve Cards', and managed using specialized IT management systems referred to as 'RollsMary' and 'SunPeople' which recorded client data, betting volumes, credit issuance and debts, hotel room bookings, and more.[12]

Screenshot of Suncity Group online gambling platform and VIP Reserve Card. Source: Suncity Group Wechat.

In financing and expanding Suncity's illegal side-betting business, Chau targeted high-net worth VIP members in various jurisdictions and offered company equity and gaming commissions as an incentive to 'invest' and provide capital and liquidity to the side-betting companies he controlled, with these customers in turn becoming agents of Suncity.[13] Extensive discussions with law enforcement and financial intelligence officials indicate that Suncity also offered high interest rates in exchange for storing money with the junket, with many investors preferring the junket as opposed to traditional financial institutions. This was due to

5 Wenzhou City Public Security Bureau, 26 November 2021.
6 Ibid.
7 Acusação do Ministério Público n.º: 1345/2022. Accessed at: https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.
8 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.
9 Conversations with law enforcement and review of criminal intelligence documents indicate that Suncity was also active in Lao PDR and Myanmar, facilitating both illegal gambling and payment services for organized crime (see map 4 in regional overview).
10 Multiplier betting refers to a form of 'under-the-table gambling' in which a bet formally denominated at the casino gambling tables only represents only a fraction of the total amount of a private bet made between gamblers and junket operators to avoid gaming revenue levies. It allows clients to pre-negotiate their preferred payment method, betting currency, and cash-out method while increasing the commissions received by the junket promoter, and can be used as a tactic to conceal the total amount of money transmitted through the casino by an individual bettor and obfuscate the source and destination of funds. Such arrangements are understood to have grown in popularity due to most junket customers in Macau SAR originating from mainland China. These customers do not—and in any case cannot—bring money with them to play due to strict capital controls and a nation-wide gambling ban in mainland China, and instead rely on credit issued by junket agents. For instance, should a customer request a HK $1 million credit, the junket agent can request the casino to provide HK $100,000 worth of chips, with the understanding between the junket agent and customer that a ten times multiplier is in effect.
11 Wenzhou City Public Security Bureau, 26 November 2021.
12 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.
13 Ibid.

higher returns, greater flexibility, and virtually no due diligence and screening, effectively rendering it an international bank for criminals that needed to move money globally.[14]

In turn, whenever other Suncity VIP members wished to have (what appeared to be) gambling credit issued at one of the junket's overseas operations using the side-betting business, the Suncity exchange rate department would devise an offsetting arrangement[15] by selecting at random an agent in possession of both a Suncity currency account and bank account in the desired destination and currency where the funds may be disbursed.[16] The department then requested the agent to help conduct an informal money transfer by issuing the corresponding amount of credit. The fund recipient (gambler) at the desired destination would transfer funds to the agent's preferred account, and the Suncity currency exchange department would transfer the corresponding funds to the player's Suncity account, minus the junket fee (commission). The same process was reversed if funds needed to be moved from the respective destination country and into another jurisdiction, and as many as 100 calls per day are understood to have been received regarding facilitating such cross-border transfers prior to the closure of Suncity junket operations.[17]

Suncity is also understood to have developed a multi-billion-dollar real estate portfolio through its payment settlement arrangements which were devised to cover what appeared to be VIP customer losses incurred through gambling.[18] In effect, clients using this system would be able to bypass the formal financial system and informally transmit large amounts of value from one jurisdiction into another without moving any hard currency and with no scrutiny.

To reach a broader consumer base, Suncity increasingly turned to online gambling and e-junkets beginning in 2016. Using proprietary 'integrated entertainment platforms' including Easy Bet, Universal e-city, SCM Alliance e-city, and SCPP Alliance e-city, in-game points (non-fungible tokens) would be credited onto individual Suncity-linked online gambling accounts, with gamblers having to 'recharge' and 'buy code' by converting money from their Suncity VIP accounts and doing the opposite upon withdrawal. Points could be exchanged for chips, services, or cashed out in various currencies.[19] Usernames and passwords on these platforms would be linked to the client's original Suncity VIP account, and Suncity VIP account credit could be obtained using a number of methods including cash and various assets at the time of collection.

According to the initial indictment, Chau and Suncity associates involved in the Main Camp business had set up a network of front companies in mainland China including real estate and property development companies through which to launder the proceeds of their operation under various identities. These assets would ultimately be held and managed by the Suncity asset department. Other illicit proceeds would be placed, layered, and integrated through a sophisticated structure involving Suncity VIP room accounts, allowing related funds to appear as legitimate Suncity revenues.[20] At the same time, utilizing Suncity's regional network of VIP rooms and offsetting would enable billions of dollars in underground cross-border payments to be transmitted and effectively laundered into jurisdictions where Suncity had operations through traditional cash-in cash-out casino-based money laundering.

Confirmed links to organized crime

Australia

In recent years, Alvin Chau, Suncity Group, and several other junkets have been the subject of law enforcement and regulatory investigations and inquiries in Australia in relation to illegal bookmaking, drug trafficking, and large-scale

14 Meetings with regional law enforcement and financial intelligence authorities, 2023.

15 As described in the earlier regional section of this report, junket-based offsetting arrangements, also referred to as mirror transactions, are ultimately a means of junket financing in which the gambler deposits money into a junket account or stakes their local assets in one jurisdiction, and in turn may access this credit (minus a fee) at another. While this model should be limited to gambling, in practice it has become a favoured typology for underground banking and money laundering as a system of debits and credits allowing operators to move money quickly and informally below the radar of tax and law enforcement agencies. In short, offsetting is used as a means of transferring value between jurisdictions through a junket-gambler credit and debit relationship between entities in different countries. Organizations facilitating offsetting arrange for money debited from an entity in one jurisdiction to be credited to (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both.

16 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.

17 Acusação do Ministério Público n.º: 1345/2022. https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.

18 Meetings regional law enforcement and financial intelligence officials, 2023.

19 Ibid.

20 Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.

2018 CCTV footage showing Suncity staff dealing with large amounts of cash in the junket's private gaming salon at the Star in what appeared to be money laundering. Source: Star Casino Independent Review.

money laundering activities taking place at Suncity VIP rooms in Melbourne, Perth, and Sydney, culminating in the 2021 parliamentary inquiry into casinos.[21] As revealed during the inquiry, several junkets including Suncity and the Iek Junket[22] which Chau had financed, were noncompliant with both their junket operator agreements and associated service desk processes, as well as Australian anti-money laundering laws. This included practices such as Suncity staff having operated an unlicensed[23] cash service desk for both patrons and unknown individuals being helped to use CCTV blind spots to avoid security cameras. On numerous occasions, cash was observed being carried in and out in suitcases and backpacks, including by a Suncity limousine driver, during an internal Star casino investigation into Suncity's Salon 95 operation in May 2018, titled 'Operation Moneybags'.[24] Alvin Chau, Suncity junket representatives, and key players were also found to have made numerous multi-million-dollar transfers indicative of money laundering. These transactions took place between Chau's Suncity junket deposit account and various deposit accounts at Crown casinos held by key players on Suncity junket programmes, other junket operators, and third parties unrelated to the junket, further substantiating the charges that led to his conviction in Macau SAR.

Connections between the Suncity junket and transnational organized crime were further substantiated in an unsealed 2022 Securities and Investments Commission filing,[25] which stated that Australian federal law enforcement had found Chau to have received payment into his Star Sydney casino account in cash from an individual who had subsequently plead guilty to dealing in proceeds of crime.[26] The filing also cites a Suncity report developed by the Hong Kong Jockey Club, noting Chau's 'clear' association with triad societies, including the 14K triad, and that Australian law enforcement had informed the Club that "…during 2013 to 2015 Suncity was believed to be laundering up to AU $2 million per day using various money laundering methodologies, and...it was suspected that a significant amount of that cash was the proceeds of drug trafficking activities."[27] Moreover, the Australian inquiry itself identified Chau as a probable triad associate, citing casino due diligence documents raising "extremely serious concerns about the probity of Suncity and its founder Mr. Alvin Chau [indicating] ongoing connections with triads and the facilitation of organized crime by Suncity."[28]

More recently, in February 2023, Australian authorities dismantled a money laundering organization with links to Suncity, seizing properties, cryptocurrencies, and luxury assets worth over AU

21 Parliament of New South Wales, Australia. Casino Inquiry. 2021. Accessed at: https://www.parliament.nsw.gov.au/tp/files/79129/Volume%201%20-%20Inquiry%20under%20section%20143%20of%20the%20Casino%20Control%20Act%201992.pdf.

22 It is understood that Alvin Chau was the financier of the Iek Junket. This designated room was located on Level 1 of The Star's Darling Hotel. The Iek Junket was branded the Suncity Room and was for Suncity's exclusive use in the period from 1 July 2017 to 1 September 2019, as described in the New South Wales Casino Inquiry.

23 As part of the junket arrangement, Suncity was prohibited from exchanging any cash for chips and retaining cash from players at their service desk. An internal investigation by the Star found Suncity was however storing large amounts of cash in sports bags on a balcony off its gaming room and staff were frequently exchanging casino chips for cash.

24 Australian Securities and Investments Commission, 2022. Accessed at: https://download.asic.gov.au/media/040cpjww/2022-12-12-statement-of-claim-sealed.pdf.

25 Ibid.

26 Ibid.

27 Ibid.

28 Parliament of New South Wales, Australia. Casino Inquiry. 2021. Accessed at: https://www.parliament.nsw.gov.au/tp/files/79129/Volume%201%20-%20Inquiry%20under%20section%20143%20of%20the%20Casino%20Control%20Act%201992.pdf.

Source: Seized assets under Operation Avarus-Midas, Australian Federal Police, 2023.

$150 million and charging nine suspects including a known business partner of Alvin Chau, under Operation Avarus-Midas.[29] The syndicate was designated as an Australian Priority Organization Target for acting as an "unregulated multi-national bank, able to draw on cash reserves held in multiple countries around the world to facilitate transactions for criminal clients."[30] In doing so, it is alleged that the international 'shadow banking' organization had moved an estimated AU $10 billion offshore while amassing a property portfolio comprised of mansions, commercial properties, and hundreds of acres of land near Sydney's second airport.[31] According to authorities, the group enabled multiple transnational organized crime groups to launder funds derived from criminal activities, ensuring their money was circumvented or filtered through legitimate systems, including by exploiting casino junkets as well as daigous[32] and other informal value transfer systems.[33]

29 Australian Federal Police, 2023.
30 Ibid.
31 Ibid.
32 Underground banking often utilizes the 'Daigou' system to move funds. This involves cash from criminal activity being paid into the accounts of persons buying retail goods in one jurisdiction that are in demand in another, and subsequently exported for sale there, often in contravention of national customs controls. This activity requires a large number of bank accounts in the target country, often provided by overseas students (who may be told that they are providing money transmission services for other students, but are likely to know that the activity contravenes customs controls in their country of origin.
33 Australian Federal Police, 2023.

Figure 1. International controller money laundering networks[34]

Controller

Often based in an overseas location, the Controller is responsible for directing the activities of the network and liaising with organized crime groups who want to launder money. The Controller's business model relies heavily on their reputation and ability to guarantee the transmission of value from one jurisdiction to another. The Controller charges a commission for each transaction undertaken by their network, and also generates profit by negotiating the currency exchange rate in their favour.

Coordinator

The Coordinator in the network is responsible for managing the Collectors and Transmitters. They execute the instructions of the Controller and may be based in locally or overseas. This role is not always present in an international controller network and depends on the size of the group in a given jurisdiction.

Collector

The Collector in an international controller network acts upon the direction of the Controller or Coordinator and collects the proceeds of crime from organized crime groups generally through token-based[35] exchanges. They can then provide the money to Transmitters to process, or fill the role of Transmitter themselves to deal with the proceeds of crime.

Transmitter

Transmitters in an international controller network are responsible for getting the proceeds of crime offshore. This is usually accomplished through structured depositing into bank accounts, handing cash to a registered or unregistered remittance service, or to a third party to balance unrelated transactions undertaken through informal value transfer systems, including those operated by Hawala and other similar service providers.

Source: Australian Federal Police, 2023.

Beyond the range of demonstrated criminality related to Suncity and Alvin Chau, several other documented incidents point to extensive misuse of junkets by transnational organized crime groups in Australia. Among the highest profile relate to the Sam Gor (三哥) drug trafficking network, also known as 'The Company', with several junket operators, including Suncity, known to have had relationships with the syndicate. Most notably, one former senior member of Sam Gor was known to authorities to have been a silent partner of the Macau SAR-based Hot Pot junket, which operated at Crown Casino according to intelligence obtained and presented by Australian authorities.[36] As discovered during the casino inquiry, the Hot Pot junket was found to have generated hundreds of millions of dollars in turnover for Crown Casino through its operator, Ng Chi Un.[37]

Suky Lieu, who was convicted of drug trafficking and money laundering in Australia in June 2015 for having attempted to import a commercial quantity of heroin into Australia to the country from Viet Nam, was also tied to the country's junket business. Court records describing phone taps aired during the prosecution of Lieu and his associates detail how a junket was used to wire millions of dollars to Hong Kong SAR following instructions disseminated by one senior Sam Gor member. Moreover, Lieu's associate and former junket operator, Roy Moo, was also convicted of money laundering in 2013 and imprisoned. According to Australian authorities, while Moo was subsequently barred from attending Melbourne Crown Casino, he

34 An International Controller Network specializes in laundering the proceeds of crime between jurisdictions. These professional money laundering networks have extensive global reach and employ a variety of money laundering methodologies. The networks are hierarchical in nature and consist of a number of defined roles, consisting of a controller, coordinator, collector and transmitter. At various levels, records are kept to enable the controller to balance transactions, manipulate cash pools, and keep track of remittances. The coordinators and collectors will keep ledgers or electronic records of transactions.

35 When criminal groups ultimately provide cash to the collector, the collector produces a bill with a unique serial number, and the criminal(s) is assured that the collector is the person meant to receive the cash – nobody else could have that bank note with its unique serial number. When the collector hands over the bill, that bill acts as a kind of receipt: the criminal(s) can show it to their boss in the event of a loss.

36 Bergin inquiry public hearings under section 143 of the *Casino Control Act 1992 (NSW),* Government of New South Wales, 2021. Accessed at: https://www.parliament.nsw.gov.au/tp/files/79129/Volume%201%20-%20Inquiry%20under%20section%20143%20of%20the%20Casino%20Control%20Act%201992.pdf.

37 Ibid.

continued arranging the laundering of funds back to Hong Kong on behalf of Sam Gor. Moo made several transfers to the Bank of China in Hong Kong from Crown Casino's bank account in Australia, specifically utilizing a VIP account owned by an Indonesian junket operator, the Madam Ang Junket Group, which employed him.[38] At the same time, footage of Moo taken in 2012 and presented during the casino inquiry, showed the junket operator collecting AU $191,000 in cash in a shopping bag and taking it to Crown Melbourne.[39]

Philippines

Prior to the arrest of Alvin Chau in December 2021, Suncity was a major player in the Philippine casino industry. At the time, Suncity was among the leading junket operators in the country, running half a dozen VIP rooms as well as an integrated casino resort being developed in Entertainment City, Manila, by Suntrust Homes.[40]

As described in the regional section of this report, in 2016, several Philippine-based casinos and junket operators and agents played an important role in laundering approximately US $81 million stolen in a in a Lazarus Group-attributed cyberattack from accounts of the Bangladesh Bank account held at the Federal Reserve of New York. According to filings by the Bangladesh Central Bank with the New York Southern District Court in January 2019, as well as records in the Philippines, Alvin Chau had been the recipient of a large portion of the stolen funds that were laundered through the Suncity junket in the Solaire Hotel and Casino.[41,42] More specifically, the documents confirm that the money launderers had exchanged Solaire Casino chips worth 903.7 million pesos or US $20 million for an equal amount of non-negotiable Suncity junket chips, which were then systematically transmitted through the junket as VIP rollings over several weeks and ultimately ended up in casinos in jurisdictions outside of the Philippines. This was later confirmed by Solaire's lawyer during the associated Senate Committee on Accountability of Public Officers and Investigations (Blue Ribbon Committee) hearings.[43] Beyond involvement in the Bangladesh Bank heist, Alvin Chau and Suncity are also understood to have helped facilitate sanctions evasion and oil smuggling using a sophisticated network of falsified vessel identities, ship-to-ship oil transfers, and various underground banking and money laundering schemes through Suncity associates connected to various sanctioned entities.[44]

Following Suncity's implication in the Philippine senate inquiry and growing law enforcement and regulatory pressures in both the Philippines[45] and China, in 2019 Suncity sold its Philippine-based proxy betting company to a fellow junket operator who was previously arrested for illegal betting in 2014 alongside an alleged senior 14k triad member who is understood to possess strong connections to the Hell's Angels outlaw motorcycle gang in both Australia and Canada, according to law enforcement sources.

While the company and platform were subsequently renamed to remove any association to Suncity, a Suncity executive testifying at trial in 2022 revealed that the company continued to receive 50 per cent of the business's profits and also paid staff salaries and other business costs associated with the operation.[46] At the same time, witness testimony also indicates that the Suncity I.T. team had created and maintained a new management system named 'Opsman' for the company's new ownership.

Following a series of complaints of alleged financial and investment irregularities against Suncity Group Manila, in 2021 the Philippine Amusement and Gaming Corporation (PAGCOR) Board of Directors designated a committee to conduct a

38 Ibid.

39 Supreme Court of Victoria at Melbourne, 2021. Accessed at: https://www.supremecourt.vic.gov.au/sites/default/files/2021-04/Crown%20Resorts%20Shareholder%20Group%20Proceeding%20Statement%20of%20Claim.pdf.

40 Ben Blaschke, Suncity Group issues US $148 million loan to Philippines subsidiary SunTrust for Manila casino development, Inside Asian Gaming, July 2020. Available at: https://www.asgam.com/index.php/2020/07/26/suncity-group-issues-us148-million-loan-to-philippines-subsidiary-suntrust-for-manilacasino-development/.

41 Ibid.

42 Ministry of Justice of the Philippines, 2022. Accessed at: https://elibrary.judiciary.gov.ph/assets/dtSearch/dtSearch_system_files/dtisapi6.dll?cmd=getdoc&DocId=93584&Index=*47d2af93eea3c41eede94fa5db1eb960&HitCount=16&hits=b2+d6+f5+13e+185+194+227+48f+699+784+7af+80b+845+9b7+b03+b16+-&SearchForm=C:%5celibrev2%5csearch%5csearch_form.

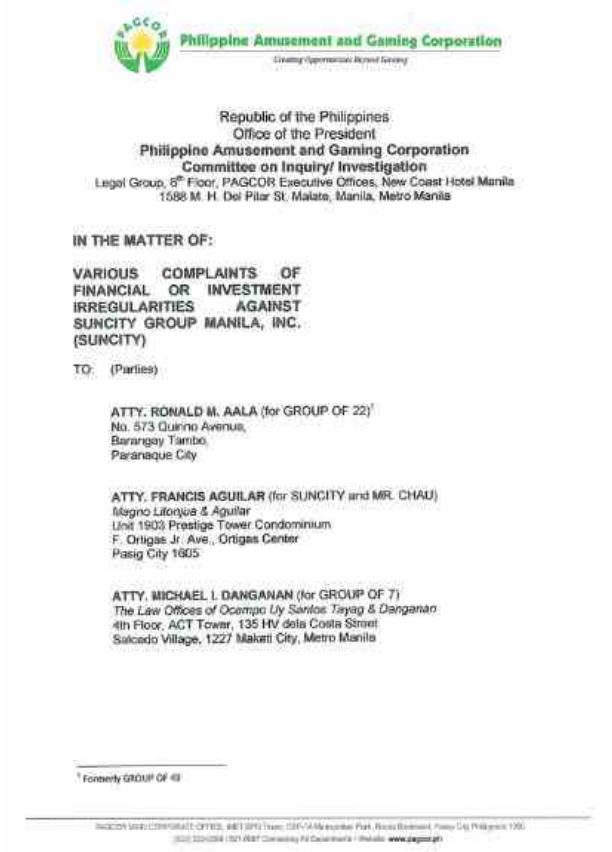
43 Senate Committee on Accountability of Public Officers and Investigations (Blue Ribbon Committee), 2016.

44 Examination of corporate records and vessel ownership documents as well as meetings with regional financial intelligence officials, 2023.

45 In addition to being implicated in the Bangladesh Bank heist, regional law enforcement authorities also informed UNODC that in 2019 they discovered a large number of junket operators offering proxy betting services through unlicensed live-dealer streaming services from their respective VIP rooms, posing significant money laundering risks.

46 Published witness testimony, public hearings transcript.

formal inquiry into the company.[47] In February 2022, the committee found Suncity and Alvin Chau unsuitable to hold any authority and license to operate a junket business in the Philippines.[48] In relation to the complaints filed against Suncity, law enforcement authorities informed that the majority of complainants were heavily connected to offshore online gaming operators based in the Philippines, with several complainants stating they chose to store large volumes of cash with the junket as a high return 'investment'.[49] According to law enforcement, most complainants involved in the case struggled to offer adequate explanations regarding the source of the funds in question.[50]



Philippine Amusement and Gaming Corporation

Republic of the Philippines
Office of the President
Philippine Amusement and Gaming Corporation
Committee on Inquiry/ Investigation
Legal Group, 8th Floor, PAGCOR Executive Offices, New Coast Hotel Manila
1588 M. H. Del Pilar St. Malate, Manila, Metro Manila

IN THE MATTER OF:

VARIOUS COMPLAINTS OF FINANCIAL OR INVESTMENT IRREGULARITIES AGAINST SUNCITY GROUP MANILA, INC. (SUNCITY)

TO: (Parties)

ATTY. RONALD M. AALA (for GROUP OF 22)[1]
No. 573 Quirino Avenue,
Barangay Tambo,
Paranaque City

ATTY. FRANCIS AGUILAR (for SUNCITY and MR. CHAU)
Magno Litonjua & Aguilar
Unit 1903 Prestige Tower Condominium
F. Ortigas Jr. Ave., Ortigas Center
Pasig City 1605

ATTY. MICHAEL I. DANGANAN (for GROUP OF 7)
The Law Offices of Ocampo Uy Santos Tayag & Danganan
4th Floor, ACT Tower, 135 HV dela Costa Street
Salcedo Village, 1227 Makati City, Metro Manila

[1] Formerly GROUP OF 49

Source: PAGCOR decision on Suncity Group Manila and Alvin Chau unsuitability, February 2022.

It is also worth noting that members of drug trafficking groups, including Sam Gor, have been known to frequent casinos with junket operators in the Philippines, a significant indication of money laundering. In 2018, Philippine authorities dismantled a synthetic drug manufacturing facility in Malabon City and arrested nine individuals.[51] According to law enforcement and criminal intelligence officials involved in the case, shipments of precursor chemicals sourced by the drug syndicate were arranged at a VIP room in Macau SAR while payments were subsequently arranged through a junket operator and disbursed using casino chips.[52] Concerningly, as reported by local law enforcement, those arrested were known to have frequented integrated casino resorts in the Philippines, namely the Solaire Hotel & Casino, where Suncity VIP rooms were operating at the time.

Cambodia

In 2018, Alvin Chau expanded Suncity into Cambodia, establishing a strategic business and consulting partnership with Golden Sun Sky Entertainment and CEO Dong Lecheng, who were both sanctioned under U.K. Global Human Rights Sanctions on December 2023[53] to develop and oversee the operational management a US $360 million beachside integrated resort casino in the coastal city of Sihanoukville.[54] That same year, Chau and Suncity signed a deal to establish a VIP room at Phnom Penh's Naga World casino, followed by the grand opening of the XiGang International Suncity VIP Club at the Xi-Hu Hotel in partnership with K99 Group and K99 Junket, with the signing ceremony attended by Alvin Chau, Dong Lecheng, and Facilitator 1.[55,56] The XiGang International Suncity VIP Club was established on the second floor of the Xi-Hu Hotel, consisting of 20 gaming tables in three rooms. Notably, the integrated resort was developed in part by Property Development Company 1 which holds the same business registration address as the Xi-Hu Hotel and was co-founded and co-directed by the late brother of Facilitator 1, Facilitator 2.

47 PAGCOR Suncity Committee, February 2022. Accessed at: https://www.pagcor.ph/regulatory/pdf/announcements/decision-regarding-suncity.pdf.
48 Ibid.
49 Discussions with regional law enforcement authorities, 2023.
50 Ibid.
51 Official briefing by regional law enforcement and criminal intelligence authorities, 2018.
52 Ibid.
53 Office of Financial Sanctions Implementation HM Treasury, Global Human Rights Sanctions, Financial Sanctions Notice, December 2023. Accessed at: https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf.
54 Suncity Group, Suncity Group Management and Consultancy Limited Announcing Strategic Partnership with Golden Sun Sky Entertainment Co., Ltd., September 2018. Available at: http://store.todayir.com/todayirattachment_hk/suncity/attachment/003258139-0.PDF.
55 K99 Group, 2019. Accessed at: k99group.com/news/17.html.
56 Suncity Group, 2019. Accessed at: https://mp.weixin.qq.com.com/s/74l9G7Pqg8kpTnvyahyiQ.

Signing ceremony between Alvin Chau, Dong Lecheng, and other associates, 2018, and Criminal verdict No. 63, 2018, issued by the People's Court of Mangshi, Yunnan Province of China. Source: Suncity Group, and People's Court of Mangshi, 2018.

With respect to the partnership between Suncity and Golden Sun Sky Entertainment, Dong Lecheng, known as Heng Tong in Cambodia following his naturalization in 2014,[57] is widely cited across Chinese criminal records for involvement in various illicit activities tied to his Yunnan Jincheng Group. For instance, a 2015 court document from the People's Court of Taoshan District, Qitaihe City, Heilongjiang, refers to a 2006 investigation into Lecheng and his partners for having established Maida Oriental Company in the Maizhayang Special Economic Zone located in Kachin State, Myanmar, and profiting by renting out and managing gambling halls illegally advertising in mainland China and facilitating cross-border gambling.[58] A separate court record from 2009 also details how the Group bribed a former deputy director of the Management Committee of the Border Cooperation Zone of Ruili City, China, to obtain a lucrative highway construction contract for its subsidiary company, Ruili Jingcheng Road and Bridge Construction Engineering.[59]

In March 2020, the World Bank issued a notice of uncontested sanctions regarding a subsidiary controlled by Lecheng, Yunnan Jincheng Construction Engineering.[60] In the notice, the Bank says the company engaged in sanctionable procurement practices in connection with the Zhejiang Rural Water Supply and Sanitation Project, a multi-million-dollar project funded in part by the World Bank.[61] The notice outlines Yunnan Jincheng's pattern of misconduct, noting in particular that Yunnan Jincheng engaged in fraudulent practices in bids for three separate contracts.[62]

More recently, in June 2023, the Yingshang County Public Security Bureau of Fujian issued a criminal notice following a multi-year investigation concerning illegal online gambling and telecom fraud operations housed in the Sunshine Bay Hotel (西哈努克海纳天) and infamous 'Chinatown' compound area in Sihanoukville. It is worth noting that Sunshine Bay was co-founded and co-directed by Facilitator 1, while a significant portion of the 'Chinatown' compound was developed by Dong Lecheng and Yunnan Jincheng Group. Sunshine Bay Hotel also shares partial common ownership with the K.B. Hotel, another sanctioned entity under UK Global Human Rights sanctions, part of what is better known as the 'Kaibo' area within the compound.[63]

57 Dong Lecheng became a naturalized Cambodian citizen under Royal Decree NS/RKT/0214/144, obtaining the name of Heng Tong on 03 February 2014.

58 People's Court of Taoshan District, Qitaihe City Criminal verdict, Tao Xing Chu Zi No. 64 (Chinese), 2015.

59 People's Court of Mangshi, Yunnan Province Criminal verdict, Cloud 3103 Xingchu No. 63 (Chinese), 2018.

60 World Bank, Notice of Uncontested Sanctions Proceedings, Sanctions Case No. 41, IBRD Loan Number 8424-CN, March 2020.

61 For more information on the project, see https://projects.worldbank.org/en/projects-operations/project-detail/P133018.

62 World Bank, Notice of Uncontested Sanctions Proceedings, Sanctions Case No. 41, IBRD Loan Number 8424-CN, March 2020.

63 Office of Financial Sanctions Implementation HM Treasury, Global Human Rights Sanctions, Financial Sanctions Notice, December 2023. Accessed at: https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf.

Source: Notice published by the Yingshang County Public Security Bureau, June 2023.

The compound area consists of some of the most well-documented,[64] violent, and heavily guarded fraud parks in Southeast Asia, serving as a human trafficking, online gambling, and cybercrime hub as widely confirmed by regional law enforcement authorities and testimonies of rescued victims. With respect to K.B. Hotel, the company was notably co-founded and directed by Facilitator 2 and Xu Aimin, a naturalized Cambodian national who is wanted[65] by Chinese authorities for leading an online gambling ring and laundering millions of dollars through multiple Hong Kong bank accounts. It is worth noting that the pair co-directed a second company, Investment Company 1, which corresponds to a Cambodian-based VIP Club and official Suncity partner. The Club claims to offer a one-stop premium service in partnership with Suncity VIP Club, offering VIP gambling credit arrangements, remittance advice, and other financial services, and listing 'Company1@Meg-Star.com' under its contact information. Incidentally, the verdict against Alvin Chau in Macau SAR repeatedly mentions the Meg-Star junket (鉅星國際) as a vehicle for laundering money.[66]

Together with Xu Aimin, both Facilitator 1 and Facilitator 2 also presided over the 2019 launch of the Junket Group 1 VIP room in the XI-Hu Hotel. In 2015, then-majority shareholder of Junket Group 1, who is also an alleged high-ranking triad member, was arrested by Hong Kong police for laundering US $231 million through a series of bank accounts in Southern China connected to property deals known to be the proceeds of organized crime. A 1992 United States Senate Hearing Report on Asian Organized Crime identified this individual as a high-ranking lieutenant of the Wo Hop To triad (和合圖)[67] which was further substantiated during an independent due diligence investigation report conducted by Las Vegas Sands, a partner of Junket Group 1, which found that the individual was "undoubtedly a leading member of the Wo Hop To Triad Society in Hong Kong SAR and Macau SAR."[68] In 2013, the individual was also implicated in the trial of former Birmingham City Football Club owner, Carson Yeung, who was convicted on five counts of money laundering totaling US $93 million, with some of this activity reportedly linked to Junket Group 1.[69]

64 UNODC, Casinos, cyberfraud and trafficking in persons for forced criminality in Southeast Asia, Policy Brief, 2023. Accessed at: https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Summary_Policy_Brief.pdf.

65 Hong Kong High Court Miscellaneous Proceedings No. 1072 of 2016, Secretary of Justice v. Xu Aimin and Another Party. Available at https://vlex.hk/vid/secretary-for-justice-v-845328111.

66 Acusação do Ministério Público n.º: 1345/2022. https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.

67 United States Department of Justice, 1992. Accessed at: https://www.ojp.gov/ncjrs/virtual-library/abstracts/asian-organized-crime-new-international-criminal-hearings-permanent.

68 International Risk Group. Accessed at: https://www.scribd.com/document/283047812/CCT-and-Reuters-Report#

69 Wanchai district court, Hong Kong SAR, 2013.

Xu Aimin, who was sentenced to 10 years imprisonment and is wanted by authorities in China, together with Associate 1 and Associate 2 and executives of Junket Group 1 during the VIP room opening in Sihanoukville, Cambodia, 2019. Source: Guangdong Group Junket VIP Club.

Similarly, in 2019, Facilitator 1 and 2, also presided over the grand opening ceremony of another Macau-based junket operator, Junket Group 2, at the Nanhai Hotel in Sihanoukville, together with the junket's senior representatives. The same 1992 Senate Hearing Report cited the director and controller of Junket Group 2 as a senior member of the Wo Hop To triad that is engaged in the "promot[ion] of heroin trafficking, illegal gambling, loansharking, extortion, and alien smuggling."[70]

Chau also established an extensive partnership with purported Heavenly Way Alliance (天道盟) triad member, Associate 1, of Taiwan PoC, and the Junket Group 2 VIP club, opening several joint VIP rooms in the Okada and City of Dreams integrated resorts in Manila, as well as MGM Macau and Macau Galaxy resort Junket Group 2 also operated within the Xi-Hu Hotel, and is connected to a hotel, casino, and tech-park in Bavet, Cambodia which has faced numerous allegations of human trafficking for forced criminality. In November 2022, Associate 1 was arrested by authorities in Taiwan PoC in connection to various business dealings with Associate 2, also of Taiwan PoC, on charges relating to money laundering and underground banking using online casinos, third-party payment platforms, and cryptocurrencies (more information available in below case study chapter on Taiwan PoC, Money Laundering Networks, and Transnational Organized Crime in the Mekong).

70 Ibid.

IN THE HIGH COURT OF THE
HONG KONG SPECIAL ADMINISTRATIVE REGION
COURT OF APPEAL
MISCELLANEOUS PROCEEDINGS NO 1072 OF 2016
(ON INTENDED APPEAL FROM HCMP 3237 OF 2013)

BETWEEN

Secretary for Justice	Applicant
and	
Xu Aimin	1st Respondent
Grand Dynasty Assets Limited	2nd Respondent

Before: Hon Lam VP and Hon Andrew Chan J in Court
Date of Hearing: 24 August 2016
Date of Judgment: 24 August 2016
Date of Reasons for Judgment: 29 August 2016

REASONS FOR JUDGMENT

Hon Andrew Chan J (giving the Reasons for Judgment of the court):

1. On 29 November 2013, a warrant of arrest was issued by a Magistrate against the first Respondent for 5 counts of "Money Laundering" contrary to s.25 of OSCO. It was alleged that the first Respondent was the ringleader of an illegal gambling network in the Mainland. The amount of suspected gambling money was over RMB 300 million.

2. Investigation by the Hong Kong authorities was sparked off by one Interpol Red Notice which the Hong Kong Police received in June 2013. In the Interpol Red Notice, it was stated that the first Respondent, being the Chairman of one gambling group, was wanted in China after a 10-year imprisonment sentence had been imposed on him by a Chinese court. The first Respondent held a Hong Kong Identity Card, Chinese Passport and Cambodian Passport, and was the sole director of the second Respondent, a BVI company.

Source: Hong Kong SAR Court of Appeal document related to Xu Aimin's online gambling case, 2016.

Fraud Park 1 is another venue characterized by confirmed incidents of unlicensed online casinos, cyberfraud, and forced labor located within Sihanoukville's 'Chinatown' compound.[71] It was developed by Dong Lecheng and his Yunnan Jincheng Group, and while the project was reportedly sold off to 'sub-owners' in 2018,[72] units within the Fraud Park 1 buildings are well-documented as having been rented to companies running a range of online gambling and cyberfraud operations.[73,74] Among them, K99 Group, which had developed several properties in the compound, was reported in October 2022 by Vietnamese state-owned media to have lured 65 Vietnamese nationals into the compound and forced them carry out cyberfraud following initial promises of high paying, legitimate employment.[75] More recently, in April 2023, a joint raid was conducted by the Sihanoukville Provincial Police and Provincial Prosecutor's Office on Xing Tian Di Casino following reports of unlawful detention,

71 Discussions with regional law enforcement authorities, 2023.

72 Khmer Times, August 2022. Accessed at: https://www.khmertimeskh.com/501137150/yunnan-jingcheng-group-co-ltd-strongly-deny-charges-of-human-trafficking-fraud-cyber-fraud/.

73 In October 2021, following a request from the Indonesian embassy, Cambodian police rescued 41 Indonesian nationals from Jinshui Park from forced labour conditions.

74 Beijing Communist Youth League, Beijing Youth Daily Newspaper, 2022. Accessed at: http://web.archive.org/web/20230321033531/https://freewechat.com/a/MjM5NzUyNjc0MA==/2650557728/1.

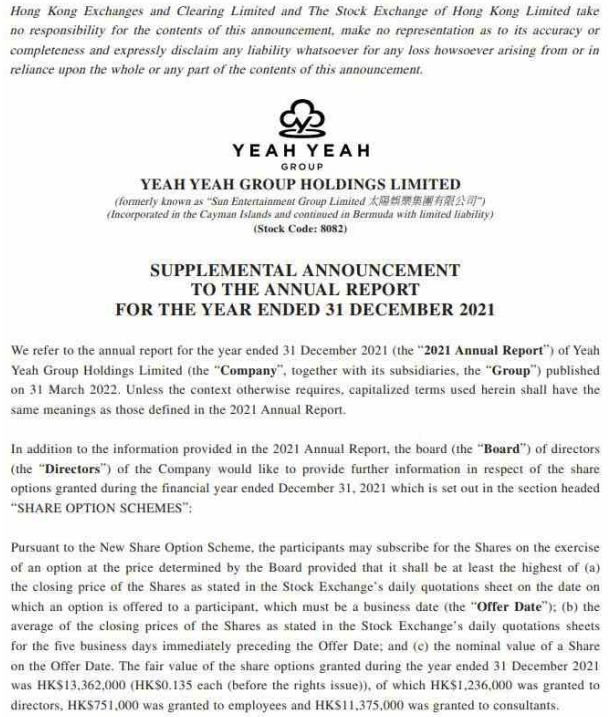
75 VietnamPlus, Viet Nam News Agency. Ministry of Information and Communications. October 28, 2022. Accessed at: https://www.vietnamplus.vn/kien-giang-tiep-nhan-them-cong-dan-viet-nam-tro-ve-tu-campuchia/825994.vnp.

torture, and extortion. Authorities confirmed the allegations on arrival, arresting several suspects at the casino belonging to Facilitator 1, and rescuing a victim from Taiwan PoC. Authorities reported that the victim had his passport confiscated when first arriving at work, with the company using the excuse of delays issuing his visa and work permit. According to victim testimony, the man was subsequently beaten, handcuffed, and forcibly indebted at gun point.[76] It is also worth noting that Xing Tian Di Casino shares the same registered address as the abovementioned Golden Sun Sky Casino.[77] Taken together, these records provide clear indication of significant criminal activity.

Suncity-controlled white-label in the Isle of Man

Following the arrest and conviction of Alvin Chau, several British Members of Parliament voiced concerns[78] through the All-Party Parliamentary Group (APPG) for Gambling Harm over apparent connections between Suncity and an Isle of Man-registered white-label company facilitating online gaming licenses for Asian-facing operators. More specifically, Chau and Suncity Group appear to have controlled White-Label Company 1 and two subsidiaries in Europe and Asia, as indicated by several documented connetions between the entities.

For instance, in August 2014, a press release published by one betting service provider following its announcement of a multi-year partnership with the European subsidiary of White-Label Company 1, stated that it "...is owned by [the company], part of the Suncity Group, the largest provider of live dealer casinos in Asia."[79] Moreover, an annual return and notice of change of directors filed by White-Label Company 1 with the Isle of Man authorities shows that Associate 3, a national of a Southeast Asian country, served as the Chief Executive Officer of the Asia-based subsidiary of White-Label Company 1 since 2019. In an official company filing, Associate 3 was given 637,000 share options as reward for "services in relation to the company's integrated entertainment platform and non-fungible token (NFT) production business" by Yeah-Yeah Group, formerly known as the 'Sun Entertainment Group Limited, part of Suncity Group, in a Hong Kong Stock Exchange filing from 2022.[80]



Hong Kong Exchanges and Clearing Limited and The Stock Exchange of Hong Kong Limited take no responsibility for the contents of this announcement, make no representation as to its accuracy or completeness and expressly disclaim any liability whatsoever for any loss howsoever arising from or in reliance upon the whole or any part of the contents of this announcement.

YEAH YEAH GROUP

YEAH YEAH GROUP HOLDINGS LIMITED

(formerly known as "Sun Entertainment Group Limited 太陽娛樂集團有限公司")
(Incorporated in the Cayman Islands and continued in Bermuda with limited liability)
(Stock Code: 8082)

SUPPLEMENTAL ANNOUNCEMENT TO THE ANNUAL REPORT FOR THE YEAR ENDED 31 DECEMBER 2021

We refer to the annual report for the year ended 31 December 2021 (the "**2021 Annual Report**") of Yeah Yeah Group Holdings Limited (the "**Company**", together with its subsidiaries, the "**Group**") published on 31 March 2022. Unless the context otherwise requires, capitalized terms used herein shall have the same meanings as those defined in the 2021 Annual Report.

In addition to the information provided in the 2021 Annual Report, the board (the "**Board**") of directors (the "**Directors**") of the Company would like to provide further information in respect of the share options granted during the financial year ended December 31, 2021 which is set out in the section headed "SHARE OPTION SCHEMES":

Pursuant to the New Share Option Scheme, the participants may subscribe for the Shares on the exercise of an option at the price determined by the Board provided that it shall be at least the highest of (a) the closing price of the Shares as stated in the Stock Exchange's daily quotations sheet on the date on which an option is offered to a participant, which must be a business date (the "**Offer Date**"); (b) the average of the closing prices of the Shares as stated in the Stock Exchange's daily quotations sheets for the five business days immediately preceding the Offer Date; and (c) the nominal value of a Share on the Offer Date. The fair value of the share options granted during the year ended 31 December 2021 was HK$13,362,000 (HK$0.135 each (before the rights issue)), of which HK$1,236,000 was granted to directors, HK$751,000 was granted to employees and HK$11,375,000 was granted to consultants.

Corporate records connecting Sun Entertainment to Associate 3 and White-Label Company 1.
Source: Companies Registry, Isle of Man and Hong Kong Stock Exchange.

Associate 3 also previously sat on the board of of a leading I.T. solutions provider and systems integrator which operates from Taguig, Philippines, while also serving as a Head of Development for a Singaporean gaming company. Associate 3's profile on the former's website states that he was "the CEO and Director for both White-Label Company 1, a B2B online gaming company ands 138.com, a B2C online gaming company, concurrently." 138.com[81] is the predecessor of 138Sungame, an Asian-facing online live-dealer casino which was owned and operated by Suncity Group in the First Cagayan Special Economic Zone in the Philippines,

76 Cambodia General Commissariat of National Police, April 2023. Accessed at: https://police.gov.kh/detail/6M9qGkFrFc1XiQKl4RRd?fbclid=IwAR2cvtIfdO0IeaJ6uC0ho2UEPpIBn8VOA2GQU6wTrE2MWnxNOUya5cP9Tjk.

77 Cambodia Ministry of Commerce, Online Business Registry. Accessed at: https://www.businessregistration.moc.gov.kh/cambodia-br-companies/viewInstance/view.html?id=48e104de66a7c46f0057fe540258afcddbc8ed467de4151aa706d7be037b99fa&_timestamp=3163463575750529.

78 Manx Radio, Isle of Man, 2023. Accessed at: https://www.manxradio.com/news/isle-of-man-news/mps-call-for-investigation-into-manx-company-with-alleged-links-to-jailed-billionaire/?fbclid=IwAR1iOoWemvt_2i1jK70lgcomK8odYGjswmzWLD26I9tFoZVeOdJ9oIehnYw.

79 Official press release of unnamed betting service provider, 2014.

80 Hong Kong Stock Exchange filing by Yeah Yeah Group Holdings (formerly known as Sun Entertainment Group) Ltd, 2022.

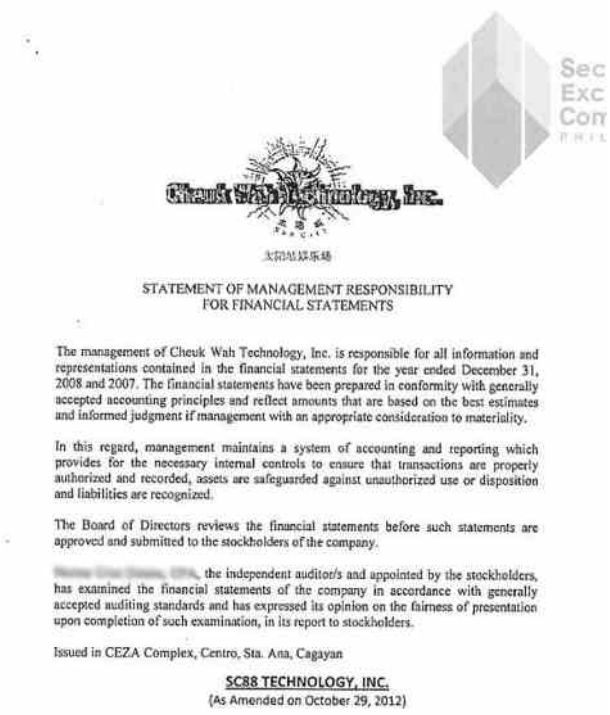
81 See 138.com's official YouTube channel. Accessed at: https://www.youtube.com/@138Sungame/videos

Webarchive of 138sungame gameplay, 2013.

as confirmed by former 138.com commercial director by a former 138.com commercial director and other industry experts.[82] The company was one of Suncity's first UK-licensed online gambling operation dating back to 2013 when the platform formed a partnership with high profile English Premier League football clubs. Corporate filings and legal documents reviewed for this report also indicate that Chau is linked to a group of Philippine-registered gaming companies connected to White-Label Company 1, including Sun Ventures Development and Cheuk Wah Technology (later renamed SC88 Technology) which had operated multiple Suncity online casino websites from within the Cagayan Special Economic Zone since 2008.

While beneficial ownership remains undisclosed at the time of writing, numerous suspicious Asian-facing offshore online gaming companies targeting jurisdictions where gambling is illegal such as China, Thailand, and Viet Nam, have been able to obtain UK gaming licenses through White-Label Company 1. These companies have subsequently been able to obtain lucrative sponsorship deals with professional football clubs in the UK, resulting in calls by officials to launch an investigation led by the British gaming regulator. In April 2023, the UK Gambling Commission (UKGC) also issued a £316,250 fine against White-Label Company 1, which runs 19 gambling websites at the time of writing, for anti-money laundering (AML) and social responsibility failures. The AML failures included not having a money laundering and terrorist financing risk assessment which adequately addressed risks; not adequately considering and mitigating the money laundering risks posed by their business-to-business relationships, and having ineffective policies and procedures in relation to due diligence undertaken prior to white-label agreements.

82 UNODC meetings with UK-based gaming industry experts, 2023.



STATEMENT OF MANAGEMENT RESPONSIBILITY
FOR FINANCIAL STATEMENTS

The management of Cheuk Wah Technology, Inc. is responsible for all information and representations contained in the financial statements for the year ended December 31, 2008 and 2007. The financial statements have been prepared in conformity with generally accepted accounting principles and reflect amounts that are based on the best estimates and informed judgment if management with an appropriate consideration to materiality.

In this regard, management maintains a system of accounting and reporting which provides for the necessary internal controls to ensure that transactions are properly authorized and recorded, assets are safeguarded against unauthorized use or disposition and liabilities are recognized.

The Board of Directors reviews the financial statements before such statements are approved and submitted to the stockholders of the company.

[redacted], the independent auditor/s and appointed by the stockholders, has examined the financial statements of the company in accordance with generally accepted auditing standards and has expressed its opinion on the fairness of presentation upon completion of such examination, in its report to stockholders.

Issued in CEZA Complex, Centro, Sta. Ana, Cagayan

SC88 TECHNOLOGY, INC.
(As Amended on October 29, 2012)

Source: Corporate documents for Cheuk Wah Technology and SC88 Technology, Philippines Security Exchange Commission.

As of January 2023, 10 Premier League football clubs were partnered with 8 Asian-facing betting companies licensed by White-Label Company 1.

Taiwan PoC, Money Laundering Networks, and Organized Crime in the Mekong

Taiwan PoC-based organized crime groups have a longstanding history in Southeast Asia, and particularly the Mekong region. These roots go back to the heroin trade in north Shan State, and in recent years have included industrial-scale synthetic drug production and trafficking, money laundering, underground banking, and increasingly online casinos, cyberfraud, and associated human trafficking. Authorities attribute and connect several cases in particular to the Bamboo Union (竹聯幫) and Heavenly Way Alliance (天道盟) (also known as the Celestial Way) groups.

In addition to the well-documented presence of trafficking and chemist networks from Taiwan PoC in and around the Golden Triangle area of Myanmar, in recent years Cambodia has been increasingly targeted by Taiwanese networks for the illicit manufacture and trafficking of synthetic drugs, and particularly ketamine, as well as money laundering. Seizures of the ketamine in Cambodia have increased significantly, amounting to nearly 2.8 tons in 2021 and over 13.5 tons of the drug in 2022.[1] During the week of 4 July 2022, for instance, Cambodian authorities arrested 11 suspects from China and Taiwan PoC, seizing a sophisticated clandestine ketamine laboratory together with several chemical storage facilities in Svey Rieng province approximately 10 km from the Viet Nam border.

Images of seized clandestine synthetic drug laboratory, Kampong Speu, Cambodia. Source: UNODC, 2022.

More recently, In July 2023, Cambodian authorities conducted a joint operation with U.S. and Taiwanese PoC law enforcement officials, seizing 789 kg of ketamine in Sihanoukville and arresting six traffickers including a believed high-level member of the Bamboo Union. Authorities stated

1 UNODC, Synthetic Drugs in East and Southeast Asia, 2023. Accessed at: https://www.unodc.org/roseap/uploads/documents/Publications/2023/Synthetic_Drugs_in_East_and_Southeast_Asia_2023.pdf.

that the drugs originated in Myanmar and entered Cambodia by transiting through Lao PDR to a storage facility in Sihanoukville, with the shipment ultimately destined for Taiwan PoC.[2] According to the Criminal Investigation Bureau of Taiwan PoC, the ringleader of the group, Chen Qixiang (陳啟祥), was a high-ranking member of the Heavenly Way Alliance triad.[3] In 2019, Taiwan PoC authorities also convicted high-profile trafficker Lin Hsiao-tao (林孝道). Hsiao-tao was reported by police as controlling approximately one-third of the drug supply in Taiwan PoC and was convicted for arranging large maritime shipments of methamphetamine, ketamine, and heroin from the Golden Triangle area of Myanmar through Cambodia and Thailand using a fishing fleet for shipment and high sea exchanges.[4] Law enforcement in the region have reported Taiwan PoC-based traffickers as receiving payments in part through the Suncity junket network.[5]

Unsurprisingly, the vast profits generated through the regional drug trade in Southeast Asia, and particularly in the Mekong, among other crime types, have necessitated parallel industrial-scale money laundering and underground banking operations to disburse payments and facilitate informal cross-border value transfers, and it is clear that both land-based and online casinos have been one of the preferred methods used to do so. In its 2021 anti-money laundering risk assessment, Taiwan PoC authorities stated the following in relation to online casinos which it designated as a 'very high' overall risk rating:

> "Criminal groups usually put illicit gains such as fraud and drug trafficking into gambling websites or third-party payment services in the form of stored value or exchange tokens, and exchange cash for chips, and then require the gambling website to remit the money to a designated account. The proceeds are mixed with legitimate funds to confuse the cash flow and create multiple breakpoints to achieve the purpose of [money laundering]. Furthermore, the gambling company also requires employees to open a payroll account in the bank, but the deposit book, card and account use rights must be turned over, which in fact become the company's nominee account, and the employees are carefully monitored, which shows the criminals' [money laundering] knowledge very capable.
>
> Illegal gambling companies need a large number of nominee accounts to convert gambling money for [money laundering]. The distribution of labor, people from mainland China are the capital owners, the IP address is set up in the Philippines, and Taiwan is used as the gambling [original equipment manufacturing] industry base, setting up offshore internet data center in Hong Kong SAR, Macau SAR, Southeast Asia or the United States, and use the Virtual Private Network … to avoid detection. The countries or regions involved in the inflow and outflow of criminal proceeds are all over Asia, mainly including Mainland China, Hong Kong SAR, the Philippines, the United Arab Emirates, Viet Nam, and Cambodia."[6]

Conversations with regional law enforcement have widely confirmed these findings and revealed extensive use of casinos and junket operators by drug production and trafficking networks based in Hong Kong SAR, Macau SAR, and Taiwan PoC in order to facilitate payments and underground cross-border money transfers. Notably, the abovementioned clandestine laboratory was located closed to the Cambodian casino enclave of Bavet, situated along National Road 1 at the Vietnamese border. Bavet has become a regional hub for Taiwan PoC-based organized crime groups involved in online gambling, particularly operations targeting customers based in Viet Nam where most forms of gambling for locals is illegal. This is concerning given that online casinos could be used to facilitate drug trafficking-related payments and money laundering, in addition to servicing actors associated with other crime types.

There are several notable cases relating to Taiwan PoC and online casinos, cyberfraud, and associated money laundering operations based in the Mekong

2 National Authority for Combating Drugs of Cambodia, August 2023.

3 Criminal Investigation Bureau, National Police Agency of Taiwan PoC, August 2023.

4 Hualien Branch of Taiwan High Court. Accessed at: https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=HLHM%2c109%2c%e4%b8%8a%e9%87%8d%e8%a8%b4%2c2%2c20210302%2c2&ot=in.

5 Meetings with regional law enforcement and financial intelligence authorities, 2023.

6 Anti-Money Laundering Office of Taiwan PoC, Risk Assessment, 2021. Accessed at: https://www.amlo.moj.gov.tw/media/20211832/2021%E5%B9%B4%E5%9C%8B%E5%AE%B6%E6%B4%97%E9%8C%A2%E8%B3%87%E6%81%90%E5%8F%8A%E8%B3%87%E6%AD%A6%E6%93%B4%E9%A2%A8%E9%9A%AA%E8%A9%95-%E4%BC%B0%E5%A0%B1%E5%91%8A%E8%8B%B1%E6%96%87%E7%89%88.pdf?mediaDL=true.

region. Most notably, at the request of Taiwan PoC police, in July 2023, authorities in Thailand arrested Associate 2 (referenced in above case study chapter on Alvin Chau and Suncity) for his alleged role in a regional telecommunication fraud and money laundering network which included leading a large-scale online casino operation, underground money and cryptocurrency exchanges, and forced labour.[7] Associate 2, who left Taiwan PoC in October 2022 after receiving a tip-off on his likely upcoming arrest and travelled between other Southeast Asian countries on a Cambodian passport issued in December 2021, was charged for his role in laundering an estimated US $86.62 million in addition to violating banking, organized crime, gambling, and fraud laws. Additionally, authorities later stated that Associate 2 had laundered as much as 20 billion Thai baht (approximately US $562 million) through his operation.[8]

Investigation chart shared by Royal Thai Police, 2023.

Authorities also seized luxury real estate and cryptocurrency wallets totaling US $6.4 million of USDT associated with the underground exchange and money laundering charges. Associate 2 was found hiding in a luxury condominium in Bangkok, Thailand, and extradited in August 2023.

It is important to note that Associate 2's arrest and extradition from Thailand followed charges announced by New Taipei City prosecutors in November 2022 which resulted in the arrest of his partner and mentor, Associate 1, an alleged Heavenly Way Alliance member and former business partner of Alvin Chau.

Information released by authorities in Taiwan PoC and Thailand confirm that Associate 2 headed several online gambling companies operating in Asia and Europe to support money laundering operations. More specifically, Associate 2 led a syndicate which controlled a conglomerate consisting of several international companies used for laundering the proceeds of online gambling and cyberfraud groups based in Cambodia.

While other case details remain undisclosed due to the ongoing trial, Associate 2, in partnership with Associate 1, is understood to have serviced his online gambling operations using Software Company 1,[9] which he registered in Taiwan PoC, as well as companies in several offshore gambling hubs including, the British Virgin Islands, Curaçao, Cyprus, and Vanuatu, among others. Among Associate 2's largest ventures was high-profile i-gaming white-label, Entertainment Group 1, which houses major operations in Bavet, Cambodia[10] and remains active, legally or illegally, online across multiple jurisdictions in Europe, Asia, and the Americas.

Beyond its online gaming portfolio, Entertainment Group 1 claimed to have established Casino 1 and an associated tech-park in Bavet as well as Junket Group 2 VIP club which until recently operated in Macau SAR, the Philippines, and in Cambodia within the Xi-Hu Hotel.[11] Junket Group 2 also held an extensive business partnership with Suncity and Alvin Chau, opening a joint entertainment company in Taiwan PoC alongside several joint VIP rooms in the Philippines and Macau beginning in 2014 , with both Associate 1 and Associate 2 appearing alongside Chau at various grand opening events throughout the region.

According to prosecutors, Associate 1 and Associate 2 had created several international shell companies and used money mule accounts to transfer and commingle clean funds and criminal proceeds using online gambling platforms and cryptocurrency. Beyond online gambling operations, Associate 1 and Associate 2 are also understood to have developed

7 Ministry of Justice Investigation Bureau, Taiwan PoC, 2023. Accessed at: https://www.mjib.gov.tw/news/Details/1/892.
8 Royal Thai Police press briefing, 16 August 2023.
9 Taiwan Company Information Network, 2023. Accessed at: https://www.twfile.com/item.aspx?no=55797570&sn=2719159.
10 Awesome Entertainment. Accessed at: https://aegroup.info/.
11 The Venus VIP room within the Xi-Hu Hotel Xigang Casino was opened in 2019. criminality associated with the Xi-Hu Hotel is described at length in the above Suncity case study chapter under the Cambodia subsection.

Alvin Chau and Associate 1, among others, at the official launch of the joint Suncity VIP Club in the Philippines, 2018.
Source: Suncity Group official social media platforms, 2018.

online shopping and instant messaging platforms which provided third-party payment processing and further helped to obfuscate the source and destination of criminal proceeds. Additionally, prosecutors reported that they uncovered evidence linking both to kidnapping and extortion rings which allegedly offered and advertised jobs overseas.

It is worth noting that Casino 1 and some of the online operations of Entertainment Group 1, which are housed in its nearby tech-park, are located in the Moc Bai commune of Bavet, Cambodia, which has emerged as a major hub for online gambling, cyberfraud, and trafficking for forced criminality. Operations in the area are largely staffed by workers recruited from China, Taiwan PoC, and Viet Nam, and while some areas are accessible, others are blocked by high walls, razor wire, and guarded gates. Multiple law enforcement sources and victim testimonies have named both Casino 1 and its corresponding gated compound as locations where crimes including human trafficking, forced labour, and extortion have taken place.

The casinos in the Moc Bai complex are located on the main road, however, behind them are dozens of buildings that house online gambling operations, staffed largely by workers from Viet Nam and China. While some areas are accessible, others are blocked by high walls, razor wire, and guarded gates. Moreover, Vietnamese reports, together with other local reports from across Southeast Asia, have named both Casino 1 and the broader Moc Bai area as locations where workers have been sold and held against their will. These reports include an interview featuring a man who helped to rescue three teenagers from Casino 1 in mid-2022, paying a ransom of US $6,000 per person.[12] Online recruiters regularly post work opportunities at the tech-park associated with Casino 1 on Facebook and Tiktok, with basic job descriptions similar to those used by other online gambling and cyberfraud operators.

Aerial overview of Moc Bai commune, Bavet, Cambodia.

12 VN Express, 2022. Accessed at: https://web.archive.org/web/20230519171332/https:/vnexpress.net/hai-lan-sang-campuchia-chuoc-bay-nguoi-bi-ban-vao-casino-4506294.html.

Additional cases

Beyond the casino and cyberfraud hub of Bavet, in a separate case from April 2023, prosecutors in Kaohsuing, Taiwan PoC arrested 21 individuals for their role in an international money laundering operation that facilitated the laundering of approximately US $146.1 million over a 10-month period for criminal groups using online casinos in Viet Nam. Authorities in Taiwan PoC seized large numbers of mobile phones, Vietnamese SIM cards, computers, and a telecommunication network system, stating that "the phones can receive calls from Viet Nam, and people can call and enter a password to transfer profits from gambling."[13]

According to authorities, the money that passed through online casino platforms was meant to appear as remittances primarily originating from Viet Nam and processed in Vietnamese Dong. The group processed the money through foreign bank accounts and overseas shell companies, taking a 'handling fee' to 'white-wash' the money in Taiwan PoC and evade law enforcement, allowing for the money to be returned to Viet Nam and appear as legitimate, clean profit.[14] The use of Viet Nam is particularly concerning as Viet Nam-facing online gambling operations are proven to have extremely high cross-table rollings and often utilize cryptocurrency (see below table). These revenues can help to comingle clean money derived from legitimate recreational gambling with proceeds of crime that are processed through online casinos, obfuscating the source of funds to make them difficult to trace.

It is also worth noting that law enforcement sources have confirmed that Sam Gor (三哥)network members, including senior syndicate members, had previously made visits to casinos in Cambodia, including NagaWorld. Sam Gor has also been known to arrange underground cross-border payments for drug shipments from the Golden Triangle and East Asia (namely Macau SAR, Hong Kong SAR, and Taiwan PoC) through Mekong-based casinos and junket operators, as well as Vietnamese money launderers.[15] A member of the Sam Gor syndicate that frequented casinos including NagaWorld is Hsieh Tsung Lun of Taiwan PoC, who was arrested in 2018 and extradited from Cambodia to Myanmar where he is serving a prison sentence.[16] According to criminal intelligence officials in the Mekong, Hsieh organized shipments of large quantities of methamphetamine as well as heroin for the syndicate while he was working out of a Golden Triangle-based casino.

Seizure made in relation to Taiwan-PoC and Viet Nam international money laundering network, April 2023.

With respect to related human trafficking into online casino and cyberfraud compounds from Taiwan PoC to the Mekong region, in August 2022, the Criminal Investigation Bureau of Taiwan PoC reported details of a human trafficking investigation into associates of the Bamboo Union and Heavenly Way Alliance, together with other crime groups based in Hsinchu, New Taipei City, Taichung, and Taoyuan. Authorities described how the trafficking network lured unsuspecting Taiwan PoC residents with high paying jobs in Cambodia but were instead being handed to gangs upon arrival and forced to work in cyberfraud operations.[17] Members of the international human trafficking ring were also found to have previous narcotics and fraud convictions. The investigation also revealed the use of a professional travel agent who was recruited to help procure passports, order air tickets, and arrange transport to Taiwan Taoyuan International Airport, where she allegedly advised the outbound travelers on how to answer questions at customs upon arrival in Cambodia.

13 Kaohsiung Police Department's Criminal Investigation Corps, 2023.
14 Ibid.
15 Conversations with regional law enforcement, 2023.
16 Ibid.
17 Taiwan PoC Taipei District Court. Accessed at: https://tpd.judicial.gov.tw/tw/cp-2850-2019907-76179-151.html.

Table 1. Major illegal online gambling ring betting volume reported by authorities in Viet Nam, 2019-2022

Date	Website	Betting volume (USD)	Location
11/2022[18]	Bong88.com and Agbong88.com	$83 million	Ho Chi Minh City
12/2021[19]	Swiftonline.live and Nagaclubs.com	$3.8 billion	Ho Chi Minh City
11/2021[20]	cp.starcsn.com	$1.3 billion	Hanoi
11/2021[21]	Tai.bxx	$609 million	Hanoi
11/2021[22]	Undisclosed	$4.35 million	Nghe An
02/2020[23]	powgs.com	$43.53 million	Cau Giay
06/2019[24]	Undisclosed	$430 million	Hai Phong
04/2019[25]	Fxx88.com	$1.28 billion	National

Source: Viet Nam Ministry of Public Security and provincial police.

According to information released by Taiwan PoC authorities, one of the groups lured 82 Taiwanese jobseekers to Cambodia in a 3-month period which were confined and held in prison-like conditions upon arrival and forced to perpetrate cybercrime. Authorities further revealed that the group received approximately US $1.67 million in commissions for sending these Taiwanese citizens into "cyberslavery."[26]

In November 2022, police in Taiwan PoC raided multiple residential buildings, finding 58 victims kept in captivity in extreme conditions.[27] Victims were handcuffed, beaten, and reportedly drugged, however, unlike similar cases for forced criminality based in the Mekong, the victims were held purely for the purpose of money laundering. According to court records, a group of 29 perpetrators controlled almost 100 bank accounts and individual banking information using the identities and documents of 61 enslaved victims, with the accounts being used as the second or third layers in a sophisticated money laundering process. The funds are believed to have been derived from 246 victims of investment scams connected to the money laundering operation, generating approximately US $12.66 million.[28]

More recently, in April 2023 the Taipei District Court sentenced alleged Bamboo Union member, Lee Chen-hao (李振豪), to 18 years in prison for his role in trafficking 88 people into a Cambodia-based cyberfraud ring, with 8 other accomplices receiving between 11 to 16.5 year prison terms.[29] At trial, prosecutors had alleged the trafficking network received US $18,000 per trafficked person, with victim passports confiscated upon arrival in Cambodia where several would be subject to physical violence, punishment, and resold.[30]

Victims of human trafficking rescued in Taipei. Source: New Taipei City Police, 2022.

18 Viet Nam Ministry of Public Security, Available at: https://baochinhphu.vn/world-cup-2022-triet-pha-duong-day-danh-bac-ca-do-nghin-ty-102221123095348978.htm.

19 Lao Cai Police Department, Available at: https://congan.laocai.gov.vn/1246/28094/39632/648558/bo-cong-an/triet-pha-duong-day-danh-bac-tren-mang-lon-nhat-tu-truoc-den-nay-bat-giu-gan-60-nguoi.

20 Viet Nam Ministry of Public Security, Available at: http://bocongan.gov.vn/tin-tuc-su-kien/tin-an-ninh-trat-tu/bo-cong-an-triet-pha-duong-day-danh-bac-voi-so-tien-khoang-30000-ty-dong-d22-t30428.html.

21 Khanh Hoa Police Department, Available at: https://congan.khanhhoa.gov.vn/so-thich-khac-nguoi-cua-ong-trum-trong-duong-day-danh-bac-14-nghin-ty_475127_1_2_article.html.

22 Nghe An Police Department, Available at: http://congan.nghean.gov.vn/tin-tuc-su-kien/202111/pha-thanh-cong-chuyen-an-danh-bac-quy-mo-lon-nhat-tu-truoc-toi-nay-tren-dia-ban-thi-xa-thai-hoa-938871/.

23 Lai Chau Police, Avalable at: https://congan.laichau.gov.vn/view/tin-an-ninh-trat-tu/cong-an-quan-cau-giay-triet-pha-duong-day-danh-bac-nghin-ty-qua-mang-52803?mid=2434.

24 Viet Nam Ministry of Public Security, Available at: Ministry of Public Security of Viet Nam. Accessed at: http://conganthanhhoa.gov.vn/tin-tuc-su-kien/tin-trong-nuoc/hon-380-nguoi-trung-quoc-tham-gia-duong-day-danh-bac-khung-o.html.

25 Viet Nam Ministry of Public Security, Available at: http://en.bocongan.gov.vn/tintuc/Pages/news-events.aspx?ItemID=5626.

26 Central Investigation Bureau, Taiwan PoC, 2022.

27 Ministry of Justice of Taiwan PoC, 2023. Accessed at: https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=SLDM%2c111%2c%e7%9f%9a%e9%87%8d%e8%a8%b4%2c1%2c20230322%2c2&ot=in.

28 Ibid.

29 Taipei District Court, decision, April 2022.

30 Ibid.

Kokang, Special Region 1 of Myanmar

The Special Regions (SRs) of Myanmar in Shan State are home to significant illicit economies, including globally significant production of methamphetamine and heroin, as well as sophisticated, industrial-scale money laundering, underground banking, cyberfraud, and unregulated gambling operations. Intensifying armed conflict, socioeconomic insecurity, and governance challenges in the SRs which are under de-facto control of armed groups, together with the country's increased regional integration with neighbouring countries, has further exacerbated the situation and deepened connections to transnational organized crime.

While drug production, trafficking and connections between armed groups and major organized crime groups are well documented, the country's sprawling, high-tech, and unregulated casino operations that facilitate the laundering of proceeds generated within the illicit economy have not been examined in significant detail. The Kokang Self-Administered Zone of Myanmar, known as Special Region 1 or SR 1, under the control of the Kokang Border Guard Force (BGF), is among the most casino-dense areas of Myanmar, while other areas including Mongla SR 4, Wa State SR 2, Tachileik, and Myawaddy are also home to a high number of unregulated physical and online casino operations. While SR 1 has been known for its casino industry since the 1989 ceasefire agreement between the Government and Myanmar National Democratic Alliance Army (MNDAA),[1] the industry has exhibited rapid growth and evolution following the instalment of the Kokang BGF in 2009 and subsequent displacement of the online gambling business from Macau SAR into Laukkai, the commercial and administrative center of SR 1 that shares its border with China. The growth of the casino industry in SR 1 has been made possible due to the Kokang BGF's relations with Nay Pyi Taw, which has permitted both formal business access and an autonomous regulatory environment. Kokang also enjoys close cultural and business ties with Yunnan.

As is the case with many armed groups located in Shan State and other border enclaves of Myanmar, the Kokang BGF has a documented history of involvement in drug production and trafficking. Law enforcement and criminal intelligence officials in the Mekong region have reported the presence of large-scale drug production sites near Laukkai, and analysis of court records in China shows that over 1,300 cases were registered involving cross-border crimes emanating from SR 1 between 2010 and 2021, with approximately 800 cases related to illicit drugs, 181 to illegal cross-border gambling and money laundering, and 40 involving kidnapping.[2] These cases include multiple incidents relating to companies and operations controlled by BGF leadership which oversee SR 1's Gambling and Entertainment Management Committee.[3]

1 In 2009, MNDAA split into two groups, with one rejecting the Government's proposal to lay down its arms and the other allying with the Government and transforming their local troops into BGF 1006.

2 UNODC analysis of Chinese court records, 2022.

3 The Kokang Gambling and Entertainment Management Committee oversees the approval of all casino and entertainment operations of SR 1. Most notably, this includes large-scale online casino operations which function using underground banking and money laundering networks and have been implicated in major money laundering cases in mainland China.

Money laundering notice issued by Werner International, 2023.

More recently, in December 2023, the Criminal Investigation Bureau of the Ministry of Public Security of China issued ten arrest warrants for high-ranking members of the Kokang BGF leadership on charges relating to their roles in leading multiple violent criminal groups engaged in telecommunications and network fraud against Chinese citizens.[4] Most of those charged are members of SR 1's Gambling and Entertainment Management Committee, and are heavily involved in Kokang's online gambling and underground banking industry, including the Werner International, Yuxiang International, and GOBO East online casino platforms (see below).

In December 2019, the Ministry of Public Security of China launched a special investigation into two interconnected online gambling platforms, Kokang-based Warner International and Yuxiang International, which function using live-dealer streaming within large land-based casinos in Laukkai. Authorities reported that both platforms served as conduits to facilitate underground banking and money laundering, developing a business consisting of over 40,000 agents, 300,000 active members, and generating an annual betting volume of at least US $3.6 billion as of 2021.[5] During the course of the investigation, authorities also discovered two affiliated gambling software companies, Dayun Technology (renamed Chengdu Jinan Tiancheng Technology), and Sichuan Qiante Technology, posing as research and development companies, while in fact servicing both platforms, with the latter reportedly established by representatives of Yuxiang International.[6] The investigation resulted in the arrest of individuals in Guangxi, Hainan, Sichuan, Fujian and Guizhou and the seizure of nearly 15,000 bank cards used to facilitate underground banking using the cover of online gambling through so-called 'points running' syndicates that deposit money and cryptocurrency to obtain virtual casino chips which could subsequently be 'withdrawn' and cashed out.[7] Both online casinos continue to operate across multiple 'mirror websites'[8] at the time of writing, despite notifications confirming their use in money laundering activities. Users who register through the Werner International agent network may 'top up' in-game credit using a range of underground payment methods and currencies, and cash out using 'settlement methods' in other jurisdictions through various 'fund disbursement' options.

In another case involving a Kokang-based casino and junket operator, GOBO East Entertainment,[9] also known as Dongfanghui Casino (東方匯賭场), a Cambodian subsidiary of the Fully Light International conglomerate which is held by members of the BGF leadership, was implicated by the People's Procuratorate in Guizhou and Shaanxi of China in the 2019 convictions of members of local triad groups who had outsourced online gambling operations by partnering with the company.[10]

4 Official WeChat of the Criminal Investigation Bureau of the Ministry of Public Security, December 2023. Accessed at: https://mp.weixin.qq.com/s/sm3wSWuxPSFcuSg4zlEfsQ.

5 Ministry of Public Security of China, 2021. Available at: http://www.gdqy.gov.cn/xxgk/zzjg/zfjg/sgaj/xxgk/jwyw/content/post_1384757.html

6 Ibid.

7 Ibid.

8 Mirror sites or 'mirrors' are replicas of other websites. The concept of mirroring applies to network services accessible through any protocol, such as HTTP or FTP. Such sites have different URLs than the original site, but host identical or near-identical content. Mirror sites are regularly utilized by illegal online gambling and cyberfraud syndicates based in East and Southeast Asia to overwhelm authorities, circumvent law enforcement efforts and ensure business continuity in the event that a URL is brought down.

9 Open Corporates, Gobo East Entertainment Co., Ltd. Accessed at: https://opencorporates.com/officers/275933656).

10 Official announcement from the Shaanxi Higher People's Court, 2019. Available at: https://sxfy.chinacourt.gov.cn/article/detail/2020/01/id/4777038.shtml, https://credit.shaanxi.gov.cn/345/8528001.html and http://news.jcrb.com/jxsw/201910/t20191010_2058522.html.

Source: Fully Light International Telegram Channel and Warner International TikTok and Douyin channels, 2023.

Authorities found that GOBO East colluded with the syndicate by facilitating end-to-end online live dealer and telephone gambling operations through the company's platform, offshore servers, call centres, brand and marketing resources, and underground credit network, and multi-currency payment and settlement solutions, from Kokang SR 1.[11] The investigation resulted in the conviction of 121 individuals affiliated with the syndicate, representing China's largest record number of convictions in a single case at the time. GOBO Entertainment continues to operate, claiming to be licensed and supervised by the Myanmar Gaming Inspection and Coordination Bureau, and licensed to operate under the Cagayan Economic Zone Authority (CEZA) and First Cagayan Leisure and Resort Corporation (FCLRC) in the Philippines.

While official records are limited in Myanmar, it is worth noting that the director of GOBO East Cambodia is closely affiliated with Warner International, actively referenced as a senior member of the company's leadership across several official social media channels,[12] and both online platforms have been developed using almost identical source code.[13] Concerningly, both platforms also appear to be connected to a variety of formal banking institutions and licensed cryptocurrency exchanges. Video files of Kokang-based casino operators including Warner and Fully Light International also depict casino cages filled with extremely large volumes of cash packaged in Wa State Bank bags, an unregulated bank based in SR 2 run by the United Wa State Army (UWSA) – a sanctioned[14] armed group which has historically been known to be among the region's largest drug producers connected to the sanctioned Zhao Wei transnational organized crime group in Lao PDR.[15]

Official announcement from the Shaanxi Higher People's Court, 2019.

11 Ibid.

12 See various regional news articles including: https://k.sina.com.cn/article_6601369739_18978e88b00100ox8w.html and https://page.om.qq.com/page/OA4oWW5RmGytl1TPpyJZWr1w0.

13 GOBO East Entertainment. Accessed at: http://web.archive.org/web/20220721233013/http://zm98.com/ and http://51mnls.com/.

14 U.S. Department of the Treasury Office of Foreign Assets Control, Treasury Sanctions United Wa State Army Financial Network, November 2009. Accessed at: https://home.treasury.gov/system/files/136/archive-documents/linkdata--document.pdf.

15 U.S. Department of the Treasury Office of Foreign Assets Control, Treasury Sanctions on the Zhao Wei Transnational Criminal Organization, Press Releases, 30 January 2018. Available at: https://home.treasury.gov/news/ press-releases/sm0272.

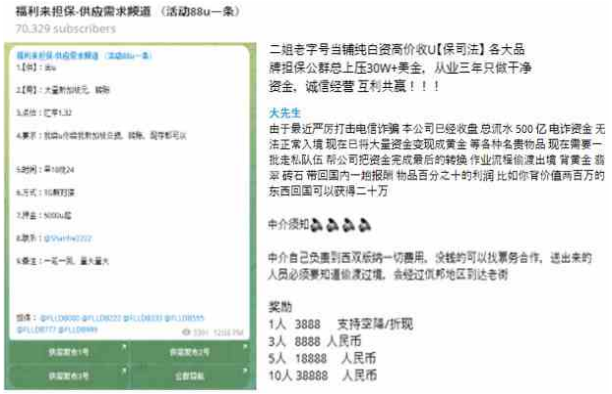
东方汇佣金表

代理级别	业绩制度	返佣比例
1.玩家	1万以内	0.2%
2.小玩家	1万至10万	0.4%
3.小赌怡情	10万至50万	0.5%
4.初级VIP	50万至100万	0.6%
5.进阶VIP	100万至300万	0.7%
6.刷单高手	300万至500万	0.8%
7.黄金刷手	500万至800万	0.9%
8.钻石刷手	800万以上	1.0%
9.盘口大鳄	3000万以上	1.2%

GOBO East Exchange 'Agent Commission Table' and live-dealer casino Telegram livestream, 2023.

Providing further indication of criminal activity, Kokang casinos and associated companies have developed a robust presence across so-called 'grey and black business' Telegram channels facilitating cross-border 'blockchain' gambling, underground banking, money laundering, and related recruitment in Myanmar, Cambodia, China, and several other countries in East and Southeast Asia. Among others, this includes underground cryptocurrency exchanges and money laundering 'motorcade' (also known as fleet) teams (車隊) offering 'black USDT to cash bleaching services' facilitated using affiliated online casinos and peer-to-peer transfers arranged through groups linking back to the official Fully Light and GOBO East Telegram channels. The community established by the companies consists of hundreds of thousands of members and agents and breaks down into groups facilitating underground banking and cryptocurrency exchange 'pass-through' activities, cybercrime as a service, recruitment of migrant smugglers, and development of underground banking and money laundering teams. The community also features multiple 'supply and demand' and 'VIP' groups which advertise calls for underground cross-border value transfers requests utilizing a variety of methods in real time. Calls shared in the groups are exclusively issued by Fully Light administrator accounts, with some backed by an official 'Fully Light guarantee'.

For instance, in a post published within one of the channel's many 'supply and demand' groups, administrators share a call requesting a large amount of Singapore dollars in exchange for USDT at the rate of SGD $1.32. The request goes on to state: "I will provide USDT, you will provide Singaporean white capital transfer…one transaction, one return, large quantity." Directly beneath the call, another user claiming to represent the 'Second Sister's Pawnshop' advertises exchanging USDT for 'pure white capital' at a high rate, citing their strong business reputation. In another affiliated Fully Light 'VIP communication channel', a user named 'Mr. Big' cites difficulty in transferring his company's multi-billion-dollar cyberfraud proceeds into China and posts a paid recruitment ad hiring a team to "help the company complete the final conversion operation process" and smuggle gold and precious stones into China, offering a 10 per cent fee. In the same channel, a different user representing an overseas labor service, which appears to be an affiliate of Fully Light International, issues a notice to brokers to inform that recruited migrant workers should be aware that they will be illegally smuggled into Laukkai City in Kokang SR 1 of Myanmar through Wa State SR 2, and details the intermediary's bonus per each recruited labourer. It is also worth noting that several other connected groups linked to the channel advertise having large amounts of capital, robust money mule networks, online casino operations, and other related resources in countries including Malaysia, Taiwan PoC, the Philippines, Viet Nam, the UAE, and elsewhere in South Asia, the Middle East, and Africa.



Source: Fully Light International official underground money exchange Telegram groups, 2023.

While each individual incident described above requires verification, the open advertisement of services and nature of the activities within Fully Light's Telegram channels becomes even more concerning when taking into account that the conglomerate is known to have developed large construction projects and an 'entertainment city' along the Thai border in Myawaddy, Myanmar, which is known as a major regional hub for USDT-based cyberfraud and online casino operations.[16] In recent months, several reports confirmed by law enforcement authorities have emerged of foreign nationals seeking rescue after being lured into one of these venues under fraudulent employment schemes and held for ransom by human traffickers. The conglomerate also appears to have been engaged in similar illicit activities in the Philippines using a company with the same name as the Myawaddy-based entertainment city.

16 Myawaddy, Myanmar is a BGF-controlled township known to house one of the largest concentrations of cyberfraud compounds in Southeast Asia.

UNODC
United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific
United Nations Building, 4th floor, Secretariat Building, Raj Damnern Nok Avenue, Bangkok 10200, Thailand
Tel. (66-2) 288-2100 Fax. (66-2) 281-2129 E-mail: unodc-thailandfieldoffice@un.org
Website: http://www.unodc.org/roseap
Twitter: @UNODC_SEAP