

EXPERT INSIGHT

Casinos and Cryptocurrency Driving Illicit Finance in East and Southeast Asia



Table of Contents

- 03** Background
- 05** Casinos: Ripe for Abuse
- 07** Special Economic Zones
- 08** Underground Banking
- 11** Money Laundering Through Junkets
- 12** Online Casino Vulnerabilities and Challenges
- 15** Conclusion and Key Takeaways

Background

A new UN Office on Drugs and Crime (UNODC) [report](#), “Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden, Accelerating Threat,” has found that casinos, junkets, and cryptocurrencies are exacerbating transnational organized criminal activity in East and Southeast Asia as part of the region’s underground banking and money laundering infrastructure. Although the use of casinos to launder money is not new, the proliferation of online gambling since the COVID 19 pandemic has aggravated the existing problem and has given rise to underregulated online gambling venues as more gamblers began playing from home.

The proliferation of cryptocurrency exchanges has resulted in quicker money movements, and technological advances facilitate anonymous transactions favored by illicit actors. Illicit economies in Southeast Asia, and particularly in the Mekong region, have grown rapidly in recent years owing to these developments. Some transnational organized crime (TOC) groups operate in the open, making public investments in vital sectors of the economy. The UN report notes that TOC leaders have been forming alliances with influential local figures and exploiting these relationships for financial gain and to expand their criminal activities.

- A 2019 [report](#) issued by the UNODC highlighted that the smuggling of Indonesian migrants to Malaysia often involved organized networks led by prominent local figures that operate unlicensed recruitment agencies in both countries to facilitate irregular entry and job placement.
- The US Institute of Peace in November 2022 [wrote](#) that Burma’s military regime reaps profits from increased criminal activity in remote areas of the country and ungoverned areas of Cambodia and Lao PDR (Laos). In the years before the pandemic, corrupt governing elites in the affected countries ignored and sometimes even promoted development of unregulated areas, identified as “special economic zones” (SEZs), that were meant to facilitate economic development, but in fact, were meant for illegal gambling operations established by Chinese triads. As lockdowns and strict border controls stymied the plans for the development of gambling centers, TOC groups began to [traffic](#) alternative labor into these zones to engage in cyber fraud.
- Although TOC groups continue to primarily rely on fiat currencies and transactions, they are increasingly exploiting emerging value transfer opportunities, such as virtual assets, to launder the proceeds of crime, according to a 2022 Europol [report](#).
- According to a recent Reuters [report](#), Chinese businessman Wang Yicheng, the vice president of a local Chinese trade group in Thailand, during the past several years cultivated relationships with members of the country’s law enforcement and political elite, while receiving millions of dollars into his cryptocurrency account from pig-butcher schemes—a scam that usually involves the scammers engaging with unsuspecting victims, developing a relationship of trust, and persuading them to invest in cryptocurrency scams.

The growing use of cryptocurrencies and largely unregulated virtual asset service providers (VASPs) operating in certain parts of Southeast Asia region have compounded the challenges for law enforcement.

Proceeds of increasingly innovative crimes, such as pig-butcher and other online fraud scams, coupled with the continued expansion of the synthetic drug trade, are generating billions of dollars in revenue for organized crime in the region, necessitating access to underground banking and money laundering solutions capable of moving high volumes of state-backed fiat and cryptocurrencies undetected.

Designated Non-Financial Businesses and Professions (DNFBPs) also have become an attractive channel for money laundering and financial crime, consisting of reporting entities, including casinos; real estate agents; dealers in precious metals and stones; lawyers; notaries; other independent legal professionals and accountants; and trust and company service providers (TCSPs).



Casinos: Ripe for Abuse

The casino industry in Southeast Asia, and particularly the Mekong region, in recent years has experienced exponential growth. UNODC estimated that by early 2022 there were more than 340 licensed and unlicensed casinos in the region and 45 casinos in the Macau special administrative region (SAR). Restrictions implemented in the region during the COVID-19 pandemic impacted people's gambling habits, resulting in the expansion of the online casino industry as a response. UNODC reports that industry experts in the Philippines, for example, noted a significant growth in gross gaming revenue (GGR) from online operators for 2023. They project that GGR for the year will reach more than \$438 million—an increase from \$109.2 million prior to the COVID-19 pandemic in 2019.

A unique feature of the casino industry in the region is the large number of unauthorized online operators, particularly in Cambodia, Burma, the Philippines and, increasingly, Laos. Although the exact number of unlicensed casinos operating in the region is unclear, recent operations that dismantled illegal online gambling and cyberfraud activities, rescued victims of human trafficking, seized bulk cash and virtual assets, and arrested known organized crime figures indicate the vast size of the criminal industry in the region.

Organized crime groups operating in Southeast Asia have become increasingly sophisticated, demonstrating the ability to adapt to changes in political and business environments. An evolution in regional underground banking and money-laundering has resulted in increased criminal use of the online gaming industry to move assets. TOC groups have managed to integrate developments in information, financial, and blockchain technology, with thousands of sophisticated online casinos and so-called "e-junkets," according to the UNODC.

Casinos can be used in the placement stage of the money laundering process, in which the illicitly derived funds are placed into circulation. Unlicensed casinos face little oversight or auditing, unlike regulated establishments that implement rules to protect players and prevent money laundering.

- The Basel Institute's Cambodia [briefing](#) highlighted that the Financial Action Task Force's (FATF) 2017 Mutual Evaluation Report on Cambodia identified the country's casino industry and real estate sectors as having severe AML/CFT shortcomings. Thai authorities in July [arrested](#) Kuo Che-min and in September extradited him to Taiwan, where he was wanted for running a major online gambling and underground banking network based out of a casino in Cambodia, which may have laundered more than \$500,000 in illicit proceeds.
- According to Asia Times, media [reports](#) indicate that in Macau, the world's largest gambling center, many VIP rooms in casinos operate as sites for money laundering or illegal money lending, among other illicit activities.
- The State Department in 2021 [noted](#) that the proliferation of casinos, remittance networks, and drug trafficking in the border regions of Burma represent money-laundering vulnerabilities, and illegal and informal gaming in the country occurs through lotteries and card games.

China restricts the transfer of funds outside of China on behalf of others, but those seeking to transfer money overseas have found innovative workarounds. Underground banks and exchanges as well as cross-border gambling and tourism groups, junket operators and, increasingly, online casinos and e-junket operators help those wanting to transfer money abroad evade currency controls. The Government of China, in response to the evolving money-transfer techniques, has formally said 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." Chinese public security officials have also noted the rising use of cryptocurrencies, the dark web, and other technologies by organized crime groups, highlighting that the country has experienced growing concern over rampant cross-border and online gambling in Southeast Asia linked to criminal activities including drug trafficking, money laundering, kidnapping, and unlawful detention.



Special Economic Zones

The Mekong region has also seen a marked increase in the number of SEZs in recent years, driven by governments seeking to accelerate economic growth, particularly in key border and coastal areas attractive to foreign investors. However, several SEZs in the region are located in key areas close to illicit drug and precursor production and trafficking facilities, while high-profile criminals and organized crime syndicates are also known to be involved in SEZs as owners, developers, and investors.

In Karen State, Burma, several SEZs—the Shwe Kokko (also known as Yatai New City), Huanya International City, Saixigang Industrial Zone, and KK Park—are home to cyberfraud compounds and other companies with documented links to criminal networks. These “smart city” developments have attracted gambling operations looking to relocate from Macau SAR, the Philippines, and elsewhere in Asia because of law enforcement pressure and have evolved into havens for organized crime and cyberfraud operations.

- Radio Free Asia in 2022 [reported](#) that 700 Malaysian migrant workers were stranded and held for ransom in the Golden Triangle SEZ in Laos, forced to work as online scammers via torture and violence. Workers who managed to escape the zone said that their Chinese employers confiscated their passports and cell phones and confined them to the buildings on the compound.
- The FBI in 2023 [warned](#) US citizens and individuals who travel or live abroad that they were being targeted by false advertisements linked to labor trafficking at Southeast Asia-based compounds where victims are held against their will, intimidated, and forced to commit international cryptocurrency investment fraud. The schemes cover a wide range of opportunities, including tech support, call center customer service, and beauty salon technicians. Job seekers are offered competitive salaries, lucrative benefits, and paid travel expenses.
- In January, the Government of the Republic of Korea [announced](#) a travel alert for the Golden Triangle region of Lao PDR, citing a rise in criminality targeting its nationals and prohibiting travel into the area.
- Binance, the world's largest cryptocurrency exchange, in October [said](#) that it cooperated with Thai Police and the US Department of Homeland Security to help seize various crypto assets in a Binance account registered in Thailand associated with a pig-butcher scam.

Underground Banking

One major challenge in Southeast Asia relates to underground banking which has become more widespread and sophisticated, in part due to China's currency controls and regulations meant to reduce cross-border gambling. According to industry estimates, cross-border illegal gambling resulted in at least \$145 billion of illegal capital outflows from China alone through offshore gambling websites and casinos in 2020. Much of these outflows almost certainly move through casino junkets and sophisticated offsetting arrangements, as well as offshore online casino websites that use other underground money laundering and banking networks, such as so-called "points running" syndicates, money mule "motorcades," and third- and fourth-party payment providers. As of 2020, the Government of China estimated that at least 5 million participants use these underground industries.

Underground banking involves financial activities that run parallel to, and operate outside of, the formal banking system, commonly in the form of informal value transfer. Dealers in China and third parties in another jurisdiction facilitate the transfer of value without physically moving the funds or other assets. In East and Southeast Asia, underground banking 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 other means.

Casinos and junkets represent a critical part of the underground banking and money laundering infrastructure, serving the needs of TOC groups operating in the region and globally. Recent law enforcement action across Southeast Asia highlights that in recent years many land-based casinos and SEZs housing cyberfraud operations are using casino-related businesses for cover. 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 Vietnam, have caused a partial displacement into countries such as Laos and various parts of Burma.

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, Laos. Located adjacent to the porous border with Burma and Thailand, Kings Romans also has various connections to the drug trade in Shan State and other parts of Asia and has been identified as a key drug trafficking and money laundering hub connected to other criminally implicated casinos and junkets in the region. Regional law enforcement and financial intelligence officials have also confirmed the use of affiliate gold traders and money exchange networks across the Thailand and Burma border area.

- OFAC in 2018 [sanctioned](#) the Kings Romans Casino and its owner, Zhao Wei, pursuant to EO 13581, "Blocking Property of Transnational Criminal Organizations" for engaging in drug trafficking, human trafficking, money laundering, bribery, and wildlife trafficking. Wei, since then, has become a [major investor](#) in a Laotian port development project near the Golden Triangle Special Economic Zone—a Chinese-backed infrastructure project—through his Osiano Trading Sole Co.
- In response to underground banking using third- and fourth-party payment platforms and the casino industry, Beijing in 2015 initiated "[Operation Chain Break](#)"—an effort stop the flow of Chinese money into foreign casinos. The country's efforts to disrupt the flow of money from mainland China and Macau SAR to countries in Southeast Asia included an August 2020 "blacklist" of casino destinations.

Most countries in the region do not possess a functioning, enforceable casino regulatory management and supervision system, and many pay virtually no attention to casino junket operators and other VIP tour companies. Therefore, 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.

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 through VIP programs or tours. Through their relationships with casinos, junket operators can offer incentives and perks to their VIP club members and other prospective VIP gamblers. Some junket operators have evolved into 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.

Junket operators provide credit to customers wishing to evade capital controls and have become debt collectors when loans are not repaid. Because these activities are illegal in mainland China, junket operators rely on their organized crime connections to collect debts. Junkets have been involved in online gambling since the early 2000s, vastly expanding their potential market and exponentially increasing their revenues.





Money Laundering Through Junkets

TOC groups use a variety of methods to launder money through casino junkets. These transactions take place outside the formal banking sector, circumvent international funds transfer reporting requirements, and facilitate the laundering of domestically generated criminal proceeds. Some of the main methods include offsetting, MSB lending, cryptocurrency transactions, the “Vancouver model,” and multiplier betting.

- **Offsetting:** Offsetting is used as a means of transferring value between jurisdictions via financial credit and debit relationships between entities in different countries, according to the UNODC. Offsetting arrangements are also known as mirror transactions and can be used to move funds abroad and [evade sanctions](#). In the case of casino junkets, a gambler deposits money into a junket account or stakes using credit issued by a junket in one country and is subsequently issued a corresponding amount of value abroad, theoretically for the purpose of gambling. Money laundering organizations in the Asia-Pacific region increasingly engage in offsetting using casinos and junkets to move money connected to drug trafficking and production, the shipment of drug precursor chemicals, and cybercrime.
- **MSB lending:** The use of unlicensed money services businesses (MSBs) to lend money to gambling patrons, often from East and Southeast Asia, plays a key facilitation role in money laundering, according to the UNODC. The funds from the unlicensed 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 facilitates circumvention of strict currency controls in some jurisdictions, allows access to capital to gamble in different countries, and lets the money operator convert cash from one jurisdiction into a bank deposit within another.
- **Cryptocurrency transactions:** Although the use of cryptocurrencies by online casino and junket operators is not authorized by casino regulators in Southeast Asia, UNODC in its report has documented widespread advertising of cryptocurrency exchange and payment services being provided by both licensed and unlicensed operators across the region. Online gambling platforms have emerged as some of the most popular vehicles for cryptocurrency-based money launderers, particularly for those using Tether or USDT on the TRON blockchain.
- **Vancouver model:** Organized crime networks in Southeast Asia also have been using the “Vancouver model” for money laundering and underground banking—first uncovered through the [Cullen Commission](#) money laundering inquiry in Canada—in which Chinese gamblers would deposit money into local bank accounts controlled by criminal gangs, receiving Canadian cash in return. They would then visit Vancouver-area casinos, carrying bags full of Canadian bills, which they used to gamble, repaying the TOC groups with clean money from their winnings, which would then be deposited into accounts in China and Hong Kong. The same technique can be used in other countries, using local cash to clean illicit funds via gambling venues.
- **Multiplier betting:** Multiplier betting in the junket industry 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. The technique 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. Because most junket customers in Macau SAR originate from mainland China and cannot bring money with them to play because of China’s strict capital controls and a nationwide gambling ban in the mainland, these customers rely on credit issued by junket agents, who make arrangements with the casino to issue a multiplier on their behalf.

Online Casino Vulnerabilities and Challenges

Despite intensifying regulatory and enforcement efforts across East and Southeast Asia, millions of new online betting customers have emerged following the COVID-19 pandemic. The most significant AML vulnerabilities identified within the online casino sector in East and Southeast Asia and the Pacific, according to the UNODC, include but are not limited to:

Anonymity: non-face-to-face business relationships can present unique AML risks when customers register for online gambling accounts. Stolen identities frequently have been used for online gambling purposes, and player profiles have been set up with stolen IDs or provided to third parties who facilitate transactions for high-risk clients, including criminals, politically exposed persons (PEPs), or those subject to sanctions without the appropriate enhanced customer due diligence (CDD) procedures.

Third party transactions: in third party transactions, money deposited by one player could be withdrawn and deposited into another party's account. If one player deposits illicitly derived funds via an e-wallet, the money can potentially be withdrawn to a crypto address that is owned by another party.

Miscoding transactions: miscoding transactions are a common technique used by online casinos in the region to avoid government scrutiny. A charge on a gambler's credit card may appear as payment at a legitimate or innocuous venue, such as a restaurant, but is, in fact, a payment for an online casino, making identification of the gambling transaction challenging.

Gambling in exchange for luxury goods using in-game online gambling points: e-junket operators in East and Southeast Asia allow the redemption of in-game online credits for high-value items including luxury watches, handbags, vehicles, and vacations.

Use of online gambling account to redeem funds for illicit goods: A buyer and a seller of illegal goods often participate in the same game. The buyer transfers funds to the seller via a bet, and the seller then collects the funds from their payment account in exchange for the goods, using the gambling account in lieu of a bank account and making the tracing of illicit funds difficult.

Dedicated online gambling accounts: 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.

Unregulated live-dealer proxy betting: authorities in Southeast Asia have reported widespread unregulated and unauthorized live-dealer proxy betting taking place within junket VIP rooms and online casino operations. Proxy betting 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 behalf of the individual outside the casino. In more sophisticated operations, casinos can provide a live video feed of table games, giving gamblers the ability to watch the game from another jurisdiction online while instructing the proxy via mobile phone.

Source of Funds Verification: authorities in the region report major challenges with verifying the source of funds used in online-casino gambling and the misuse of online platforms for commingling illicit proceeds with recreational gambling flows by TOC groups. These challenges largely result from 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 online gambling platforms, and general lack of CDD. 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 for a small fee to add additional layers of commingling.

Beneficial ownership: infiltration of casinos, MSBs, and VASPs by organized crime increases the potential for money laundering and makes tracking beneficial ownership difficult. Technological advances have significantly lowered the barriers to entry for TOC actors. These advances, coupled with the advent of “white labeling” have attracted significant numbers of new actors into the sector, while effectively decentralizing money-laundering operations. White label service providers allow gambling websites to act as franchises, with operators outsourcing complex betting software, website design, customer data and relationship management, technical support, and other business functions to third-party service providers and enable online casino operators to quickly set up a gambling website with virtually no bookmaking experience or technical expertise.

Inadequate AML/CDD policy implementation and inadequate enforcement capacity: 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, according to the UNODC. Lack of understanding and prioritization of risk management, internal controls, reporting, and AML measures represents multiple vulnerabilities in the gaming sector, and gaps in awareness and investigative capacity result in increased vulnerabilities.

Difficulties in prosecuting predicate offenses: The recent proliferation of online casinos has increased the use of these platforms for money laundering and caused significant challenges tracing the proceeds of crime and subsequently prosecuting offenders. Prosecutors have trouble tracing illicitly gained assets, and some players may even divide funds into several different betting accounts to make their activity appear less suspicious and create further difficulties for prosecutors.

Online gambling platforms and e-junkets have emerged as popular vehicles for cryptocurrency-based money launderers while also fueling Southeast Asia’s rapidly growing illicit digital economy. The FATF 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.

The UNODC report comes on the heels of a warning from the office in October that Southeast Asia’s increasingly digital gambling industry is being exploited by illicit actors to covertly move and launder more illicit proceeds. Media [reports](#) cited UNODC’s assessment that the region’s casinos and online gambling sites handle as much as hundreds of billions of dollars in returns annually from illicit gambling, drug and human trafficking, cyber scams, and other criminal activities.





Conclusion and Key Takeaways

The Institute for Financial Integrity's DOLFIN platform details numerous red flags that may indicate money laundering using underground banking schemes. An operational alert from Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) last year highlighted numerous indicators to help reporting entities recognize financial transactions that could be related to the laundering of illicit proceeds linked to the underground banking infrastructure in China. Underground banking and the formal financial system intersect when certain transactions, such as the purchase of financial instruments, require access to the formal banking system.

Indicators for financial institutions to monitor may include the movement of funds sourced from individuals or entities in China—especially in Hong Kong—within a short period of time involving the real estate, automotive, or legal sectors or that are immediately transferred to a client's associated personal or business account or an unrelated party.

Additional indicators flagged by FINTRAC involve a client depositing a high volume of bank drafts to a patron gaming fund account, regularly using bank drafts as a form of gaming buy-in, or residing in a jurisdiction that is subject to currency control restrictions or sanctions and has no local ties to family or business.

Although red flags do not necessarily indicate illicit activity, their presence should qualify these clients as high-risk and alert financial institutions to be extra cautious and monitor their activities.