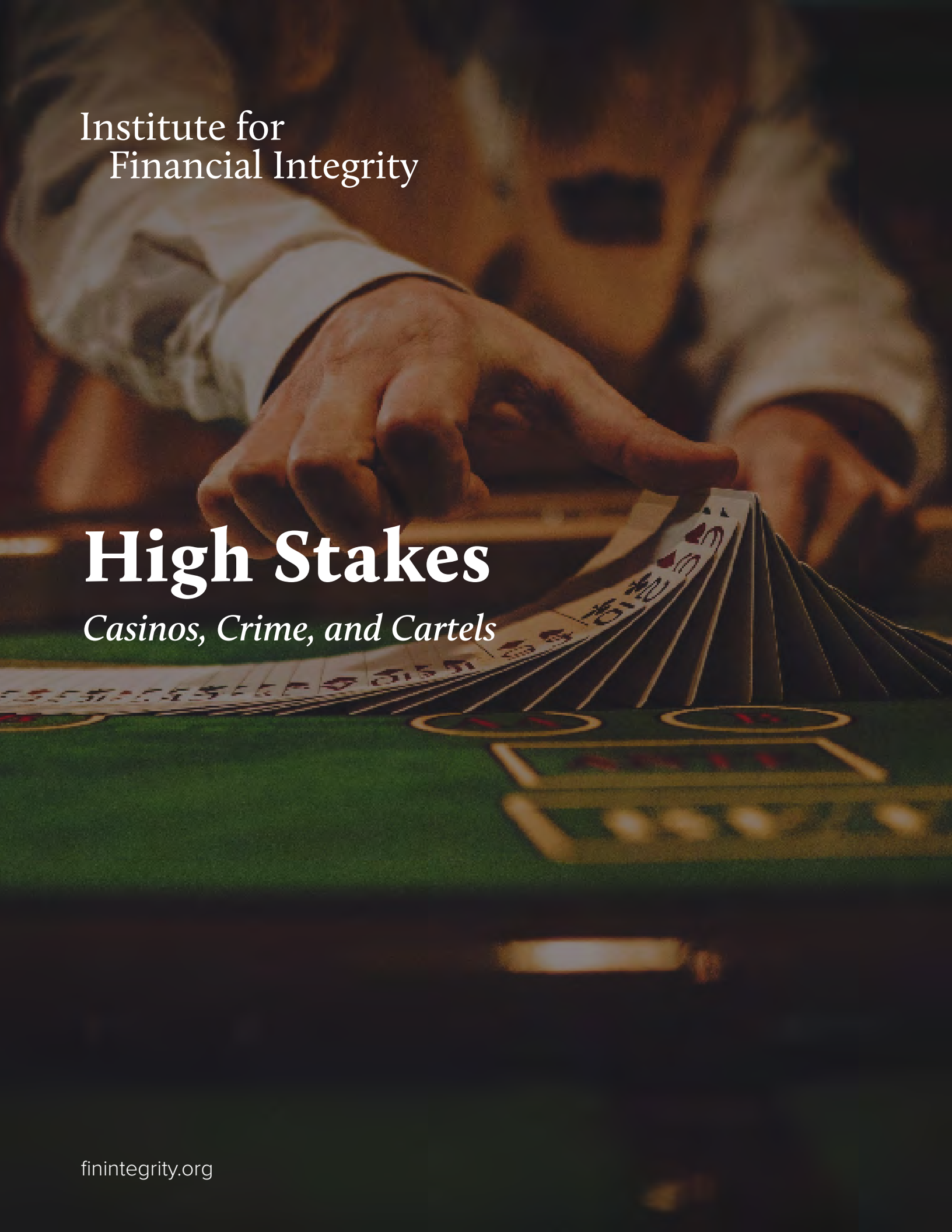


Institute for
Financial Integrity

High Stakes

Casinos, Crime, and Cartels

finintegrity.org

Table of Contents

Introduction

"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."

– United Nations Office on Drugs and Crime report (2024)

Gambling and gaming are significant sources of revenue and entertainment. They include casinos – both "land-based" and online – as well as online gaming and sports betting.

Indicators of the global scale include:

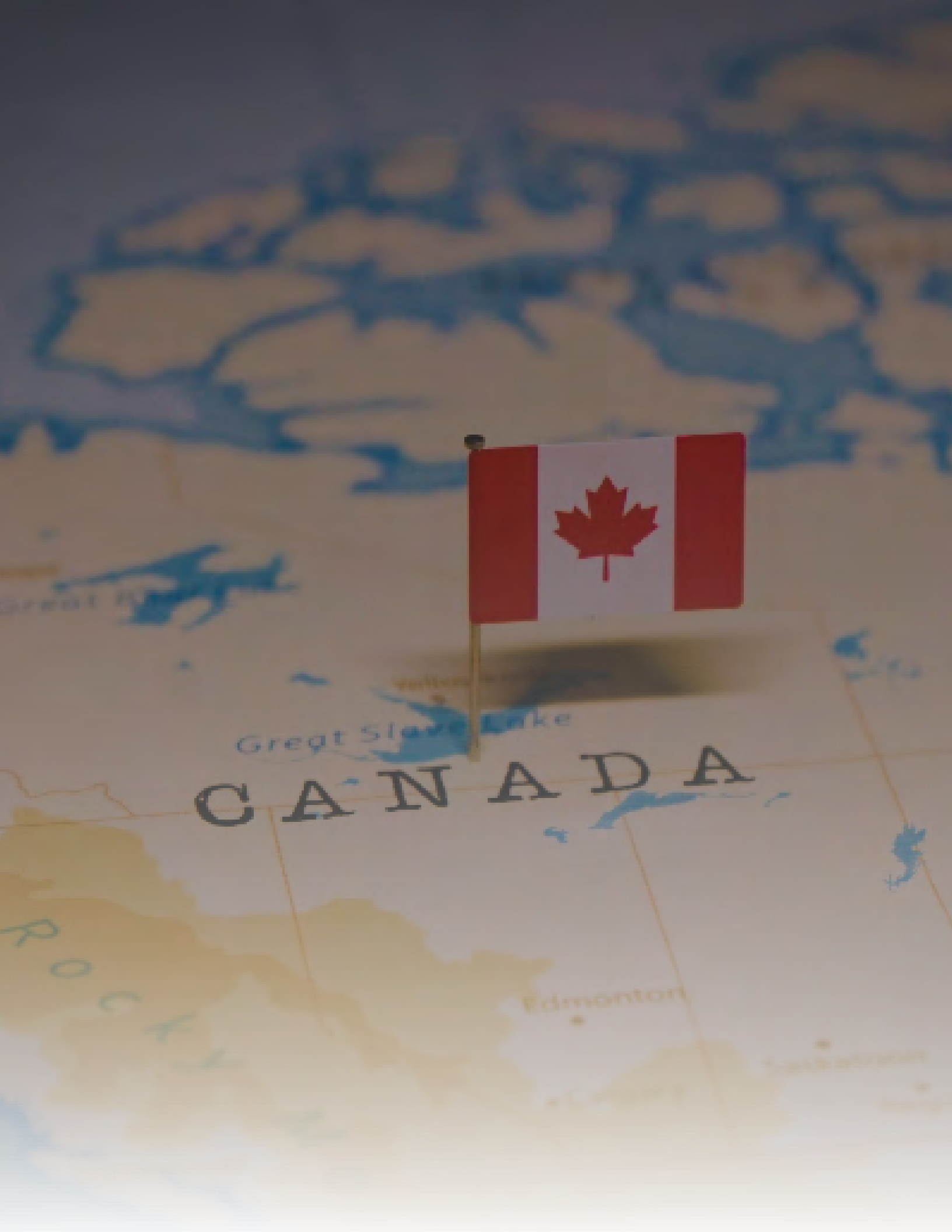
- The United Nations estimates that global gambling revenues will reach **$205 billion** by 2030 while industry estimates are even higher with estimated revenues of **$700 billion** by 2028.
- In the United States, commercial gaming generates **$72 billion** in revenues (2024) according to the American Gaming Association and a further **$43.9 billion** is generated in tribal gaming enterprises (2024) according to the National Indian Gaming Commission. "Revenue" is the money wagered by players minus the amounts paid out as winnings, representing the revenue the gambling operator earns before deducting expenses.
- In the United Kingdom, there are 2,343 gambling operators and 8,301 gambling premises, including 5,995 betting shops and 144 casinos (2024).
- In Australia, 38% of the population gambles weekly and in the state of New South Wales, there is the equivalent of one gaming machine for every 88 people.
- The European gambling market reached €123.4 billion ($144 billion) in gross gaming revenues in 2024, an increase of 5% over the previous year. Online gambling represents 39% of total revenue.

Gambling and gaming continue to be targeted by illicit actors such as cartels, organized crime networks, professional money launderers, and other illicit actors seeking to launder funds.

Significant progress has been made in many jurisdictions to establish regulatory regimes, deliver effective implementation, and to continuously monitor and enforce protections against unlawful activity. However, even jurisdictions with strong regulation and enforcement are vulnerable, with the real life examples of Canada and Australia providing illustrations.

Some jurisdictions are particularly vulnerable. This includes those where gambling has only recently been legalized, where regulatory regimes have yet to be fully implemented, or where gambling businesses and law enforcement are still developing capacity to detect and respond to illicit activity, meaning the likelihood of being targeted and misused by criminal actors is higher. The lessons learned in more established jurisdictions, both of money laundering methodologies and the necessary countermeasures, provide valuable instruction on how to build a well-protected gambling/gaming sector right from the start.

Global Cases


CANADA
Great Slave Lake
Edmonton

Canada: The Vancouver Model and Mirror Transfers

The Cullen Commission (2022) identified that millions of dollars were laundered through casinos in British Columbia between 2008 and 2018, including the proceeds of drug cartels based in Mexico and South American countries. In a single month, July 2015, more than $20 million in suspicious cash was reported by casinos to their regulators. This included more than $14 million that was accepted in $20 bills – this is not the total volume of cash handled, it is only the activity identified as meeting the suspicious reporting threshold.

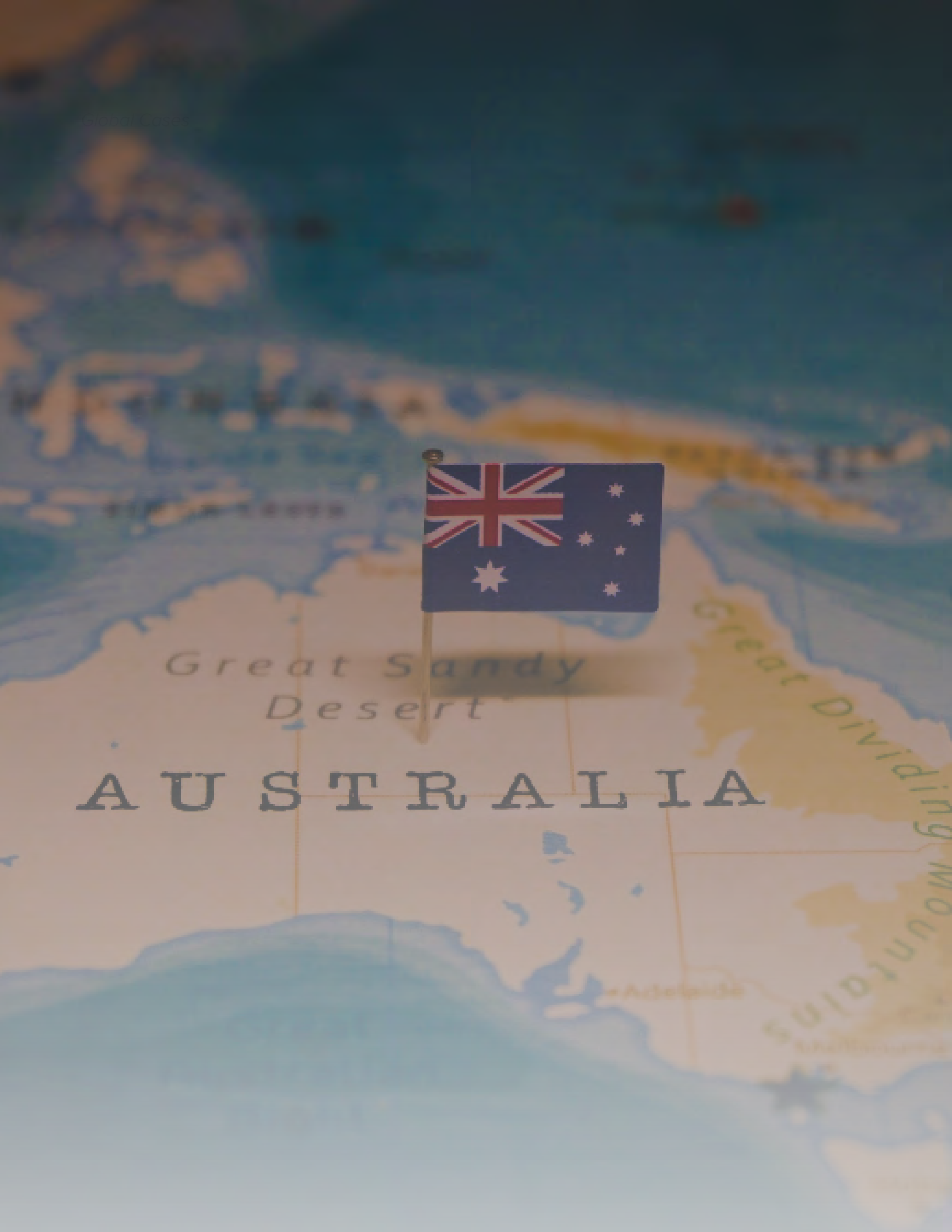
The gamblers were often "high rollers" from Asian countries who required access to significant volumes of cash to fund betting on their visits to Canada, with bets of up to $100,000 on a single hand of baccarat. Many of these gamblers had significant wealth abroad, but with China imposing a limit of $50,000 per year on removal of capital, and the practical difficulties of gamblers from other Asian countries acquiring and bringing cash with them, casino patrons had difficulty accessing these funds in Canada.

In contrast, cartel networks selling narcotics and involved in other types of illicit activity had large volumes of cash in Canada and a need to launder it. Money laundering network operatives made this available as cash or chips in casinos, carparks, and nearby locations. Gamblers used it to gamble, genuinely putting it at risk and often losing it. The Commission identified that the "loans" were repaid in electronic funds transfers or using other methods, enabling launderers in Canada to convert bulky, illicit cash into more convenient and less suspicious forms of value.

The Commission identified multiple red flags indicative of the criminal origin of cash and/or that laundering was occurring:

- "Cash facilitators" were identified in casinos passing cash and/or chips between players but rarely playing. Casino staff initially characterized them as "loan sharks".
- Cash was provided to gamblers in plastic bags, shoeboxes, and knapsacks, usually in $20 bills held together in bundles with elastic bands. The bundles were irregularly arranged such as some notes being face-up, others face-down, or and in other varied orientations. In contrast, cash withdrawn from financial institutions is well arranged and in appropriate packaging.
- Bags of cash were brought into the casino, converted into chips, then exchanged back into cash without any play having occurred, or only minimal or low-value bets.

The use of the Vancouver method declined significantly in 2018 when source of funds recommendations were implemented in British Columbia. However, similar methods have also been identified in Australia, Macau SAR, Cambodia, Laos, Myanmar, and the Philippines. An evolution of the mirror transfer method is also currently being used in the United States: it involves USD cash narcotics proceeds being exchanged using mirror transfers with electronic fund transfers in China, avoiding cross-border payments and therefore minimizing detection.


Great Sandy
Desert
AUSTRALIA
Great Dividing Mountains
Adelaide

Australia: Casino Junkets and High Rollers

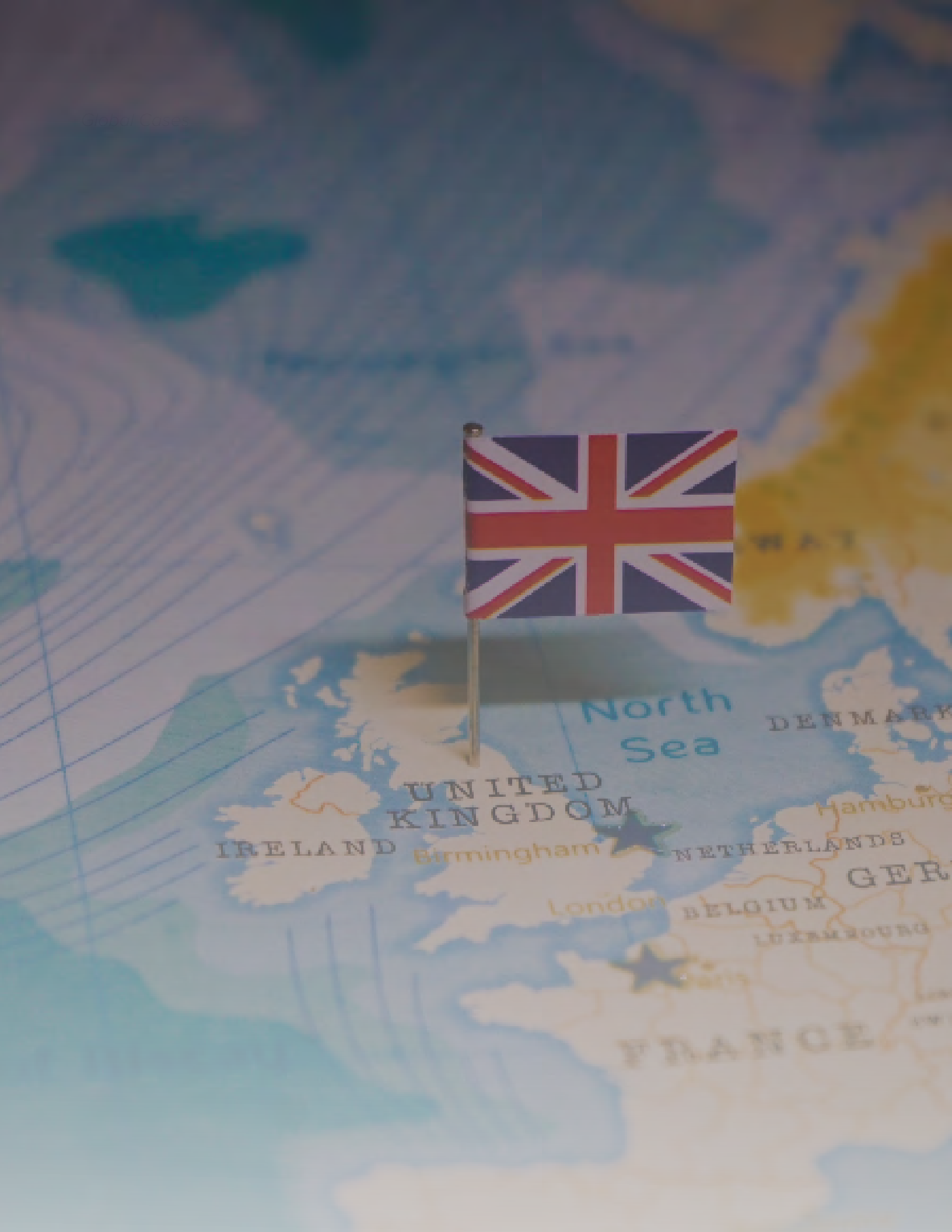
Crown Casinos, 2023

Crown Melbourne and Crown Perth are casinos in Australia that provide gaming and gambling services. In 2023, they were ordered to pay a penalty of AUD 450 million (approximately U.S. $300 million) for deficiencies in their AML program.

Among other failures, Crown regularly dealt with customers presenting higher risk including junket operators, international "VIP" customers, "high rollers", and foreign politically exposed persons (PEPs). Crown also continued a business relationship with a major casino operator while aware of allegations it was linked with organized crime.

"Junket operators" are third parties who enter agreements with casinos to facilitate gambling for high rollers. The gambler/client deposits money into a junket account in one jurisdiction, or stakes other assets, then accesses credit in another jurisdiction to gamble. Their wins and losses are offset against the original amount deposited. They involve higher AML risks because they enable large informal transfers of value between jurisdictions.

Regulations required Crown to identify higher risk customers and subject them to Enhanced Client Due Diligence. However, Crown's programs did not include appropriate measures to identify these customers, or to obtain, analyze, and record their source of wealth and source of funds information.


North
Sea
UNITED
KINGDOM
IRELAND
Birmingham
London
NETHERLANDS
BELGIUM
FRANCE

United Kingdom: Online Sports Betting

William Hill, 2023

The William Hill Group, which is headquartered and listed in the United Kingdom, operates global betting and gaming businesses. It offers online sports betting and gaming in multiple countries including through the William Hill, 888casino, 888sport, 888poker, and Mr Green brands, as well as 1,300 physical betting shops in the United Kingdom.

In 2023, the William Hill Group was ordered by the UK regulator, the Gambling Commission, to pay £19.2 million ($25.9 million) for AML and social responsibility failures. ("Social responsibility" refers to protection for customers at risk of gambling-related harm.) These included customers who were permitted to deposit large amounts and stake large amounts of money without being adequately scrutinized.

Appropriate **client due diligence** was not performed for customers depositing large amounts of money or was not completed before significant spending had occurred, including:

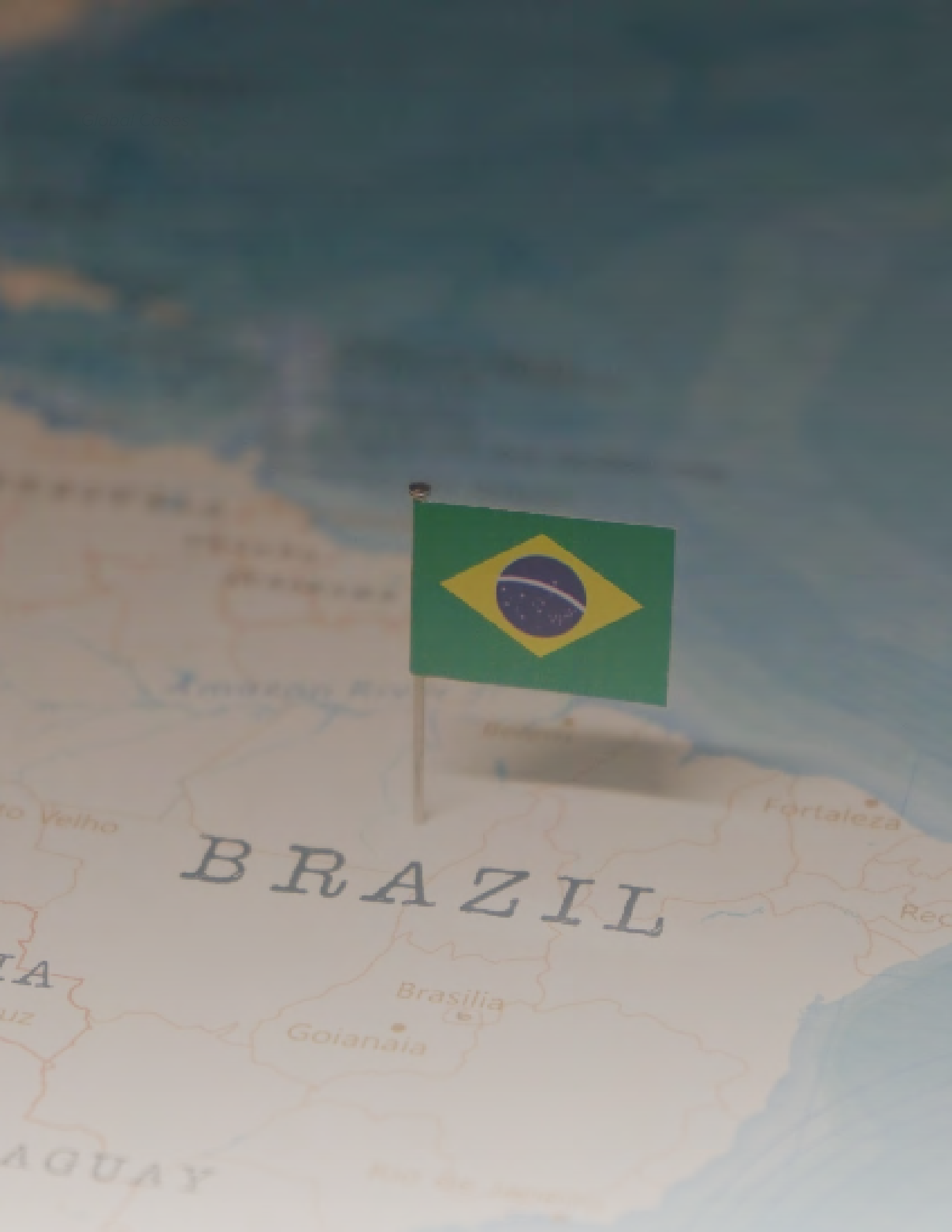
- Customer A spent £36,137 ($48,800) before the required enhanced due diligence was completed.
- Customer B deposited £73,535 ($99,300) and lost £14,068 ($19,000) in four months. William Hill focused on the net worth of the companies for which the customer was identified as a director rather than establishing their personal income from salary or dividend payments.

Evidence of **source of funds** was not requested in situations where large amounts were staked (bet) and/or lost within short periods including the following:

- Customer 1 staked £19,000 ($25,650) in a single bet
- Customer 2 lost £36,000 ($48,600) in four days
- Customer 3 staked £39,324 ($53,000) and lost £20,360 ($27,500) in 12 days
- Customer 4 staked £276,942 ($373,900) and lost £24,395 ($32,900) over two months

Oversight and account monitoring were also inadequate. William Hill had information that indicated Customer C was placing bets on behalf of unknown third parties but did not have sufficient depth and frequency of monitoring to effectively detect and respond. The customer had winnings of approximately £195,000 ($263,230) when the account was finally suspended in February 2021.

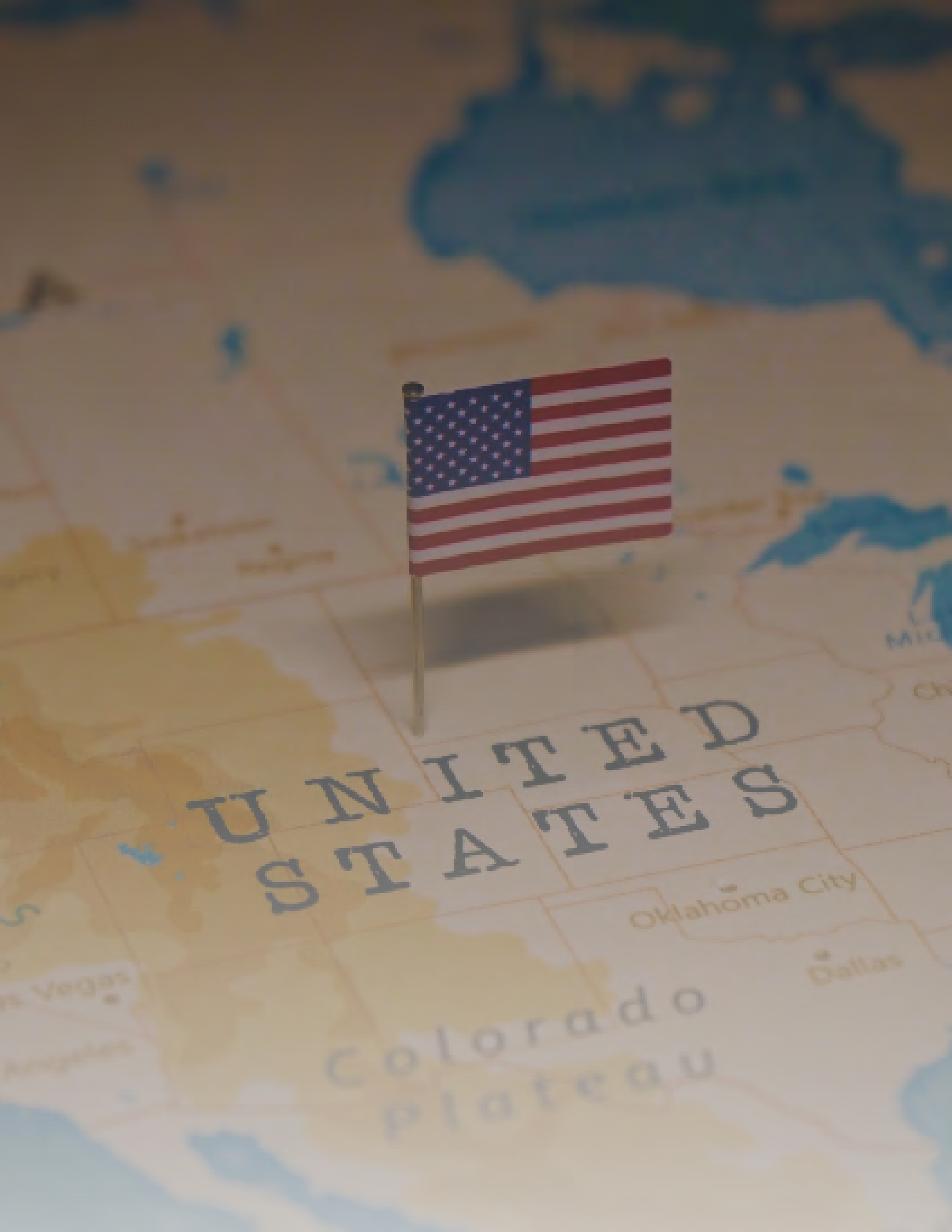
William Hill's **policies, procedures, and controls were also inadequate** and **training was insufficient** on how to identify and manage risks.


BRAZIL
Brasilia
Goianàia
Fortaleza

Brazil: Sports Betting

A Brazilian Parliamentary Commission of Inquiry (called “CPI das Apostas Esportivas”), which has been ongoing since 2023, identified links between organized crime groups and sports betting platforms, including use of shell companies and match fixing.

Also in Brazil, the São Paulo Public Ministry (MPSP) and Military Police arrested six suspects in June 2025 as part of Operation Cash Out (Operação Cash Out). According to MPSP, the group laundered drug trafficking proceeds, which were primarily laundered using online betting platforms.


UNITED
STATES
Oklahoma City
Dallas
Colorado
Plateau

United States: Card Club

Lake Elsinore, 2024

FinCEN imposed a civil money penalty of $900,000 against Sahara Dunes Casino, LP, doing business as Lake Elsinore Hotel and Casino. Lake Elsinore is a "card club" in California which operates 22 tables and offers card games such as poker. It is subject to the Bank Secrecy Act (BSA). During the relevant period from 2014 – 2019:

- Lake Elsinore did not undertake an institutional risk assessment. Instead, its 2018 AML program "Risk Assessment and Profile" consisted primarily of a list of factors with little relevance to Lake Elsinore or gaming. The document also stated that Lake Elsinore was not a cash-intensive business whereas, as a card club, it dealt in large amounts of cash.

- Lake Elsinore did not have an appointed compliance officer until 2017. After that, the responsibility was assigned to the person already holding the position of Chief Operations Officer, who did not have professional experience or training related to BSA compliance.

- The club did not have adequate policies, procedures, and controls in place. It did not effectively track chip cashing, for example bartenders cashed out clients' chips, and there were multiple inaccuracies and inadequacies in written policies and procedures.

- Lake Elsinore failed to file timely Currency Transaction Reports and Suspicious Activity Reports, or did not file at all. Staff were confused about what information had to be recorded to meet reporting requirements, how to record it, or to whom information must be provided.

- Prior to 2016, no testing was conducted of Lake Elsinore's AML program, and to the extent that testing was subsequently conducted it was inadequate in scope and depth, and it was not independent.

- As of 2017, no staff at Lake Elsinore had received AML training since 2014.

> "Lake Elsinore operated for years without the most basic AML controls, putting its customers and the U.S. financial system at risk and denying law enforcement information on suspicious activity. This action should serve as a reminder that all financial institutions—regardless of their type or size—must comply with their obligations under the BSA and FinCEN's regulations."
>
> – FinCEN Director Andrea Gacki

Red Flags

Red Flags

There are many red flags that can indicate illicit activity in the gambling/gaming sector. While some of these may appear obvious, and jurisdictions with strong regulation and enforcement may have effective measures in place, all jurisdictions should ensure their regulations impose comprehensive requirements to avoid being targeted by illicit actors searching for weak points.

Additionally, gambling/gaming operators would be well-advised to implement effective counter illicit finance programs, even if not yet mandated by regulation, to ensure they are ahead of likely future regulatory requirements, as well as to minimize the risk of illicit activity.

This section sets out a selection of red flags for gambling and gaming and is not intended to be a complete list of all possible risk indicators.

Red Flags for Gambling/Gaming

Some red flags are applicable to multiple types of gambling/gaming activity. These include:

- Client transactional activity is inconsistent with the client profile (e.g. large bets are placed by individuals expected to have lower income, such as students).
- Client transactional activity is indicative of structuring or pass-throughs (e.g. multiple individuals transfer funds to a single beneficiary).
- There are unexplained changes in the client's gambling/gaming activity.
- The client conducts transactions or bets just below the reporting threshold (e.g. $10,000) or changes their bets to stay under the threshold.
- A client gambles large amounts of money and appears to find losses acceptable. This may indicate that they are spending the proceeds of crime and sees the losses as an acceptable "cost" of laundering.

There are also red flags that are specific to types of gambling/gaming.

Red Flags for Land-Based Casinos

The following red flags are most relevant to land-based casinos:

- The client seeks to buy-in using cash, which appears likely be the proceeds of crime (e.g. it is brought in shoe boxes or plastic bags in bundles of misoriented notes).
- The client arrives with large amounts of cash/funds to purchase chips/ticket/tokens, then after minimal or no gaming, or placing only low value bets, redeems the chips/tickets/tokens for a casino check.
- The client bets large amounts over only a few bets.
- The client closes their casino account after making an initial deposit.
- The client buys chips and leaves the casino taking the chips with them, especially without playing.

  > In 2016 at the River Rock Casino in British Columbia, Canada, CAD$ 12 million in chips had been taken offsite, in comparison with the usual volume of CAD $1 million. The Cullen Commission identified that the chips were being used as stored value instruments.

- The client places bets that ensure minimal losses (e.g. bets equal amounts on a player and the banker or places the same bets on black and red in roulette), ensuring minimal losses and allowing money to be represented as winnings when it is paid out.
- The client works together with other gambler(s) during play, supplies other patrons with cash to purchase chips, or uses other patrons to cash out.
- The client is accompanied to the casino by an individual subject to a gaming ban.
- The client exchanges smaller-denominations of value for larger ones, such as exchanging small bills for larger bills. This may indicate attempts to change denominations associated with illicit activity (e.g. $20) into ones which are less bulky and less closely associated with illicit activity.
- The client exchanges multiple monetary instruments (e.g. travelers checks) for one casino check.
- There are discrepancies between the amount cashed in and out (e.g. an individual named as winning large amount is not recorded as bringing cash in).
- The client has access to multiple overseas bank accounts.
- The client is resident in a jurisdiction subject to currency control restrictions or sanctions, and has few local family or business links.
- The client is part of a junket (see above Australia case).

Red Flags for Online Gambling/Gaming including Online Casinos

The following red flags are most relevant to online gambling/gaming including online casinos:

- The client attempts to open an account using fraudulent identity documents.
- The client closes their account after minimal or no gaming, or placing only low value bets.
- The client bets large amounts over only a few bets.
- The client closes their account after making an initial deposit.
- The client places bets that ensure minimal losses (e.g. bets equal amounts on a player and the banker or places the same bets on black and red in electronic roulette), ensuring minimal losses and allowing money to be represented as winnings when it is paid out.
- Funds deposited by one player are transferred to a third party (e.g. they are withdrawn to a crypto wallet owned by a different person).

  > In addition to being a possible indicator of laundering, this may indicate use of gambling as a cover for illegal sales. For example, a buyer and seller of an illicit substance can use their gambling account to make and receive payment. Once the seller's account is credited, the money can be cashed out claiming it was a successful gamble.

- The client opens multiple gaming accounts or wallets in an attempt to obscure their spending levels or avoid threshold-based due diligence checks.
- The client regularly changes the bank account they use to fund their gaming activities and/or their address.
- The client has access to multiple overseas bank accounts.
- The client is resident in a jurisdiction subject to currency control restrictions or sanctions, and has few local family or business links.
- The customer uses a shared IP address or VPN connection, which may indicate that a group of individuals are using the same device, location, or account to circumvent identity checks or commit fraud.

Red Flags Identifiable by Financial Institutions

While gambling/gaming businesses are well-positioned to identify indicators of laundering, financial institutions whose customers are using their bank accounts to fund gambling/gaming may be able to detect this illicit activity too.

Red flags identifiable by financial institutions include:

- The client's account is funded by casino checks, however the check memo indicates the funds are not the result of casino winnings.
- The client's account activity appears to be circular (e.g. deposits of casino checks followed by bank drafts used at casinos, followed by deposits from casino checks, especially if the memo indicates they are not the result of casino winnings).
- The client's account appears to be used exclusively for casino gaming (e.g. the activity is casino check deposits, bank draft issuances to casinos, or cash withdrawals at casinos, rather than everyday banking such as payroll and bill payments).
- The client issues multiple bank drafts to themselves or third parties that are used at casinos.
- The client's account shows high volumes of gaming activity (e.g. casino checks) and transactions involving high value goods such as real estate or luxury vehicles.
- Credit card activity is primarily casino-related and paid off in cash.

More detailed information can be found in investigations and alerts, such as the U.S. Internal Revenue Service FAQs, the Cullen Commission report, Canada's FINTRAC alert on laundering criminal proceeds through casino-related underground banking which remains relevant, or from the United Kingdom Gambling Commission Guidance.

Compliance Best Practices

Compliance Best Practices

The compliance program for a gambling/gaming business contains similar elements to those applicable to financial institutions. These include:

- ☑ Appoint a compliance officer with responsibility for the program
- ☑ Undertake an organization-level risk assessment
- ☑ Implement written policies and procedures, and effective controls including client due diligence, funding and cashing out, and ongoing monitoring
- ☑ Comply with record-keeping requirements
- ☑ Fulfil reporting obligations and take other action as appropriate
- ☑ Provide training for staff appropriate for their role
- ☑ Maintain and update the compliance program

While there are similarities with financial institution compliance programs, there are also some key differences, in particular relating client due diligence. For financial institutions, the client due diligence process is performed prior to the relationship being established and before any transactions are undertaken. In the gambling/gaming industry, due diligence requirements are applied at various points in the client relationship, usually when specific thresholds or triggers are reached, or if a client is identified as being “high risk”.

While a detailed analysis of every element of a compliance program for the gambling/gaming industry is beyond the scope of this report, this section sets out best practices for key elements. Jurisdictions or regulators may impose more specific requirements.

☑ *Appoint a Compliance Officer*

The organization should appoint a compliance officer who is responsible for the compliance program. This person should have sufficient experience, resources, and authority to be effective.

☑ *Organizational Risk Assessment*

The organizational risk assessment should identify illicit finance risks as they present to that specific type of business taking into consideration its clients, jurisdictions, products and services, and the channels through which its services are offered (e.g. land-based casino vs online gaming).

Some questions the organization could consider are:

- Is the business high volume with many low-spending clients? Is it low volume with high spending clients? Are there occasional customers (e.g. tourists coming to a land-based casino or occasional gamblers who only place online bets during key sporting events)?
- Are there are a large proportion of overseas clients using foreign currency or overseas-based bank checks, debit cards, or electronic payments? Are clients likely to be politically exposed persons (PEPs)?
- Are there likely to be situations where the source of funds cannot easily be established or explained by the client?

Examples of higher risk products and services include:

- Games involving multiple operators (e.g. poker games taking platforms shared by multiple operators) or peer-to-peer gaming, which can facilitate laundering.
- Gaming machines, which may be used to launder stained or fraudulent banknotes.
- Ticket-In Ticket-Out (TITO) or similar technology. TITO enables cash to be inserted into gaming machines, “withdrawn” as TITO tickets after minimal or no gambling, then redeemed to represent legitimate winnings when it is paid out. TITO tickets are also susceptible to theft or fraud.

Examples of higher-risk funding sources include:

- Cash and pre-paid cards, which have a similar risk profile to cash because operators cannot perform the same level of checks as they can on bank accounts
- E-wallets which accept cash or crypto, which may be used to disguise the origin of funds

An organizational risk assessment should also consider risks presented by business partners and suppliers, including their beneficial ownership and source of funds, as well as employees.

☑ *Policies and Procedures – Client Due Diligence*

The level of due diligence performed on a client – and the timing of that due diligence – depend on factors including:

- Client risk profile
- Thresholds
- Triggers

Due diligence requirements range from identification and verification of the customer through to more extensive due diligence including collecting and evaluating the source of funds.

Client Risk Profile

Higher risk clients include those with characteristics that can be readily identified (e.g. through screening) as well as characteristics that can be identified through monitoring over time, including:

- Clients who are PEPs, including family members of PEPs and known associates
- "High spenders", where the level of spending that is considered "high" will vary depending on the specific characteristics of the client
- Junkets, which can facilitate informal movement of funds, obscure the source and ownership of money, and may be associated with criminal networks
- Unknown or anonymous clients, especially if they purchase large amounts of chips then redeem them with minimal or no play
- Infrequent clients such as tourists or infrequent local customers
- Regular clients with changing or unusual spending patterns

What is impersonation fraud?
Impersonation fraud occurs where an individual attempts to hide their real identity, for example because they have known criminal associations or because they are a high-risk customer seeking to avoid enhanced due diligence requirements.
The following lists can be used to assist with identifying impersonation fraud:

- Lists of known fraudulent individuals
- Lists of known fraudulent identity documents
- Lists of individuals associated with fraudulent identity documents
- Registers of deceased persons
- Registers of PEPs
- Lists of sanctioned individuals
- Information on fraud trends and activities

Thresholds

Financial thresholds can be used as an input to client due diligence requirements. The below examples show how a $2,000 * threshold can be applied depending on the gambling/gaming service: ** used for illustrative purposes and not as a recommendation*

- Land-based casinos: identification and verification are required when a customer purchases casino tokens with a value of $2,000 or more.
- Land-based gaming machines: identification and verification are required when a customer pays $2,000 or collects winnings of $2,000 or more.
- Online gambling/gaming: identification and verification are required when a customer deposits funds or withdraws funds/winnings of $2,000 or more.

Triggers

In addition to due diligence performed when a relationship is established and during the client lifecycle, due diligence should also be performed where specific triggers occur, including:

- Money laundering or terrorism financing is suspected.
- There are doubts about the documents previously obtained for identification and verification (e.g. it is later identified that they may have been falsified).
- There are unusual transactional patterns.

☑ *Policies and Procedures – Funding and Cashing Out*

Key control points to identify and intercept illicit funds are when a client is funding their gambling/gaming activity, or when they are cashing out. These represents the points when illicit funds commence laundering and when they are removed with the (attempted) appearance of legitimacy.

Controls that can be put in place to mitigate these risks include:

- Only accepting transactions funded from regulated institutions (e.g. regulated financial institutions or crypto exchanges), which provides additional assurance that the account owner has been subject to identity verification and checks on source of funds.
- A client buying-in with cash, a bank draft, or a certified cheque of $10,000 or more in a 24-hour period must complete a source of funds declaration and provide proof of where the money came from (e.g. a withdrawal record from a regulated financial institution for the corresponding amount).
- Identity verification for all buy-ins of above a specified threshold.

☑ *Policies and Procedures – Ongoing Monitoring*

Operators should monitor customer transactions using appropriate technology and detection methods for their business type. Some examples are:

- Monitor activity and patterns for all high-risk customers.
- Monitor customer transactions across multiple outlets/products/platforms to mitigate money laundering potential (e.g. placing bets at multiple different betting shops), including deposits and withdrawals.
- Preventing multiple accounts (called “indexing”). Holding multiple accounts may be used to avoid restrictions or to manipulate betting.
- Block VPNs, which may be used to obscure the location of a customer and/or that multiple individuals are operating the same account.

For land-based premises, ongoing monitoring can include:

- Taking a photograph of new customers on their first visit. This forms part of their client due diligence (CDD) records and assists with tracking.

- Land-based casinos can compare the "total drop" (the cash used to purchase chips) against the amount recorded in individual customer spending. The difference is the amount not attributed to specific customers. By identifying attendance numbers and excluding tracked customers, the average spend per untracked customer can be calculated. This should be subject to ongoing review to inform the organizational risk assessment.

Where unusual activity is identified, it should be investigated and appropriate action should be taken.

☑ *Record-Keeping*

Operators should ensure they fulfil regulatory requirements for retention and disposal of records. For example, they should retain records of the CDD performed, including source of funds, as well as evidence of the ongoing monitoring performed.

☑ *Reporting*

Casinos and other gambling/gaming operators are subject to obligations to report suspicious activities/transactions to their appropriate regulator.

When filing a SAR/STR, the following should be included where available:

- The customer's identity
- The customer's physical description (if available)
- Any records for the customer such as credit or debit card details
- Product preferences and activity (e.g. customer prefers land-based casino gambling but occasionally uses online gaming)

An operator should also undertake other actions as appropriate. This may include terminating the relationships in circumstances such as:

- The customer has been identified or is suspected of attempting to launder or spend criminal proceeds.
- The customer is identified as not being the person they claim to be.
- CDD requirements cannot or have not been complied with.

Where CDD requirements have temporarily not been complied with, for example where a threshold is reached that requires additional CDD but the customer has not yet fulfilled the requirements, the following steps can be taken to mitigate risks:

- Place all customer funds into an account where it is not possible to make withdrawals.
- Deposits and bets may be permitted provided any winnings are locked until CDD is completed.
- Once CDD is completed, the account can be unlocked and business can continue as normal.

If CDD cannot be completed, the relationship should be terminated, as described above, and a SAR/STR should be filed if there are suspicions of criminal activity. The amount repaid should be the funds owed at the time the threshold was reached plus deposits made after that point. Funds should be returned to the originating account.

☑ *Training*

Training should be customized to the operator including its jurisdictions, clients, products and services, as well as the roles of staff. For example, the red flags and typologies applicable to an online sports betting operator will be different from those that apply to a land-based casino.

Training should be mandatory and should include:

- Staff responsibilities under the operator's policies and procedures to prevent money laundering and terrorism financing.
- The risks and red flags specific to that business and the role of the staff being trained.
- The actions required of staff to manage those risks e.g. if a customer is identified as high risk, what are the implications and what steps should be followed.
- The implications of a breach on the operator, its business, and staff, and on the integrity of the financial system.
- The requirements for CDD and when CDD requirements apply, including identification of PEPs.
- The identity, role, and responsibilities of the key contact points such as the responsible officer.

Regulatory enforcement actions, such as William Hill, included findings on the lack of adequate staff training.

☑ *Maintain and Update the Compliance Program*

The compliance program should be adapted and updated to ensure it fulfils regulatory requirements and addresses new typologies and red flags. Operator compliance teams should monitor enforcement actions, regulatory advisories, news, and other resources to identify content relevant to their business. These should then be integrated into the compliance program and communicated to staff.

Conclusion

Joint Action to Protect Financial Integrity

While this report has focused on the action required by operators, the public sector has a key role in countering misuse of the gambling/gaming sector for illicit activity.

Regulators must implement and enforce regulations to set expectations and create a consistent environment. Regulations should include directions on when verification of identity and source of funds are required.

Financial intelligence units and law enforcement must engage closely with operators to respond to incidents of potential criminality. They must also analyze SAR/STRs to identify trends and networks, and communicate findings back to the gambling/gaming industry to enable effective ongoing action.

For jurisdictions in the process of establishing their gambling/gaming industry, the lessons learned from money laundering failures – and the compliance programs that can provide protection – are a valuable resource to provide a head-start for their own initiatives.

By working together, operators, financial institutions, regulators, financial intelligence units, and law enforcement can ensure the gambling/gaming sector continues to generate economic benefits while protecting the integrity of the financial system.

Join Us in Protecting the Integrity of the Financial System

Institute for
Financial Integrity

finintegrity.org