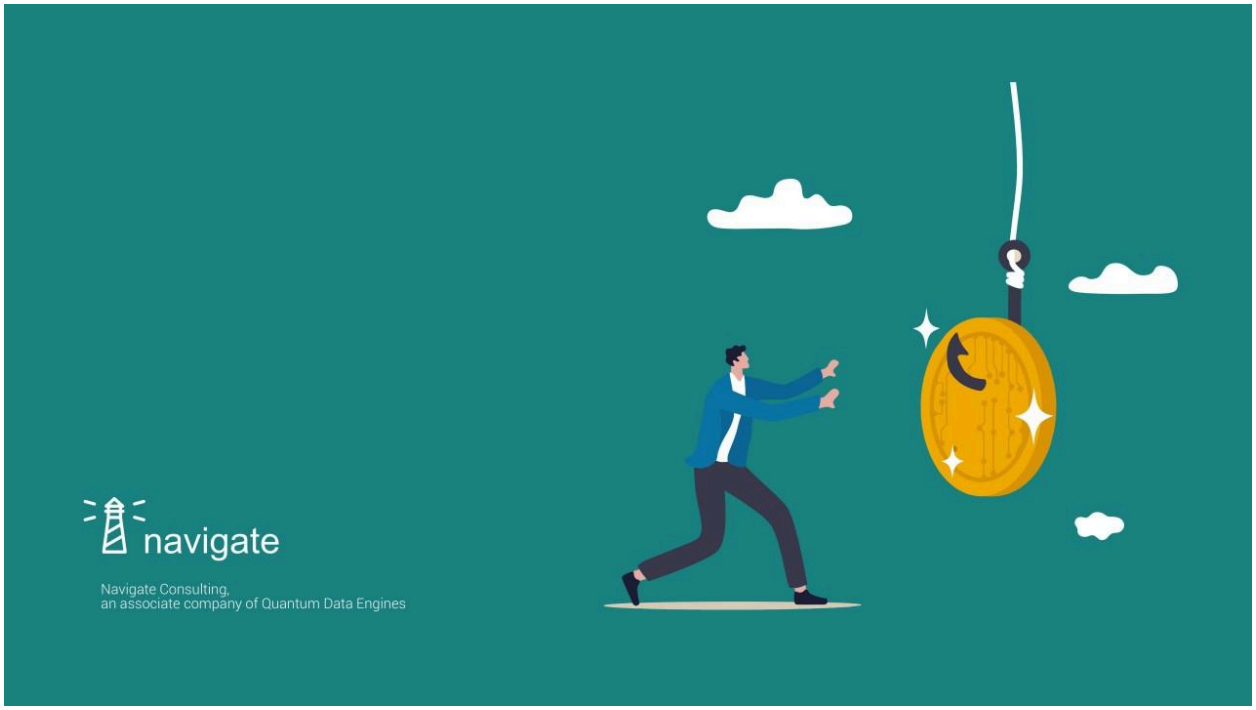


How a California man laundered $263 million | Canada updates AML regime | Money laundering risks in online gambling and more

May, 2026

A recent $263 million laundering case in the U.S shows how financial crime networks continue to evolve and work across sectors, while Canada's updates to Bill C-12 signals a move towards increasing regulatory expectations. This edition also explores common typologies in online gambling, whose anonymity and cross border nature is creating the need for strong AML frameworks and risk detection.

TOP STORY

How a California man helped launder $263 million

By Shivani Shetty

Evan Tangeman of California was sentenced to 70 months in prison for his role in laundering millions of dollars through social engineering and stealing cryptocurrency. The criminal network was active from October 2023 to May 2025, spanning multiple U.S. states, ultimately stealing over $263 million in digital assets. The proceeds were used to support the extravagant lifestyles of the criminals, including luxury homes, expensive cars and high-end consumer goods.

While Evan Tangeman enabled the group to move illicit proceeds, the criminal group also included database hackers, organisers and residential burglars to steal hardware cryptocurrency wallets. Members and associates of the social engineering enterprise used stolen virtual currency to purchase luxury items. Tangeman converted the stolen cryptocurrency into fiat cash and worked with real estate agents in Los Angeles to procure mansions for members of the social engineering enterprise. The members were unemployed young men, often under 20 years old, who had to avoid drawing attention for renting homes for $40,000 to $80,000 per month with no legitimate source of income.

One of the co-conspirators would convert stolen digital assets into cash and legitimate-looking transactions. He established multiple shell companies to open bank accounts and create an image of legitimacy, routing funds through layered blockchain techniques and coordinated wire transfers. Since the group spent lavishly on luxury items, to conceal ownership, he registered assets under shell companies and recruited paid “straw signers” to act as nominal owners, masking the involvement of young, unemployed co-conspirators.

This case highlights the vulnerabilities in property transactions since high-value rental properties in Los Angeles and Miami were secured despite no visible income. Given the emergence of such risks, FinCEN's Final Rule, effective March 1, 2026, requires filing of the Real Estate Report in non-financed residential real estate deals, which includes beneficial ownership, transferee and payment details.

Institutions can adopt the following measures to detect and prevent similar schemes:

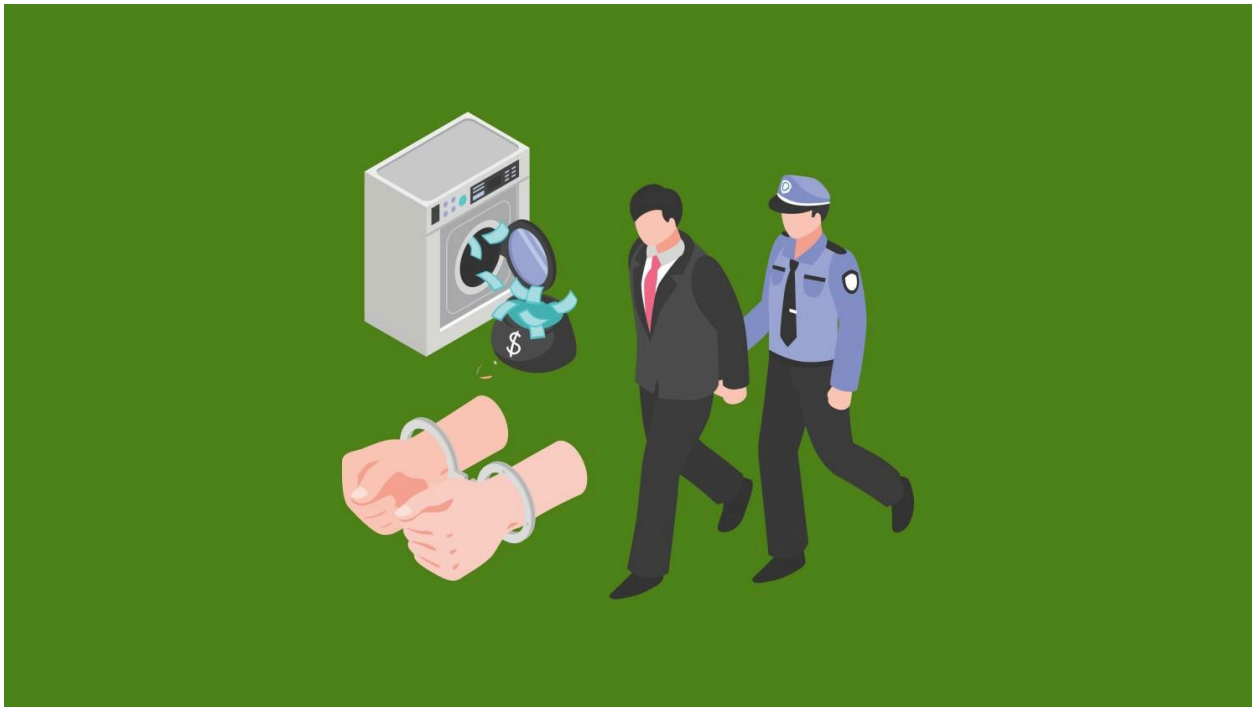
- Source of Funds Verification: The monitoring of high-value transactions, especially crypto-to-fiat conversions to ensure clear and legitimate origin of funds
- Beneficial Ownership: Identify the true individuals behind shell companies and high-value asset purchases
- Behavioral Monitoring: Flag mismatches between customer profiles such as young, unemployed individuals and high-value transactions or lifestyles
- Enhanced Due Diligence (EDD): Apply additional checks on high-risk customers, including those dealing in crypto or luxury assets

This case is an example of the increasing use of technology and cryptocurrency to conduct large scale money laundering operations. It is critical that AML frameworks at financial and non-financial institutions have a holistic approach that analyses behavioral, transactional, and ownership information.

Source: U.S Department of Justice

NEWS SNIPS FROM AROUND THE WORLD

[Collated from other publishers and sources from the Internet, as referenced after each snippet]



Taiwanese man and 6 bank managers laundered NT $3.6 billion

Prosecutors in Taichung have indicted a local businessman and six bank managers for their involvement in money laundering through fraud and gambling. Prosecutors traced suspicious transactions across multiple accounts. They found that the fraudster collaborated with branch managers from a bank to open corporate accounts for 12 shell companies between September 2024 and April 2025. These managers not only facilitated the account setup but also raised transfer limits to as much as NT$20 million and failed to properly respond to money laundering alerts. Despite triggering internal warnings, the accounts were not suspended or restricted, allowing continuous movement of illicit funds. Approximately over US$114 million was funnelled through these accounts.

Source: Focus Taiwan

FIU-IND signs MoU with SEBI for information sharing

India has taken a significant step to strengthen its fight against financial crime by signing a Memorandum of Understanding (MOU) between the Financial Intelligence Unit-India (FIU-IND) and the Securities and Exchange Board of India (SEBI). This partnership aims to improve coordination and information sharing between the two agencies to better detect and prevent money laundering and terrorist financing. Under the agreement, both bodies will exchange relevant financial data, enhance reporting standards for regulated entities, and work together on risk assessments and identifying suspicious transactions. The collaboration also includes training and awareness initiatives to improve compliance with AML/CFT regulations, along with regular reviews to ensure effective implementation.

Source: PIB

Ireland police caution citizens against cryptocurrency fraud

The Police Service of Northern Ireland (PSNI) has issued a warning to the public following a rise in cryptocurrency-related fraud cases, highlighting the growing financial and emotional impact on victims. Authorities have reported that these scams are becoming increasingly sophisticated, often targeting individuals with promises of high returns through seemingly legitimate investment opportunities. Between April 2024 and April 2025, police recorded 192 reports of investment fraud, resulting in losses of over £3.6 million. The financial loss of the victims has increased to £5 million for the period of April 2025 to April 2026. The PSNI is urging individuals to exercise caution when approached with investment opportunities involving cryptocurrency.

Source: Police Service of Northern Ireland

AUSTRAC flags AML weaknesses and money mule risks in foreign-owned banks

AUSTRAC(Australia Transaction Reports and Analysis Centre) has flagged serious money laundering risks in foreign-owned banks. Despite processing a high volume of cross-border transactions, many entities have been found to possess inadequate monitoring systems. Businesses that appear low-risk might still be exposed to higher-risk clients, including politically exposed persons (PEPs), trusts, foundations, and high-net-worth individuals. Money mule accounts are widely used by criminals to move illegal funds through other people's bank accounts to avoid detection. The regulator warned that poor reporting, weak transaction monitoring, and high exposure to global money flows could allow illicit funds to move across borders unnoticed, highlighting the need for stronger controls and better detection of suspicious activity.

Source: AUSTRAC

Bank of Bhutan fined Nu 228 M for AML failures

The Bank of Bhutan was fined following an incident due to a major technology overhaul. According to the Central Bank, this is not an isolated incident, but rather a result of weak governance, poor internal controls, and delays in reporting suspicious transactions. The bank was fined over Nu 228 million and ordered to strengthen its monitoring systems, fix reporting gaps, and hold responsible officials accountable.

Source: Royal Monetary Authority Of Bhutan

REGULATORY UPDATE

By Neha Treesa Joy

Canada tightens AML regime

On March 26, 2026, Bill C-12 introduced several important changes that significantly strengthened Canada's anti-money laundering (AML) framework, particularly in terms of enforcement, accountability, and compliance expectations.

One of the most notable changes is the increase in maximum administrative monetary penalties (AMPs). Regulators now have the authority to impose higher financial penalties on entities that fail to meet AML obligations. The penalties have increased by 40% for each violation category. The new maximum penalties are $40,000 for minor, $4 million for serious and $20 million for very serious violations. The legislation introduces a

mandatory compliance agreement regime where organizations identified as non-compliant may be required to enter into enforceable agreements committing to specific corrective actions. This ensures that compliance gaps are actively addressed and resolved within defined timelines, rather than relying solely on penalties.

Another key development is the introduction of higher standards and expectations for AML compliance programs. Regulated entities are now expected to implement more robust controls, including enhanced risk assessments, stronger internal monitoring, and improved documentation.

The bill also prohibits opening accounts for anonymous clients or under clearly fictitious names, reinforcing the importance of strong customer identification and due diligence as the foundation of AML compliance. This ensures greater transparency in financial transactions and reduces risks for financial institutions.

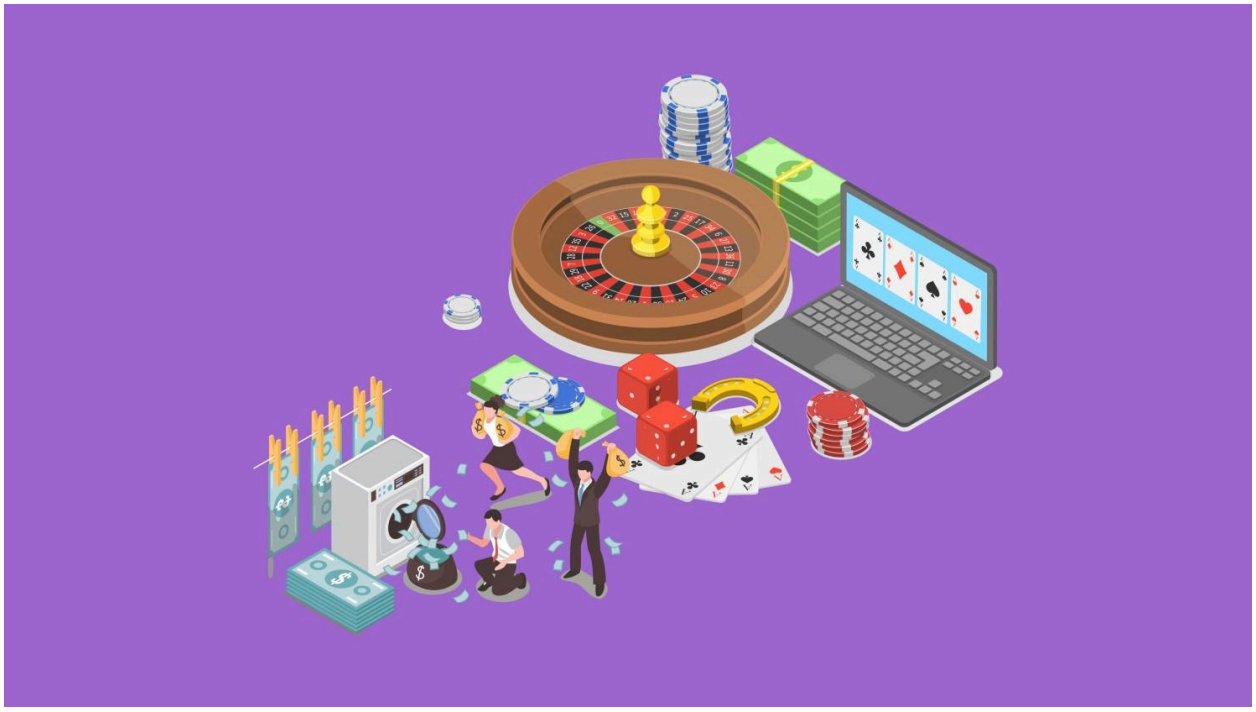
At the same time, the bill expands the enforcement and monitoring powers of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), granting it greater authority to oversee compliance, conduct examinations, and take enforcement actions, thereby strengthening regulatory oversight and ensuring more consistent adherence to AML requirements.

Source: Parliament of Canada

DOMAIN MATTERS

Money laundering through online gambling: key risks and controls

By Adhila Thirumalai



The gambling industry acts as a convenient platform for criminals to launder illicit funds. It includes a wide variety of businesses that handle large and rapid transactions (often in cash), such as physical casinos, online casinos, bars and clubs housing poker machines, and both physical and online sports betting services.

Online gambling platforms, in particular, present elevated risks. They offer a greater degree of anonymity, support the cryptocurrency payment process, allow high volumes of

fast transactions, and facilitate cross-border fund movements. These characteristics make them highly attractive to criminals seeking to obscure the origin and destination of illicit funds.

Following are some common typologies:

- Cash in, Cash out: The most common laundering method involves converting illicit funds into gambling credits, engaging in minimal or low-risk betting, and then withdrawing the funds as “winnings”. Criminals create an appearance of legitimate gambling activity by depositing illicit funds into an online betting account, placing limited risk wagers, and cashing out shortly after. To avoid detection, funds are often split across multiple accounts or withdrawn in different jurisdictions. In more sophisticated schemes, organised networks distribute smaller amounts across numerous individuals and accounts to bypass reporting thresholds.
- Chip Dumping/Collusion: Players intentionally manipulate the outcome by ensuring that one person consistently loses while another gains, a tactic commonly referred to as chip dumping. This practice enables discreet value transfer without relying on traditional banking channels. It is often used to settle debts across borders, making it difficult for authorities to trace the transaction flow.
- Debt settlement: Illicit funds are used to settle the gambling debts of other players, followed by repayment through formal financial channels. The origin of the money is obscured, as the funds re-enter the financial system under the appearance of legitimate transactions.

While money is laundered through primary gambling services, criminals also use other non-gambling instruments and assets such as cryptocurrencies, shell companies and real estate as additional layers of complexity in obscuring the origins of illicit funds.

Online gambling's anonymity, speed, and global reach make it highly vulnerable to money laundering through methods like cash-in-cash-out and collusion. The integration of cryptocurrencies further compounds these risks. To mitigate these risks, online gambling operators and financial institutions must adopt a comprehensive and risk-based approach to anti-money laundering controls. This includes implementing robust customer due diligence measures, such as strong identity verification and enhanced scrutiny for high-risk customers, alongside continuous monitoring of customer activity. Advanced transaction monitoring systems should be deployed to detect unusual betting patterns, rapid fund movements, and behaviours indicative of structuring or collusion.

Source: The Isle of Man Financial Intelligence Unit

Navigate Consulting enables banks and financial institutions to better understand Financial Crime Management and make the most productive use of their AML and Fraud Management systems through training and knowledge sharing.