Know when to fold ‘em: Special bulletin on money laundering through online gambling sites

February 23, 2024

In light of online gambling’s evolution and the increased money laundering risks associated with it, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has issued a special bulletin on laundering the proceeds of crime through online gambling sites (the Special Bulletin). The Special Bulletin is important for businesses servicing casinos and other online gambling sites, including payment service providers (PSPs), money service businesses (MSBs) and financial institutions such as banks.

The Canadian government has elevated the money laundering threat of unlicensed online gambling from high to very high,[1] highlighting risks associated with both licensed and unlicensed gambling sites. Understanding and implementing FINTRAC’s guidance is crucial for maintaining compliance in this sector.

This may be an opportune time to review your business’s anti-money laundering (AML) compliance program to ensure it incorporates the Special Bulletin’s guidance, particularly if you are an MSB, PSP or a financial institution that works with or supports casinos and other gambling sites.

What you need to know about the Special Bulletin

- **Scope:** The Special Bulletin provides specific guidance on money laundering and terrorist financing risks, supporting FINTRAC reporting entities involved in the online gambling sector. As with AML programs of businesses in all relevant sectors, it is crucial that businesses implement robust controls for detecting and reporting suspicious transactions, enabling FINTRAC to disclose actionable financial intelligence to law enforcement and national security agencies.
- **Key risks identified:** The Special Bulletin warns of increased risks associated with online gambling sites that operate outside strict legal and regulatory boundaries, particularly in locations with weak AML laws and controls and/or highly secretive banking regulations.
- **Suspicious trends and patterns:** The Special Bulletin, based on FINTRAC’s analysis of suspicious transaction reports (STRs) from 2016 to 2023, identifies trends in laundering through online gambling. Rapid and frequent online gambling transactions that appear circular – to and from online gambling sites –

suggest accounts exist mainly to facilitate laundering through online gambling. Generally, bank accounts (deposits) are still a key tool for many methods of money laundering.

- **To STR or not:** Reporting entities must assess the facts and money laundering indicators within the full context of a transaction to determine if there are reasonable grounds to suspect a connection to money laundering or terrorist financing activities. This assessment will guide the decision on whether to submit a STR to FINTRAC as soon as practicable. Proof of money laundering is not required to meet the reporting threshold, but it should be more than a "hunch".
- **Money laundering indicators:** All impacted businesses (and relevant personnel) should review the Special Bulletin's list of indicators specific to online gambling activities to understand the transaction patterns and contextual factors that warrant further investigation.
- **Upcoming regulatory changes:** Forthcoming compliance requirements under the *Retail Payment Activities Act* and its regulations mark a shift in Canada's regulatory approach. Starting Nov. 1, 2024, certain PSPs will be required to register with the Bank of Canada, with a strict deadline for submitting applications by Nov. 15, 2024. This new mandate underscores a commitment to enhancing the supervision of PSPs, with the aim of bolstering national security, mitigating operational risk, and safeguarding end-user funds in Canada's retail payment sector

Context

The digital transformation of the gambling industry has led to a surge in online gambling, projected to reach US$100 billion by 2026. This shift to online platforms was accelerated by the COVID-19 pandemic, with lockdown measures pushing gamblers to seek alternative avenues for gaming. In Canada, this surge has coincided with regulatory developments, including the legalization of single-event sports betting on August 27, 2021, and the entry of new gambling operators into the market.

However, this surge has not been without its challenges. As the migration to online platforms continues, these sites pose a heightened risk for money laundering and terrorist financing activities. These sites, often located in jurisdictions with weak AML and anti-terrorist financing regimes, present an increased risk of facilitating illicit activities. In response, Canada's Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing, released in March 2023, elevated the threat level associated with unlicensed online gambling from high to very high.

FINTRAC's STR analysis and additional intelligence on online gambling

Building on this context, FINTRAC's analysis provides deeper insights into the specific patterns and trends in money laundering through online gambling sites.

The Special Bulletin synthesizes findings from FINTRAC's examination of STRs spanning 2016 to 2023, augmented by insights from various financial intelligence bodies and organizations across the globe. It delineates emergent patterns and trends suggestive of laundering crime proceeds through online gambling platforms, including:

a) Exploitation of financial entities and MSBs, including PSPs

Operators of unlicensed gambling sites may exploit Canadian bank accounts for laundering, despite not holding accounts with Canadian financial institutions. These companies often operate from jurisdictions with weak AML regimes and may use secretive banking and tax haven capabilities. Consequently, bank accounts may show signs of misuse through excessive email money transfers, ATM smurfing, and mismatched cash deposits. Particularly indicative of laundering are circular patterns in bank accounts, where funds are received and sent back to the same gambling sites multiple times without regular banking activity.

b) Prepaid cards and vouchers

Prepaid cards and vouchers are high-risk funding methods on online gambling sites due to their potential to mask the origins of illicit funds. Reporting entities can track such card purchases made with debit or credit cards at retail outlets. Users often load these cards - sometimes several times a day - with funds from various sources, including cash and bank transfers. These funds are then quickly used at unlicensed gambling sites or for e-wallet transactions.

c) E-wallets and PSPs

Individuals laundering through online gambling often utilize e-wallets and PSPs to facilitate deposits and withdrawals between bank accounts and accounts at gambling sites.

d) Virtual currencies

Unlicensed online gambling sites increasingly deal in virtual currencies, attracting Canadian players with the allure of instant and potentially pseudo-anonymous cross-border payments. These sites are particularly vulnerable to money laundering, especially those without stringent customer verification, beneficial ownership transparency, or betting limits. Criminal may target these sites, employing MSBs to funnel potentially illicit virtual currency funds.

e) Exploitation of licensed online gambling sites to launder crime proceeds

Money launderers and organized crime groups don’t limit themselves to unlicensed gambling platforms; they also take advantage of regulated sites. FINTRAC has documented several suspicious behaviors and typologies employed by money launderers, including:

- Providing false or mismatched personal information to gambling operators, including forged identity and/or income verification documents, to evade gambling sites’ “know your client” procedures.
- Using “mule accounts,” or multiple accounts controlled by the same individual.
- Buying prepaid cards/vouchers using suspected proceeds of crime, which were used to deposit funds into gambling accounts, followed by withdrawals through wire or e-transfer to a Canadian bank account under the guise of gambling winnings.

- Sudden changes in depositing/withdrawal activity, such as sudden and uncharacteristic spikes in deposits.
- Minimal gambling activity before withdrawal or exclusively betting on low-risk matches.
- “Chip-dumping,” a method that involves purposely losing to another player early on in a game.
- Unusual betting behavior that cannot be explained, or activity that is indicative of match fixing or other illicit activity.
- Evidence of account sharing, where a gambling account is accessed from locations that are inconsistent with the client’s registered address or log-in history, further indicates that the account is being used for passthrough activity.

To STR or not to STR?

Reporting entities must base their decision to submit a STR to FINTRAC on more than mere intuition. While proof of money laundering is not required, entities must carefully consider the facts, context, and money laundering indicators (i.e., red flags) associated with a transaction. Although an individual indicator may not seem suspicious on its own, it may prompt reporting entities to scrutinize the transaction further. Any aggravating and mitigating factors uncovered by an internal investigation should be weighed as part of the determination. By evaluating the transaction in its entirety, entities can determine if additional facts or contextual elements exist that would warrant submitting a STR to FINTRAC, as outlined in the FINTRAC Guidance on Suspicious Transaction Reports.

Money laundering indicators for online gambling

Reporting entities are required to evaluate money laundering indicators comprehensively, considering the full context of a client’s conduct and surrounding circumstances of a transaction(s) to establish reasonable suspicion for suspecting a money laundering offence. According to FINTRAC, the following indicators are critical for businesses and personnel in online gambling to be aware of in support of a robust compliance program:

a) Indicators for financial entities and MSBs, including PSPs, involving online gambling

- Transactional activity is inconsistent with the client’s apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- Excessive transactions with one or more gambling sites that are not provincially or federally authorized.
- Excessive transactions with one or more gambling sites that do not require any know-your-client information from users.
- Excessive transactions with one or more gambling sites that do not publish information about their ownership or their jurisdiction of registration.
- Excessive transactions with one or more gambling sites that do not impose limits on volumes and values of bets.
- Client’s wallet has direct and/or indirect exposure to virtual currency mixers/tumblers and online gambling sites.

- Deposits (e.g. through automated banking machine, in-branch, email transfers, other forms of electronic transfers) are followed rapidly by transfers or credit card payments to gambling sites, virtual currency exchanges, and/or PSPs known for facilitating transactions with gambling sites.
- Client's account activity appears to be circular in nature (e.g. client engaged in repeated cycles of receiving online gambling disbursements followed by more outbound transfers to the same gambling sites.)
- Client's account appears to be used exclusively for online gambling at one or more websites with no evidence of everyday banking activity.
- Excessive transactions with PSPs and/or e-wallets known for facilitating transactions with gambling sites.
- Client's account receives funds from online gambling sites, or PSPs known for facilitating transactions from gambling sites, without having first sent funds to the same gambling sites.
- Client's account receives an excessive number of email money transfers from unrelated third parties, especially where the remittance information references gambling terms (e.g. jackpot) or gambling sites.
- Information provided by the client (e.g. email address, phone number) or social media accounts is linked to an unlicensed gambling site.
- Client frequently reload prepaid cards multiple times on the same day and consecutive days for the purpose of sending funds to online gambling sites.
- Round-dollar transactions are made at retail outlets (e.g. convenience stores) indicative of prepaid card purchases.
- Adverse media or other reliable sources identify a client, or related transacting parties, as linked to criminal activity.

b) Indicators for licensed Canadian online gambling sites

- Transactional activity is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- Client provides information/identification that is suspected to be false, stolen, altered, inaccurate, forged, based on aliases or generic addresses such as post office boxes.
- Client opens more than one account under different identities (e.g. friends, family) and uses the same IP address when logging in.
- Client's details for a funding/deposit method do not match player registration details (e.g. credit card or bank account details do not match the player's name).
- Client engages in limited or no gaming activity, despite significant deposits to accounts, followed by a request to withdraw in excess of any winnings.
- Client requests the transfer of winnings to the bank account of another party, or to a high-risk jurisdiction.
- Geolocation of client log-ins are not consistent with registered client addresses or log-in history.
- Client's deposit and withdrawal methods (i.e. player makes deposits using e-wallets and prepaid cards, and withdraws using wire transfer to a bank account) are inconsistent.
- Client attempts to register more than one account with the same operator.
- Common credit card used by multiple online players for deposits.
- Notification of a chargeback on the financial instrument used by a client for deposit, indicative of unauthorized use.

- Client makes excessive deposits using prepaid cards, which may involve an excessive number of cards.
- Client deposits funds well in excess of what is required to sustain usual gambling patterns.
- Client suddenly changes their gambling patterns (e.g. sudden increase in deposits and betting activity).
- Client displays suspicious behaviour while gambling (e.g. client engages in chip-dumping in poker, or makes suspicious bets indicative of illicit activity such as match fixing).
- Client appears to be making multiple below-threshold deposits or withdrawals from the same or multiple gaming sites to avoid reporting thresholds.
- Clients use common bank account that are used by multiple online players for disbursements.
- Adverse media or other reliable sources identify a client, or related transacting parties, as linked to criminal activity.

The Special Bulletin serves as a crucial reminder for MSBs (including PSPs) and other reporting entities to remain vigilant and proactive in their compliance efforts amidst evolving money laundering and terrorist financing risks.

BLG offers specialized services to assist in reviewing and updating compliance programs, ensuring your business is prepared for upcoming regulatory changes and can effectively mitigate risks. For assistance with your AML needs, navigating the upcoming RPAA registration process for PSPs, or for any related inquiries, please reach out to our key contacts below.

[1] Government of Canada, Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (March 2023) at 19.

By

Cindy Y. Zhang, Matthew Connors, Kaliopi Dimitrakoudis

Expertise

Banking & Financial Services, Financial Services, FinTech

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749