Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada
Canada

Reference number: FINTRAC-2024-SB001
January 2024

Special Bulletin on laundering the proceeds of crime through online gambling sites

Purpose

Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) produces strategic intelligence on the nature and scope of money laundering and terrorist activity financing. This Special Bulletin provides background and updated information on online gambling intended to support reporting entities, especially those involved in online gambling, as well as banks and money services businesses, including payment service providers. Its purpose is to help identify and assess money laundering and terrorist activity financing risks, apply controls and measures to mitigate these risks, and effectively detect and report suspicious transactions to FINTRAC. By reporting suspicious financial activity, reporting entities enable FINTRAC to disclose actionable financial intelligence to law enforcement and national security agencies in the detection, deterrence and prevention at all stages of money laundering (placement, layering and integration) and the financing of terrorist activities.

Project Dolus

Project Dolus targets the laundering of proceeds from various crimes through online gambling sites.

Background

In an increasingly digitalized world, the prevalence of online gambling has skyrocketed, with the industry projected to grow to USD 100 billion by 2026, according to the International Center for Gaming Regulation. Industry growth accelerated during the COVID-19 pandemic, as traditional brick-and-mortar casinos closed their doors. This forced many gamblers to move to online platforms. In Canada, this industry growth has coincided with new regulatory changes, such as the legalization of single event sports betting that came into force August 27, 2021 and the entrance of new gambling operators.

Although online gambling site operators can and should take actions to mitigate such risks, transactions involving sites operating outside legal and regulatory authorities—particularly if situated in jurisdictions with weak anti-money laundering or anti-terrorist financing regimes—may present a higher risk of facilitating money

laundering or terrorist financing activity.[1] In March 2023, Canada's Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing upgraded the money laundering threat from unlicensed gambling, including specifically online gambling, from high to very high. Law enforcement agencies have found that organized crime groups can operate or more easily exploit these sites both in Canada and in foreign jurisdictions accessible from Canadian locations.

Overview of FINTRAC's analysis of suspicious transaction reports and other sources related to online gambling

In preparing this Special Bulletin, FINTRAC analyzed suspicious transaction reports related to online gambling between 2016 and 2023. Additionally, FINTRAC analyzed data from other financial intelligence units, assessments from domestic and international government and non-government organizations, and information from open sources to enhance and corroborate suspicious trends and patterns.

Exploitation of financial entities and money services businesses, including payment service providers, to launder proceeds of crime through licensed and unlicensed gambling sites

Bank accounts provide a crucial step in the placement and layering of proceeds of crime through licensed and unlicensed online gambling sites, hosted both domestically and internationally. As such, bank accounts are vulnerable to exploitation using many laundering methods. For example, bank deposits were found to include excessive email money transfers suspected to be linked to various predicate offenses, such as drug and human trafficking; suspected automated banking machine smurfing[2]; and cash deposits inconsistent with the client's financial standing. These bank accounts were then depleted using rapid and frequent credit card online gambling purchases, transfers to virtual currency exchanges, and/or transfers to payment service providers known for facilitating transactions at gambling sites. Other accounts appeared to exist mainly to facilitate money laundering through online gambling activity. This included transactional activity that appeared circular in nature where funds were received and sent back to the same gambling sites multiple times. These types of accounts often lacked everyday banking activity and primarily consisted of transfers to/from online gambling sites.

Funds derived from Canadian bank accounts may be used to operate unlicensed gambling sites or to facilitate gambling on behalf of others. For example, domestic and foreign gambling sites can be established and operated by organized crime groups using their proceeds of crime. These sites are also used to launder funds related to various criminal activities, such as the purchase of drugs. In one notable case, an organized crime group laundered proceeds of crime by operating an unlicensed gambling site through the accounts of unrelated businesses. Although it will not always be clear that a client is using a bank account to facilitate unlicensed gambling activities, client identifiers (such as a phone number) and adverse media have been useful in linking clients to the operation of an unlicensed gambling site.

---

[1] It should be noted that under the *Criminal Code of Canada*, taking bets is a criminal offence unless conducted and managed by the government of a province, or if there is a prescribed exception such as for private bets. This prohibition includes online casinos and sports betting operations.

[2] Smurfing is a technique that involves breaking down a large amount of criminal proceeds into smaller less detectable transactions.

Although unlicensed gambling sites may not hold accounts at financial institutions in Canada, the companies and individuals that operate these sites have been observed sending funds to Canada-based accounts. Frequently, these gaming companies are located in jurisdictions that have weak anti-money laundering regimes, engage in highly secretive banking, and provide tax haven capabilities. Individuals involved in criminal activity have also been observed gambling on behalf of others at both licensed and unlicensed gambling sites, by receiving email money transfers from unrelated third parties, which reference terms relating to gambling (such as "jackpot") or the names of gambling sites.

Prepaid cards and vouchers

Prepaid cards and vouchers are considered high-risk funding methods at online gambling sites because of their potential use to obscure illicit sources of funds. Although reporting entities lack visibility on the purchase of prepaid cards using cash, they are able to flag online casino gambling cards/vouchers purchased at retail outlets using debit/credit cards.

Reporting entities have observed clients making frequent rounded-sum purchases at retail outlets, such as convenience stores. Additionally, individuals also acquired reloadable prepaid debit/credit cards for the purpose of online gambling. In such instances, individuals frequently topped-up their cards (often multiple times per day) using a variety of funding methods, including cash deposits at multiple locations, frequent and small email money transfers from bank accounts, as well as reload services. These funds were rapidly used for payments at unlicensed gambling sites or transfers to e-wallets known for facilitating transactions with gambling sites.

E-wallets and payment service providers

Individuals who use online gambling sites to launder proceeds of crime frequently use e-wallets and payment service providers to facilitate deposits and withdrawals between bank accounts and accounts at gambling sites. For example, members of organized crime groups were observed depositing funds to unlicensed offshore gambling sites using e-wallets and withdrawing funds using a wire transfer to financial institutions in Canada.

Virtual currencies

Virtual currencies are not considered legal tender and are not accepted at online gambling sites licensed to operate within Canada; however, unlicensed sites are increasingly dealing in virtual currencies.

Virtual currency permits online gambling sites to receive instantaneous and potentially pseudo-anonymous cross-border payments from Canada-based players, despite Canadian legislation and regulations, making offshore gambling sites that accept virtual currency attractive destinations for those seeking to launder proceeds of crime. In particular, sites that are at a higher risk of facilitating money laundering include those that do not require "know your client" information from players, do not publish any information about their beneficial ownership, and do not impose any limits on volumes/values of bets.

Individuals involved in criminal activity may use money services businesses to send suspected proceeds of crime to these types of gambling sites using virtual currency. Additionally, the use of virtual currency mixers/tumblers prior to deposit to or after withdrawal from online gambling sites is a known money laundering typology. Money services businesses were able to detect suspicious behaviour when their client's wallet had direct and/or indirect exposure to both mixer/tumbler services and online gambling sites.

Exploitation of licensed online gambling platforms to launder proceeds of crime

In addition to using unlicensed gambling sites, criminals may also seek to exploit licensed online gambling sites to launder proceeds of crime. Suspicious behaviour was detected by online gambling sites when reviewing clients' identity and source of wealth, deposit and withdrawal methods, and account/gambling activity.

In many cases, money launderers attempt to subvert or mislead online gambling sites' "know your client" process, in order to conceal their identity and/or the source of their funds. In some cases, this involved the provision of false, stolen, and misleading information to gambling operators—including forged identity and/or income verification documents. In other cases, money launderers would provide information that is mismatched (e.g. a player's credit card or bank account details did not match their registration details). The use of mule[3] accounts at online gambling sites is a known typology used by organized crime groups and other criminals to launder proceeds of crime in smaller amounts through a large number of gambling accounts. Gambling sites licensed to operate in Canada only allow prospective gamblers to open one account. As a key indicator of money laundering, multiple accounts controlled by the same individual can be identified with the same internet protocol addresses, client identifiers, repeated and interconnected gambling activity and intermingled financial activity.

Online gambling sites offer prospective money launderers opportunities to conceal the source of their funds by using multiple different deposit and withdrawal methods. For example, a commonly observed typology involved the purchase of 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. Although less common at licensed sites than at unlicensed, individuals made use of payment service providers and e-wallet companies to deposit and withdraw funds. Other suspicious activity included sudden changes in depositing/withdrawal activity, such as sudden and uncharacteristic spikes in deposits.

Furthermore, there were many suspicious patterns involving both gambling accounts and activity. Minimal gambling activity before withdrawal is a common money laundering method used by criminals both at online and brick-and-mortar casinos. At sites that offer sports betting, this behaviour can include clients exclusively betting on low-risk matches, thereby minimizing losses and creating the illusion of gambling before withdrawal. Suspicious gambling behaviour can take many forms. For example, money launderers may attempt to circumvent restrictions on peer-to-peer transactions by engaging in "chip-dumping", a method that involves purposely losing to another player early on in a game. This method has been commonly used in conjunction with credit card fraud, where stolen credit cards are used to deposit funds into one gambling account, and are transferred to another account through chip-dumping. For example, online gambling sites were able to detect the deposit of suspicious funds into gambling accounts upon receipt of chargeback notifications related to the use of credit cards, eChecks, or other financial instruments. Although when considered on their own, chargebacks may simply reflect fraud, they may also represent a money laundering technique when considered in combination with other indicators. Finally, suspicious activity at sports betting sites can include unusual betting activity 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

[3] "Money mule" refers to an individual who, wittingly or unwittingly, transfers or transports proceeds of crime on behalf of a criminal organization or money launderer.

client's registered address or log-in history, further indicates that the gambling account is being used for pass-through activity.

Reasonable grounds to suspect and how to use indicators

How reporting entities determine if they must submit a suspicious transaction report to FINTRAC (for either a completed or attempted financial transaction) requires more than a "gut feel" or "hunch," although proof of money laundering is not required. Reporting entities are to consider the facts, the context as well as money laundering indicators of a transaction. When these elements are viewed together, they create a picture that is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario. Reporting entities must reach reasonable grounds to suspect that a transaction, or attempted transaction, is related to the commission or attempted commission of a money laundering offence before they can submit a suspicious transaction report to FINTRAC.

Indicators of money laundering can be thought of as red flags explaining that something may very well be wrong. Red flags typically stem from one or more characteristics, behaviours, patterns and other contextual factors related to financial transactions that make them appear inconsistent with what is expected or considered normal. On its own, an indicator may not initially appear suspicious. However, it could lead reporting entities to question the legitimacy of a transaction, which may prompt them to assess the transaction. They can then determine whether there are further facts, contextual elements or additional money laundering or terrorist financing indicators that would increase their suspicion to the point where submitting a suspicious transaction report to FINTRAC would be required (see FINTRAC Guidance on Suspicious Transaction Reports).

Money laundering indicators

The following indicators related to the laundering of proceeds of crime through online gambling sites were derived from FINTRAC's analysis of its transactions holdings and other domestic and international sources. These indicators reflect the types and patterns of transactions, along with contextual factors. Indicators should not be treated in isolation; on their own, these indicators may not be indicative of money laundering or other suspicious activity, but may, for example, be related to problem gambling. They should be assessed by reporting entities in combination with what they know about their client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence.

Several indicators may reveal otherwise unknown links that, taken together, could lead to reasonable grounds to suspect that the transaction or attempted transaction is related to the laundering of proceeds of crime through online gambling sites. It is a constellation of factors that strengthen the determination of suspicion. These indicators aim to help reporting entities in their analysis and assessment of suspicious financial transactions.

Reporting entities should also consider that several or all of the listed transactional and contextual indicators play a key role in maintaining a strong compliance program when considered as risk factors in a money laundering and terrorist financing risk assessment of potential and current clients. Understanding and applying these indicators can help mitigate against the money laundering and terrorist financing exploitation of a reporting entity's business. Business-client relationship risk factors dynamically evolve over time and fall into the following categories:

- products, services and delivery channels that create anonymity and obscure source or destination of funds;
- geographical location of the client and their transactions related to high-risk jurisdictions;
- new developments and technologies made available to clients; and
- client characteristics and the purpose of their relationship with a business that define expectations for what are normal or suspicious patterns of activity or transactions.

Please see the following links for FINTRAC's risk assessment guidance and compliance requirements.

- Risk assessment guidance
- Compliance program requirements

Money laundering indicators for financial entities and money services businesses, including payment service providers, 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 payment service providers 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 payment service providers and/or e-wallets known for facilitating transactions with gambling sites.
- ⊗ Client's account receives funds from online gambling sites, or payment service providers 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.

Money laundering 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.

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **#ProjectDolus** or **#Dolus** in Part G – Description of suspicious activity on the Suspicious Transaction Report. More than one hashtag may be included in a G section. See also, Reporting suspicious transactions to FINTRAC.

Contact FINTRAC

- **Email**: guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Special Bulletin FINTRAC-2024-SB001 in the subject line)
- **Telephone**: 1-866-346-8722 (toll free)
- **Facsimile**: 613-943-7931
- **Mail**: FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

FD4-35/2024E-PDF
978-0-660-69326-2

FINTRAC Special Bulletins provide information related to new, emerging and particularly topical methods of money laundering and terrorist activity financing. However, these Bulletins should not be considered legal advice. Please refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations for the full description of the reporting entities' obligations.