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

Numéro de référence : CANAFE-2024-SB001
Janvier 2024

Bulletin spécial sur le recyclage des produits de la criminalité au moyen de sites de jeu en ligne

Objectif

> **Projet Dolus**
>
> Le projet Dolus cible le recyclage des produits de divers crimes au moyen de sites de jeu en ligne.

Conformément à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) produit des renseignements stratégiques sur la nature et la portée du blanchiment d'argent et du financement des activités terroristes. Ce bulletin spécial fournit des renseignements contextuels et à jour sur le jeu en ligne à l'intention des entités déclarantes, plus particulièrement celles du secteur du jeu en ligne ainsi que les institutions financières et les entreprises de services monétaires, y compris les fournisseurs de services de paiement. Il vise à aider ces entités à repérer et à évaluer les risques de blanchiment d'argent et de financement d'activités terroristes, à appliquer des contrôles et des mesures pour atténuer ces risques, et à cerner et à déclarer efficacement les opérations douteuses à CANAFE. En signalant les activités financières douteuses, les entités déclarantes permettent à CANAFE de communiquer des renseignements financiers exploitables aux organismes d'application de la loi et de sécurité nationale aux fins de détection, de dissuasion et de prévention du blanchiment d'argent (placement, dispersion et intégration) et du financement des activités terroristes à toutes les étapes.

Contexte

Dans un monde de plus en plus numérique, la prévalence du jeu en ligne a monté en flèche et cette industrie devrait atteindre 100 milliards de dollars américains d'ici 2026 selon l'International Center for Gaming Regulation. La croissance du secteur s'est accélérée pendant la pandémie de COVID-19, alors que les casinos traditionnels ont fermé leurs portes, ce qui a forcé de nombreux joueurs à passer aux plateformes en ligne. Au Canada, cette croissance de l'industrie a coïncidé avec de nouvelles modifications réglementaires, comme la légalisation des paris sur une seule épreuve sportive, entrée en vigueur le 27 août 2021, et l'arrivée de nouveaux exploitants de sites de jeu.

Bien que les exploitants de sites de jeu en ligne puissent et doivent prendre des mesures pour atténuer les risques liés à la facilitation du blanchiment d'argent ou du financement des activités terroristes, les opérations effectuées sur des sites échappant aux autorités légales et réglementaires, en particulier ceux qui sont situés dans des pays dotés de faibles régimes de lutte contre le blanchiment d'argent ou les activités terroristes,

peuvent présenter un risque plus élevé.[1] En mars 2023, la Mise à jour de l'évaluation des risques inhérents au recyclage des produits de la criminalité et au financement des activités terroristes au Canada a fait passer la menace de recyclage des produits de la criminalité liée au jeu non autorisé, et plus particulièrement au jeu en ligne, d'élevée à très élevée. Les organismes d'application de la loi ont constaté que les groupes du crime organisé peuvent faire fonctionner ou exploiter plus facilement ces sites au Canada ainsi que dans des pays étrangers où les sites Web sont accessibles à partir du Canada.

Aperçu de l'analyse effectuée par CANAFE des déclarations d'opérations douteuses et d'autres sources liées au jeu en ligne

Pour préparer ce bulletin spécial, CANAFE a analysé des déclarations d'opérations douteuses liées au jeu en ligne, datant de 2016 à 2023. De plus, CANAFE a analysé des données provenant d'autres unités du renseignement financier, des évaluations d'organisations gouvernementales et non gouvernementales nationales et étrangères, ainsi que de l'information provenant de sources ouvertes afin de mieux comprendre les tendances ainsi que les comportements suspects et de les corroborer.

Exploitation d'entités financières et d'entreprises de services monétaires, y compris des fournisseurs de services de paiement, pour blanchir les produits de la criminalité au moyen de sites de jeu autorisés et non autorisés

Les comptes bancaires sont utilisés à une étape cruciale dans le placement et la dispersion des produits de la criminalité dans des sites de jeu en ligne autorisés et non autorisés, hébergés au pays ou à l'étranger. Par conséquent, ils sont vulnérables à l'exploitation au moyen de nombreuses méthodes de blanchiment. Par exemple, on a découvert que les dépôts bancaires comprenaient des virements de fonds excessifs par courriel soupçonnés d'être liés à diverses infractions sous-jacentes, comme le trafic de drogues et de personnes, des activités soupçonnées de schtroumpfage au moyen de guichets automatiques bancaires[2] et des dépôts en espèces incompatibles avec la situation financière du client. Ces comptes bancaires ont ensuite été vidés au moyen d'achats rapides et fréquents par carte de crédit sur des sites de jeu en ligne, de virements vers une plateforme d'échange virtuelle ou de virements à des fournisseurs de services de paiement reconnus pour faciliter les opérations sur des sites de jeu. D'autres comptes semblaient servir principalement à faciliter le blanchiment d'argent au moyen d'activités de jeu en ligne. Cela comprenait des opérations qui semblaient circulaires, où les fonds étaient reçus et renvoyés aux mêmes sites de jeu à plusieurs reprises. Bien souvent, ces types de comptes ne présentaient aucune opération bancaire courante et les activités consistaient principalement en des virements à destination ou en provenance de sites de jeu en ligne.

Les fonds tirés de comptes bancaires canadiens peuvent servir à exploiter des sites de jeu non autorisés ou à faciliter les activités de jeu d'autres personnes. Ainsi, des sites de jeu canadiens et étrangers peuvent être établis et exploités par des groupes du crime organisé à l'aide de produits de la criminalité. Ces sites servent également

[1] Il est à souligner que, conformément au *Code criminel du Canada*, la prise de paris est une infraction criminelle, à moins qu'elle ne soit effectuée et gérée par le gouvernement d'une province ou en cas d'exception prescrite, comme pour les paris privés. Cette interdiction s'applique aux casinos en ligne et aux paris sportifs.

[2] Le schtroumpfage est une technique qui consiste à fractionner un montant important de produits de la criminalité en petites opérations difficiles à détecter.

à blanchir des fonds liés à diverses activités criminelles, comme l'achat de drogues. Dans un cas digne de mention, un groupe du crime organisé a blanchi des produits de la criminalité en exploitant un site de jeu non autorisé au moyen de comptes d'entreprises non apparentées. Bien qu'il ne soit pas toujours clair qu'un client utilise un compte bancaire pour faciliter des activités de jeu non autorisées, les identificateurs du client (comme son numéro de téléphone) et les articles défavorables dans les médias ont été utiles pour relier les clients à l'exploitation d'un site de jeu non autorisé.

Bien que les sites de jeu non autorisés ne puissent pas détenir de comptes dans des institutions financières au Canada, on a vu les entreprises et les personnes qui exploitent ces sites envoyer des fonds dans des comptes situés au Canada. Souvent, ces entreprises de jeu sont situées dans des pays qui ont de faibles régimes de lutte contre le blanchiment d'argent, qui pratiquent des activités bancaires très secrètes ou qui sont des paradis fiscaux. Des personnes impliquées dans des activités criminelles ont également été observées en train de jouer pour le compte d'autres personnes dans des sites de jeu autorisés et non autorisés; elles avaient reçu des virements de fonds par courriel de tierces parties non apparentées qui mentionnent des termes liés au jeu (comme « gros lot ») ou les noms de sites de jeu.

Cartes prépayées et bons

Les cartes prépayées et les bons sont considérés comme des méthodes de paiement à risque élevé dans les sites de jeu en ligne, car ils peuvent être utilisés pour masquer des sources de fonds illicites. Bien que les entités déclarantes n'aient pas accès aux renseignements sur l'achat de cartes prépayées avec de l'argent comptant, elles peuvent signaler les cartes ou les bons de jeu de casino en ligne achetés à des points de vente au détail au moyen de cartes de débit ou de crédit.

Les entités déclarantes ont observé des clients faire des achats fréquents avec un montant arrondi dans des points de vente au détail, comme des dépanneurs. De plus, des personnes se sont également procuré des cartes de débit ou de crédit prépayées rechargeables aux fins de jeu en ligne. Dans ces cas, elles ont fréquemment rechargé leur carte jusqu'à la limite (souvent plusieurs fois par jour) au moyen de diverses méthodes de paiement, y compris des dépôts en espèces à plusieurs endroits, de fréquents virements par courriel de petits montants à partir de comptes bancaires ainsi que des services de recharge. Ces fonds ont rapidement été utilisés pour effectuer des paiements dans des sites de jeu non autorisés ou des virements vers des portefeuilles électroniques reconnus pour faciliter les opérations avec des sites de jeu.

Portefeuilles électroniques et fournisseurs de services de paiement

Les personnes qui utilisent les sites de jeu en ligne pour blanchir les produits de la criminalité recourent fréquemment aux portefeuilles électroniques et aux fournisseurs de services de paiement pour faciliter les dépôts et les retraits entre les comptes bancaires et les comptes sur les sites de jeu. Par exemple, on a observé des membres de groupes du crime organisé déposer des fonds dans des sites de jeu non autorisés à l'étranger au moyen de portefeuilles électroniques, puis les retirer par virement électronique vers des institutions financières au Canada.

Monnaie virtuelle

La monnaie virtuelle n'est pas considérée comme ayant cours légal et n'est pas acceptée dans les sites de jeu en ligne autorisés à être exploités au Canada. Toutefois, les sites non autorisés traitent de plus en plus d'opérations en monnaie virtuelle.

La monnaie virtuelle permet aux sites de jeu en ligne de recevoir de façon instantanée et potentiellement pseudo-anonyme des paiements transfrontaliers de la part de joueurs canadiens, malgré les lois et les règlements canadiens, ce qui rend les sites de jeu à l'étranger qui acceptent la monnaie virtuelle attrayants pour ceux qui cherchent à blanchir les produits de la criminalité. Plus particulièrement, les sites qui présentent un risque plus élevé de faciliter le blanchiment d'argent incluent ceux qui n'exigent pas de renseignements sur l'identité des joueurs, qui ne publient aucune information sur leur propriété effective et qui n'imposent aucune limite aux volumes et aux valeurs des paris.

Les personnes impliquées dans des activités criminelles peuvent utiliser des entreprises de services monétaires pour envoyer des produits présumés de la criminalité à ce genre de sites de jeu en utilisant de la monnaie virtuelle. De plus, l'utilisation de services de mélange de monnaie virtuelle avant le dépôt sur les sites de jeu en ligne ou après le retrait est caractéristique du blanchiment d'argent. Les entreprises de services monétaires ont été en mesure de détecter des comportements suspects lorsque le portefeuille de leurs clients était directement ou indirectement exposé à la fois à des services de mélange de monnaie virtuelle et à des sites de jeu en ligne.

Exploitation de plateformes de jeu en ligne autorisées pour blanchir les produits de la criminalité

En plus d'utiliser des sites de jeu non autorisés, les criminels peuvent également chercher à exploiter les sites de jeu en ligne autorisés pour blanchir les produits de la criminalité. Les sites de jeu en ligne ont détecté des comportements suspects lorsqu'ils ont examiné l'identité et la source de richesse des clients, les méthodes de dépôt et de retrait, ainsi que les activités liées aux comptes et au jeu.

Dans de nombreux cas, les blanchisseurs d'argent tentent de contourner ou de tromper le processus de renseignements sur l'identité des joueurs sur les sites de jeu en ligne afin de dissimuler leur identité ou la source de leurs fonds. Dans certains cas, ils fournissaient des renseignements faux, volés ou trompeurs aux exploitants de sites de jeu, y compris de faux documents d'identité ou de vérification des revenus. Dans d'autres cas, les blanchisseurs d'argent fournissaient des renseignements qui ne concordaient pas (p. ex., les renseignements sur la carte de crédit ou le compte bancaire d'un joueur ne correspondaient pas aux renseignements fournis à son inscription). L'utilisation de comptes mules[3] dans les sites de jeu en ligne est une pratique connue utilisée par les groupes du crime organisé et d'autres criminels pour blanchir des produits de la criminalité en plus petites quantités au moyen d'un grand nombre de comptes de jeu. Les sites de jeu autorisés à être exploités au Canada ne permettent aux joueurs potentiels d'ouvrir qu'un seul compte. Parmi les indicateurs clés de blanchiment d'argent, on peut déceler de multiples comptes contrôlés par la même personne au moyen d'une même adresse de protocole Internet ou d'un même identificateur de client ainsi qu'en cas d'activités de jeu répétées et interconnectées et d'activités financières entremêlées.

Les sites de jeu en ligne offrent aux blanchisseurs d'argent potentiels l'occasion de dissimuler la source de leurs fonds en utilisant plusieurs méthodes de dépôt et de retrait différentes. Par exemple, une pratique couramment observée concernait l'achat de cartes prépayées ou de bons de paiement à l'aide de produits présumés de la criminalité, qui étaient utilisés pour déposer des fonds dans des comptes de jeu, le tout suivi de retraits par virement télégraphique ou par virement électronique à un compte bancaire canadien sous le couvert de gains de jeu. Bien que ce soit moins fréquent dans les sites autorisés que dans les sites non autorisés, des personnes ont fait appel à des fournisseurs de services de paiement et à des entreprises de portefeuille électronique pour

[3] Une « mule financière » est une personne qui, sciemment ou non, transfère ou transporte des produits de la criminalité pour le compte d'une organisation criminelle ou d'un blanchisseur d'argent.

déposer et retirer des fonds. Dans le cadre d'autres activités suspectes, on a observé des changements soudains dans les activités de dépôt ou de retrait, comme des pics soudains et inhabituels dans les dépôts.

En outre, il y avait de nombreux comportements suspects se rapportant à la fois à des activités et à des comptes de jeu. Le fait de réduire au minimum les activités de jeu avant le retrait est une méthode courante de blanchiment d'argent utilisée par les criminels, tant dans les casinos en ligne que les casinos traditionnels. Dans les sites qui offrent des paris sportifs, cela peut inclure des clients qui misent exclusivement sur des matchs à faible risque, ce qui réduit au minimum les pertes et donne l'illusion que le client a joué avant d'effectuer un retrait. Les comportements de jeu suspects prennent de nombreuses formes. Par exemple, certains blanchisseurs d'argent peuvent tenter de contourner les restrictions sur les transferts entre pairs en perdant délibérément au profit d'un autre joueur au début d'un jeu. Cette méthode est couramment utilisée de pair avec la fraude par carte de crédit. Ainsi, des cartes de crédit volées sont utilisées pour déposer des fonds dans un compte de jeu, qui sont ensuite transférés à un autre compte à la suite de parties perdues délibérément. Par exemple, des sites de jeu en ligne ont été en mesure de détecter le dépôt de fonds suspects dans des comptes de jeu à la réception d'avis de rétrofacturation liés à l'utilisation de cartes de crédit, de chèques électroniques ou d'autres instruments financiers. Bien que, prises isolément, les rétrofacturations puissent simplement indiquer un cas de fraude, elles peuvent également indiquer le recours à une technique de blanchiment d'argent, de concert avec d'autres indicateurs. Enfin, les activités suspectes dans les sites de paris sportifs peuvent comprendre des activités de paris inhabituelles qu'on ne peut expliquer ou des activités qui indiquent des matchs truqués ou d'autres activités illicites. Le partage avéré d'un compte de jeu, auquel l'accès a lieu à partir d'emplacements qui ne correspondent pas à l'adresse inscrite du client ni à son historique d'ouverture de session, peut également indiquer que le compte sert à des activités de transfert.

Motifs raisonnables de soupçonner et utilisation des indicateurs

Les entités déclarantes doivent appuyer leur décision de déclarer des opérations douteuses à CANAFE (qu'elles soient réalisées ou tentées) sur plus qu'une « intuition » ou qu'un « pressentiment », bien que la preuve du blanchiment d'argent ne soit pas exigée. Les entités déclarantes doivent tenir compte des faits, du contexte ainsi que des indicateurs de blanchiment d'argent entourant une opération. En considérant ces éléments ensemble, il est possible de créer une image essentielle à la distinction d'une opération douteuse d'une opération raisonnable dans un scénario donné. Les entités déclarantes doivent avoir des motifs raisonnables de soupçonner qu'une opération ou une tentative d'opération est liée à la perpétration, réelle ou tentée, d'une infraction de blanchiment d'argent avant de pouvoir présenter une déclaration d'opération douteuse à CANAFE.

Les indicateurs de blanchiment d'argent peuvent être considérés comme des signaux d'alarme indiquant que quelque chose semble très louche. Les signaux d'alarme tirent généralement leur origine d'une ou de plusieurs caractéristiques, ou d'un ou de plusieurs comportements, schémas et autres facteurs contextuels relatifs aux opérations financières qui les font paraître incohérentes par rapport aux attentes ou à la normalité. En soi, un indicateur peut ne pas sembler suspect au départ. Il pourrait toutefois amener les entités déclarantes à mettre en doute la légitimité d'une opération, les incitant ainsi à l'évaluer pour établir si d'autres faits, éléments contextuels ou indicateurs de blanchiment d'argent ou de financement d'activités terroristes renforceraient leurs soupçons au point qu'elles devraient soumettre une déclaration d'opérations douteuses à CANAFE (voir les directives de CANAFE sur les déclarations d'opérations douteuses).

Indicateurs de blanchiment d'argent

Les indicateurs suivants liés au blanchiment des produits de la criminalité au moyen de sites de jeu en ligne ont été tirés de l'analyse par CANAFE de ses fonds d'opérations et d'autres sources nationales et étrangères. Ces indicateurs reflètent les types d'opérations et les comportements liés à ces opérations ainsi que les facteurs contextuels. Les indicateurs ne devraient pas être traités séparément, car pris isolément, ils ne constituent pas nécessairement un signe de blanchiment d'argent ou d'une autre activité douteuse. Ils peuvent, par exemple, être liés au jeu compulsif. Les entités déclarantes devraient donc les évaluer en combinaison avec les renseignements dont elles disposent sur le client et avec d'autres facteurs se rapportant aux opérations afin de déterminer s'il existe des motifs raisonnables de soupçonner qu'une opération ou une tentative d'opération est liée à la perpétration ou à la tentative de perpétration d'une infraction de blanchiment d'argent.

Plusieurs indicateurs peuvent révéler des liens autrement inconnus qui, pris conjointement, pourraient mener à des motifs raisonnables de soupçonner que l'opération ou la tentative d'opération est liée au blanchiment de produits de la criminalité au moyen de sites de jeu en ligne. C'est donc le regroupement de différents facteurs qui peut corroborer la détermination de soupçons. Les indicateurs suivants ont été établis pour aider les entités déclarantes dans leur analyse et leur évaluation des opérations financières douteuses.

Les entités déclarantes doivent également tenir compte du fait que plusieurs ou la totalité des indicateurs transactionnels et contextuels énumérés jouent un rôle clé dans le maintien d'un solide programme de conformité lorsqu'ils sont considérés comme des facteurs de risque dans l'évaluation des risques de blanchiment d'argent et de financement des activités terroristes pour les clients actuels et potentiels. La compréhension et l'application de ces indicateurs peuvent contribuer à atténuer l'exploitation des activités d'une entité déclarante à des fins de blanchiment d'argent et de financement d'activités terroristes. Les facteurs de risque liés à la relation avec la clientèle évoluent de façon dynamique au fil du temps et sont répartis dans les catégories suivantes :

- les produits, les services et les moyens de prestation qui créent l'anonymat et qui cachent la source ou la destination des fonds;
- l'emplacement géographique du client et ses opérations liées à des pays à risque élevé;
- les nouveaux développements et les nouvelles technologies mis à la disposition des clients;
- les caractéristiques du client et l'objet de sa relation avec une entreprise qui définissent les attentes à l'égard des opérations et comportements normaux ou suspects.

Veuillez consulter les liens suivants pour obtenir des conseils sur l'évaluation des risques et les exigences en matière de conformité de CANAFE.

- Directive sur l'évaluation des risques
- Exigences relatives au programme de conformité

Indicateurs de blanchiment d'argent pour les entités financières et les entreprises de services monétaires, y compris les fournisseurs de services de paiement, concernant le jeu en ligne

⊗ Les opérations ne correspondent pas à la situation financière apparente du client, à ses activités habituelles ou à sa situation de travail (p. ex., étudiant, sans emploi, aide sociale, etc.).

⊗ Des opérations excessives avec un ou plusieurs sites de jeu qui ne sont pas autorisés par le gouvernement d'une province ni par le gouvernement fédéral.

- ⊗ Des opérations excessives avec un ou plusieurs sites de jeu qui n'exigent pas de renseignements sur l'identité du joueur auprès de leurs utilisateurs.
- ⊗ Des opérations excessives avec un ou plusieurs sites de jeu qui ne publient pas de renseignements sur leur propriété ou leur pays d'inscription.
- ⊗ Des opérations excessives avec un ou plusieurs sites de jeu qui n'imposent pas de limites sur les volumes et la valeur des paris.
- ⊗ Le portefeuille du client est directement ou indirectement exposé à des services de mélange de monnaie virtuelle et à des sites de jeu en ligne.
- ⊗ Des dépôts (p. ex., par l'intermédiaire d'un guichet automatique bancaire, de virements de fonds par courriel et d'autres formes de virements électroniques ou en succursale) sont rapidement suivis de virements ou de paiements par carte de crédit vers des sites de jeu, d'échanges de monnaie virtuelle ou d'un recours à des fournisseurs de services de paiement reconnus pour faciliter les opérations avec des sites de jeu.
- ⊗ Les opérations effectuées dans le compte du client semblent de nature circulaire (p. ex., répétitions cycliques de déboursements de jeu en ligne suivis de virements à destination des mêmes sites de jeu).
- ⊗ Le compte du client semble être utilisé exclusivement pour le jeu en ligne sur un ou plusieurs sites Web sans activités bancaires courantes.
- ⊗ Des opérations excessives avec des fournisseurs de services de paiement ou des portefeuilles électroniques reconnus pour faciliter les opérations avec des sites de jeu.
- ⊗ Dans le compte du client, des fonds sont déposés provenant de sites de jeu en ligne ou de fournisseurs de services de paiement reconnus pour faciliter les opérations de sites de jeu, sans que des fonds aient d'abord été envoyés à ces mêmes sites de jeu.
- ⊗ Dans le compte du client, un nombre excessif de virements de fonds par courriel proviennent de tiers sans lien apparent, plus particulièrement lorsque les renseignements sur le versement font référence à des termes de jeu (p. ex., « gros lot ») ou à des sites de jeu.
- ⊗ Les renseignements fournis par le client (p. ex., adresse courriel, numéro de téléphone) ou ses comptes de médias sociaux sont liés à un site de jeu non autorisé.
- ⊗ Le client recharge souvent des cartes prépayées plusieurs fois le même jour et des jours consécutifs dans le but d'envoyer des fonds à des sites de jeu en ligne.
- ⊗ Des opérations en montants arrondis sont effectuées à des points de vente au détail (p. ex., dépanneurs), ce qui laisse supposer des achats de cartes prépayées.
- ⊗ Des articles défavorables dans les médias ou d'autres sources fiables relient un client ou ses parties apparentées qui procèdent aux opérations à une activité criminelle.

Indicateurs de blanchiment d'argent pour les sites canadiens de jeu en ligne autorisés

- ⊗ Les opérations ne correspondent pas à la situation financière apparente du client, à ses activités habituelles ou à sa situation de travail (p. ex., étudiant, sans emploi, aide sociale, etc.).
- ⊗ Le client fournit des pièces d'identité ou des renseignements soupçonnés d'être faux, volés, altérés, inexacts, contrefaits ou fondés sur des pseudonymes ou des adresses génériques, comme des cases postales.
- ⊗ Le client ouvre plus d'un compte sous différentes identités (p. ex., amis ou membres de la famille) et utilise la même adresse IP lorsqu'il ouvre une session.

- ⊗ Les renseignements sur la méthode de paiement ou de dépôt d'un client ne correspondent pas aux renseignements fournis à l'inscription du joueur (p. ex., les renseignements sur la carte de crédit ou le compte bancaire ne correspondent pas au nom du joueur).
- ⊗ Le client se livre à des activités de jeu limitées ou n'en effectue aucune, même si les montants déposés dans ses comptes sont importants, avant d'effectuer une demande de retrait allant au-delà de tout gain.
- ⊗ Le client demande le transfert de ses gains au compte bancaire d'une autre partie ou dans un pays à risque élevé.
- ⊗ La géolocalisation des ouvertures de session du client ne correspond pas aux adresses ni à l'historique d'ouverture de session du client inscrit.
- ⊗ Les méthodes de dépôt et de retrait du client sont incohérentes (p. ex., le joueur effectue des dépôts au moyen de portefeuilles électroniques et de cartes prépayées, et il fait des retraits au moyen de virements télégraphiques vers un compte bancaire).
- ⊗ Le client tente d'enregistrer plus d'un compte auprès du même exploitant.
- ⊗ Carte de crédit commune utilisée pour les dépôts par plusieurs joueurs en ligne.
- ⊗ Avis de rétrofacturation lié à l'instrument financier utilisé par un client aux fins de dépôt, indiquant une utilisation non autorisée.
- ⊗ Le client effectue des dépôts excessifs au moyen de cartes prépayées, dont le nombre peut également être excessif.
- ⊗ Le client dépose des fonds bien au-delà de ce qui est requis pour maintenir ses comportements de jeu habituels.
- ⊗ Le client change soudainement ses comportements de jeu (p. ex., augmentation soudaine des dépôts et des activités de pari).
- ⊗ Le client affiche un comportement suspect pendant qu'il joue (p. ex., le client perd délibérément au poker ou fait des paris suspects qui laissent présager une activité illicite, comme des matchs truqués).
- ⊗ Le client semble effectuer plusieurs dépôts ou retraits inférieurs au seuil dans un ou plusieurs sites de jeu pour éviter les seuils de déclaration.
- ⊗ Le client utilise un compte bancaire commun utilisé par de multiples joueurs en ligne pour des déboursements.
- ⊗ Des articles défavorables dans les médias ou d'autres sources fiables relient un client ou ses parties apparentées qui procèdent aux opérations à une activité criminelle.

Déclaration à CANAFE

Pour faciliter le processus de communication de CANAFE, veuillez inclure la mention **#projetDolus** ou **#Dolus** dans la partie G – Description de l'activité douteuse de la Déclaration d'opérations douteuses. Vous pouvez inscrire plus d'un mot-clic dans cette partie. Voir aussi la page Déclaration d'opérations douteuses à CANAFE.

Communiquer avec CANAFE

- **Courriel :** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (mentionnez le bulletin spécial CANAFE-2024-SB001 dans la ligne d'objet)
- **Téléphone :** 1 866 346-8722 (sans frais)
- **Télécopieur :** 613-943-7931
- **Poste :** CANAFE, 234, avenue Laurier Ouest, 24e étage, Ottawa (Ontario) K1P 1H7, Canada

FD4-35/2024F-PDF
978-0-660-69327-9

Les bulletins spéciaux de CANAFE fournissent de l'information sur les méthodes nouvelles ou émergentes de blanchiment d'argent et de financement des activités terroristes ainsi que sur celles qui sont particulièrement d'actualité. Toutefois, leur contenu ne doit pas être considéré comme des conseils juridiques. Veuillez vous reporter à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* et à sa réglementation connexe pour connaître l'entièreté des obligations des entités déclarantes.