



Avis sectoriel et géographique

Le rôle des guichets automatiques de monnaie virtuelle dans le blanchiment des produits de la criminalité



Le rôle des guichets automatiques de monnaie virtuelle dans le blanchiment des produits de la criminalité

Objet de l'avis

Le présent avis sectoriel et géographique décrit les principaux risques de blanchiment d'argent et de financement d'activités terroristes qui sont associés aux guichets automatiques de monnaie virtuelle. Il est conçu pour aider les entreprises, les institutions financières et le grand public à comprendre et à reconnaître les caractéristiques des activités illicites liées aux guichets automatiques de monnaie virtuelle, ainsi que les types de personnes et d'entités qu'elles impliquent. En particulier, cela aidera les entreprises de services monétaires pour les monnaies virtuelles et les exploitants de guichets automatiques de monnaie virtuelle à mieux repérer les opérations financières douteuses à déclarer à CANAFE à l'appui des enquêtes des organismes chargé d'application de la loi et des activités de conformité de CANAFE. Les exploitants de guichets automatiques de monnaie virtuelle doivent mettre en œuvre des politiques de conformité, des procédures et des contrôles internes, notamment en ce qui concerne l'identification des clients, la formation et la surveillance continue des relations d'affaires pour les transactions et les relations d'affaires identifiées comme présentant un risque élevé.

Selon un examen des déclarations d'opérations douteuses qui ont été reçues, le présent avis décrit les principaux attributs des usages de guichets automatiques de monnaie virtuelle au Canada qui sont soupçonnés d'être liés au blanchiment d'argent ou au financement d'activités terroristes. En particulier, les opérations douteuses liées à des guichets automatiques de monnaie virtuelle sont concentrées dans les zones suivantes, qui sont demeurées notables même après la prise en compte de la taille de leur population : la région du Grand Toronto, la région



métropolitaine de Montréal et Metro Vancouver. CANAFE a également observé des volumes notables d'opérations douteuses à des guichets automatiques de monnaie virtuelle à Edmonton, à Calgary, à Winnipeg, à Nelson, à Abbotsford, à Victoria, à Ottawa et à Hamilton.

Aperçu

LES MONNAIES VIRTUELLES SONT DES ACTIFS NUMÉRIQUES QUI UTILISENT LA TECHNOLOGIE DES REGISTRES DISTRIBUÉS DES CHAÎNES DE BLOCS

Les monnaies virtuelles, aussi dénommées « cryptomonnaies », consistent en un instrument d'échange numérique chiffré au moyen duquel les opérations sont vérifiées et des registres sont tenus par un système décentralisé utilisant la cryptographie — plutôt que par une autorité centralisée telle qu'une banque — sur ce qu'on appelle une chaîne de blocs. Les monnaies virtuelles représentent un phénomène mondial qui n'est pas limité par les frontières et elles sont accessibles partout dans le monde par l'entremise d'un appareil et d'une connexion à Internet.

LES ÉCHANGES DE MONNAIE VIRTUELLE CONSTITUENT DES ENTREPRISES DE SERVICES MONÉTAIRES

CANAFE prend diverses mesures pour assurer la conformité de certaines entreprises avec la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (la Loi) et doit s'acquitter d'obligations précises pour combattre le blanchiment d'argent et le financement des activités terroristes au Canada. Les personnes et entités qui se livrent au commerce de la monnaie virtuelle (c.-à-d. qu'elles fournissent des services d'échange de monnaie virtuelle ou de transfert de valeur), comme les exploitants de guichets automatiques de monnaie virtuelle, sont considérées comme des entreprises de services monétaires aux termes de la Loi et de ses règlements d'application. Elles sont tenues d'inscrire leur entreprise auprès de CANAFE, de déclarer certains types d'opérations financières à CANAFE, de tenir des documents, de vérifier l'identité de leurs clients et de mettre en œuvre un régime de conformité.

Opérer une entreprise de services monétaires non enregistrée est une violation et une infraction selon la Loi et les Règlements associés.¹ Les exploitants de guichets automatiques de monnaie virtuelle qui ne sont pas inscrits auprès de CANAFE et qui, donc, ne s'acquittent pas des obligations en matière de rapports et d'autre nature qui sont imposées par la Loi et ses règlements d'application, sont susceptibles de voir leurs services utilisés de manière malveillante par des criminels à des fins de blanchiment d'argent ou de financement d'activités terroristes. Une entreprise de services monétaires qui ne remplit pas ses obligations aux termes de la Loi et de ses règlements d'application, y compris l'obligation de s'inscrire auprès de CANAFE, peut faire l'objet de sanctions pénales ou de pénalités administratives pécuniaires pouvant atteindre 2 000 000 \$ CA et/ou cinq ans d'emprisonnement.

¹ Ce n'est pas parce qu'une entreprise est inscrite auprès de CANAFE qu'elle a reçu un appui ou un permis. L'inscription signifie seulement que l'entreprise a respecté l'exigence législative de s'inscrire auprès du gouvernement fédéral. CANAFE ne réglemente pas les entreprises de services monétaires au-delà du cadre de cette législation et, par conséquent, ne peut pas fournir une évaluation de leurs pratiques commerciales générales. Ainsi, les consommateurs sont invités à procéder à leur propre vérification avant de recourir aux services d'une entreprise de services monétaires et ils devraient s'assurer de comprendre pleinement les modalités afférentes à ces services.

LES GUICHETS AUTOMATIQUES DE MONNAIE VIRTUELLE REPRÉSENTENT L'UN DES PRINCIPAUX MOYENS DE CONVERTIR DE LA MONNAIE FIDUCIAIRE (MONNAIE LÉGALE GARANTIE PAR LE GOUVERNEMENT) EN MONNAIE VIRTUELLE

Les guichets automatiques de monnaie virtuelle (aussi appelés « guichets automatiques de bitcoin », « guichets automatiques de cryptomonnaie » et « kiosques de monnaie virtuelle ») sont des terminaux connectés à Internet qui permettent aux utilisateurs d'échanger de la monnaie fiduciaire, comme des dollars canadiens, en vue de l'achat ou de la vente de monnaie virtuelle. Les guichets automatiques de monnaie virtuelle facilitent les transferts d'argent entre un exploitant de guichets automatiques de monnaie virtuelle et le portefeuille de monnaie virtuelle d'un client. Contrairement aux guichets automatiques conventionnels, pour lesquels un compte bancaire est nécessaire pour déposer ou retirer des fonds, les guichets automatiques de monnaie virtuelle lient directement l'utilisateur à l'échange de monnaie virtuelle en vue de l'achat ou de la vente de monnaie virtuelle. Le taux de change pour la monnaie virtuelle peut varier selon le taux du marché en vigueur au moment d'une opération. Bien que la plupart des opérations effectuées à l'aide d'un guichets automatiques de monnaie virtuelle soient probablement légitimes, il se peut que des criminels aient recours à des guichets automatiques de monnaie virtuelle pour convertir des produits illicites en monnaie virtuelle, mettant en branle la première étape de ce qui est appelé le stade de placement du cycle de blanchiment d'argent.

Tendances et constantes de l'utilisation de guichets automatiques de monnaie virtuelle au Canada

RÔLE EMERGENT DANS LE BLANCHIMENT D'ARGENT

Avec l'augmentation du nombre de déclarations d'opérations douteuses concernant l'utilisation de guichets automatiques de monnaie virtuelle par des criminels, CANAFE considère que les guichets automatiques de monnaie virtuelle sont en train de devenir un outil clé lors du stade de placement du cycle de blanchiment d'argent, puisqu'il est essentiellement impossible de retracer la source de l'argent déposé. Les guichets automatiques de monnaie virtuelle jouent un rôle de plus en plus important dans l'écosystème des actifs virtuels en tant que moyen rapide et fiable de convertir de la monnaie fiduciaire en monnaie virtuelle ou vice-versa. Toutefois, la facilité, l'accessibilité et le caractère quasi anonyme des guichets automatiques de monnaie virtuelle rendent ceux-ci susceptibles d'être utilisés de manière malveillante par des criminels qui cherchent à blanchir leurs fonds illicites à l'extérieur du système financier conventionnel en leur permettant d'envoyer ou de recevoir des fonds de partout dans le monde.

UTILISATION DE LA MONNAIE VIRTUELLE POUR TRANSFÉRER DES FONDS ILLICITES, MASQUER LES ORIGINES CRIMINELLES DES FONDS ET CONVERTIR CEUX-CI EN MONNAIE FIDUCIAIRE

Selon l'analyse des déclarations d'opérations douteuses effectuée par CANAFE, la fraude est la principale infraction sous-jacente soupçonnée qui est associée aux guichets automatiques de monnaie virtuelle, suivie de la traite de personnes à des fins d'exploitation sexuelle, et des cybercrimes. En outre, CANAFE a relevé des cas où des identités falsifiées et des mules ont été utilisées lors du dépôt ou du retrait de fonds à un guichets automatiques de monnaie virtuelle soupçonné d'être lié à des activités criminelles.

La plupart des déclarations d'opérations douteuses se rapportant à des guichets automatiques de monnaie virtuelle qui ont été analysées par CANAFE font état d'une exposition opérationnelle à des services illicites ou à

risque élevé, par exemple des **marchés de l'Internet clandestin**, des **plateformes de jeux d'argent en ligne**, des **échanges poste à poste** et à **risque élevé** et des **services de mélange**. Les guichets automatiques de monnaie virtuelle peuvent également servir à échanger de la monnaie virtuelle en vue d'obtenir de la monnaie fiduciaire, une fois que les produits de la criminalité ont été recyclés par un éventail de services permettant de dissimuler leur origine et de les éloigner de l'activité criminelle initiale.

L'analyse de CANAFE a permis de cerner des volumes élevés d'opérations douteuses liées à des guichets automatiques de monnaie virtuelle dans les grandes zones métropolitaines suivantes, lesquels volumes demeurent substantiels en dépit de l'ajustement en fonction de la densité de population : la région du Grand Toronto, la région métropolitaine de Montréal et Metro Vancouver. CANAFE a également observé des volumes notables d'opérations douteuses à des guichets automatiques de monnaie virtuelle à Edmonton, à Calgary, à Winnipeg, à Nelson, à Abbotsford, à Victoria, à Ottawa et à Hamilton.

DES FRAUDEURS EXPLIQUENT À DES VICTIMES LA FAÇON D'UTILISER DES GUICHETS AUTOMATIQUES DE MONNAIE VIRTUELLE

CANAFE a observé une typologie où des fraudeurs donnent des instructions à leurs victimes afin de limiter les interactions directes avec l'exploitant du guichets automatiques de monnaie virtuelle. Dans les déclarations d'opérations douteuses transmises par des exploitants de guichets automatiques de monnaie virtuelle, on constate que ceux-ci disent remarquer de plus en plus souvent que, dans les vidéos de surveillance de leurs guichets automatiques de monnaie virtuelle, la victime est au téléphone au cours de l'opération, ce qui invite à penser qu'elle est probablement en train de recevoir des directives du fraudeur sur la manière d'effectuer le transfert de monnaie virtuelle. Les nouveaux investisseurs, les personnes âgées et les nouveaux immigrants sont particulièrement susceptibles d'être victimes de stratagèmes frauduleux liés à la monnaie virtuelle. Les criminels peuvent employer tout un éventail de techniques à un guichets automatiques de monnaie virtuelle pour opérer un transfert de valeur et masquer l'identité des parties qui contrôlent les fonds.

TECHNIQUES LIÉES AUX GUICHETS AUTOMATIQUES DE MONNAIE VIRTUELLE QUI SONT UTILISÉES POUR TRANSFÉRER DE LA VALEUR ET MASQUER L'IDENTITÉ DE CEUX QUI EXERCENT UN CONTRÔLE SUR LES FONDS

Ces techniques comprennent le fait d'utiliser des mules financières pour effectuer des opérations, d'éviter les contacts avec les exploitants de guichets automatiques de monnaie virtuelle et de fournir des identifiants falsifiés ou modifiés, par exemple le numéro de téléphone ou la date de naissance. La même personne peut créer plusieurs profils de compte de guichets automatiques de monnaie virtuelle en utilisant différents numéros de téléphone et identifiants personnels. Les déclarations d'opérations douteuses font également état de quantités excessives de dépôts ou de retraits de moins de 999 \$ CA sur une période donnée (jour, semaine ou mois) à plusieurs guichets automatiques de monnaie virtuelle, ces opérations étant effectuées à l'aide de numéros de téléphone prépayés partagés ou de la téléphonie voix par protocole Internet pour éviter l'identification.

Habituellement, dans un cas de fraude, le fraudeur commande à la victime de placer de la monnaie fiduciaire dans un guichets automatiques de monnaie virtuelle ou fournit lui-même un code QR associé à son portefeuille de monnaie virtuelle que la victime utilisera pour l'opération.

Une fois placés dans l'écosystème de monnaie virtuelle, les fonds sont déplacés par une série d'adresses de portefeuille privé et peuvent être mélangés à d'autres portefeuilles contenant des produits issus d'activités frauduleuses. Le fraudeur peut ensuite utiliser diverses méthodes de dissimulation pour blanchir les produits de la fraude et masquer la source des fonds.

La vérification de l'identité des clients est un élément fondamental du régime canadien dans la lutte contre le blanchiment d'argent et le financement d'activités terroristes. Les entreprises de services monétaires, comme les exploitants de guichets automatiques de monnaie virtuelle, doivent s'assurer que les identificateurs figurant dans un document d'identification ou les renseignements provenant d'une autre source correspondant au renseignement fourni par la personne ou l'entité.

Les **marchés de l'Internet clandestin** sont des sites Web commerciaux qui mettent en contact des acheteurs et des vendeurs qui échangeront de la monnaie virtuelle pour obtenir des biens ou des services illicites.

Les **plateformes de jeux d'argent en ligne** accroissent les risques de blanchiment d'argent puisque les criminels peuvent utiliser ces sites Web pour disperser les produits de la criminalité.

Les **échanges à risque élevé** comportent peu ou pas de procédures de lutte contre le blanchiment d'argent, comme une procédure d'identification des clients à l'ouverture d'un compte, et peuvent avoir des liens connus publiquement avec des activités criminelles, et/ou présenter une exposition considérable à des services risqués. Ces échanges ont lieu dans des administrations étrangères connues pour leur corruption publique ou la faiblesse de leur système judiciaire ou de leurs règlements de lutte contre le blanchiment d'argent et le financement des activités terroristes.

Les **échanges poste à poste** permettent aux utilisateurs de faire des affaires directement entre eux. Contrairement aux échanges centralisés, qui exigent que les utilisateurs fournissent des renseignements sur leur identité pour traiter une transaction, certains services poste à poste permettent à leurs utilisateurs d'envoyer ou de recevoir de la monnaie virtuelle sans vérification d'identité.

Les **mixeurs de cryptomonnaie** sont des sites Web ou des logiciels qui sont utilisés pour rassembler des fonds qui proviennent d'adresses sur la chaîne de blocs pour ensuite les redistribuer de sorte qu'il n'y ait plus de lien direct avec la source d'origine. Ainsi, ils permettent de dévier des fonds pour vendre de la monnaie virtuelle « propre ».

MASQUER L'IDENTITÉ DES CLIENTS ET CONTOURNER LES SEUILS DE DÉCLARATION

Les déclarations d'opérations douteuses mentionnent des personnes qui utilisent des pièces d'identité ou des identifiants partagés ou modifiés, tels que le nom, l'adresse, la date de naissance ou le numéro de téléphone, l'objectif étant probablement de contourner les exigences en matière d'identification. Souvent, le niveau et le volume d'activité opérationnelle qui ont été observés ne concordaient pas avec les renseignements sur le client en question, comme le profil professionnel ou la situation financière de la personne effectuant l'opération. Les utilisateurs qui ont falsifié leur identité étaient également soupçonnés de faciliter des dépôts ou des retraits associés à des marchés de l'Internet clandestin, à la traite de personnes à des fins d'exploitation sexuelle ou à des fraudes en matière d'investissement ou d'autorité. CANAFE a observé qu'une fois que les fonds étaient placés dans des terminaux de guichets automatiques de monnaie virtuelle, ils étaient envoyés à une multitude d'adresses intermédiaires liées à des échanges à risque élevé, y compris des échanges poste à poste qui ne nécessitent pas de vérification de l'identité du client pour l'ouverture d'un compte, ce qui fait d'eux un choix attrayant pour les activités de blanchiment d'argent.

Les entités déclarantes doivent prendre des mesures raisonnables pour vérifier l'identité de toute personne ou entité qui effectue ou tente d'effectuer une opération douteuses, quel que soit le montant de l'opération, et y compris les opérations qui seraient normalement exemptées des exigences relatives à l'identification des clients.

TECHNIQUES DE DISPERSION ET D'INTÉGRATION REPOSANT SUR DES SERVICES À RISQUE ÉLEVÉ

Les acteurs criminels chercheront possiblement à éviter les seuils standards de vérification de l'identité du client ainsi que les heures d'ouverture habituelles

Selon l'analyse de CANAFE visant les opérations douteuses effectuées à des guichets automatiques de monnaie virtuelle, des utilisateurs à travers le Canada font beaucoup de dépôts de faible valeur, entre 100 \$ et 999 \$ CA, et envoient les fonds à des marchés de l'Internet clandestin (en vue de l'achat de drogues ou de matériel d'exploitation sexuelle d'enfants), à des marchés de cyberexploitation en vue de l'achat de cyberoutils ou de cyberservices malveillants ou à des magasins de produits de fraude en vue de l'achat de renseignements en matière de paiement ou de documents d'identification compromis.

Les déclarations d'opérations douteuses font état de techniques de dispersion reposant sur le recours à des services à risque élevé, comme des marchés de l'Internet clandestin, des plateformes de jeux d'argent en ligne, des échanges à risque élevé, des échanges poste à poste et des mixeurs de cryptomonnaie. Ces services peuvent aider à dissimuler l'origine des fonds et à masquer le cheminement de l'argent afin de créer une perception de légitimité. En outre, dans bien des cas, les utilisateurs qui effectuent des opérations douteuses à un guichets automatiques de monnaie virtuelle se livrent à ces activités à l'extérieur des heures d'ouverture normales, de tard en soirée jusqu'à tôt le matin (entre 21 h et 3 h).

Des produits présumés de la criminalité déposés dans un guichets automatiques de monnaie virtuelle sont déviés lors d'échanges à risque élevé

Les déclarations d'opérations douteuses transmises à CANAFE font état de dépôts dans des guichets automatiques de monnaie virtuelle destinés à des échanges à risque élevé de 999 \$ à 10 000 \$ CA qui étaient associés à des produits de la fraude, de la cybercriminalité et de la traite de personnes à des fins d'exploitation sexuelle. D'après les activités sur les chaînes de blocs, les fonds ont été retirés lors d'échanges ayant lieu en Iran, en Russie, au Bélarus ou dans des pays avoisinants ayant une réglementation laxiste en matière de lutte

contre le blanchiment d'argent et le financement des activités terroristes, ou bien dans d'autres pays faisant l'objet de sanctions complètes.

Selon les déclarations d'opérations douteuses, une forte proportion de fonds envoyés à des mixeurs de cryptomonnaie élangés et retirés dans une multitude de guichets automatiques de monnaie virtuelle à travers le Canada était associée à des activités frauduleuses, à des rançongiciels, à des articles de magasins de produits de fraude ou à l'achat de stupéfiants sur des marchés de l'Internet clandestin. CANAFE a constaté que les retraits aux guichets automatiques de monnaie virtuelle semblent être effectués de tard en soirée jusqu'à tôt le matin et qu'il s'agit de grandes quantités d'opérations de faible valeur.

Détecter et décourager les activités illicites aux guichets automatiques de monnaie virtuelle

LES ENTITÉS DÉCLARANTES DEVRAIENT PORTER UNE ATTENTION PARTICULIÈRE AUX PERSONNES QUI SEMBLENT FRACTIONNER LEURS DÉPÔTS DE SORTE QU'ILS SOIENT TOUT JUSTE INFÉRIEURS AUX SEUILS DE DÉCLARATION

Dans les cas de fractionnement de dépôts à un guichets automatiques de monnaie virtuelle, il peut s'agir d'une personne qui utilise des pièces d'identité ou des identifiants partagés ou modifiés, tels que le nom, l'adresse, la date de naissance ou le numéro de téléphone, afin de contourner les exigences en matière d'identification des clients. À cette fin, il arrive également qu'une personne fasse des dépôts tout juste inférieurs au seuil de déclaration dans plusieurs guichets automatiques de monnaie virtuelle, et ce, maintes fois par jour et en utilisant un numéro de téléphone différent pour chaque opération. Les entités déclarantes devraient envisager d'incorporer des contrôles et des mesures d'atténuation adaptés à ces risques dans leur approche axée sur les risques applicable aux activités commerciales continues et aux clients.

LES RISQUES LIÉS AUX GUICHETS AUTOMATIQUES DE MONNAIE VIRTUELLE APPELLENT DES MESURES DE DILIGENCE ACCRUES

La forte concentration de guichets automatiques de monnaie virtuelle au Canada et leur facilité d'accès rendent ceux-ci susceptibles de servir à des opérations illicites qui comportent un risque inhérent de blanchiment d'argent ou de financement d'activités terroristes. Les fournisseurs de guichets automatiques de monnaie virtuelle sont obligés à appliquer des politiques de conformité, des procédures et des contrôles internes stricts, notamment en ce qui concerne l'identification des clients, l'éducation/la sensibilisation et la surveillance continue des relations d'affaires dans le cas des opérations et des relations d'affaires désignées comme présentant un risque élevé. Les fournisseurs de guichets automatiques de monnaie virtuelle sont invités à cerner et à évaluer les lacunes ou faiblesses potentielles dans leur programme de conformité. Par exemple, en utilisant une [approche axée sur les risques](#), les fournisseurs de guichets automatiques de monnaie virtuelle peuvent déterminer et évaluer les risques susceptibles d'avoir une incidence sur d'autres aspects de leur programme de conformité, comme les lacunes dans les politiques écrites, les procédures ou les programmes de formation. On encourage également les entités déclarantes à faire preuve de prudence concernant les clients ayant une exposition en matière d'envoi, directe²

² Exposition directe : S'entend de l'envoi de fonds d'une partie à une autre sans intermédiaire. Il existe un lien direct entre la source et la destination des fonds.

SIGNAUX D'ALARME LIÉS AUX GUICHETS AUTOMATIQUES DE MONNAIE VIRTUELLE

- L'utilisateur envoie, ou reçoit, fréquemment une grande quantité de sommes de faible valeur à l'intention, ou en provenance, d'adresses de portefeuille privé, de plateformes poste à poste, de mixeur de cryptomonnaie, de plateformes de jeux d'argent, d'activités d'escroquerie, de marchés de l'Internet clandestin (p. ex. matériel d'exploitation sexuelle d'enfants, marchés de cyberexploitation, magasins de produits de fraude et rançongiciels) ou d'échanges à risque élevé.
- L'utilisateur atteint la limite de fonds quotidienne au guichets automatiques de monnaie virtuelle.
- Les vidéos de surveillance montrent que l'utilisateur est au téléphone ou accompagné d'une personne et qu'on lui explique comment effectuer l'opération.
- L'utilisateur tente de dissimuler son identité en utilisant des pièces d'identité (adresse, numéro de téléphone, courriel) partagées, falsifiées, volées ou modifiées.
- Le niveau ou le volume de l'activité transactionnelle impliquant un guichets automatiques de monnaie virtuelle ne correspond pas au profil financier apparent du client, à ses activités habituelles, à ses informations professionnelles ou à ses informations commerciales déclarées.
- L'utilisateur se sert de la téléphonie voix par protocole Internet ou de numéros de téléphone prépayés lorsqu'il s'agit de déposer ou de retirer des fonds à un guichets automatiques de monnaie virtuelle.
- Une exposition en matière d'envoi à des échanges à risque élevé pour lesquels la procédure de vérification de l'identité du client, les mesures de diligence pour les opérations et la conformité aux lois/règlements sont lacunaires ou qui ont lieu dans des administrations étrangères connues pour leur refuge fiscal, leur secret bancaire ou leur corruption publique.
- Un nombre excessif de dépôts sous le seuil des 999 \$ CA vers la même adresse pendant une courte période et maintes fois par jour ou par semaine et/ou à plusieurs guichets automatiques de monnaie virtuelle différents.
- Des opérations sont effectuées par une personne seule ou accompagnée de plusieurs personnes tard en soirée ou tôt le matin (entre 21 h et 3 h).

ou indirecte³, à des marchés de l'Internet clandestin (matériel d'exploitation sexuelle d'enfants, marchés de cyberexploitation, magasins de produits de fraude et rançongiciels), à des plateformes de jeux d'argent en ligne, à des échanges poste à poste ou à risque élevé, à des services de mixage de cryptomonnaies ou à d'autres activités illicites connexes. Des outils d'analyse des chaînes de blocs peuvent cerner les adresses de monnaie virtuelle liées à des services illicites ou à risque élevé, ce qui permet aux exploitants de guichets automatiques de monnaie virtuelle d'établir les cas d'exposition en matière d'envoi ou de réception qui présentent des risques.

Les consommateurs doivent se protéger

Les individus doivent se méfier des personnes qui, sur les médias sociaux ou les sites de rencontres, tentent de solliciter des investissements en monnaies virtuelles, ainsi que des acteurs criminels qui se font passer pour des gouvernements, des forces de l'ordre ou des entreprises du secteur privé afin d'extorquer un paiement pour une action criminelle ou une facturation présumée, ou d'obtenir l'accès à des informations personnelles ou financières.

³ Exposition indirecte : S'entend d'une situation où il existe un intermédiaire, un portefeuille ou un service entre la source et la destination des fonds.

Il s'agit là de signaux clairs indiquant que l'offre est probablement frauduleuse. Aucune agence gouvernementale ne demandera de paiement en monnaies virtuelles.

Les individus doivent également éviter de participer involontairement à des activités de blanchiment d'argent associées à des distributeurs automatiques de monnaies virtuelles. Méfiez-vous des offres d'emploi ou des offres financières basées sur le transfert physique de fonds vers et depuis des guichets automatiques de monnaie virtuelle.

Les consommateurs qui transfèrent des fonds vers et depuis des guichets automatiques de monnaie virtuelle peuvent se protéger en faisant preuve de diligence, en étudiant soigneusement un investissement en monnaie virtuelle et en se méfiant des offres qui semblent trop belles pour être vraies. Vérifiez toujours la légitimité d'un échange, d'un fournisseur de porte-monnaie ou d'une opportunité d'investissement avant d'envoyer des fonds. Une fois qu'une transaction en monnaie virtuelle est effectuée, il n'y a aucun moyen de l'annuler ou de la renverser.

En générale, les utilisateurs doivent être vigilants et prendre les précautions nécessaires pour protéger leurs informations personnelles et financières lorsqu'ils utilisent des guichets automatiques de monnaie virtuelle.

Signalez tout soupçon de blanchiment d'argent ou de financement d'activités terroristes

Les consommateurs doivent signaler immédiatement toute opération inhabituelle ou irrégulière à leur institution financière. Quiconque peut [transmettre volontairement des renseignements](#)⁴ à CANAFE au sujet de soupçons de blanchiment d'argent ou de financement d'activités terroristes. Si vous jugez que la situation nécessite une intervention immédiate de la part des organismes d'application de la loi, vous devriez signaler le cas directement à l'organisme d'application de la loi de votre région. Si vous croyez avoir été victime de fraude, nous vous encourageons à signaler votre situation au [Centre antifraude du Canada](#).

Déclaration à CANAFE

Pour faciliter le processus de déclaration à CANAFE, les entités déclarantes devraient inclure le terme **#SGA2024** dans la partie G – Description de l'activité douteuse de la Déclaration d'opérations douteuses. Pour obtenir des instructions sur la manière de soumettre des déclarations d'opérations douteuses à CANAFE, veuillez consulter la page [Déclaration d'opérations douteuses à CANAFE](#)⁵ de notre site Web.

COORDONNÉES DE CANAFE

- **Courriel** : guidelines-lignesdirectrices@fintrac-canafe.gc.ca (indiquer « SIRA-2024-005 » dans l'objet)
- **Téléphone** : 1-866-346-8722 (sans frais)
- **Télécopieur** : 613-943-7931
- **Poste** : CANAFE, 234, avenue Laurier Ouest, 24^e étage, Ottawa (Ontario), K1P 1H7, Canada

⁴ Transmettre volontairement des renseignements au sujet de soupçons de blanchiment d'argent ou de financement d'activités terroristes <https://fintrac-canafe.canada.ca/individuals-individus/vol/1-fra>

⁵ Déclaration d'opérations douteuses à CANAFE : <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-fra>

© Sa Majesté le Roi du chef du Canada, 2024.
No de cat. FD4-33/2024F-PDF
ISBN 978-0-660-68214-3