

DEUXIÈME ÉDITION DU FORUM SUR L'INTELLIGENCE
ARTIFICIELLE DANS LE SECTEUR DES SERVICES FINANCIERS :
**UNE APPROCHE COLLABORATIVE À L'ÉGARD
DES MENACES, POSSIBILITÉS ET PRATIQUES
EXEMPLAIRES LIÉES À L'IA**

ATELIER 2 – CRIMINALITÉ FINANCIÈRE

NOVEMBRE 2025



**GLOBAL
RISK**
INSTITUTE



Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada



Ce forum est essentiel, car il se concentre sur l'un des défis les plus pressants et complexes auxquels nous faisons face aujourd'hui : la lutte contre la criminalité financière à l'ère de l'intelligence artificielle. Plus que jamais, nous avons besoin d'un réseau fort, bien équipé et engagé pour vaincre les réseaux criminels et terroristes modernes. Nous savons que nous ne pouvons pas y parvenir seuls. Nous avons besoin d'une approche à l'échelle globale de l'écosystème qui rassemble les institutions financières, les fournisseurs de technologies, les organismes de réglementation et les chercheurs afin de mettre au point des solutions d'IA résilientes, éthiques et efficaces.

Sarah Paquet, Directrice et présidente-directrice générale, le 1^{er} octobre 2025

AVANT-PROPOS

Le 1^{er} octobre 2025, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) et l'Institut du risque mondial (GRI) ont coparrainé un atelier sur la criminalité financière et l'intelligence artificielle dans le cadre de la Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers : Une approche collaborative à l'égard des menaces, possibilités et pratiques exemplaires liées à l'IA. Ce deuxième atelier de la Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers a réuni plus de 60 experts canadiens et internationaux en criminalité financière et intelligence artificielle (IA) issus du secteur des services financiers et de leurs organismes de réglementation.

Le premier atelier, tenu en mai 2025, a permis de cerner les possibilités, les risques et les menaces liés à la sécurité et à la cybersécurité. Le rapport documentant les points de vue des participants est disponible [ici](#).

L'objectif de l'atelier sur la criminalité financière et l'IA était le suivant :

Déterminer les risques, les mesures d'atténuation et les possibilités liés à la criminalité financière et à l'IA afin de découvrir comment l'IA peut aider à détecter et à prévenir la criminalité financière grâce à une gestion des risques plus intelligente, plus rapide et plus adaptative, axée sur i) la fraude et la gestion de la fraude, ii) la lutte contre le blanchiment d'argent, iii) le respect et le contournement des sanctions, et iv) les menaces internes et l'intégrité des données.

Cette initiative s'inscrit dans la continuité du travail entamé il y a trois ans, lorsque le BSIF et le GRI ont lancé une discussion sur les risques et les possibilités liés à l'IA, en organisant la Première édition du Forum sur l'intelligence artificielle dans le secteur des services financiers en 2022 afin de promouvoir une utilisation responsable de l'IA dans le secteur financier canadien. Le rapport qui en a résulté, « Une perspective canadienne sur l'intelligence artificielle responsable », a souligné l'importance de mettre en œuvre des stratégies complètes de gestion des risques pour relever les défis précis posés par l'IA.

Il reste deux ateliers dans le cadre du processus de la Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers : un portant sur la protection des consommateurs et l'autre portant sur la stabilité financière. En plus des rapports intermédiaires pour chaque atelier, il y aura aussi un rapport final qui couvrira les principales analyses et pratiques exemplaires issues des quatre ateliers.

L'IA est à la fois source de possibilités et de risques pour le système financier. Les commanditaires, le CANAFE et le GRI, tiennent à exprimer leur sincère gratitude à tous les participants à l'atelier pour leur engagement dans ce dialogue collaboratif.

Institut du risque mondial

Centre d'analyse des opérations et
déclarations financières du Canada
(CANAFE)

**CRIMINALITÉ FINANCIÈRE –
PERSPECTIVES SECTORIELLES ET
RÉGLEMENTAIRES SUR LES RISQUES,
L’ATTÉNUATION ET LES OCCASIONS**

La criminalité financière, y compris la fraude, le blanchiment d’argent, le contournement des sanctions et la fraude interne, a pris de l’ampleur, tant en termes d’échelle que de portée et de rapidité. La révolution de l’IA a accru ces risques et compliqué la capacité du Canada à prévenir et à se défendre contre cette criminalité financière.

**Perspectives issues de l’atelier sur
l’adoption de l’IA et la criminalité
financière**

L’atelier a permis de déterminer qu’un investissement ciblé adéquatement dans l’IA peut améliorer à la fois l’efficacité et l’efficience des efforts d’une institution financière pour lutter contre la criminalité financière. Cette adoption de l’IA passe maintenant des projets pilotes vers une mise en œuvre plus large.

Interrogés sur les obstacles empêchant les organismes d’adopter l’IA pour améliorer la détection de la criminalité financière, 48 % des participants aux ateliers ont mentionné les contraintes de coûts et de ressources comme le principal obstacle.

Les participants au forum ont également mentionné la « fraude » comme le crime financier le plus susceptible d’augmenter en raison de l’utilisation de l’IA au cours des deux à trois prochaines années.

Figure 1: Questionnaire des participants, 1^{er} octobre 2025

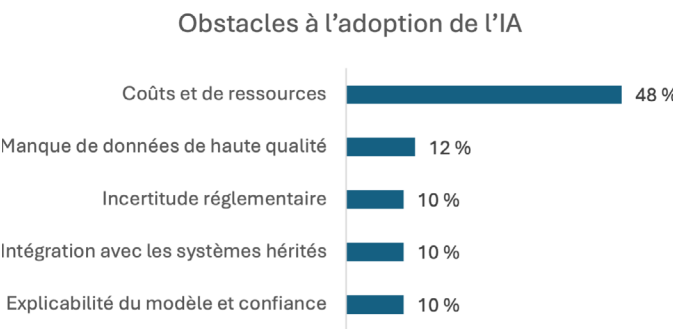
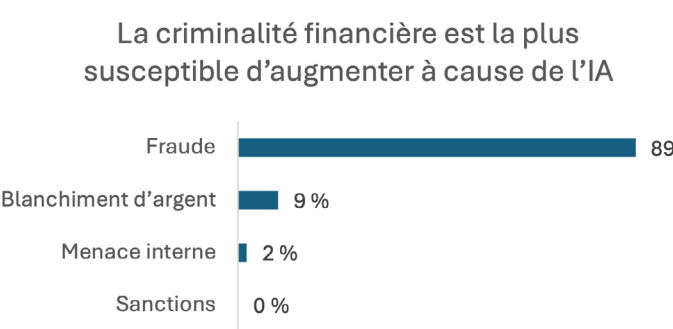


Figure 2: Questionnaire des participants, 1^{er} octobre 2025



**IA et criminalité financière –
perspectives sectorielles et
réglementaires sur le risque**

Les participants à l’atelier ont relevé cinq menaces liées à l’IA qui pourraient aggraver la criminalité financière : des ressources limitées, des enjeux de cybersécurité, des barrières à l’entrée faibles pour les auteurs de menaces, des défis posés par le cadre réglementaire canadien, ainsi que des enjeux liés à la technologie et aux données. Chaque menace amplifie le risque. Les fraudeurs sont souvent perçus comme ayant « dix coups d’avance », tandis que les institutions financières restent largement réactives et concentrent leurs efforts à éteindre des feux.

Ressources limitées

Nature du risque

Les participants ont indiqué que l'investissement limité dans l'adoption et la mise en œuvre de l'IA, ainsi que la réduction des lacunes en matière de compétences, freineront les efforts pour lutter contre la criminalité financière.

1. Objectifs concurrents en matière d'IA

Les membres du forum ont exprimé leur inquiétude quant au fait que la réduction des coûts pourrait devenir un objectif privilégié à court terme. Ils ont fortement insisté sur le fait que le meilleur moyen d'améliorer la dissuasion consiste à privilégier les investissements dans l'IA axés sur l'amélioration de l'efficacité avant de se concentrer sur les investissements dans l'IA qui permettraient de gagner en efficacité.

2. Échec à poursuivre des résultats mesurables

Les participants ont estimé que les entreprises qui adoptent l'IA simplement parce qu'il s'agit de la dernière tendance risquent d'échouer tant dans le développement technologique que dans leurs efforts pour lutter contre la criminalité financière. Les participants ont souligné leur conviction profonde que l'IA devrait être adoptée sur la base d'analyses de rentabilité claires. Les initiatives en IA devraient générer un retour sur investissement mesurable. Les participants à l'atelier ont cerné le défi : « La mauvaise question est « Comment adopter l'IA? » La bonne question est : « Comment utiliser l'IA pour aider notre entreprise? »

3. Défis d'investissement et contraintes liées aux systèmes hérités

Même en se concentrant sur le retour sur investissement, les institutions financières peuvent être limitées dans l'adoption de nouvelles solutions d'IA parce que ces solutions dépendent de la modernisation des systèmes hérités. Pour certaines, surtout les petites institutions, les ressources nécessaires à la modernisation peuvent être difficiles, surtout comparées à d'autres priorités d'investissement.

4. Pénurie de compétences et de connaissances en matière d'IA

L'accès limité à l'expertise ou aux connaissances en IA crée des vulnérabilités, ce qui peut entraver le déploiement des technologies d'IA appropriées et restreindre la capacité de l'institution à évaluer les avantages de l'adoption de l'IA. De plus, l'impact de l'IA sur les employés débutants pourrait remettre à l'épreuve le développement des compétences nécessaire pour développer une expertise en criminalité financière, qui a historiquement bénéficié d'un modèle d'apprentissage.

5. La taille de l'entreprise influence l'exposition au risque

Les petites institutions financières, avec une capacité limitée à investir dans la technologie IA, sont plus vulnérables aux cybermenaces ou aux menaces internes pilotées par l'IA, ce qui fait peser le risque institutionnel et le risque pour les consommateurs sur ces petits acteurs. La disparité avec les grandes institutions peut mener à l'exploitation par des auteurs de menaces qui utilisent les petites institutions comme points d'entrée, augmentant ainsi le risque institutionnel ou potentiellement systémique.

6. *Contraintes imposées aux gouvernements et aux organismes de réglementation*

Les gouvernements et les organismes de réglementation canadiens font aussi face à des défis en matière de ressources, ce qui pourrait ralentir l'adoption de l'IA au sein du gouvernement, tant en ce qui concerne le secteur que les auteurs de menaces. Une adoption lente de l'IA pourrait limiter les organismes de réglementation financiers fédéraux et provinciaux du Canada, les organismes d'application de la loi et le système judiciaire dans leurs efforts pour identifier, poursuivre et condamner les criminels.

Questions de cybersécurité

Nature du risque

La croissance rapide des risques de cybersécurité activés par l'IA, tels que les hypertrucages, l'hameçonnage sophistiqué et les identités synthétiques (un risque de fraude où les criminels combinent des données réelles et fabriquées), augmente l'impact et la menace de la criminalité financière contre les individus et les institutions financières.

1. *Personnalisation accrue*

Les incidents cyberincidents associés à l'IA, souvent exploités par la manipulation des médias sociaux, ont permis aux auteurs de menaces de mener des attaques frauduleuses de plus en plus « personnalisées » contre des individus, rendant ces événements de plus en plus malveillants et difficiles à détecter ou à éviter.

2. *Augmentation des événements transfrontaliers*

Les avancées en IA aggravent les défis transfrontaliers déjà importants en matière de criminalité financière. Les auteurs de menaces

utilisant l'IA depuis l'étranger font face à des taux de détection et de poursuites plus faibles, et le partage de renseignements entre les pays est plus limité.

3. *Auteurs de menaces internes et accès aux données*

Les menaces de cybersécurité associées à l'IA créent de nouvelles occasions pour les personnes de l'intérieur de devenir des auteurs de menaces. Ces personnes peuvent exploiter les lacunes de contrôle et de gouvernance pour accéder à des données privées sur les consommateurs ou à des données commerciales exclusives. Les capacités améliorées par l'IA dont disposent les auteurs de menaces augmentent également le risque que des organismes embauchent des personnes dont l'objectif pourrait être de compromettre l'intégrité des données des institutions financières ou des organismes de réglementation gouvernementaux.

4. *Érosion de la confiance*

Les participants ont noté que les outils d'IA rendent de plus en plus difficile la distinction entre communications et identités authentiques et inventées, ce qui érode la confiance du public envers les institutions financières et autres.

Faibles barrières à l'entrée pour les auteurs de menaces

Nature du risque

Des experts en criminalité financière présents à l'atelier ont déclaré que l'IA a mené à la « démocratisation de la technologie », car les individus n'ont plus besoin de s'appuyer sur des compétences technologiques avancées ou de grands réseaux criminels organisés.

1. Facilité et fréquence d'utilisation

L'accessibilité de l'IA a abaissé les barrières pour les auteurs de menaces, permettant désormais à ceux ayant des compétences limitées d'utiliser l'IA efficacement. Les barrières moins solides permettent d'augmenter la fréquence des attaques, d'améliorer la capacité à dissimuler des renseignements et d'élargir considérablement leur portée. L'IA a également facilité l'émergence de la fraude en tant que service (FaaS), suivant le même modèle que le « logiciel en tant que service (SaaS) », augmentant l'efficacité et la fréquence. De plus, l'IA a éliminé le besoin de connaissances en langues étrangères, qui représentait auparavant un obstacle important à la criminalité financière transfrontalière.

2. Coûts financiers asymétriques

Les participants à l'atelier ont souligné le déséquilibre entre le coût financier relativement faible et le risque liés à la réalisation d'attaques pilotées par l'IA, au contournement des sanctions ou au blanchiment d'argent, et les coûts et efforts plus élevés exigés par les institutions financières pour contrer cette menace.

Défis dans le cadre réglementaire canadien

Nature du risque

Les participants à l'atelier ont cerné les défis dans le régime réglementaire canadien qui pourraient créer des obstacles à l'adoption de l'IA, pouvant potentiellement nuire à l'identification, au signalement et à la condamnation des auteurs de crimes financiers. La structure fédérale du Canada

et sa division constitutionnelle des pouvoirs signifient qu'aucune juridiction, qu'aucun élu ou fonctionnaire, ministère ou organisme ne possède à lui seul le pouvoir d'agir, depuis la détection et le signalement jusqu'aux poursuites et à la condamnation. Cette complexité rend la coordination et le partage de renseignements plus difficiles.

Maturité réglementaire et risques de non-conformité

Les participants ont observé que le rythme de l'adoption de l'IA par les auteurs de menaces s'accélère. Parallèlement, le régime canadien de réglementation de la criminalité financière a également évolué. Ces participants ont exprimé leur inquiétude quant à la capacité du secteur financier à suivre le rythme à la fois de l'augmentation des menaces liées à l'IA et des changements réglementaires.

Certains membres du forum ont souligné la nécessité de mettre en place des bacs à sable réglementaires où les institutions pourraient mettre à l'essai l'IA sans craindre de sanctions.

Les auteurs de menace sont de plus en plus capables d'utiliser des outils d'IA pour masquer la propriété effective des sociétés, rendant la nécessité d'un registre complet de propriété encore plus cruciale. Bien que Corporations Canada ait lancé un registre fédéral de propriété effective en janvier 2024, certaines lacunes subsistent, particulièrement au niveau provincial.

Les cadres juridiques et réglementaires ont également une incidence sur l'échange rapide de renseignements entre le secteur financier, les organismes de réglementation et les organismes d'application de la loi.

Technologie et problèmes de données

Nature du risque

Trois risques importants liés à la technologie et aux données importantes ont été relevés en lien avec les systèmes hérités, l'intégrité des données, ainsi que les cadres de gouvernance et de contrôle.

1. Plateformes héritées et intégration de l'IA – défis liés aux délais et à la technologie

Presque toutes les institutions financières font face à des systèmes hérités vieillissants qui entravent parfois l'intégration de l'IA et allongent les délais d'adoption. Les membres du forum ont parlé de risque que présente la « technologie héritée », les criminels exploitant ces délais d'adoption plus longs comme une vulnérabilité.

2. Qualité inégale des données

La qualité des données est essentielle pour l'adoption de l'IA et influe sur la qualité des analyses basées sur l'IA. La qualité des données varie au sein du secteur financier canadien, avec des plateformes fragmentées, et elle est parfois incohérente et incomplète. Les différentes classifications et méthodes de stockage entre les banques entravent le partage des données. Les modèles d'IA doivent être formés et exploités dans cet environnement complexe, qu'un participant a décrit comme le défi de « construire une voiture tout en conduisant ».

3. Cadres de gouvernance et de contrôle

Beaucoup de participants ont indiqué que des cadres de gouvernance et de contrôle forts et efficaces constituaient la première ligne de défense contre la criminalité financière. Le développement de l'IA met en lumière des lacunes potentielles dans les cadres existants,

telles que les règles d'accès aux données qui pourraient involontairement permettre des fuites de données par des auteurs de menace internes, l'introduction potentielle de données corrompues, et la confusion potentielle sur la propriété des données lorsque l'IA crée de nouveaux liens. De plus, certaines institutions financières peuvent accorder moins d'importance aux contrôles traditionnels lorsqu'elles évaluent l'efficacité des nouvelles solutions en matière d'IA.

Pratiques exemplaires en matière d'atténuation des risques liés à la criminalité financière

Les membres du forum ont cerné les pratiques exemplaires en matière de gouvernance, de technologie et d'exploitation pour atténuer les risques liés à la criminalité financière. Les pratiques exemplaires d'abord se concentrer sur les fondamentaux : gestion des risques, gouvernance et contrôles.

1. Maintenir des cadres de gouvernance et de contrôle efficaces, y compris, mais sans s'y limiter, l'IA

Les participants ont décrit des efforts constants mis sur les cadres de gouvernance et de contrôle existants comme l'outil le plus efficace pour atténuer les risques liés à l'IA. La mise à jour continue permettra de faire face aux nouvelles menaces liées à l'IA; le maintien de l'accent sur les mécanismes de contrôle traditionnels reste la meilleure pratique pour atténuer les crimes financiers facilités par l'IA. Pour que les cadres de gouvernance et de contrôle de l'IA soient efficaces, ils doivent être transparents et exiger une documentation claire des processus d'IA afin de répondre aux exigences du conseil d'administration, aux objectifs de gestion et aux normes réglementaires en matière de risques.

2. Garantir la qualité et l'accessibilité des données

Un principe clé dans la lutte contre la criminalité financière consiste à s'assurer que les données sont exactes, accessibles et « adaptées à l'usage prévu ». La qualité des données ne répondra à cette norme qu'à condition de continuer à investir dans une infrastructure de données résiliente. Un investissement potentiel consiste à mettre en place des bases de données fédérales et provinciales accessibles, complètes et élargies sur l'enregistrement des sociétés, qui aideront à déterminer les liens entre les propriétés effectives effectifs et à lutter contre la criminalité financière liée à l'IA.

3. Investissement continu et adoption d'outils d'IA efficaces

L'investissement continu dans les outils d'IA est essentiel. Une IA efficace peut analyser les comportements, détecter des crimes financiers complexes comme le blanchiment d'argent et le contournement de sanctions, et effectuer des analyses de réseau pour détecter la fraude. Ces outils améliorent l'authentification et protègent contre les risques émergents tels que les robots logiciels dans la criminalité financière et la surveillance des transactions cryptographiques, car ces plateformes sont utilisées pour transférer des fonds. Comme l'ont souligné les participants, les investissements continus doivent offrir des avantages mesurables en matière d'IA et devraient se concentrer, autant que possible, sur l'efficacité plutôt que sur les économies d'efficacité.

4. Éducation, communication et formation continues en IA

L'éducation et la formation en IA sont des investissements essentiels pour le secteur des services financiers, les décideurs politiques et

les organismes de réglementations. La mise à niveau des compétences devrait être une priorité absolue pour maintenir la sécurité des infrastructures contre les auteurs de menace. La formation et l'autonomisation du personnel devraient également être une priorité afin de favoriser le déploiement d'outils d'IA qui améliorent l'efficacité et l'efficience. Les institutions financières peuvent également proposer des formations sur l'intelligence artificielle à leurs intervenants, y compris leurs clients, afin de les sensibiliser aux occasions et aux risques liés à cette technologie. Tout aussi important, les pratiques exemplaires recommandent que le conseil d'administration et la direction générale aient des connaissances en matière d'IA, afin que les décideurs puissent comprendre les capacités, les risques et les limites de l'IA.

5. Déploiement à grande échelle de l'IA

Les institutions financières peuvent renforcer leur résilience opérationnelle en déployant l'IA à grande échelle. Les meilleures pratiques recommandent de commencer par déterminer les occasions pilotes ou fondamentales, puis de passer à des initiatives opérationnelles plus larges, et enfin de se concentrer sur les investissements stratégiques, selon une approche progressive.

Occasions de détecter et de restreindre la criminalité financière

Les participants au forum ont relevé des occasions prospectives pour minimiser la criminalité financière et atténuer les risques associés à l'adoption de l'IA.

1. Adoption et mise en œuvre accrues de l'IA

- La modernisation de l'infrastructure technologique comprendrait la mise à jour des systèmes existants, la modernisation de

l'infrastructure de données, la normalisation des formats de données et la consolidation des données entre les différents fournisseurs afin d'uniformiser l'accès.

- L'évaluation des risques en temps réel permettrait le déploiement de l'IA aux points de contact et l'intégration pour soutenir les décisions du personnel et renforcer les défenses.
- L'automatisation des déclarations de transactions douteuses (STR) et le déploiement de l'IA pour la reconnaissance de schémas amélioreraient la qualité et la cohérence tout en réduisant la charge de travail des analystes.

2. Transformation organisationnelle

- Les participants ont suggéré que le secteur des services financiers pourrait tirer profit d'orienter ses investissements vers des améliorations de plus en plus stratégiques et analytiques. Les facteurs contributifs incluent l'investissement continu dans les talents en IA, la création d'équipes multifonctionnelles chargées de lutter contre la criminalité financière, et l'accent mis sur la transformation stratégique plutôt que sur les « gains rapides réalisés grâce à l'IA ».
- Pour les gouvernements, une collaboration significativement accrue augmenterait l'efficacité et l'efficience et faciliterait la coordination entre les différents piliers.
- La collaboration entre les piliers est devenue une priorité absolue, et certains participants ont suggéré qu'une coordination centralisée accrue, potentiellement par l'intermédiaire d'un organisme dédié ou de coordination, pourrait renforcer l'approche canadienne en matière de lutte contre la criminalité financière.

- À peine deux semaines après cet atelier, le premier ministre a annoncé que le budget de novembre 2025 introduira une « Stratégie nationale antifraude » complétée par une Agence contre les crimes financiers pour « diriger les efforts du Canada dans la lutte contre les crimes financiers sophistiqués ».ⁱ Ces annonces pourraient potentiellement combler certaines des lacunes en matière de coordination et d'échange d'informations relevées par les participants aux ateliers.

3. Initiatives réglementaires

- Les bacs à sable et les environnements de mise à l'essai devraient être mis en place de toute urgence. Afin de pallier les risques liés au non-respect des exigences réglementaires par les solutions d'IA, les participants à l'atelier ont vivement encouragé les organismes de réglementation à concevoir et à fournir un modèle de bac à sable qualifié. Ce modèle devrait offrir un cadre sécurisé pour mettre à l'essai des outils et des méthodes d'IA innovants, par exemple en les faisant fonctionner en parallèle avec les systèmes existants lors de leur mise en œuvre.
- Étant donné que l'IA améliore la capacité à masquer les relations entre les entreprises, les participants ont recommandé que le critère actuel de participation de 25 % soit réduit et que la définition soit élargie pour inclure « le contrôle et l'influence ». Cela pourrait inclure l'accès aux données qui rendent les dirigeants, les conseils d'administration et les investisseurs plus transparents.
- Bien que la protection de la vie privée ait été exclue du cadre de cet atelier, plusieurs participants ont noté que cet élément a un impact significatif dans la lutte contre

ⁱ Communiqué de presse, 20 octobre 2025, ministère des Finances Canada. « Le ministre Champagne s'attaque à l'exploitation financière et annonce une stratégie antifraude et une nouvelle agence contre les crimes financiers »

la criminalité financière assistée par l'IA, notamment dans le partage d'informations. Des modifications du régime de confidentialité pourraient être nécessaires pour équilibrer les droits individuels à la vie privée avec la rapidité de collaboration nécessaire pour lutter contre la criminalité financière renforcée par l'IA.

4. *Établir un régime collaboratif à trois piliers*

- Soixante pour cent des participants à cet atelier ont répondu que les efforts conjoints de renseignement entre le secteur et le gouvernement amélioreraient au mieux la collaboration public/privé sur l'IA et la criminalité financière.ⁱ
- Les participants au Forum ont reconnu l'importance d'une plus grande coopération entre les institutions financières, les organismes de réglementation et les organismes d'application de la loi. Cela devrait faciliter le partage et la réception en temps opportun de données précises et exploitables afin de contrer l'utilisation de l'IA par des auteurs de menaces pour masquer des fonds et dissimuler des liens, augmentant ainsi la fréquence et la gravité de la fraude.

PROCHAINES ÉTAPES

Les participants à ce deuxième atelier de la Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers ont apporté leurs connaissances et leur expertise pour soutenir un effort collaboratif visant à mieux comprendre comment l'adoption de l'IA dans le secteur financier et par les auteurs de menaces touchera les risques. Ils ont également conclu que des initiatives collaboratives

comme la Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers sont un facteur important pour faire avancer les intérêts communs du secteur financier et de ses organismes de réglementation. Leurs délibérations ont également permis de déterminer les pratiques exemplaires actuelles pour réduire les risques connus ainsi que les occasions pour le secteur et le gouvernement, ce qui améliorerait considérablement la capacité du Canada à détecter et à prévenir la criminalité financière.

Compte tenu du rythme rapide de développement de l'IA et de la criminalité financière assistée par l'IA, l'industrie, les organismes de réglementation et le gouvernement exigent des investissements et des discussions dans ce domaine simplement pour suivre le rythme des auteurs de menaces dans ce domaine. Des améliorations significatives dans la mise en œuvre de l'IA, les actions sectorielles et réglementaires, ainsi qu'une meilleure collaboration aideraient à protéger les consommateurs canadiens et le système financier canadien.

Deux autres tables rondes dans cette phase du Forum sur l'intelligence artificielle dans le secteur des services financiers auront lieu en octobre et novembre 2025. Des rapports intermédiaires pour chacun de ces ateliers seront publiés, suivis en 2026 d'un rapport final qui synthétisera les perspectives du forum sur les risques, les menaces et les occasions.

Le CANAFE et le GRI ont apprécié la contribution de tous les participants au forum et continueront de favoriser des discussions collaboratives entre le secteur, les décideurs, les organismes de réglementation et les surveillants.

ⁱ Résultats du sondage des participants, Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers – Criminalité financière, 1^{er} octobre 2025.

© Sa Majesté le Roi du Chef du Canada, 2025

Deuxième édition du Forum sur l'intelligence artificielle dans le secteur des services financiers : Une approche collaborative à l'égard des menaces, possibilités et pratiques exemplaires liées à l'IA Atelier 2 - Criminalité financière

IN4-35/2-2-2026E-PDF

ISBN 978-0-660-79418-1