IA générative et évolution de l'univers de la fraude

Un virage qui change la donne dans le secteur bancaire

Meilleure la question,
meilleure la réponse.
Pour un monde meilleur.

feedzai

EY
Façonner l'avenir
en toute confiance

SOMMAIRE

L'intelligence artificielle (IA) générative transforme rapidement l'univers de la fraude avec lequel doivent composer les institutions bancaires. Les mesures antifraudes classiques s'avèrent insuffisantes, car les fraudeurs tirent parti de divers stratagèmes, en exploitant notamment l'IA générative pour manipuler les clients de sorte qu'ils leur ouvrent la voie à la perpétration d'opérations frauduleuses. Dans le présent article, rédigé en collaboration par EY Canada et Feedzai, nous verrons comment l'IA et l'IA générative changent la donne dans la lutte contre les arnaques, tout en présentant des informations sur les innovations dont les institutions bancaires peuvent tirer parti pour conserver une longueur d'avance.

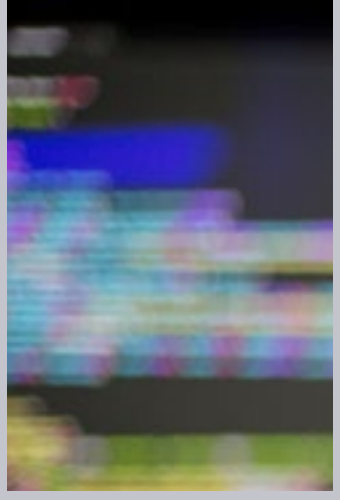
En bref

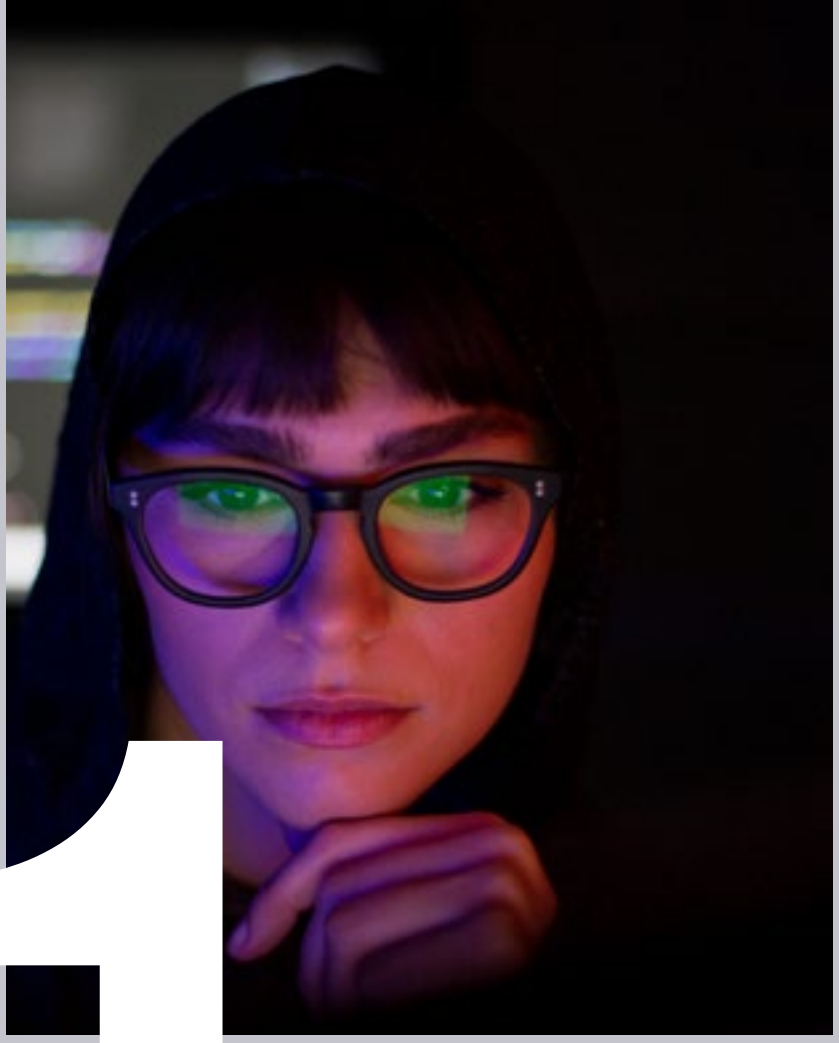
Bien que l'IA offre une protection contre les arnaques, les fraudeurs peuvent faire une utilisation abusive de l'IA générative.

C'est en gérant efficacement les arnaques que les institutions bancaires peuvent fidéliser leurs clients et éviter d'obtenir des résultats négatifs. Le Royaume-Uni fait figure de leader en matière de réglementation visant à assurer la protection des consommateurs.

Pour bien se prémunir contre la fraude et veiller à la sécurité de leurs clients, les institutions bancaires doivent exploiter l'IA dans un environnement laissant place à l'exercice du jugement professionnel.

Table des matières.





SECTION 01

Arnaques – Un défi grandissant pour les systèmes antifraudes classiques

Dans un contexte où les fraudeurs travaillent au perfectionnement de leurs tactiques et tirent parti des progrès technologiques, les arnaques sont devenues un défi majeur pour les institutions bancaires. L'époque où celles-ci pouvaient s'appuyer sur des mécanismes antifraudes classiques, tels que les systèmes de détection à base de règles et les campagnes généralistes de sensibilisation des clients, ne sera bientôt plus qu'un vague souvenir. Désormais, les cybercriminels contournent ces mécanismes de protection, en ciblant directement leurs victimes d'arnaques, lesquelles reposent notamment sur l'usurpation d'identité, les arnaques sentimentales, la fraude à l'investissement et la fraude par cryptomonnaie. Ce revirement de situation a mené à une chute brusque des taux de détection des cas de fraude, la majorité des arnaques parvenant à échapper aux mécanismes antifraudes.

Pourquoi les arnaques posent-elles un tel défi?

Dans un contexte où les arnaques amènent les clients à ouvrir inconsciemment la voie à l'exécution d'opérations frauduleuses, les solutions de gestion de la fraude classiques perdent souvent en efficacité. Contrairement aux tentatives de fraude classiques, ces arnaques ne sont pas facilement signalées par les systèmes de détection de la fraude, car les opérations effectuées semblent avoir été autorisées par les détenteurs de compte légitimes.

Les répercussions sont désastreuses, non seulement pour les victimes de telles arnaques, mais aussi pour les institutions bancaires concernées. Plus ces manœuvres frauduleuses gagnent en complexité et se multiplient, plus les institutions financières ont du mal à s'adapter. De tels défis obligent les institutions bancaires à revoir leur stratégie antifraude, ainsi qu'à adopter une approche plus globale intégrant des campagnes de sensibilisation des clients personnalisées, des activités de surveillance en temps réel et des solutions d'IA évoluées.

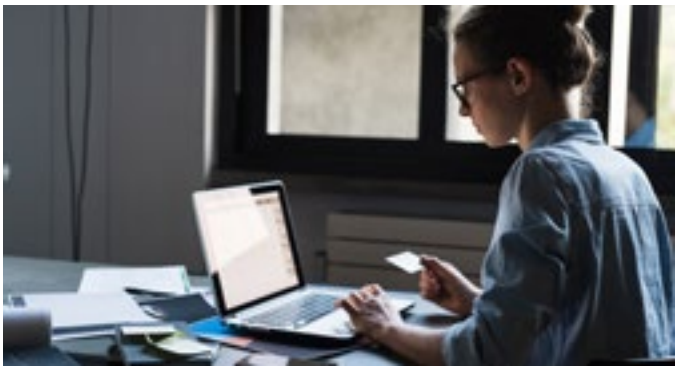
Les répercussions des arnaques sur les institutions bancaires

Les arnaques ne portent pas seulement préjudice aux clients; elles représentent aussi une menace multidimensionnelle pour les institutions bancaires.

Les conséquences financières, émotionnelles et réputationnelles découlant de tels crimes sont considérables et souvent sous-estimées.

Conséquences émotionnelles 01/03

Les clients victimes d'arnaques éprouvent souvent un sentiment de honte et de l'embarras, ce qui les dissuade de les signaler. Un taux de signalement aussi bas a pour effet de priver les institutions bancaires de données essentielles, dont elles ont besoin pour analyser et contrer les tactiques en mutation qui sont mises en œuvre dans ces circonstances.



Conséquences financières 02/03

Les arnaques peuvent avoir des conséquences financières désastreuses pour les clients lorsque la décision est prise de ne pas procéder au remboursement des sommes subtilisées. En revanche, dans les cas où les victimes obtiennent un remboursement, les institutions bancaires peuvent être amenées à essuyer des pertes considérables au titre de la fraude.

Conséquences réputationnelles 03/03

Les atteintes à la réputation engendrées par des arnaques peuvent être très importantes. Les institutions bancaires qui donnent l'impression de ne pas soutenir les victimes ou de ne pas être à leur écoute risquent de devoir faire face à l'attrition de leur clientèle, à une couverture médiatique défavorable, voire à des poursuites judiciaires. Sur un marché hautement concurrentiel, la confiance et la loyauté des clients peuvent s'en trouver compromises à long terme.

Exploitation de l'IA et de l'IA générative par les fraudeurs

Il s'avère que la propagation rapide de l'IA générative change considérablement la donne pour les cybercriminels. Parmi les utilisateurs des nouvelles technologies, ce sont les fraudeurs qui s'y convertissent le plus rapidement, alors que, contrairement aux entreprises légitimes, ils n'ont guère à se soucier des contraintes réglementaires ou en matière de protection de la vie privée. Grâce à l'IA générative, les fraudeurs peuvent intensifier leurs activités criminelles, en procédant avec une rapidité et un degré de précision inédits, et en mettant au point des stratagèmes plus sophistiqués leur permettant de déjouer les dispositifs de sécurité classiques.

Nous présentons ci-après plusieurs tactiques et tendances grâce auxquelles les cybercriminels peuvent exploiter l'IA générative de façon à défier les institutions bancaires.

Démocratisation de la cybercriminalité

L'IA générative facilite la tâche aux cybercriminels dans l'exécution de manœuvres frauduleuses complexes, peu importe qu'ils détiennent ou non des compétences pointues en la matière. Ils n'ont plus besoin de maîtriser l'orthographe ou de savoir bien écrire, ni même de parler la langue de leurs victimes. Les outils d'IA générative leur permettent de générer et de transmettre en permanence des messages d'hameçonnage en plusieurs langues, ainsi que de mieux adapter leurs tentatives d'escroquerie.

Hypertrucage vidéo

Les cybercriminels ont commencé à recourir à l'hypertrucage vidéo pour berner leurs victimes. Citons le cas notoire d'un employé d'une entreprise technologique qui a reçu un appel vidéo provenant apparemment de son chef des finances, alors qu'il s'agissait en fait d'une vidéo hypertruquée. L'hypertrucage vidéo est également utilisé pour générer des contenus à caractère disruptif, tels qu'une vidéo hypertruquée d'un incendie au Pentagone ayant semé un vent de panique sur les marchés.

Données synthétiques et cyberattaques

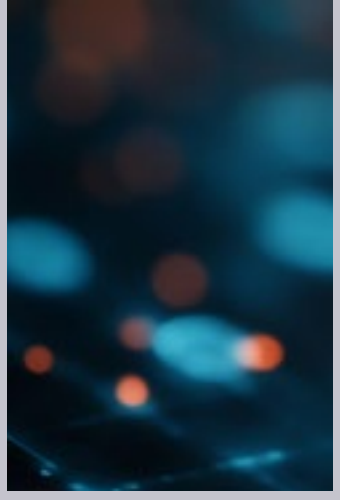
Les cybercriminels peuvent exploiter l'IA générative pour générer des données synthétiques qui ressemblent grandement à celles qui sont utilisées dans le cadre d'opérations légitimes, de sorte qu'il devient beaucoup plus difficile pour les systèmes de détection de la fraude classiques de signaler les cas d'escroquerie. Ils peuvent aussi lancer des cyberattaques sophistiquées reposant sur l'IA; par exemple, en introduisant des données d'entrée malveillantes parmi les données d'entraînement du modèle d'IA d'une institution bancaire ou en infiltrant des requêtes leur permettant de manipuler des modèles d'IA.

Imitation de la voix

La capacité de l'IA générative à imiter la voix humaine est préoccupante. Les cybercriminels peuvent perpétrer des actes frauduleux en se faisant passer pour un chef de la direction d'une entreprise dont ils ont usurpé la voix au téléphone, de façon à pouvoir autoriser des paiements frauduleux. À titre d'exemple, on peut aussi mentionner le cas d'une femme de l'Arizona qui a reçu un soi-disant appel de sa fille lançant un cri d'appel à l'aide, alors qu'il s'agissait en fait d'une imitation générée à partir d'un extrait de quelques secondes seulement d'un message vocal capté sur son site de réseau social.

Sophistication des types de cybercrimes classiques

L'IA générative peut permettre de perfectionner les arnaques classiques, telles que les tentatives d'hameçonnage et les courriels censés émaner de personnes dont l'identité a été en fait usurpée. Comme les messages provenant de cybercriminels ayant usurpé l'identité d'un proche du destinataire, ou celle d'un membre de la haute direction d'une entreprise, revêtent désormais un caractère plus persuasif, le taux de réussite de ces types de cybercrimes a augmenté, même dans les cas où le taux de réponse est faible.

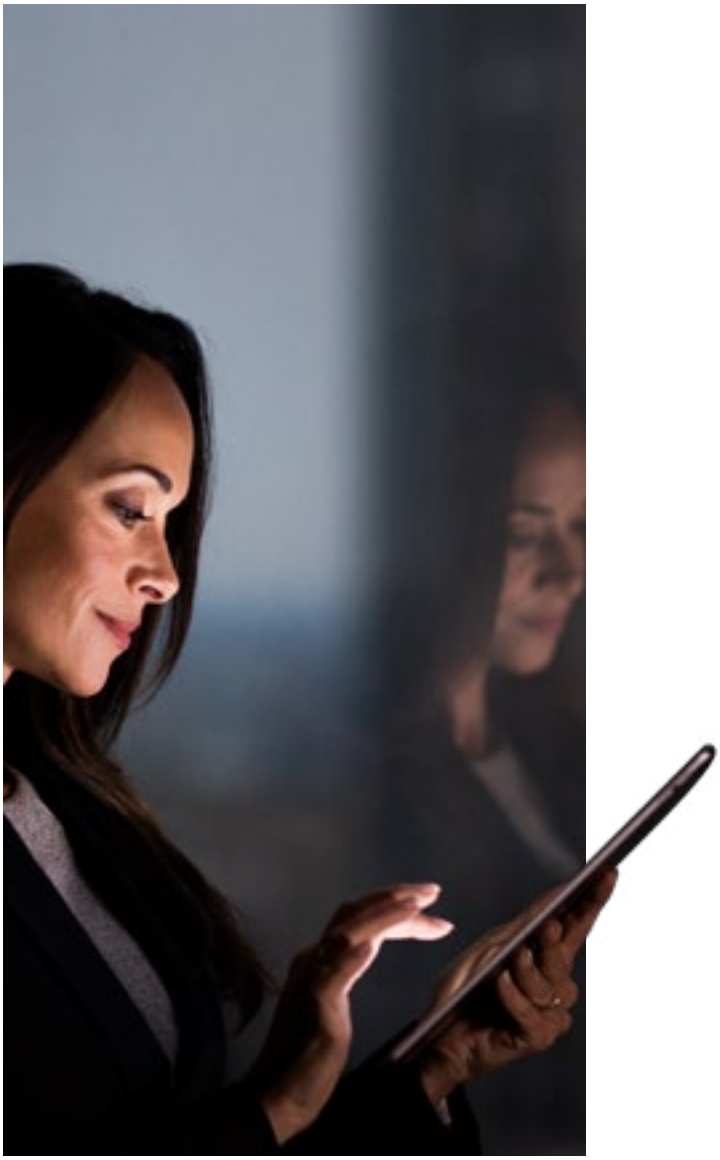


SECTION 02

Pourquoi l'IA et l'IA générative changent la donne dans la lutte contre les arnaques

Depuis des décennies, l'IA joue un rôle important dans la gestion des risques de fraude, en aidant les institutions financières à améliorer leurs stratégies de détection et de prévention. Néanmoins, dans le contexte de la prolifération des arnaques, qui sont de plus en plus sophistiquées, les limites des méthodes de protection classiques – comme les procédures d'authentification, les systèmes d'aide à la décision à base de règles, le profilage de dispositifs et la biométrie – sont mises en évidence. Bien qu'elles soient efficaces pour certains types de fraude, ces méthodes sont loin de suffire lorsqu'il s'agit de prévenir les arnaques. La question n'est pas de savoir si les institutions bancaires devraient continuer de faire évoluer leurs méthodes, mais plutôt de déterminer la mesure dans laquelle elles peuvent adopter rapidement les innovations dont elles ont besoin pour suivre le rythme auquel évoluent ces nouvelles menaces, notamment en exploitant plus largement l'IA aux fins de la prévention et de la détection de la fraude, de même que dans le cadre des interventions face à des cas de fraude.

Pour les institutions bancaires, le moment est venu de renforcer leurs capacités de collaboration, d'accorder la priorité aux relations avec les consommateurs et d'adopter de nouvelles technologies telles que l'IA et l'IA générative. Ces technologies ne représentent pas seulement des améliorations progressives, mais également une transformation fondamentale des méthodes de gestion des risques de fraude. En tirant parti des innovations et de la collaboration, les institutions financières peuvent prévenir les arnaques de façon proactive, avant qu'elles se produisent.



L'application de méthodes de gestion des risques de fraude classiques ne suffit plus

Bien que les méthodes de gestion des risques de fraude classiques se soient souvent avérées efficaces, elles ont du mal à contrer les tentatives d'arnaque reposant sur le piratage psychologique et la manipulation de clients. Même si les tactiques faisant appel à l'application d'une approche réactive continuent de jouer un rôle important, il arrive souvent qu'elles ne permettent pas de gérer les subtilités des arnaques qui amènent des clients à ouvrir la voie à la perpétration d'opérations frauduleuses, sans le savoir.

Les arnaques – notamment l'usurpation d'identité, la fraude à l'investissement et les arnaques sentimentales – reposent sur l'exploitation du lien de confiance qui existe entre les clients et leur institution bancaire. Pour s'attaquer à de tels défis, les institutions bancaires doivent se départir de leurs méthodes antifraudes réactives pour adopter des stratégies de prévention de la fraude proactives qui leur permettent de tirer parti de l'IA de façon à conserver une longueur d'avance sur les menaces en évolution.

IA et IA générative – La prévention des arnaques à l'avenir

L'IA et l'IA générative changent véritablement la donne dans la prévention des arnaques. En exploitant plus largement ces technologies, les institutions bancaires peuvent améliorer les méthodes antifraudes qu'elles appliquent déjà et faire figure de pionniers en recourant à de nouvelles méthodes de protection de leurs clients.

La collaboration joue un rôle essentiel. Les institutions bancaires doivent collaborer, en échangeant leurs connaissances et leurs données, de façon à se doter de méthodes de défense plus résilientes.
La priorisation des relations avec les clients s'avère déterminante, car elle permet de faire en sorte que les stratégies de prévention de la fraude soient articulées autour de l'expérience client et du maintien de la confiance. Finalement, l'IA et l'IA générative sont des technologies novatrices qui peuvent faire passer la prévention des arnaques à un stade d'évolution supérieur.

Démystification de l'IA générative – Principaux cas d'utilisation

Le potentiel d'exploitation de l'IA générative dans la lutte contre les arnaques est énorme. Nous vous présentons ci-après des applications possibles.

Génération de données synthétiques 01/07

Les systèmes de détection de la fraude ont souvent du mal à composer avec des ensembles de données déséquilibrés. Or, l'IA générative excelle dans la génération de données synthétiques, ce qui représente une valeur inestimable quand il s'agit de renforcer les ensembles de données en situation de manque de données ou d'exemples étiquetés de grande qualité. C'est ainsi que les modèles antifraudes peuvent en arriver à mieux reconnaître et signaler les activités frauduleuses, même lorsque se produisent des incidents peu fréquents, comme dans le cas des types d'arnaque émergents.

Entraînement contradictoire 02/07

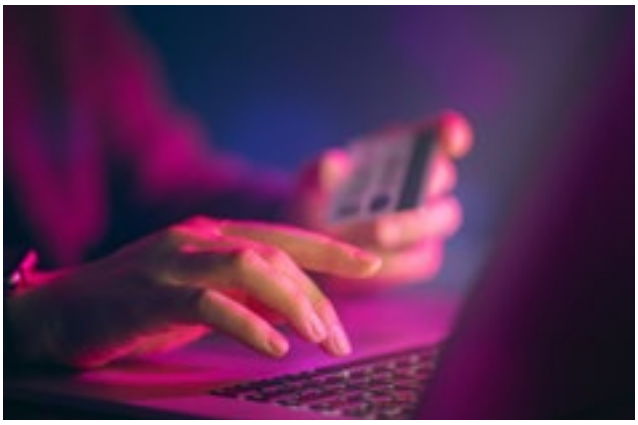
L'IA générative peut simuler la perpétration de cyberattaques reposant sur l'exploitation de données synthétiques, de sorte que les modèles antifraudes puissent être soumis à des simulations de crise visant à permettre de contrer d'éventuelles cybermenaces. Cette méthode favorise non seulement le renforcement des mécanismes de défense intégrés à un modèle, mais également la réduction des risques de partis pris, ce qui s'avère essentiel à la préservation des liens de confiance avec la clientèle.

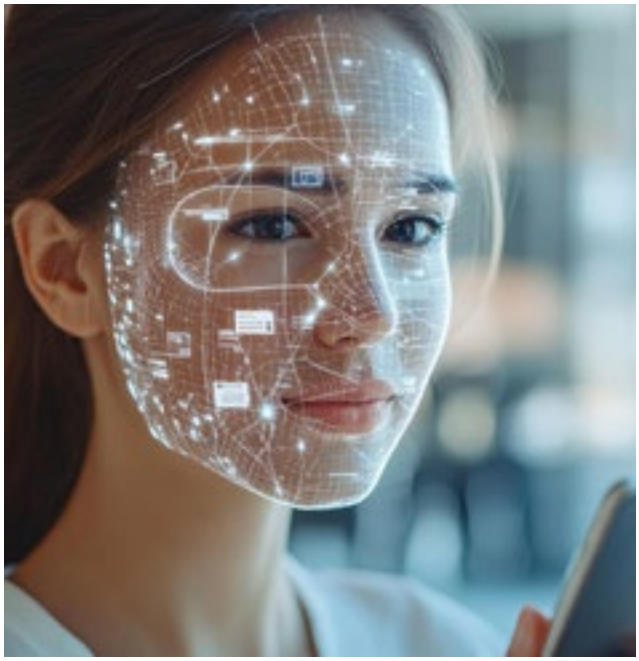
Détection et correction des anomalies 03/07

L'IA s'est avérée efficace dans le recensement des anomalies présentes dans les données quantitatives, et l'exploitation de l'IA générative permet de renforcer davantage ces capacités. Elle améliore la performance et l'efficacité des modèles de détection de la fraude, ce qui mène ultimement à l'obtention de meilleurs résultats pour les clients, grâce à la réduction du nombre de faux positifs et à la rationalisation du processus de correction des anomalies.

Authentification 04/07

L'IA générative peut générer des profils perfectionnés sur les habitudes des clients, en relevant des indices subtils d'activités suspectes, tels qu'une vitesse de frappe ou des habitudes de navigation en ligne anormales, ou encore des incohérences géographiques. C'est ainsi que les institutions bancaires peuvent détecter et prévenir les tentatives d'accès non autorisé ou de prise de contrôle de comptes avant qu'elles dégénèrent, tout en faisant en sorte que leurs clients légitimes soient exposés à un minimum de désagréments dans l'exécution de leurs opérations.





Modélisation des cybermenaces 05/07

L'IA générative peut être exploitée pour simuler des cyberattaques frauduleuses ou créer des scénarios d'escroqueries auxquels les institutions bancaires pourraient avoir à faire face éventuellement. En simulant de telles menaces réalistes et complexes, elles peuvent tester de façon proactive leurs mécanismes antifraudes en place. Ce processus, connu sous le nom de modélisation des cybermenaces, leur facilite la tâche dans le recensement des faiblesses potentielles dans leurs systèmes, avant que de réels cybercriminels puissent exploiter celles-ci.

Bref, en tirant parti de l'IA générative, les institutions bancaires peuvent s'entraîner de façon à se prémunir contre l'utilisation de nouvelles techniques de fraude, ce qui les aide à conserver une longueur d'avance sur les cybermenaces en évolution et à mieux se préparer à faire face aux éventuelles tentatives de fraude.

Automatisation des processus d'enquête 06/07

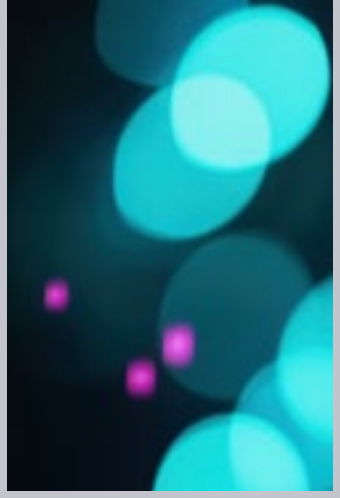
Les modèles d'IA peuvent permettre de rationaliser les processus de gestion de cas appliqués dans les enquêtes en matière de fraude, en automatisant les tâches répétitives qui requièrent beaucoup de temps. Par exemple, au lieu de recourir à des enquêteurs chargés de procéder à la collecte et à l'analyse manuelles de données, ou de produire manuellement des rapports, les institutions bancaires peuvent confier à l'IA la réalisation de ces tâches courantes. Les enquêteurs peuvent ainsi se concentrer sur le traitement des cas plus complexes hautement prioritaires, qui requièrent l'exercice d'un jugement et d'une expertise de nature humaine, de sorte que le processus global soit plus rapide et plus efficace.

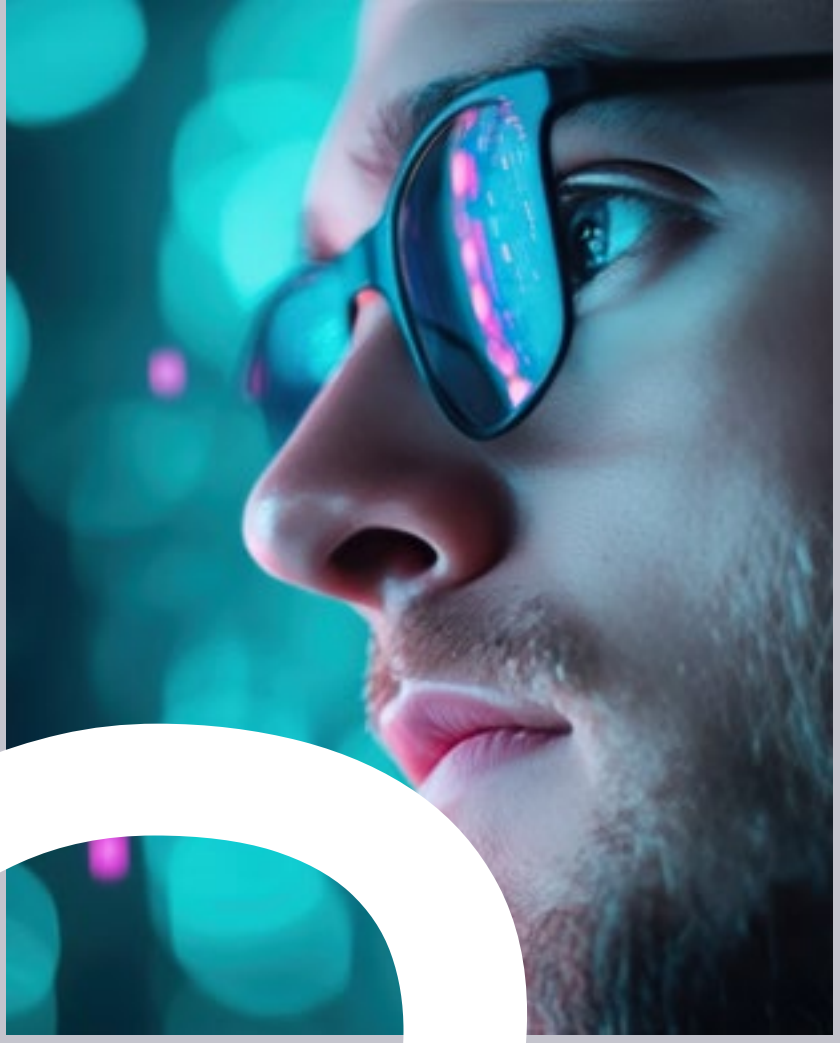
Documentation de modèles 07/07

L'IA simplifie le processus de documentation des modèles, en générant automatiquement des documents détaillés sur la façon dont ceux-ci sont construits, testés et exploités. Cette documentation est essentielle pour que les institutions financières puissent se conformer aux exigences réglementaires, en vertu desquelles elles doivent faire preuve de transparence dans l'exploitation de leurs modèles d'IA et s'acquitter de leurs obligations de reddition de comptes à cet égard.

Généralement, la création manuelle de cette documentation peut s'échelonner sur plusieurs jours, voire sur des mois, car il faut assurer le suivi de divers aspects techniques associés à la mise au point et à la performance du modèle. Le recours à l'IA permet d'automatiser une grande partie de ces tâches, grâce à la journalisation des données ainsi qu'à la modélisation de la prise de décisions et des processus, de sorte que le temps d'exécution puisse être réduit, passant d'une semaine à quelques heures seulement. Par suite de cette automatisation, les équipes disposent de plus de temps pour se concentrer sur des tâches plus stratégiques, tout en continuant d'assurer la conformité aux exigences réglementaires.

Une institution bancaire de premier ordre s'est déjà dotée de cette technologie et peut donc désormais s'acquitter en quelques heures seulement d'une charge de travail dont l'exécution pouvait auparavant s'échelonner sur toute une semaine.





SECTION 03

La voie à suivre pour les institutions bancaires en matière de prévention de la fraude

À mesure de l'évolution des tactiques de fraude, les institutions financières doivent s'adapter en recourant davantage à l'IA – et pas seulement à l'IA générative – dans la gestion de leurs risques de fraude, et ce, sur le plan aussi bien de la prévention que de la détection et de l'intervention. Bien que l'IA puisse générer de puissantes informations et ouvrir la voie à l'automatisation de certaines tâches, elle doit être intégrée consciencieusement à la stratégie d'une institution bancaire. Il est essentiel de privilégier les cas d'utilisation novateurs et de les reproduire en fonction des leçons apprises. En mettant à l'essai et en perfectionnant des applications d'IA, les institutions bancaires peuvent générer continuellement des avantages concrets, tout en conservant une longueur d'avance sur les menaces en évolution.

Les humains continuent néanmoins de jouer un rôle essentiel dans l'exploitation de telles innovations technologiques. L'IA ne saurait être substituée à l'intervention de professionnels de la gestion des risques de fraude; elle leur permet de faire un meilleur travail, en ayant ainsi la possibilité de se concentrer sur des tâches plus complexes auxquelles est associée une plus grande valeur. À mesure que de nouveaux progrès en matière d'IA générative seront réalisés, des utilisateurs continueront d'innover, aussi bien à bon escient qu'à des fins malveillantes. Le défi consistera à trouver des utilisations positives de l'IA générative, dans une optique d'atténuation des risques.

Par ailleurs, les institutions bancaires doivent également revoir leur stratégie de sensibilisation des clients aux arnaques. Leurs communications à l'intention de leur clientèle doivent être claires et personnalisées, tandis que leurs employés de première ligne doivent pouvoir bénéficier d'une formation axée sur le traitement agile et éclairé des éventuelles tentatives d'arnaque.

Vu la nature dynamique de l'IA générative, les applications et les stratégies de protection qui y sont associées sont destinées à connaître une évolution rapide. Pour conserver une longueur d'avance, les institutions bancaires doivent rester vigilantes et s'adapter continuellement aux avancées et menaces nouvelles. En adoptant une approche proactive et centrée sur l'humain dans l'exploitation de l'IA, elles peuvent contribuer à l'avènement d'un avenir meilleur aussi bien pour leurs clients que pour elles-mêmes.

SECTION 04

Conclusion

Dans le monde entier, les tentatives d'arnaque continuent de poser des défis importants aux systèmes antifraudes classiques, ce qui rend nécessaire l'application de stratégies de prévention, de détection et d'intervention novatrices permettant d'atténuer efficacement les cyberrisques. Les institutions qui refilent aux clients la responsabilité en matière d'arnaques risquent de subir les contrecoups de l'attrition de leur clientèle et d'une couverture médiatique défavorable, tout en incitant les autorités de réglementation à modifier leurs exigences, comme c'est le cas au Royaume-Uni, où de nouvelles règles de protection des consommateurs sont en voie d'être mises en œuvre.

Bien qu'un potentiel immense soit associé à l'IA générative, aussi bien en termes de gains d'efficience et d'efficacité que d'amélioration de l'expérience client, la mise en œuvre de cette technologie requiert des efforts continus en matière de vigilance et d'adaptation, de sorte que les avantages pouvant en découler puissent être réalisés, dans un contexte où les risques qu'elle comporte sont réduits au minimum.

En définitive, il n'y a pas de solutions de gestion des risques de fraude universelles qui puissent être appliquées aussi bien à l'IA qu'à l'IA générative. Il est essentiel d'adopter une approche globale qui intègre à la fois l'IA et l'IA générative, tout en prenant en compte des aspects plus vastes, tels que les évaluations de risque, la sensibilisation des clients et des employés aux risques de fraude, l'application de procédures d'authentification robustes et la réalisation d'interventions exhaustives en cas de fraude. En se dotant d'une approche multidimensionnelle, les institutions financières seront plus à même de contrer les tentatives d'escroquerie et de protéger leurs clients dans le contexte d'un univers de la fraude en pleine évolution.

EY | Travailler ensemble pour un monde meilleur

EY contribue à un monde meilleur en créant de la valeur pour ses clients, pour ses gens, pour la société et pour la planète, tout en renforçant la confiance à l'égard des marchés financiers.

Grâce aux données, à l'intelligence artificielle et aux technologies de pointe, les équipes d'EY aident les clients à façonner l'avenir en toute confiance et proposent des solutions aux enjeux les plus pressants d'aujourd'hui et de demain.

Les équipes d'EY fournissent une gamme complète de services en certification, en consultation et en fiscalité ainsi qu'en stratégie et transactions. S'appuyant sur des connaissances sectorielles, un réseau mondial multidisciplinaire et des partenaires diversifiés de l'écosystème, les équipes d'EY sont en mesure de fournir des services dans plus de 150 pays et territoires.

EY est *All in* pour façonner l'avenir en toute confiance.

4625365

ey.com/ca/fr

Feedzai | Plus de confiance, moins de crime.

Chez Feedzai, nous avons pour mission de faire du monde du commerce un milieu plus sûr, une opération à la fois.

Chaque année, nous analysons des milliards de points de données, en nous appuyant sur des modèles propulsés par l'IA pour détecter et prévenir les cas de fraude en temps réel. Notre plateforme RiskOps aide les institutions à remplir leurs obligations de conformité, à enrayer les activités illicites et à déjouer les stratagèmes de blanchiment d'argent et du crime organisé. Nous sommes les gardiens de votre écosystème financier dans son ensemble, du début à la fin de votre parcours client.

Les institutions financières de premier plan du monde entier font confiance à Feedzai pour sécuriser des opérations d'une valeur se chiffrant dans les billions de dollars, gérer les risques et améliorer l'expérience client.

Identité | Gestion des risques de fraude de l'entreprise | Lutte contre le blanchiment d'argent

info@feedzai.com