CELENT

RENDRE OPERATIONNELLE LA PREVENTION DE LA FRAUDE SUR IBM Z16

Réduire les pertes associées aux banques, cartes et paiements

Neil Katkov

5 avril 2022

Ce rapport a été commandé par IBM, qui a demandé à Celent de le concevoir et de le mettre en œuvre. L'analyse et les conclusions sont celles de Celent et IBM n'a aucun contrôle éditorial sur le contenu de ce rapport.

SOMMAIRE

SYNTHESE

Les progrès en matière d'intelligence artificielle (IA), tels que l'apprentissage en profondeur, permettent des améliorations significatives dans la détection des fraudes. Cependant, de grandes banques et sociétés de traitements des paiements qui utilisent des modèles d'IA ne les appliquent souvent qu'à une fraction des transactions en raison des contraintes de débit et de latence de leur système de détection des fraudes. C'est pourquoi de nombreuses transactions frauduleuses demeurent sans surveillance et ignorées.

L'accélérateur d'IA intégré d'IBM, composant du nouveau processeur Telum pour mainframe, est conçu pour exécuter des inférences de charges de travail en temps réel, à grande échelle et avec une faible latence. La puce vise à permettre la détection des fraudes en temps réel, même dans les environnements bancaires, de cartes ou de paiements à fort volume.

Pour aider les banques et les sociétés de traitement des paiements à comprendre la valeur potentielle de cette innovation pour les opérations anti-fraude, Celent a estimé la réduction possible des pertes dues à la fraude dans le cadre d'une application de l'inférence de l'IA à 100 % de leurs transactions.

Avantages quantifiables de la détection des fraudes par l'IA sur des mainframes IBM z16 :

Réduction des pertes sectorielles dues à la fraude de		Réduction des pertes par banque de		Réduction des refus de transactions par cartes de
États-Unis	Monde	Banque américaine de niveau 1	Banque américaine de niveau 2	
5,6 ¢ par tranche de 100 $	2,0 ¢ par tranche de 100 $	105 millions de dollars	18 millions de dollars	46 %

Celent estime que l'application de modèles d'inférences avancés à toutes les transactions bancaires et par carte et aux paiements exécutés sur des mainframes IBM zSystems pourrait potentiellement réduire les pertes dues à la fraude de près de 161 milliards de dollars à l'échelon mondial. Les banques pourraient alors éviter une perte de 140 milliards de dollars, et de 21 milliards de dollars pour les cartes et les paiements. Rien qu'aux États-Unis, les pertes dues à la fraude bancaire pourraient être réduites de 44 milliards de dollars et de 6 milliards de dollars pour les cartes et les paiements.

Il existe certes des obstacles à l'adoption de l'inférence de l'IA sur mainframe pour les opérations de lutte contre la fraude, notamment des problèmes de gouvernance des modèles, les coûts de remplacement, la disponibilité des ressources internes spécialisées en science des données et la démonstration des analyses de rentabilité.

Néanmoins, l'exécution de modèles d'IA avancés directement dans l'environnement des mainframes est une innovation puissante dans un secteur où l'on estime que 70 % de la valeur des transactions mondiales s'effectuent sur des mainframes IBM. La détection des fraudes est un cas d'utilisation important de cette nouvelle capacité d'IBM, avec des avantages démontrables tant au niveau des résultats que de l'expérience client.

LE COUT ELEVE DES FRAUDES LIEES AUX OPERATIONS BANCAIRES, AUX CARTES ET AUX PAIEMENTS

La fraude a généré une perte mondiale estimée à 385 milliards de dollars dans les secteurs des opérations bancaires, des cartes et des paiements en 2021.

La fraude liée aux opérations bancaires et aux paiements prend de nombreuses formes dans les secteurs de la vente au détail et de l'entreprise. La fraude ciblant les banques inclut la prise de contrôle de comptes, la fraude par paiements automatiques autorisés (authorized push payments, APP), la fraude aux factures ainsi qu'une large gamme de programmes d'hameçonnage et d'ingénierie sociale conçus pour déclencher des virements illégitimes ou pour obtenir des droits d'accès de compte. Les cartes et les paiements sont aussi vulnérables à la prise de contrôle de compte et à l'hameçonnage, ainsi qu'à des programmes spécifiques dont l'identification synthétique, la fraude par détournement avec fuite et la fraude par attaque de l'intercepteur.

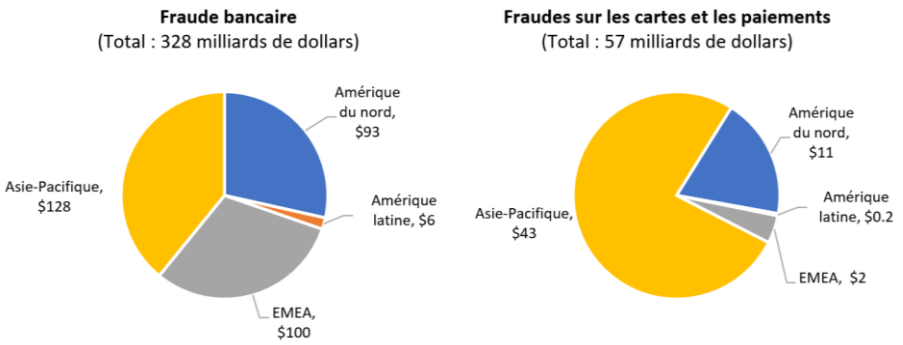
Figure 1: Stratagèmes courants de fraude bancaire et de fraude à la carte

Fraude bancaire	Fraude à la carte
Prise de contrôle de compte	Fraude à l'application
Fraude au paiement automatique autorisé	Fraude par détournement avec fuite
Fraude par chèque	Attaque de l'intercepteur
Fraude aux factures	Hameçonnage
Ingénierie sociale	Identification synthétique

Source : Celent

Ces fraudes, ainsi que d'autres visant les comptes bancaires, les cartes et les paiements, préoccupent sérieusement les établissements financiers. Celent estime la perte annuelle moyenne due à la fraude à 209 millions de dollars pour une banque de niveau 1 aux États-Unis (total des actifs supérieur à 100 milliards de dollars) et à 35 millions de dollars pour une banque de niveau 2 (total des actifs compris entre 50 et 100 milliards de dollars). À l'échelle du secteur, les banques ont subi 328 milliards de dollars de pertes liées à la fraude dans le monde en 2021. Le secteur des cartes et celui des paiements ont subi des pertes supplémentaires de 57 milliards de dollars. Au total, la fraude a entraîné une perte mondiale estimée à 385 milliards de dollars dans les secteurs des banques, des cartes et des paiements en 2021.

Figure 2: Pertes liées à la fraude bancaire, sur les cartes et sur les paiements en 2021



Source : Estimations de Celent basées sur des données de transactions de la BRI et les données des banques centrales sur la fraude.
Remarque : La fraude bancaire concerne les virements, les prélèvements automatiques et les chèques. La fraude aux cartes et aux paiements concerne les cartes de crédits et de débit, les paiements électroniques et d'autres paiements.

Bien que les banques et les sociétés de traitement des paiements se soient engagées dans une bataille de plusieurs décennies pour contenir la fraude par des systèmes de détection et par la sécurité des cartes à puce, les pertes continuent à augmenter. Les fraudeurs gardent en effet une longueur d'avance en concevant de nouveaux stratagèmes fondés sur la technologie et l'ingénierie sociale.

La pandémie de COVID-19 a fait augmenter le nombre de fraudes. Pour les banques, la fraude trouve majoritairement son origine dans l'hameçonnage et des schémas d'ingénierie sociale qui exploitent l'anxiété et les besoins médicaux liés à la pandémie. En ce qui concerne les transactions par carte, la pandémie a conduit à une augmentation des services bancaires numériques et du commerce électronique, les consommateurs ayant évité les transactions en magasin. Comme les transactions avec carte non présente (CNP) se taillent la part du lion de la fraude à la carte (près de 65 %), les pertes dues à la fraude à la carte ont augmenté.

De l'aide en perspective : modèles de fraude basés sur l'apprentissage en profondeur

Les progrès de l'intelligence artificielle, comme l'apprentissage en profondeur, fournissent désormais aux banques les outils nécessaires pour lutter beaucoup plus efficacement contre la fraude en analysant les données à grande échelle. Les banques peuvent ainsi déployer des modèles qui identifient les fraudes, y compris à l'aide de nouvelles typologies inédites.

L'apprentissage en profondeur est un type de modèle d'apprentissage automatique basé sur un réseau de neurones profond (DNN). Un DNN est constitué de nœuds informatiques, ou neurones, qui utilisent des poids progressifs pour renforcer les connexions entre les nœuds. Les nœuds sont disposés en plusieurs couches (constituant un réseau « profond ») qui augmentent la capacité et le taux d'apprentissage du modèle. Les modèles d'apprentissage en profondeur sont formés à l'aide de données existantes, telles que des transactions historiques dans le cas des modèles de fraude. Le modèle formé est alors exécuté sur des données en direct, comme une transaction en temps réel, pour générer un résultat ou une inférence. Dans le cas des modèles de fraude, l'inférence est généralement un score exprimant la probabilité que la transaction soit frauduleuse.

Sur la base de conversations et de recherches dans le secteur, Celent estime que l'inférence de l'IA sur des modèles d'apprentissage en profondeur peut augmenter la précision et la détection des fraudes de 60 % par rapport aux modèles de fraude existants.

Le potentiel de l'inférence pour améliorer le taux de détection de la fraude est toutefois considérablement limité par le fait que, dans des environnements de mainframes à volumes élevés, ces modèles ne sont souvent exécutés que sur une fraction des transactions (moins de 10 %) en raison des problèmes de latences, de coûts et d'insatisfaction du client. Cela signifie qu'environ 90 % des fraudes potentiellement évitables demeurent indétectées. La capacité des banques à bénéficier des progrès de l'IA pour récupérer les pertes dues à la fraude s'en trouve fortement limitée.

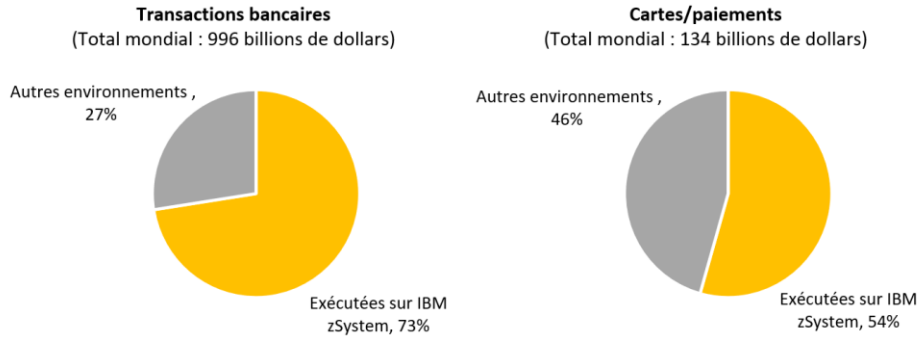
Les problèmes de latence et de coûts associés au traitement de toutes les transactions bancaires et par carte à l'aide de modèles avancés appartiennent désormais au passé. Le nouveau processeur IBM z16 Telum contient un accélérateur d'IA qui, pour la première fois dans des IBM zSystem, peut exécuter des modèles d'IA directement sur la puce, en temps réel. L'amélioration exponentielle du débit et des temps de réponse qui en résulte permet, pour la première fois, de faire passer virtuellement toutes les transactions par des modèles de détection des fraudes basés sur l'apprentissage en profondeur.

LES LIMITES DU STATU QUO EN MATIERE DE DETECTION DES FRAUDES

Avec la technologie de détection des fraudes et les approches opérationnelles traditionnelles appliquées aux environnements de mainframes, la détection des fraudes s'exécute à l'aide de systèmes hors plateforme sur des transactions sélectionnées ou après la transaction. La capacité des banques et des sociétés de traitement des paiements à exécuter des modèles d'IA avancés sur toutes les transactions en est considérablement amoindrie.

De nombreuses grandes banques et sociétés de traitement des paiements exécutent leurs systèmes de base dans des environnements informatiques de mainframe. IBM estime que 45 des 50 plus grandes banques au monde fonctionnent sur des mainframes IBM zSystem. La plupart des grandes sociétés de traitement des paiements et de cartes utilisent également ce type de plateformes. Au niveau mondial, Celent estime que 70 % de la valeur des transactions bancaires par carte et des paiements s'obtient dans des environnements IBM zSystems.

Figure 3: Valeur des transactions bancaires et par carte et des paiements sur IBM zSystem



Source : Celent

La latence entre les systèmes centraux et les systèmes de détection hors plateforme peut être tolérée pour certaines transactions. Toutefois, dans le cas de routines d'inférence de l'IA à forte intensité de données appliquées à des transactions en temps réel (comme les paiements en temps réel, les transactions par carte et les transactions bancaires numériques), la latence rend peu pratique le passage de toutes les transactions par une plateforme de détection de l'IA dans des environnements à volume élevé. Quand les transactions du système central sont envoyées du mainframe vers un système de détection hors plateforme pour une analyse en temps réel, les temps de réponse pour recevoir les résultats de la détection varient de 50 à 80 millisecondes, alors que les transactions sont en attente. L'approbation des transactions prend plus de temps, ce qui peut créer de l'insatisfaction chez les clients, en particulier dans le cas des transactions par carte.

Surtout, une latence élevée peut rendre impossible le traitement de toutes les transactions par un système de détection hors plateforme. La latence entre le système central et le logiciel

de détection peut retarder la réception par le système central des résultats de la détection au point que les transactions en temps réel sont interrompues. C'est pourquoi certaines banques n'appliquent des modèles d'apprentissage en profondeur à la détection de la fraude qu'après la transaction.

De ce fait, les banques n'envoient qu'une fraction des transactions (moins de 10 %) en temps réel vers leur moteur de détection des fraudes. Cette approche a de graves conséquences. Les modèles d'apprentissage en profondeur permettent désormais une amélioration importante, d'environ 60 %, des taux de détection. Cependant, les banques n'en retirent pas tous les bénéfices possibles puisqu'elles n'appliquent ces modèles qu'à un échantillonnage de transactions. Autrement dit, une proportion plus élevée de fraudes reste non détectée, ce qui augmente les pertes. La fraude devenant le point de mire de la conformité en matière de lutte contre la criminalité financière, les banques peuvent également être confrontées à un risque réglementaire si elles ne parviennent pas à faire passer toutes leurs transactions par la détection anti-fraude.

Problèmes historiques dans une banque américaine de niveau 1

Une banque américaine de niveau 1 dont le système central repose sur une plateforme IBM zSystem déploie un système de détection des fraudes basé sur l'IA hors plateforme. En raison de problèmes de coût et de latence, la banque ne fait passer que les transactions à très haut risque dans le système d'IA. La majorité des transactions sont soumises à un classement basé sur des règles, approuvées par commodité pour le client, puis soumises à une analyse une fois la transaction réalisée. Les avantages de l'IA sont fortement limités par l'incapacité à exécuter les modèles sur toutes les transactions, ce qui signifie que l'IA n'est pas utilisée à son potentiel maximal.

REDUIRE LES PERTES DUES A LA FRAUDE AVEC L'INFERENCE DE L'IA SUR LE MAINFRAME

IBM a développé un processeur pour son mainframe IBM z16 comportant un accélérateur d'IA, conçu pour exécuter des inférences avancées directement sur la puce, à grande échelle. Celent estime que le nouveau processeur IBM z16 peut prendre en charge la détection des fraudes basée sur l'apprentissage en profondeur pour pratiquement toutes les transactions, réduisant potentiellement les pertes liées aux fraudes bancaires, aux cartes et aux paiements de 161 milliards de dollars dans le monde.

Les algorithmes d'apprentissage en profondeur tendent à être plus gourmands en ressources informatiques que les anciens modèles de lutte contre la fraude. Lorsque les banques mettent en œuvre des inférences de l'IA basées sur l'apprentissage en profondeur, elles se heurtent à des difficultés dans la gestion des charges de travail essentielles. Quand la détection des fraudes est effectuée sur des systèmes hors plateforme, les temps de réponse de la détection peuvent atteindre plus de 80 millisecondes, avec des débits compris entre 1 000 et 1 500 transactions par seconde (tps).

En raison de ces limites de latence et de débit, les banques ont vu des transactions s'interrompre alors qu'elles attendaient les résultats de la détection. Ces problèmes et d'autres ont conduit les banques à ne faire passer qu'une fraction des transactions (moins de 10 %) dans leur moteur de détection.

Apprentissage en profondeur sur le mainframe

Sur la base d'un modèle d'apprentissage en profondeur pour la fraude à la carte de crédit, 32 puces IBM Telum s'exécutant sur un serveur unique peuvent fournir jusqu'à 3,5 millions d'inférences par seconde avec un temps de réponse moyen d'1,2 milliseconde.

Source : IBM microbenchmark, août 2021

CLAUSE DE PROTECTION : Les résultats de performances sont extrapolés à partir de tests internes d'IBM.

IBM a développé un accélérateur pour son ordinateur mainframe IBM z16 capable d'exécuter des modèles d'inférences de l'IA directement sur la puce. Selon IBM, le débit et les améliorations de l'exécution des modèles d'IA sur le mainframe sont suffisants pour prendre en charge l'analyse des fraudes en temps réel de pratiquement toutes les transactions dans les environnements de traitement des opérations bancaires, des cartes ou des paiements à fort volume.

En outre, cette analyse peut s'effectuer pratiquement sans impact sur le temps de traitement des transactions. IBM affirme que son accélérateur intégré pour IA, qui est un composant du nouveau processeur Telum, peut exécuter des modèles d'IA sur le mainframe avec un temps de réponse très rapide d'à peine 1,2 milliseconde pour chaque demande d'inférence. Dans le cas spécifique de la détection des fraudes à la carte, les premiers bancs d'essai ont indiqué qu'une configuration comprenant 32 puces Telum peut prendre en charge jusqu'à 3,5 millions d'inférences par seconde.

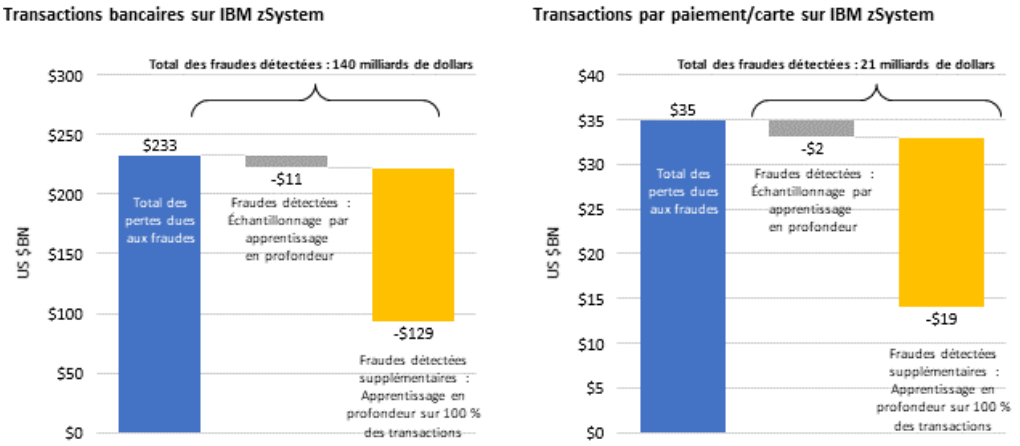
C'est une capacité suffisante pour prendre en charge même les pics dans les flux de transactions. Les banques et les sociétés de traitement des paiements peuvent ainsi appliquer des modèles d'apprentissage en profondeur à pratiquement toutes les transactions.

Les banques et les sociétés de traitement des cartes et des paiements peuvent tirer pleinement profit de la technologie moderne d'inférence en exécutant des modèles avancés sur toutes les transactions. Celent estime que l'application de modèles d'inférences avancés à toutes les transactions pourrait réduire les pertes dues à la fraude de 2 cents pour chaque centaine de dollars de transactions dans le monde (2 % de points de base).

Aux États-Unis, où les taux de fraude sont plus élevés que la moyenne mondiale (9,3 cents par tranche de 100 dollars par rapport à 3,7 cents au niveau mondial), les pertes dues à la fraude pourraient être réduites de 5,6 cents par tranche de 100 dollars. Pour la banque, cela représente une économie de 1,33 dollar pour une transaction moyenne de 2 375 dollars.

Celent estime qu'en théorie, faire passer la totalité des transactions exécutées actuellement sur des IBM zSystem par des modèles d'apprentissage en profondeur pourrait réduire les pertes dues à la fraude de 161 milliards de dollars dans le monde. Les banques pourraient éviter une perte de 140 milliards de dollars due à la fraude, ce chiffre pouvant s'élever à 21 milliards de dollars dans le cas des cartes et des paiements. Rien qu'aux États-Unis, la réduction potentielle des pertes dues à la fraude s'élève à 44 milliards de dollars pour les banques et à 6 milliards de dollars pour les cartes et les paiements.

Figure 4: Réduction potentielle des pertes dues à la fraude grâce à des modèles d'apprentissage en profondeur



Source : Celent

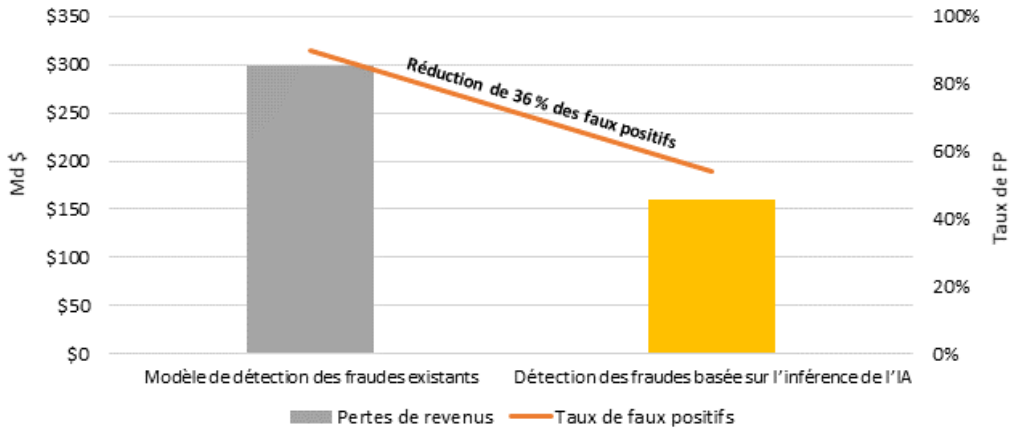
Celent estime que pour une banque de niveau 1 utilisant un IBM z16, l'application de modèles d'inférence avancés à toutes les transactions (alors que la meilleure pratique actuelle consiste à n'appliquer des modèles d'IA qu'à environ 10 % des transactions) pourrait réduire les pertes dues aux fraudes de 105 millions de dollars supplémentaires. Une banque de niveau 2 pourrait éviter des pertes supplémentaires de 18 millions de dollars. L'application de modèles avancés à toutes les transactions améliorerait aussi les modèles eux-mêmes. Des transactions plus nombreuses produiraient plus de données pour former les modèles, ce qui se traduirait par une plus grande précision dans la détection des fraudes.

MAITRISER LES FAUX POSITIFS POUR REDUIRE LA FUITE DES CLIENTS

Les anciens modèles anti-fraude ont des taux de faux positifs très élevés (généralement 90 % des transactions signalées ou plus), ce qui conduit les banques à rejeter des transactions légitimes. Le nombre accru de faux positifs et de transactions refusées crée non seulement de l'insatisfaction chez les clients, mais entraîne aussi des pertes financières importantes. En effet, les clients utilisent alors une autre carte de crédit ou de débit pour effectuer leur achat. Celent estime que les transactions par carte de crédit refusées coûtent à l'industrie 298 milliards de dollars en pertes de revenus au niveau mondial.

La nécessité de trouver un bon équilibre entre efforts de lutte contre la fraude et réduction de l'insatisfaction explique également pourquoi les banques limitent leurs procédures de détection des fraudes à un échantillon des transactions. Les faux positifs se produisent lorsque des transactions légitimes sont incorrectement signalées par le logiciel de détection comme étant frauduleuses. La précision accrue des modèles d'apprentissage en profondeur peut faire baisser sensiblement les taux élevés de faux positifs dans l'industrie. Parallèlement, le nombre de transactions refusées par erreur diminue. L'expérience vécue par les clients s'en trouve améliorée, ce qui réduit les pertes de revenus dues à la fuite de ces derniers. Il en résulte également que les banques peuvent appliquer la détection des fraudes à toutes leurs transactions avec moins de dommages dus à l'insatisfaction des clients.

Figure 5: Les modèles d'apprentissage en profondeur améliorent les taux de faux positifs



Source : Celent

L'application à toutes les transactions par carte de modèles d'apprentissage en profondeur pourrait améliorer les taux de faux positifs d'environ 55 %. Même si ceux-ci demeurent très élevés, cette démarche pourrait se traduire par une réduction des pertes de revenus liées aux frais sur les cartes de 137 à 161 milliards de dollars au niveau mondial.

Réduire les faux positifs présenterait aussi d'autres avantages. Les analystes auraient moins d'alertes à traiter, ce qui réduirait les coûts des enquêtes après transaction. En matière d'avantages pour la réputation, la réduction de l'insatisfaction et de la frustration des clients renforcerait la fidélité et la confiance de ces derniers.

Les modèles avancés pourraient aussi améliorer la détection des comportements suspects susceptibles d'indiquer un blanchiment d'argent. La loi sur le secret bancaire (Bank Secrecy Act) aux États-Unis, les directives anti-blanchiment d'argent de l'UE et d'autres réglementations font que les programmes de lutte contre le blanchiment d'argent des banques (LCB) sont examinés à la loupe par les autorités de régulation. Les autorités de réglementation sont particulièrement actives dans la condamnation des banques pour insuffisance des programmes de LCB et les amendes infligées à certaines banques dépassent le milliard de dollars. Les opérations de LCB souffrent elles aussi de taux de faux positifs très élevés, généralement supérieurs à 95 %, ce qui fait peser une lourde charge opérationnelle sur les banques. En outre, la surveillance de la LCB est généralement effectuée après la transaction, ce qui expose les banques à un risque accru. L'exploitation de modèles basés sur l'IA pour les opérations de LCB peut aider à résoudre ces problèmes en améliorant la précision de la détection des comportements de LCB et en réduisant les faux positifs.

LA VOIE A SUIVRE

Notre analyse présente les avantages quantifiables et significatifs de l'exécution des modèles d'apprentissage en profondeur sur 100 % des transactions. IBM affirme que son nouvel accélérateur peut prendre en charge cette exécution pour des transactions traitées via des mainframes IBM z16, même dans des environnements à très haut volume. Cependant, les banques et les sociétés de traitement des paiements qui franchissent le pas doivent tenir compte d'un certain nombre de facteurs.

Alors que les banques et les sociétés de traitement des cartes et des paiements évaluent les avantages de la mise en œuvre de la détection des fraudes basée sur l'apprentissage en profondeur sur mainframe, Celent leur recommande de prendre en considération les points suivants :

- **Gouvernance des modèles.** Les autorités et les auditeurs internes exigent une gouvernance solide sur les modèles de fraude. Cela signifie que les modèles d'IA doivent être transparents et explicables. Si les fournisseurs de plateformes d'IA s'éloignent généralement des approches de type « boîte noire », la gouvernance des modèles d'IA demeure une entreprise complexe.
- **Résistance des organismes de réglementation.** Si les organismes de réglementation sont à l'aise avec la détection traditionnelle basée sur les règles, ils connaissent moins bien les techniques avancées d'apprentissage en profondeur. Les banques, les scientifiques des données et leurs fournisseurs devront, dans certains cas, éduquer les organismes de réglementation sur l'efficacité et la fiabilité de l'IA avancée à mesure qu'ils progressent.
- **Coût du remplacement.** Plusieurs établissements mettent déjà en œuvre des systèmes de détection des fraudes basés sur l'IA. Ces entreprises devront soumettre le transfert de la détection sur le mainframe à une analyse de rentabilité et décider si elles doivent conserver les systèmes existants sous une forme quelconque (par exemple, pour prendre en charge l'analyse après transaction ou les petites lignes d'activités) ou les supprimer totalement.
- **Ressources en science des données.** L'accélérateur intégré d'IBM pour l'IA est optimisé pour exécuter des modèles, y compris les modèles construits avec des bibliothèques open source telles que Pytorch et TensorFlow. Cependant, il n'a pas encore été démontré qu'il prend en charge des logiciels de détection des fraudes, même si nous pensons que certains fournisseurs de produits anti-fraude finiront par proposer des logiciels susceptibles de s'exécuter sur l'accélérateur. Quoi qu'il en soit, les établissements qui transfèrent la détection de la fraude basée sur l'IA sur l'IBM z16 auront besoin de capacités en science des données pour développer et prendre en charge des modèles avancés d'apprentissage en profondeur, soit en interne, soit par l'intermédiaire de fournisseurs de modèles spécialisés.

Les établissements financiers devront prendre en considération ces facteurs et faire preuve de diligence raisonnable en ce qui concerne le nouvel accélérateur d'IA d'IBM. Cependant, les avantages potentiels en termes de réduction des pertes dues à la fraude et aux transactions refusées, ainsi que la réduction de l'insatisfaction et l'amélioration de l'expérience client, sont convaincants. Les entreprises qui utilisent des IBM zSystem doivent réfléchir soigneusement à ce qu'elles pourraient gagner en transférant la détection des fraudes sur le mainframe.

S’APPUYER SUR L’EXPERTISE DE CELENT

Si vous avez apprécié ce rapport, vous pourriez envisager de faire appel à Celent pour des analyses et des recherches personnalisées. Notre expérience collective et les connaissances que nous avons acquises en travaillant sur ce rapport peuvent vous aider à rationaliser la création, l’affinement ou l’exécution de vos stratégies.

Soutien aux établissements financiers

Les projets types que nous soutenons incluent les spécificités suivantes :

Présélection et sélection des fournisseurs. Nous effectuons une recherche spécifique à votre entreprise pour mieux comprendre vos besoins. Nous créons et nous gérons ensuite une demande de renseignements personnalisée sur les fournisseurs sélectionnés afin de vous aider à faire un choix rapide et pertinent.

Évaluation des pratiques commerciales. Nous consacrons du temps à l’évaluation de vos processus d’entreprise et de vos exigences. Sur la base de notre connaissance du marché, nous identifions les contraintes potentielles en matière de processus ou de technologie et fournissons des informations claires susceptibles de vous aider à mettre en œuvre les meilleures pratiques de l’industrie.

Création de stratégies informatiques et commerciales. Nous recueillons les points de vues de votre équipe dirigeante, de votre personnel informatique et commercial de première ligne ainsi que de vos clients. Nous analysons ensuite votre position actuelle, vos capacités et votre technologie par rapport à vos objectifs. Le cas échéant, nous vous aidons à reformuler vos plans technologiques et métiers pour répondre à vos besoins à court et long termes.

Soutien aux fournisseurs

Nous proposons des outils pour vous aider à affiner vos offres de produits et de services. En voici quelques exemples :

Évaluation de la stratégie en matière de produits et services. Nous vous aidons à évaluer votre position sur le marché en termes de fonctionnalités, de technologie et de services. Nos ateliers de stratégie vous aideront à cibler les bons clients et à adapter vos offres à leurs besoins.

Examen des messages commerciaux et du matériel auxiliaire. Sur la base de notre vaste expérience auprès de vos clients potentiels, nous évaluons votre matériel marketing et de vente, y compris votre site web et votre matériel auxiliaire.

RECHERCHES CONNEXES DE CELENT

Remaking Risk: A Taxonomy of Regtech
Octobre 2021

Technology Trends Previsory: Risk, 2022 Edition
Octobre 2021

IT and Operational Spending in AML-KYC: 2021 Edition
Décembre 2021

IT and Operational Spending on Fraud: 2021 Edition
Février 2021

Innovation In Risk: A Snapshot Through the Lens of Model Risk Manager 2021
Avril 2021

Fino Payments Bank: Remote Implementation of Enterprise-Wide Fraud Management During the Pandemic
Mars 2021

Swedbank: Modernizing Card Fraud Management and Improving Customer Experience
Mars 2021

MENTION DE DROITS D'AUTEUR

Pour de plus amples informations, veuillez contacter info@celent.com ou :

Neil Katkov nkatkov@celent.com

Amériques

États-Unis
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.424.3200

États-Unis
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.8000

États-Unis
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7800

Brésil
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

+55 11 3878 2000

EMEA

Suisse
Tessinerplatz 5
Zurich 8027

+41.44.5533.333

France
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Italie
Galleria San Babila 4B
Milan 20122

+39.02.305.771

Royaume-Uni
55 Baker Street
Londres W1U 8EW

+44.20.7333.8333

Asie-Pacifique

Japon
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokyo 107-6216

+81.3.6871.7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapour
138 Market Street
#07-01 CapitaGreen
Singapour 048946

+65 6510 9700