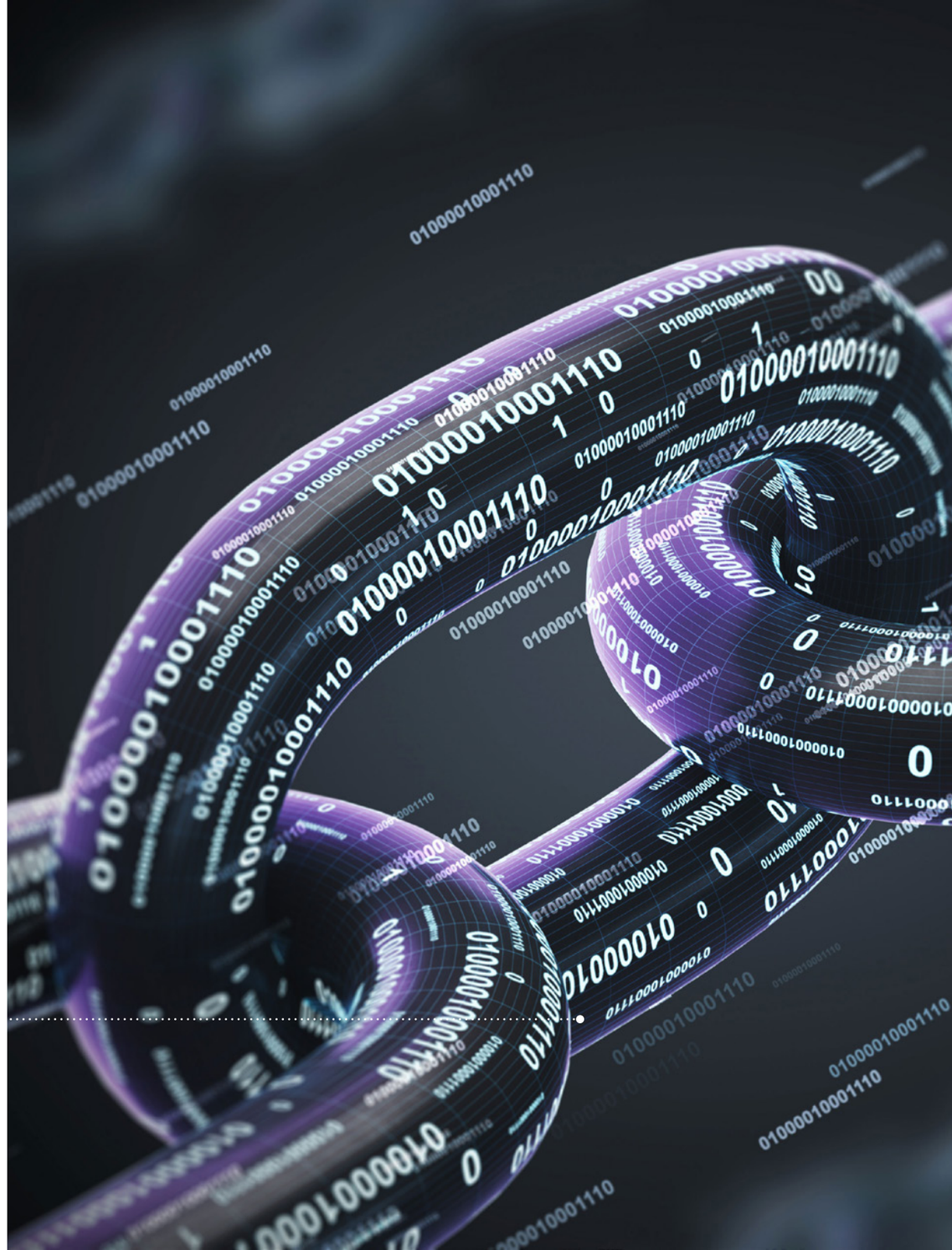
Une protection rentable contre la criminalité financière

PAR CHERYL CHIODI

Utiliser une approche globale faisant appel à l'automatisation et l'analyse peut permettre de limiter le risque, fournir une meilleure expérience client et générer du chiffre d'affaires.



Dans le cadre des expériences cumulées consécutivement à la crise de la COVID-19 en 2020, les établissements financiers ont compris qu'ils devaient réinventer leur manière d'évaluer et de gérer le risque.

Le volume des fraudes ne cesse d'augmenter et les équipes gérant les risques en première ligne doivent être renforcées avec les technologies nécessaires pour pouvoir générer des analyses efficaces, avoir une gestion des avertissements plus robuste et bénéficier au final d'une meilleure précision.

Dans les services financiers, les données ne manquent pas (données structurées, non structurées, transactionnelles, relatives au compte voire même comportementales). Lorsqu'elles sont combinées, elles peuvent fournir des informations permettant de proposer de nouvelles offres centrées sur le client.

Bien que l'utilisation des données des consommateurs fasse l'objet de toujours plus de réglementation, elle renferme un incroyable potentiel d'innovation pour apporter des avantages tant aux établissements financiers qu'à leurs clients. Cependant, les avancées technologiques permettant de fournir des produits et services innovants aux clients bancaires peuvent également être à l'origine de fraudes lorsqu'elles sont entre les mains de malfaiteurs.

Alors que les établissements financiers cherchent à réinitialiser, réinvestir et réinventer leur activité en 2021, ils doivent impérativement mettre l'accent sur la lutte effective contre la fraude, en s'appuyant sur des analyses prédictives, l'automatisation robotisée des processus et le traitement du langage naturel (TLN). Cela nécessite un changement d'état d'esprit pour passer d'un focus limité aux faux positifs et à la prévention des pertes à un accent élargi sur la collecte d'informations exploitables qui améliore sensiblement la valeur ajoutée.

LES AVANTAGES DE L'ÉLIMINATION DES SILOS

Selon l'étude 2020 True Cost of Fraud™ Study publiée par LexisNexis, (étude 2020 sur les véritables coûts de la fraude), chaque dollar de fraude coûte $3,25 aux entreprises de services financiers, soit 11 pour cent de plus que l'année précédente. La criminalité financière ne fait pas seulement courir le risque aux établissements financiers de perdre de l'argent, c'est aussi leur réputation qu'elle met en péril.

Dans le secteur des services financiers, les relations clients saines, basées sur une réputation de confiance, se traduisent par l'amélioration de la valeur client, l'augmentation de la satisfaction du client et sa fidélisation. Les coûts d'acquisition des clients étant très élevés (une récente étude a déterminé que le coût moyen total d'acquisition d'un nouveau client pour un conseiller financier est supérieur à $3000), la prévention de la criminalité financière et la préservation de la réputation ont une incidence significative sur le résultat d'un établissement financier. En faisant converger la fraude, la lutte contre le blanchiment d'argent et la cybersécurité, les établissements financiers peuvent consolider les données issues de fonctions historiquement séparées pour obtenir une vision du risque globale.

Avec d'importantes similarités dans les données collectées par les équipes de lutte contre le blanchiment d'argent, les fraudes et la cybercriminalité, l'élimination des silos peut fournir une vision plus transparente des menaces environnantes, permettre de mieux détecter les transactions suspicieuses tout en rationalisant les enquêtes. Étant donné que les criminels utilisent le cyber espace pour commettre des fraudes et qu'ils ont finalement besoin de monétiser cette information et blanchir les bénéfices afin de les faire paraître légaux, il est judicieux pour l'entreprise de rassembler ces fonctions.

Dans certains pays, les législateurs attendent des entreprises qu'elles aient une vision globale du risque à travers les différentes fonctions et qu'elles signalent les incidents cybernétiques dans le cadre de leurs obligations de reporting conventionnelles en matière de lutte contre le blanchiment d'argent et de déclaration de soupçons.

> *En faisant converger la fraude, la lutte contre le blanchiment d'argent et la cybersécurité, les établissements financiers peuvent consolider les données issues de fonctions historiquement séparées.*

Avec ce modèle, les établissements financiers peuvent bénéficier d'une réduction des coûts opérationnels et d'une amélioration de l'efficacité tout en développant une vision transversale.

QU'EST-CE QU'UNE STRATÉGIE GLOBALE ?

Une stratégie globale est ancrée dans la culture de l'établissement financier. Elle n'est pas réduite à l'état de projet, elle fait partie de son ADN. Ce type de stratégie est basée sur le risque et elle prend en compte tous les points d'accès, y compris le matériel, les logiciels, les personnes, les processus et les contenus. C'est une combinaison dynamique et en évolution permanente de prévention, de détection, d'analyse et de réponse qui permet aux établissements financiers de lutter contre les menaces complexes et les pertes potentielles.

Grâce à une approche globale basée sur les événements passés et une pensée créative afin d'identifier les problèmes avant qu'ils ne se produisent, les établissements financiers collaborer pour collecter et analyser les informations issues de toute l'entreprise. Ce modèle améliore le partage des informations dans l'ensemble du secteur et permet aux établissements financiers de participer à des exercices ou simulations afin de tester et d'améliorer continuellement leur stratégie de sécurité.

S'il est essentiel d'examiner chaque élément de la relation bancaire et chaque transaction, le meilleur élément pour commencer reste le processus d'onboarding.

Standardiser l'onboarding en utilisant les technologies modernes permet aux établissements financiers de filtrer les opérateurs suspects et frauduleux et de fournir une expérience plus fluide aux clients de confiance.

En utilisant une combinaison de technologies, y compris l'intelligence artificielle (IA), l'ARP (automatisation robotisée des processus) et le traitement du langage naturel (TLN), les établissements financiers peuvent intégrer et traiter des documents à la fois structurés et non structurés, minimiser les étapes manuelles et réduire le recours aux demandes répétitives de la part du client. Élaborer un processus d'onboarding du client efficace ne permet pas seulement une détection plus rapide d'une fraude potentielle, cela joue également un rôle essentiel pour développer de nouvelles relations solides et durables avec les clients.

Une stratégie globale fournit également la visibilité nécessaire à la préparation des exigences d'audit et de conformité. Elle améliore l'efficacité, protège la marque et sa réputation et permet d'éviter les sanctions ou les amendes. Elle fournit une meilleure protection contre l'usurpation d'identité et la fraude du point de vue du client. Un nombre réduit d'incidents de sécurité augmente la disponibilité, ce qui permet au client d'accéder plus facilement à ses données financières.

APPROCHE GLOBALE UTILISANT LES TECHNOLOGIES MODERNES

Un établissement financier peut tirer de nombreux bénéfices de la mise en œuvre d'une stratégie globale de prévention des fraudes. Bien entendu, l'avantage le plus important et essentiel est financier — réduire des pertes potentielles majeures qui, selon EY, sont estimées entre $ 1400 milliards et $ 3500 milliards chaque année.

Améliorer la visibilité de l'entreprise et réduire le travail manuel via l'IA, l'APR et le TLN peuvent également permettre aux spécialistes de la sécurité de se concentrer sur la protection et la réduction plutôt que de compiler des données issues de sources multiples et de créer des rapports récapitulatifs.

Repenser le risque dans cette optique nécessite plus qu'un investissement technologique. Comme déjà indiqué, les personnes, les processus et les contenus jouent tous un rôle dans la mise en œuvre réussie d'une approche globale. Au niveau du conseil d'administration, il faut que les opérations financières criminelles soient une priorité, afin d'y allouer suffisamment de ressources humaines et technologiques.

Les hauts responsables ne tarderont pas à être convaincus que cette approche garantit une protection solide contre les attaques les plus difficiles auxquelles les établissements financiers sont confrontés, et qu'améliorer l'expérience client, générer du chiffre d'affaires et réduire le risque de la criminalité financier sont des initiatives complémentaires qui se renforcent mutuellement.

Cheryl Chiodi est responsable du marketing des solutions pour les services financiers chez ABBYY, une entreprise mondiale d'intelligence numérique basée à Milpitas, en Californie.

ABBYY®

Améliorer

Améliorer vos rocessus KYC (Know Your Customer) et les contenus qui les alimentent

En savoir plus abbyy.com/fr/solutions/financial-services