SERVICES FINANCIERS | eBook

Miser sur l'intelligence :

Comment l'IA et le ML aident les banques à garder une longueur d'avance sur les cyber-criminels et les règles de conformité

ABBYY

Sommaire

Où se trouve l’argent

Lorsqu’on a demandé au célèbre voleur de banques américain Willie Sutton pourquoi il cambriolait des banques, il a répondu : « c’est là que se trouve l’argent ».

Aujourd’hui encore, les banques sont l’endroit « où se trouve l’argent », mais les techniques criminelles ont énormément évolué depuis les vols à main armée pour lesquels Sutton était connu. Le crime financier est désormais numérique et les cybercriminels inventent de nouvelles méthodes de fraude et de blanchiment d’argent aussi vite que les banques peuvent mettre en place des contre-mesures. La banque est le premier secteur d’activité en termes de coût annuel des cyber-attaques — plus de 18,3 millions de $ par an et par entreprise.

Les règles KYC (connaissance des clients) et AML (lutte contre le blanchiment d’argent) remontent à la loi sur le secret bancaire de 1970 et ont été renforcées après les attaques terroristes du 11 septembre 2001. Lors des investigations qui ont suivi, le Congrès américain a rapidement découvert que ces attentats avaient été financés grâce à la cybercriminalité et au blanchiment d’argent.

EN AVRIL 2020, UN GROUPE DE CYBERCRIMINELS CONNU SOUS LE NOM DE « GROUPE DES BANQUIERS FLORENTINS » A LANCÉ DES ATTAQUES CONTRE LES PLUS GRANDES FIRMES FINANCIÈRES ISRAÉLIENNES ET BRITANNIQUES, DÉROBANT

1,3 MILLION DE $

EN SEULEMENT 4 TRANSACTIONS.

Source

Pour la première fois, la cybercriminalité a été officiellement qualifiée de terrorisme et elle a bénéficié d'une attention particulière dans la formulation des mesures anti-terroristes, y compris la lutte contre le financement du terrorisme (CFT).

Être en conformité avec ces règles peut être efficace pour prévenir la fraude et le vol, mais les banques doivent rester vigilantes et prendre des mesures supplémentaires pour garder le rythme face aux méthodes des cybercriminels qui évoluent rapidement. Les règles KYC et AML prévoient également de lourdes amendes en cas de violation et sont ainsi sources de risques de marché et de réputation. Les enjeux sont donc importants en cas d'échec à mettre en œuvre des dispositifs adaptés. Depuis décembre 2019, l'ensemble des sanctions pour non-respect des règles KYC/AML dans le monde s'élève à 36 milliards de $.

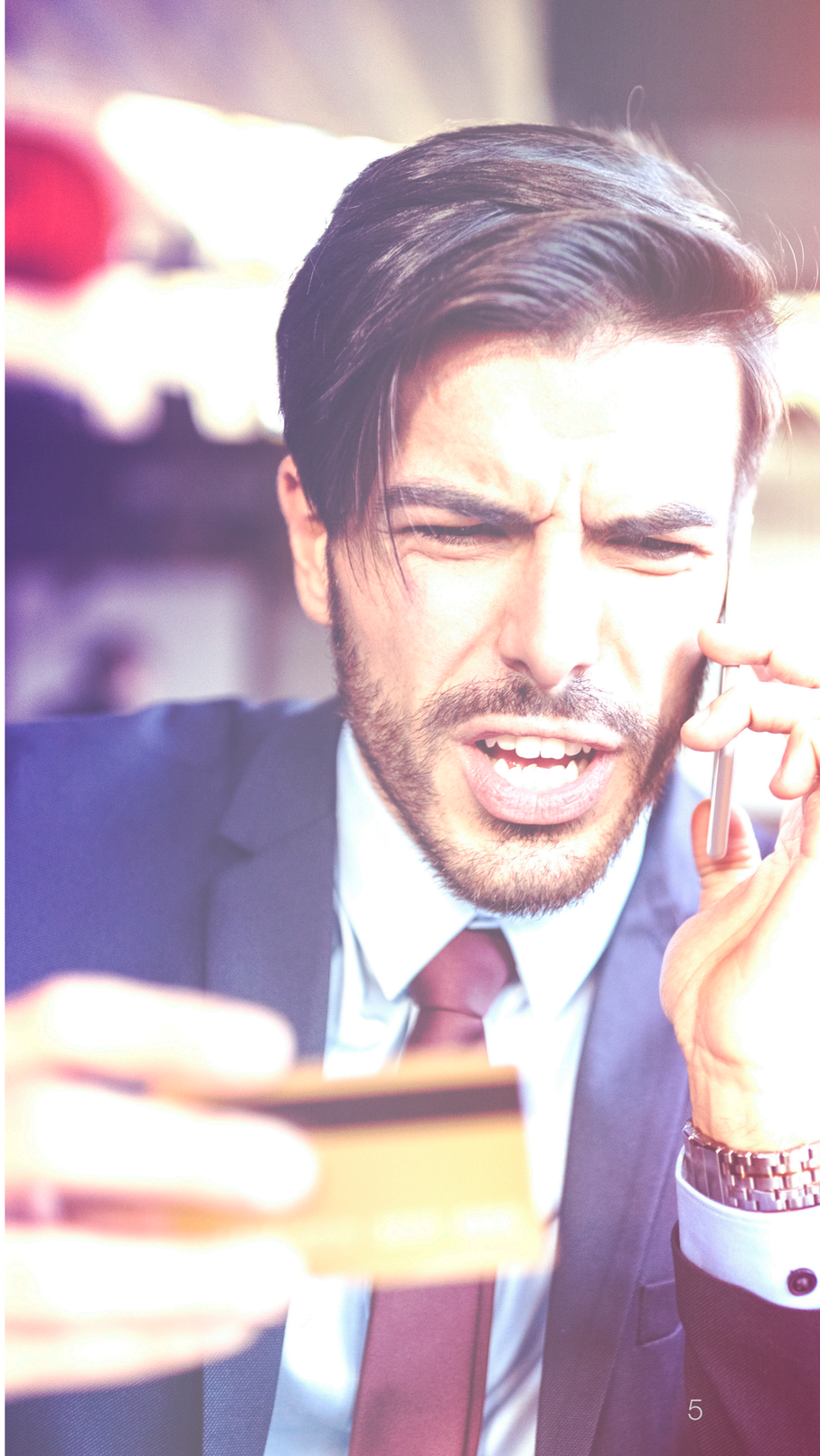
Prévenir les crimes sophistiqués requiert des mesures sophistiquées. Heureusement, aujourd'hui les technologies fonctionnant grâce à l'intelligence artificielle peuvent permettre aux banques d'avoir la visibilité dont elles ont besoin sur leurs processus et leurs contenus afin de s'aligner aux règles KYC/AML/CFT et d'être flexibles pour s'adapter à mesure que les conditions évoluent.

Les crimes financiers ont évolué

Poussées par une compétition croissante et des attentes en constante évolution de la part des clients, les institutions financières comptent de plus en plus sur l'automatisation, les technologies mobiles et les interactions sans contact, en particulier depuis la survenue de la pandémie de COVID-19. Bien que ces mesures offrent des atouts significatifs en termes de productivité et de satisfaction client, elles peuvent également créer de nouvelles failles dans lesquelles les cybercriminels peuvent s'engouffrer — et ils le font.

La COVID-19 impacte également la capacité à mettre en œuvre les obligations de lutte contre le blanchiment et le financement terroriste (AML/CFT), qu'il s'agisse de la supervision, de la réglementation, de réforme politique ou encore du traçage des transactions suspectes et de la coopération internationale.

L'augmentation des transactions à distance offre un terrain fertile aux personnes malveillantes qui ciblent les populations peut-être peu familières avec les plateformes en ligne et qui exploitent les mesures de relance.



Des collectes pour de fausses ONG, des arnaques avec investissements frauduleux, de l'hameçonnage en essor et des attaques avec des logiciels malveillants ont fait augmenter le nombre de transactions en cash. Lorsque le marché se sera stabilisé, de nombreux mouvements pour redéposer des fonds pourraient servir de couverture et permettre de blanchir des fonds illicites. La COVID-19 a également créé une pause dans de nouvelles initiatives législatives et de nouvelles politiques AML/CFT.

Aujourd'hui, les auteurs de crimes financiers ont trouvé comment tirer le meilleur parti des systèmes et des processus propres à l'institution ciblée ; ils leur servent de mécanismes pour blanchir et voler de l'argent, comme

1. **La virtualisation :** les failles des systèmes et applications peuvent être exploitées pour permettre un accès non autorisé aux données d'un compte.
2. **Automatisation des processus :** les criminels peuvent trouver des lacunes dans les processus automatisés alors qu'elles peuvent échapper aux contrôles automatisés.
3. **Identification des clients :** les éléments utilisés pour identifier les clients peuvent être volés pour procéder à des vols d'identité.
4. **Onboarding des clients :** les auteurs de cyber-crimes peuvent créer des comptes artificiels en utilisant de fausses identités de clients.

ON ESTIME QUE CHAQUE ANNÉE DANS LE MONDE SONT BLANCHIS ENTRE

800 MILLIARDS ET 2 BILLIONS DE DOLLARS, SOIT ENVIRON 2 À 5% DU PIB MONDIAL.

Source

UNE FOIS QUE LES COÛTS ASSOCIÉS SONT PRIS EN COMPTE, LES INSTITUTIONS FINANCIÈRES

PERDENT TROIS DOLLARS POUR CHAQUE DOLLAR PERDU À CAUSE DE LA FRAUDE.

Source

Comment les institutions financières peuvent-elles contrer ce flot constant d'attaques ? Une surveillance manuelle peut aider mais est immanquablement limitée par

- L'incapacité des salariés humains à garder le rythme face au volume et à la rapidité des transactions 24h/24 et 7j/7, associée à des contrôles inadéquats du monitoring et du reporting des transactions
- Le risque accru d'erreurs humaines
- La difficulté pour les salariés à rester informés des techniques criminelles les plus récentes
- Le risque pour les salariés de s'engager eux-mêmes dans le crime financier

L’angle de la conformité : répondre aux exigences KYC et AML

Pour être en phase avec les réglementations KYC et AML, les institutions financières doivent prouver qu’elles ont mis des procédures en place pour détecter et agir contre les activités criminelles, y compris la vérification de l’identité des clients et de l’authenticité des transactions.

Bien que de nombreuses banques disposent de processus de vérification et de systèmes d’enregistrement pour leurs données structurées, la grande quantité de données clients contenue dans les documents les expose à une grande vulnérabilité. Il leur manque ce qui pourrait faire le lien entre les architectures des données et les documents dans lesquels on trouve une grande quantité de comportements liés aux clients et aux transactions — et d’informations sur ces comportements.

Un exemple dans lequel les données tirées d'un document peuvent mener à des problèmes conformité est l'exigence de suivre la chaîne de responsabilité. La chaîne de responsabilité fait référence à la pratique qui consiste à suivre le cycle de vie des données, du moment où elles entrent dans l'organisation jusqu'au jour où elles sont détruites ou stockées. Un dossier conforme de chaîne de responsabilité permet de répondre à des questions telles que : d'où viennent les données dans l'organisation, où vont-elles, qui y a eu accès et – le cas échéant – quelles modifications elles ont subi.

Les documents sont des éléments essentiels de l'entreprise et doivent conserver leur intégrité tout au long de la chaîne de responsabilité. Si des modifications sont apportées, elles doivent être notées. Concernant les documents, suivre la chaîne de responsabilité peut être problématique pour trois raisons d'égale importance :

- Compréhension incomplète des documents eux-mêmes
- Compréhension incomplète des processus que suivent les documents
- Manque de visibilité sur les personnes ayant interagi avec les documents

Exemple : onboarding client

Si un client présente son permis de conduire dans le cadre du processus d'onboarding, le dossier de la chaîne des responsabilités doit inclure où et quand ce document a été scanné, comment les données ont été extraites et vérifiées, ce qu'il est advenu de l'image scannée après l'onboarding, et comment les données extraites peuvent permettre de remonter jusqu'au document. Tout manquement dans cette chaîne pourrait se traduire non seulement par une violation des règles KYC, mais aussi par des faiblesses pouvant être exploitées par les cybercriminels. L'onboarding client — lorsque la banque détermine d'abord l'identité du client via des documents—est la première étape essentielle pour bien s'engager dans la conformité KYC.

RIEN QU'EN 2017, LES BANQUES ONT DÉPENSÉ ENVIRON

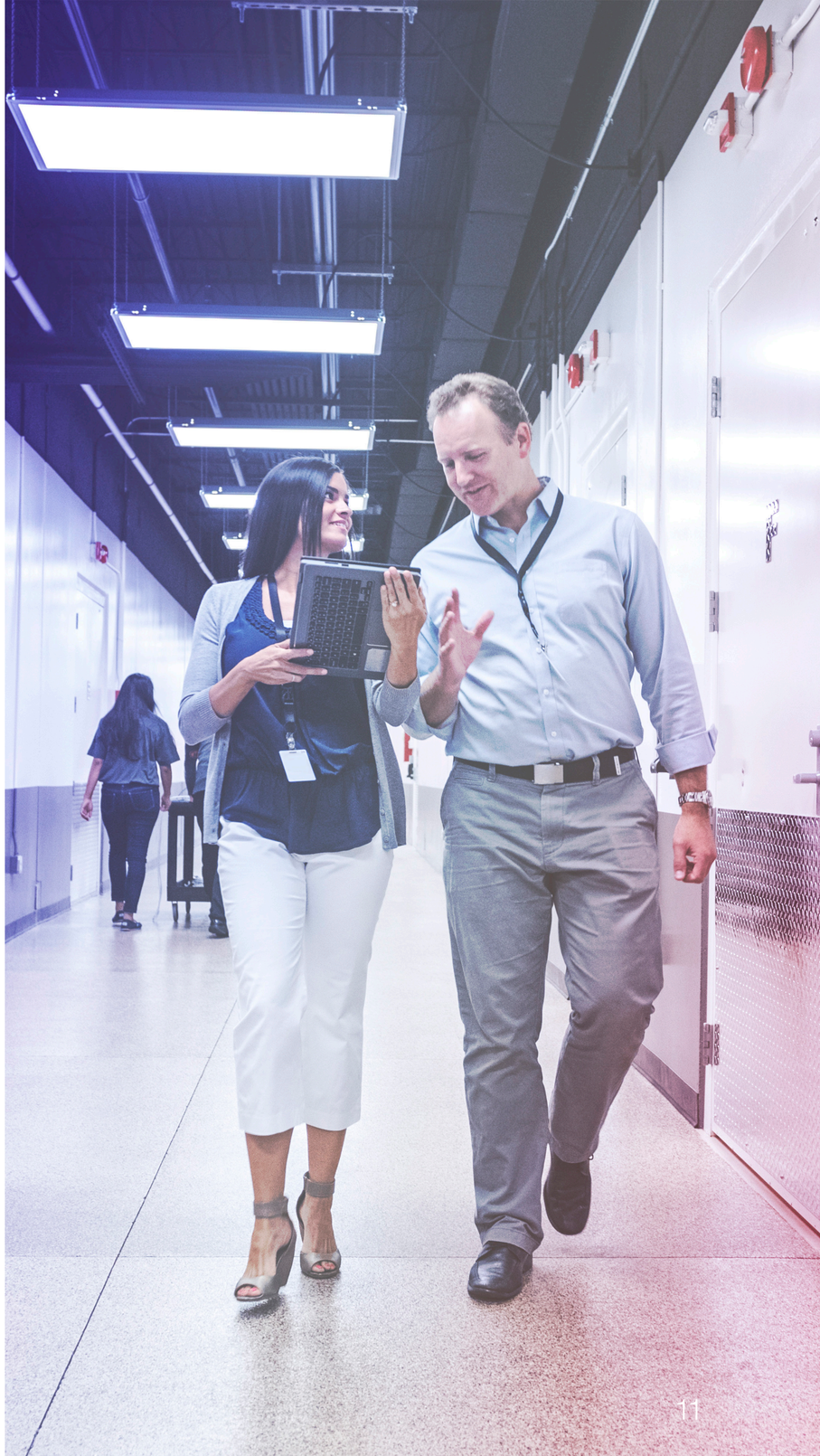
8,2 MILLIARDS DE DOLLARS

EN CONTRÔLES CONTRE LE BLANCHIMENT D'ARGENT (AML).

Source

Rester en tête avec la Digital Intelligence

Pour répondre au double problème de conformité avec les règles KYC/AML/CFT et de prévention des activités criminelles qui pourraient déroger aux exigences réglementaires, les institutions financières ont besoin d'un plan de bataille multi-fronts s'adressant aux personnes, aux processus et aux documents. Premièrement, elles doivent avoir les moyens d'examiner à la loupe les documents pour détecter les tentatives de fraude. Deuxièmement, elles ont besoin d'avoir la visibilité de leurs processus pour pouvoir contrôler en permanence les irrégularités qui pourraient indiquer des comportements frauduleux. Troisièmement, elles ont besoin d'informations sur la façon dont les gens interagissent avec leurs processus et documents, laquelle pourrait indiquer des comportements frauduleux. Cette approche dotera les banques de l'arme de la Digital Intelligence, nécessaire pour protéger leurs institutions tant des fraudes que des violations réglementaires.



La Digital Intelligence est une nouvelle approche de l'utilisation des toutes dernières technologies d'intelligence artificielle (IA) et de machine learning (ML). Elle fournit des capacités clés donnant aux banques confiance dans la chaîne de responsabilité des documents :

- Validation des documents client d'onboarding — tant structurés que non structurés — et de leur contenu au point d'entrée
- Extraction intelligente du contenu de ces documents, lequel peut être validé et/ou signalé comme suspect
- Découverte des processus qui révèle les schémas de comportement suspect entre les personnes et les documents, ainsi que les failles dans les processus pouvant ouvrir la voie à des attaques

Lorsqu'elle est utilisée pour prévenir les fraudes, la Digital Intelligence donne aux institutions financières les outils dont elles ont besoin pour répondre aux exigences de conformité et garder une longueur d'avance sur les criminels, tout en évitant les écueils d'une approche manuelle qui ne peut tenir le rythme, ni avoir assez d'ampleur pour répondre à ce défi.

Intégrité des documents

Bien que le secteur financier progresse vers sa transformation numérique, la plupart des données client d'une banque se trouve dans les documents : formulaires d'identification, preuves du niveau de formation, demandes de prêts, déclarations de revenus, etc., etc.. Si les institutions financières veulent prévenir les fraudes et répondre à leurs obligations de conformité, elles doivent disposer d'un moyen fiable d'examiner chaque document client pour repérer les irrégularités qui pourraient trahir une intention criminelle. Elles doivent aussi fournir un lien direct entre leurs systèmes d'enregistrement pour la conformité KYC/AML et les interactions clients, depuis l'onboarding et tout au long du parcours client.

L'intégrité des documents joue un rôle essentiel dans le contrôle de la chaîne de responsabilité et la documentation qui est cruciale pour la conformité KYC/AML (voir « L'angle de la conformité »).

En validant les documents et leur contenu lors du processus d'onboarding, les banques peuvent suivre les données des clients depuis leur point d'entrée dans l'organisation (onboarding client) et tout au long de leur cycle de vie, jusqu'au off-boarding. Si un agent de conformité demande les documents qui étayent la chaîne de responsabilité, l'institution financière peut en rendre compte à chaque point de contact.

Intégrité des processus

Dès qu'une donnée sur un client entre dans une institution financière, que ce soit par des documents ou des sources numériques, elle vient alimenter un certain nombre de processus, y compris l'onboarding client, la vérification de la conformité, l'approbation des prêts et bien plus. Bien que la plupart des banques aient sans doute une bonne idée de la façon dont ces processus devraient être exécutés, l'écart entre la théorie et la pratique peut être plus grand qu'elles ne l'imaginent — et cet écart pourrait présenter des opportunités de fraude ou de vol des données. Process

La découverte des processus (Process discovery) utilise des données tirées de sources numériques et physiques pour donner aux banques de la visibilité sur la façon dont leurs processus sont réellement exécutés, du début à la fin. En rassemblant et en analysant les données d'horodatage générées par les systèmes d'information, la Process Intelligence utilise des algorithmes de pointe pour créer un « jumeau numérique » des opérations et processus métier. Ces modèles visuels donnent des informations détaillées sur la façon dont les processus sont vraiment exécutés chaque jour — tant en suivant la voie « standard » ou « idéale » que pour toutes les variations.

Dans l'effort visant à prévenir la fraude et le blanchiment d'argent, le contrôle des processus (process monitoring) peut déceler des irrégularités dans le traitement des données qui pourraient être exploitées par les cybercriminels. Il peut aussi contrôler les processus 24h/24 et 7j/7 pour déceler les potentielles failles de sécurité et pour alerter automatiquement les détenteurs des processus afin qu'ils interviennent immédiatement.

Comme évoqué ci-dessus, suivre la chaîne de responsabilité, avec ses documents et ses données, est une composante essentielle de la conformité KYC/AML. En cartographiant automatiquement l'exécution des processus, les banques peuvent suivre le cycle de vie des données sur les clients et les transactions à mesure qu'elles progressent tout au long des processus et entre les processus, avec les documents essentiels et, si nécessaire, elles peuvent fournir une documentation fiable pour la chaîne de responsabilité.

Apprentissage continu

La conformité et la prévention des fraudes sont en constante évolution car de nouvelles réglementations émergent et les criminels inventent de nouvelles approches pour se livrer à la fraude. Les solutions de Digital Intelligence sont très adaptables : elles évoluent à mesure que les conditions, les règles de conformité et les consignes changent et évoluent. La technologie de ML est utilisée pour permettre à ces solutions d'apprendre de chaque itération et de s'adapter en conséquence.

Voir plus loin

Alors que les banques et autres institutions financières progressent vers la transformation numérique, ce progrès peut parfois avoir des « effets secondaires » menant à des résultats tout sauf favorables. Les cybercriminels d'aujourd'hui ont compris comment utiliser la propre infrastructure numérique d'une organisation pour se livrer à la fraude et au vol des données. Garder une longueur d'avance sur eux nécessite d'utiliser tous les outils disponibles.

Les solutions alimentées par l'IA peuvent automatiquement passer en revue et contrôler des centaines de processus et des milliers de documents, avec rapidité et précision, pour signaler les signes d'une possible activité criminelle. L'IA ne remplacera pas les experts de la conformité et de la prévention des fraudes, mais elle peut au contraire constituer un atout changeant la donne qui libère les salariés des tâches de routine et leur permet de se concentrer sur des problèmes plus complexes. Associer expertise humaine et force de travail numérique aide les institutions financières à se mettre à l'échelle et à s'adapter rapidement pour avoir un avantage unique dans la bataille contre le crime financier. Cela permet aux banques d'être en conformité avec les règles KYC/AML tout en renforçant leurs propres défenses contre le cyber-crime — aujourd'hui, demain et pour les années à venir.

ABBYY

Pour de plus amples informations, rendez-vous sur :
www.abbyy.com/fr/solutions/financial-services

Contactez nos bureaux dans le monde entier :
www.abbyy.com/fr/contacts

© ABBYY 2021 ABBYY est une marque déposée d'ABBYY Software Ltd. Tous les autres noms de produits et de marques mentionnés ici sont la propriété de leurs détenteurs respectifs. #12505