GESTION DES RISQUES SUR LES CANAUX NUMÉRIQUES DESTINÉS AUX CONSOMMATEURS

RSA FRAUD AND RISK INTELLIGENCE SUITE

PRÉSENTATION

Le monde de la consommation connaît un tournant historique. Les individus interagissent et effectuent des transactions à un rythme jamais vu jusqu'à présent. Les organisations passent par des transformations numériques et exposent de plus en plus de canaux numériques à leurs consommateurs, afin de répondre à leur besoin en matière de facilité d'utilisation. Par conséquent, ces dernières doivent faire face à des risques pour la sécurité et leur activité sans précédent, allant de la pression législative et de la concurrence de nouveaux arrivants, à l'augmentation des failles de sécurité potentielles pouvant être exploitées par les fraudeurs et les cybercriminels.

Ces changements dans l'univers du consommateur affectent différents types d'organisations, des services de santé aux organismes d'assurance, en passant par les commerçants, et plus particulièrement les institutions financières qui sont confrontées à des bouleversements considérables, comme par exemple :

- **Les attentes des clients en matière de facilité d'utilisation et de réactivité augmentent** : les clients s'attendent à pouvoir accéder aux informations à partir de n'importe quel appareil, à tout moment, et à effectuer des transactions numériques de manière instantanée, fluide, personnalisée, indépendante du canal et sécurisée.
- **L'innovation dans l'industrie de la technologie financière, la fintech,** crée une nouvelle concurrence offrant des services numériques, ce qui force les organisations à repenser leur stratégie et à créer de nouveaux partenariats soutenus par l'économie de l'API, mais introduit également des risques liés aux tiers qui doivent être gérés.
- **Les réglementations internationales drastiques**, telles que la directive **PSD2, le règlement RGPD, l'espace SEPA** et le **FFIEC**, imposent une plus grande responsabilité vis-à-vis de la protection, de la sécurité et de la confidentialité des données des consommateurs.

RSA FRAUD AND RISK INTELLIGENCE SUITE

- ***Inspirer la confiance*** *sans désagrément*
- ***Réduire la fraude*** *et non les clients ou le chiffre d'affaires*
- ***Mettre au jour le risque*** *lié à chaque échange numérique*
- ***Optimiser les connaissances*** *avec l'intelligence collective*
- ***Améliorer l'efficacité*** *des opérations liées à la fraude*
- ***Devancer la cybercriminalité***

- **Les innovations en matière de paiement**, telles que la technologie **EMV 3-D Secure (qui devrait générer davantage de trafic marchand à travers l'écosystème 3DS)**, « **les paiements plus rapides** » (sous toutes leurs formes à travers le monde), les applications de paiement participatif et d'autres applications de fintech déclenchent une croissance considérable du volume des paiements numériques. Ainsi, la valeur totale des fonds transférés via les canaux numériques augmente, exposant ainsi les organisations à des pertes potentielles dues aux fraudes plus importantes.
- L'Internet of Things (**IoT** ou Internet des objets), qui permet à différents appareils d'effectuer différentes actions à la place du consommateur (par exemple, l'assistant personnel virtuel *Alexa*) fait, par conséquent, pratiquement disparaître l'identité du détenteur du compte. Les organisations doivent donc être en mesure de différencier une interaction numérique authentique d'une interaction frauduleuse.
- Les points de compromis et failles de sécurité potentiels continuent de se développer au fur et à mesure que les organisations mettent en place leurs **stratégies omnicanales**. Bien que chaque nouveau canal offre une plus grande efficacité et un accès simplifié aux données financières, il crée également des failles de sécurité potentielles.
- **La croissance spectaculaire des activités numériques et des volumes de transactions** n'est compensée que par une croissance minime, voire nulle, des ressources organisationnelles pour limiter et enquêter sur les fraudes. Les équipes en charge de la gestion de la fraude peuvent ressentir un **épuisement face aux incidents**, leur nombre devenant trop important pour que l'équipe d'analystes déjà submergée puisse y remédier. Cette situation peut s'avérer dangereuse, car les analystes peinent à hiérarchiser les incidents et à les traiter selon leur sévérité. Ce manque de visibilité pour identifier efficacement les activités frauduleuses et ainsi les éviter, peut se traduire par des fraudes non détectées, même une fois les pertes déjà subies. Les pertes peuvent être considérables et les équipes en charge de la sécurité peuvent ne pas avoir de réponse à apporter aux dirigeants d'entreprise quant à la nature des attaques, l'exposition de l'organisation à ces attaques et l'impact global sur l'activité.

Cette croissance des interactions numériques des consommateurs avec l'organisation permet de développer son chiffre d'affaires, mais elle accroît également les points de compromis et les failles de sécurité potentiels. L'incapacité à identifier les tentatives de fraude numérique en temps réel, en fait, l'impossibilité de faire la distinction entre les utilisateurs de site légitimes et les cybercriminels peut avoir des conséquences dramatiques sur les organisations d'aujourd'hui. Par conséquent, une planification appropriée est nécessaire. La fraude en ligne réduit le chiffre d'affaires de milliards de dollars par an en pertes financières directes et indirectes, notamment les atteintes aux marques, qui influent sur la capacité d'une organisation à attirer et fidéliser les clients. Les fraudeurs tentent de plus en plus d'ouvrir des comptes non autorisés et de s'approprier les comptes existants.

Par conséquent, les organisations ont besoin de pouvoir identifier les fraudes en temps réel et de disposer des instruments nécessaires pour les arrêter en temps réel. Elles ont besoin d'une vue complète, à tout moment, sur les agissements des utilisateurs au sein de leurs canaux numériques, de façon à ce que le comportement malveillant des utilisateurs, comme la prise de contrôle de compte et le transfert d'argent frauduleux, puisse être mis au jour. Cependant, elles doivent également être capables de répondre aux incidents liés à la fraude conformément à leur tolérance aux risques, leurs ressources et leurs priorités stratégiques.

Bien que la plupart des organisations utilisent plus d'une demi-douzaine d'outils indépendants de lutte contre la fraude, chacun d'entre eux résolvant un problème spécifique, nombreuses sont celles qui n'ont pas la possibilité de relier ces outils entre eux. La nécessité de relier les données issues des différents outils de lutte contre la fraude, dans le but d'améliorer les taux globaux de détection de fraude sur l'ensemble des canaux et de centraliser la gestion des incidents, ne fera qu'augmenter à mesure que les organisations exécutent leurs stratégies omnicanales.

Au cours des années passées, la fraude était principalement considérée comme un problème technologique et les actions de prévention de la fraude étaient perçues comme un centre de coûts, mais cette époque est révolue. Les organisations voient désormais les actions de lutte contre la fraude à travers le prisme des résultats pour l'entreprise et privilégient la sécurité des éléments les plus importants pour elles. Cela comprend la protection du flux de chiffre d'affaires issu des ventes et la fourniture d'une expérience numérique sécurisée et fluide aux consommateurs.

STRATÉGIE DE GESTION DE LA FRAUDE OMNICANALE ORIENTÉE MÉTIER

Les outils de lutte contre la fraude existants sont incapables de protéger les organisations de manière adéquate contre les assauts de nouvelles menaces de fraude en constante évolution. Le temps est venu d'adopter une nouvelle approche qui tire parti de la force du partenariat entre des chefs de file techniques et commerciaux.

La gestion de la fraude omnicanale orientée métier fournit un modèle structuré en couches pour la protection de l'accès et des transactions des consommateurs sur les canaux numériques, tout en permettant aux organisations d'établir un équilibre entre le chiffre d'affaires, le risque, les coûts et la facilité d'utilisation pour les consommateurs.

Le cœur d'une stratégie de gestion de la fraude omnicanale orientée métier consiste en une traduction fidèle du résultat souhaité pour l'entreprise. Les équipes en charge de la fraude et de la sécurité doivent comprendre les objectifs métier et chaque décision doit concorder avec le résultat souhaité pour l'entreprise.

Schéma 1 : solution de prévention de la fraude omnicanale

L'établissement d'indicateurs clés de performance simples, tels que les objectifs de chiffre d'affaires, les taux d'abandon des transactions, l'intervention du client, les taux de détection de fraude ou la prévention des pertes dues aux fraudes

est une excellente base. Lorsque ces indicateurs sont établis par la direction des entreprises, les équipes de gestion de la fraude sont alors en mesure de concevoir et d'exécuter une stratégie de gestion de la fraude orientée métier, en suivant les principes ci-dessous :

- **Trouver le juste équilibre entre l'expérience consommateur sur les canaux numériques et le risque de pertes dues aux fraudes.** Aujourd'hui, les utilisateurs exigent un accès rapide et facile aux comptes, aux produits et aux services sur leurs canaux numériques et ne souhaitent pas subir d'interruption pendant leur expérience. Toute stratégie réussie de gestion de la fraude orientée métier doit conserver un équilibre entre les exigences d'une organisation en matière de sécurité et la nécessité d'un accès pratique pour les utilisateurs et d'une expérience utilisateur fluide.
- **Choisir des méthodes d'authentification de l'utilisateur appropriées.** Cela peut également s'avérer essentiel, car aucun modèle d'authentification n'est adapté à tous les cas. Les organisations doivent proposer plusieurs méthodes d'authentification pratiques d'utilisation dans différents canaux numériques. Elles devraient rechercher des méthodes rigoureuses, présentant peu de faux positifs et de faux négatifs, car cela a un impact direct sur l'expérience du consommateur d'une part, et sur les taux de prévention des fraudes d'autre part. La clé de la satisfaction des clients réside dans la fourniture d'une expérience fluide à une majorité d'utilisateurs finaux de l'organisation. Comme les consommateurs s'attendent à pouvoir interagir numériquement avec l'organisation à tout moment, depuis n'importe quel appareil, et de manière sécurisée et pratique, le fait de ne pas répondre à ces attentes peut entraîner une augmentation du taux d'abandon des transactions ou la perte de clients au profit des concurrents, ce qui se traduit par une baisse du chiffre d'affaires de l'organisation.
- **Évaluer précisément les risques associés aux échanges numériques avec les consommateurs.** Il s'agit d'un élément essentiel pour déterminer quel utilisateur peut s'authentifier de manière transparente et à quel utilisateur imposer une authentification supplémentaire. Pour atteindre cet objectif, il est indispensable de disposer d'une solution d'authentification basée sur le risque extrêmement rigoureuse, qui offre des taux de détection de fraude élevés et peu de faux positifs.
- Vérifier qu'elles disposent **d'une visibilité complète sur la manière dont les consommateurs échangent sur l'ensemble de leurs canaux numériques.** Cela s'avère d'autant plus important que les organisations cherchent à ouvrir davantage de canaux numériques à travers lesquels leurs consommateurs peuvent interagir. Les fraudeurs rechercheront le maillon le plus faible et attaqueront les canaux moins sécurisés. Les organisations doivent rechercher des solutions capables de leur fournir une visibilité et des informations sur le comportement des consommateurs au sein de leurs canaux numériques afin de pouvoir différencier correctement un fraudeur d'un utilisateur authentique.
- Comprendre qu'elles ne peuvent pas lutter contre la fraude en étant seules. Pour réussir dans la prévention et la réduction des fraudes, les organisations doivent **collaborer et partager les renseignements relatifs aux activités frauduleuses confirmées** qui permettront d'éviter des attaques frauduleuses présentant des caractéristiques similaires dans d'autres organisations. La puissance d'une communauté combattant la fraude collectivement peut permettre de réduire les pertes dues aux fraudes de manière considérable.

SOLUTIONS RSA DE GESTION DE LA FRAUDE OMNICANALE ORIENTÉES MÉTIER

La suite RSA Fraud and Risk Intelligence Suite est conçue pour les organisations souhaitant aligner leurs actions de prévention de la fraude sur leur tolérance au risque et leurs priorités stratégiques, afin de réduire la fraude, et non leur clientèle. La suite offre une vue complète sur les canaux numériques avec une stratégie centralisée de détection et de réduction de la fraude qui associe de manière unique les décisions basées sur le risque, l'analytique prédictive, un profilage approfondi des entités, une gestion flexible des politiques basée sur des règles et une gestion intelligente de la fraude globale et partagée. Elle offre également la possibilité d'intégrer des informations issues d'autres outils de lutte contre la fraude pour enrichir les évaluations des risques de fraude et mieux protéger les clients contre les attaques ciblées de la cybercriminalité.

La suite met au jour les fraudes qui, sinon, resteraient indétectées, en analysant chaque échange entre les utilisateurs finaux et le canal numérique. En outre, la suite RSA Fraud and Risk Intelligence Suite prend en charge les décisions basées sur le risque lors de points clés durant la session, tels que les connexions et les transactions. Le moteur de risque en auto-apprentissage effectue un profilage approfondi des entités et calcule un score de risque reflétant la probabilité que l'activité soit exécutée par un fraudeur.

La suite RSA Fraud and Risk Intelligence Suite protège chaque étape du parcours numérique du consommateur :

- **RSA FraudAction™** est un service de gestion des menaces externes unique qui offre une solution de démantèlement des attaques et une cyberintelligence. De la détection à la mise hors service rapide, RSA FraudAction 360 offre une couverture complète contre les attaques par phishing, par cheval de Troie, les applications mobiles malveillantes et les pages de médias sociaux malveillantes. Le service de cyberintelligence de FraudAction fournit une bonne visibilité sur le paysage et le fonctionnement de la cybercriminalité se rapportant à vos marques, en tirant profit de sa vaste visibilité sur le dark Web, associée à des recherches approfondies sur les forums des médias sociaux.
- **RSA Adaptive Authentication** est un concentrateur de détection de la fraude omnicanale avancé qui fournit une authentification multifacteur basée sur le risque aux organisations qui cherchent à protéger leurs clients contre la fraude sur les canaux numériques. S'appuyant sur le moteur RSA Risk Engine, la solution RSA Adaptive Authentication est conçue pour mesurer le risque associé aux activités de connexion et postconnexion d'un utilisateur en évaluant divers indicateurs de risque. L'utilisation d'une technologie d'apprentissage automatique puissante, en complément d'options pour des contrôles de politique précis, permet au concentrateur de lutte contre la fraude RSA Adaptive Authentication de ne nécessiter qu'une seule sécurisation supplémentaire, comme l'authentification hors bande, pour les scénarios présentant un risque élevé et/ou une violation des règles établies par une organisation. Cette méthodologie fournit une authentification transparente à la majorité des utilisateurs, ce qui garantit une expérience utilisateur fluide et des taux de détection de fraude élevés.
- **RSA Adaptive Authentication for eCommerce** est la solution EMV 3-D Secure de RSA pour les organismes chargés de l'émission et du traitement des cartes de crédit. En utilisant le protocole et l'infrastructure 3-D Secure, la solution Adaptive Authentication for eCommerce permet aux commerçants et aux émetteurs de cartes de fournir une expérience d'achat en ligne cohérente et sécurisée aux détenteurs de cartes, tout en limitant les risques de pertes dues à des refacturations. Optimisée par le moteur RSA Risk Engine, la solution Adaptive Authentication for eCommerce offre une expérience d'achat fluide en procédant à une identification discrète des détenteurs de cartes conformes, tout en augmentant la sécurité pour la minorité d'utilisateurs finaux à haut risque uniquement. Sa capacité à augmenter le niveau de sécurité et à éliminer la fraude de manière précise, tout en offrant une expérience d'achat fluide aux clients conformes, est inégalée dans le secteur.

UNE PRÉVENTION ÉPROUVÉE DE LA FRAUDE AU CONSOMMATEUR

- ***Plus de 2 milliards*** *de consommateurs protégés*
- ***Plus de 4 milliards de dollars*** *de pertes dues aux fraudes évitées par an*
- ***Plus de 1 million*** *de mises hors service de cyberattaques*
- *Un taux de* ***détection de fraude de plus de 95 %*** *avec un taux d'****intervention de 3 à 5 %*** *seulement*

Des milliers *de clients directs et indirects* ***contribuant*** *quotidiennement à* ***RSA eFraudNetwork*** *: une communauté qui combat la fraude collectivement*

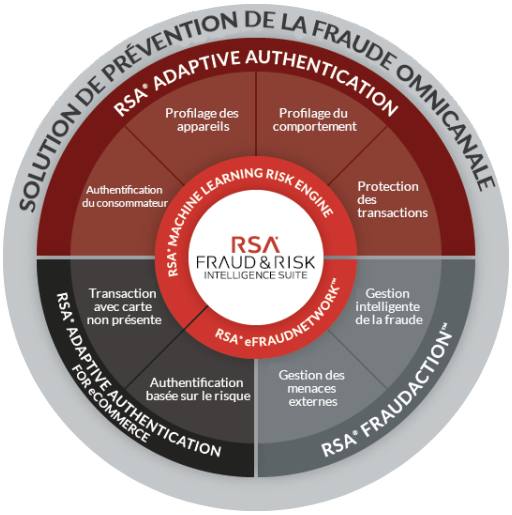

Schéma 2 : RSA Fraud and Risk Intelligence Suite - Sécurisation du cycle de vie numérique des consommateurs

La suite RSA Fraud and Risk Intelligence Suite intègre des fonctionnalités cloisonnées et des sources de données afin de fournir une vision globale des activités et comportements individuels des utilisateurs. Cette pollinisation entre les produits permet une détection des fraudes plus précise et la possibilité d'élaborer une stratégie antifraude hautement granulaire et personnalisée, conformément à la tolérance aux risques et aux priorités stratégiques de votre organisation.

Il existe de nombreux points d'intégration entre les solutions dans la suite RSA Fraud and Risk Intelligence Suite, notamment :

- **RSA eFraudNetwork™** : le premier et le plus grand référentiel d'éléments confirmés de données liées à la fraude partagés au sein de la communauté des clients RSA Fraud and Risk Intelligence. L'utilisation des données partagées par le service eFraudNetwork permet aux clients de rapidement découvrir de nouveaux types d'activités frauduleuses et de prévenir les fraudes dans leur environnement, en se basant sur des fraudes confirmées partagées par leurs pairs.
- **L'approche de l'écosystème RSA Adaptive Authentication** est conçue pour améliorer la détection des fraudes à l'aide d'éléments de données provenant de différentes sources. En utilisant des éléments tiers pour influencer l'évaluation des risques et affecter le score de risque, les clients peuvent apporter des informations supplémentaires issues de la business intelligence interne et d'autres outils de lutte contre la fraude. Actuellement, plus de 50 % des organisations exploitent entre 4 et 10 outils de lutte contre la fraude différents dans leurs opérations de prévention de la fraude. L'utilisation de l'approche de l'écosystème Adaptive Authentication peut aider les organisations à tirer profit de leur investissement existant dans différents outils de lutte contre la fraude, tout en centralisant l'évaluation des risques et la gestion des incidents dans l'écosystème Adaptive Authentication, afin de réduire les coûts d'exploitation et d'accroître la détection de fraude.

Le fait de mettre à profit les solutions intégrées RSA Fraud and Risk Intelligence peut apporter une meilleure visibilité sur les canaux numériques de votre organisation et l'aider à détecter et à limiter la fraude, plus rapidement et plus efficacement.

La suite RSA Fraud and Risk Intelligence Suite fournit des fonctionnalités complètes de détection et de réduction des fraudes omnicanales. Ainsi, les organisations peuvent prospérer et s'adapter en permanence au changement transformationnel et à la demande croissante des consommateurs pour plus de facilité d'utilisation, tout en réduisant les pertes dues aux fraudes et les coûts d'exploitation.

Avec une approche orientée métier en matière de prévention de la fraude, les chefs de file de la lutte contre la fraude sont mieux outillés pour débattre de l'impact commercial actuel des risques de fraude et se préparer pour l'avenir, en collaborant davantage avec les dirigeants d'entreprise afin de s'assurer qu'ils protègent ce qui compte le plus pour leur organisation : arrêter la fraude, pas leurs clients.

LES RISQUES NUMÉRIQUES SONT L'AFFAIRE DE TOUS
VOUS AIDER À LES GÉRER, C'EST NOTRE AFFAIRE

RSA offre aux organisations des produits et services de sécurité orientés métier qui leur fournissent une approche unifiée de la gestion du risque numérique reposant sur une visibilité intégrée, des informations automatisées et des actions coordonnées. RSA peut vous aider à détecter et à traiter efficacement les attaques avancées, à gérer le contrôle d'accès des utilisateurs et à réduire les risques métiers, la fraude et la cybercriminalité. RSA protège des millions d'utilisateurs dans le monde entier et aide plus de 90 % des sociétés du classement Fortune 500 à prospérer et à s'adapter en permanence au changement transformationnel.

Découvrez comment prospérer dans un monde numérique et dynamique où les risques sont élevés sur rsa.com/fr-fr