RSA® ADAPTIVE AUTHENTICATION FOR ECOMMERCE

PROTOCOLE 3-D SECURE BASÉ SUR LE RISQUE POUR LES ÉMETTEURS DE CARTES DE CRÉDIT

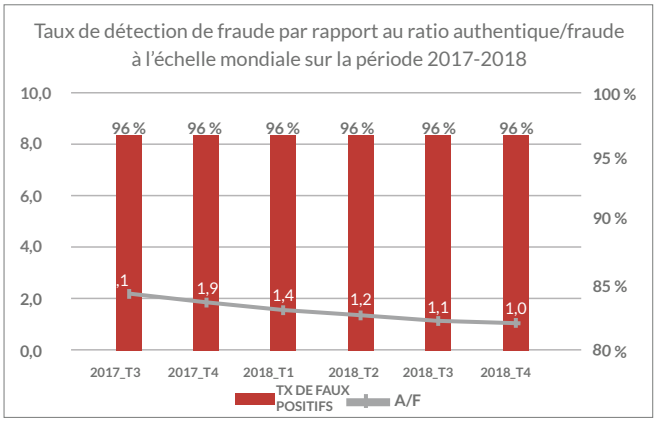
3-D Secure est un protocole antifraude adopté par MasterCard, American Express, Visa et JCB International, qui offre une couche de protection supplémentaire pour les paiements en ligne. Avec le protocole 3-D Secure, lorsqu'un détenteur de carte enregistré utilise une carte de crédit inscrite chez un commerçant participant, ce détenteur doit être authentifié avant que la transaction ne puisse être traitée. Dans un environnement 3-D Secure traditionnel, l'authentification est basée sur un mot de passe créé par les détenteurs de cartes lorsqu'ils inscrivent leur carte de crédit, et chaque transaction fait l'objet d'une vérification.

Le taux de vérification de 100 % du 3-D Secure traditionnel a un impact négatif sur les émetteurs, les commerçants et les détenteurs de cartes. Toute activité qui interrompt le déroulement d'un achat augmente la probabilité d'abandon du panier d'achats, ce qui réduit le chiffre d'affaires des émetteurs et des commerçants. L'expérience négative vécue par les détenteurs de cartes lorsqu'ils oublient leur mot de passe augmente également la probabilité d'abandon et réduit l'utilisation de cette carte particulière, ce qui affecte encore davantage le chiffre d'affaires de l'émetteur.

Le protocole 3-D Secure basé sur le risque offre un taux élevé de détection des fraudes par le biais d'une authentification forte, tout en supprimant la mauvaise expérience du détenteur de carte qui a un impact négatif sur le chiffre d'affaires de l'émetteur. Avec le protocole 3-D Secure basé sur le risque, les émetteurs de cartes de crédit peuvent minimiser la fraude tout en protégeant leur chiffre d'affaires.

UNE DÉTECTION DE FRAUDE ÉLEVÉE, UN NOMBRE D'INTERVENTIONS LIMITÉ

La solution Adaptive Authentication for eCommerce est le serveur de contrôle d'accès 3-D Secure de RSA pour les organismes chargés de l'émission et du traitement des cartes de crédit. Le moteur RSA Risk Engine est au cœur de la solution, il permet à cette dernière d'authentifier les détenteurs de cartes de manière transparente et de renforcer la sécurité uniquement pour les clients à haut risque (moyenne globale d'environ 5 % des transactions). Le haut niveau de précision du moteur de risque engendre un taux de détection de fraude très élevé, tout en maintenant un taux de faux positifs très faible.



Le graphique ci-dessus montre un taux de détection de fraude moyen de 96 % pour la solution RSA Adaptive Authentication for eCommerce et des ratios transaction authentique/fraude très bas (par exemple, le nombre de transactions authentiques faisant l'objet d'une vérification renforcée pour chaque transaction frauduleuse confirmée). RSA Adaptive Authentication for eCommerce permet de réduire considérablement les pertes dues aux fraudes tout en renforçant la sécurité auprès d'un très faible nombre de clients légitimes. Cela améliore, d'une part, l'expérience des détenteurs de cartes et la protection du chiffre d'affaires des émetteurs, et, d'autre part, cela permet de réduire les coûts d'exploitation associés à la vérification des transactions et à la gestion des demandes issues des clients authentiques.

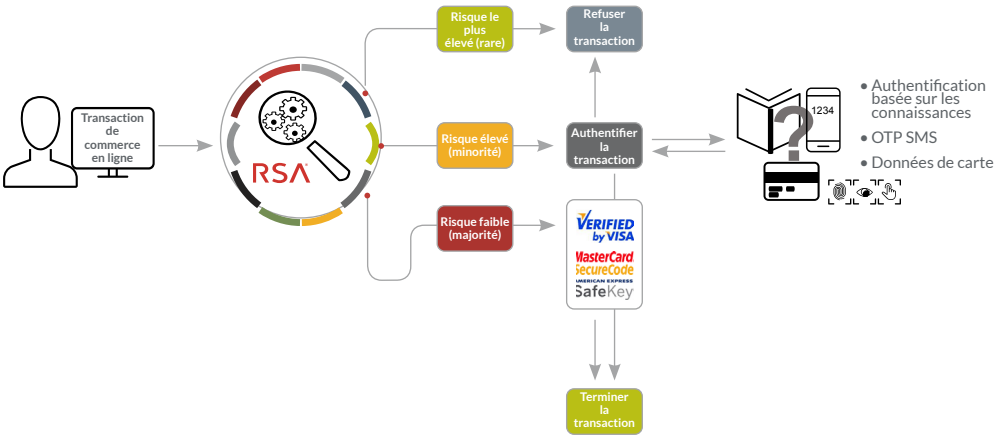
UNE AUTHENTIFICATION TRANSPARENTE POUR OPTIMISER L'EXPÉRIENCE DU DÉTENTEUR DE CARTE

En utilisant le protocole et l'infrastructure 3-D Secure, RSA 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 le risque de pertes dues à des refacturations.

RSA Adaptive Authentication for eCommerce permet aux banques émettrices de proposer la prise en charge des services Verified by Visa® (VbV), Mastercard SecureCode® et Identity Check®, ainsi qu'American Express SafeKey®, sans nuire à l'expérience d'achat de leurs détenteurs de cartes. En utilisant le moteur RSA Risk Engine, la solution Adaptive Authentication for eCommerce évalue de manière transparente chaque transaction en temps réel et détermine la probabilité que cette dernière soit frauduleuse. Seuls les détenteurs de cartes entreprenant des transactions jugées à haut risque se verront appliquer une sécurité renforcée à l'authentification, ce qui exclut environ 95 % des transactions des commerçants participants du processus de vérification 3-D Secure. En outre, en raison de la couche transparente d'authentification, les détenteurs de cartes ne sont plus tenus de passer par un processus d'inscription VbV, SecureCode, Identity Check ou SafeKey (l'émetteur inscrit préalablement l'intégralité des plages de numéros d'identification bancaire des cartes) ou de mémoriser un mot de passe (une variété de méthodes d'authentification progressive est disponible, notamment le mot de passe à usage unique et les données biométriques). Cela permet aux détenteurs de cartes authentiques d'effectuer des transactions en ligne sans être interrompus.

« Notre façon de mesurer le succès réside dans notre capacité à traiter beaucoup plus de ventes ; nos pertes dues aux fraudes sont maîtrisées et nos clients sont satisfaits de la solution. »

Le vice-président et responsable du contrôle des risques de fraude d'une grande banque



L'APPLICATION D'ANALYTIQUE

L'application d'analytique de la solution RSA Adaptive Authentication for eCommerce offre aux émetteurs de cartes une visibilité complète sur les données de leurs transactions 3-D Secure. Elle met les mesures de surveillance quotidiennes et mensuelles, les taux de détection de fraude et les données de performances des règles à la portée des émetteurs, afin qu'ils puissent aligner les solutions sur leur tolérance aux risques et leurs priorités commerciales.

Le tableau de bord est complété par des rapports qui :

- représentent et soulignent les tendances et les valeurs aberrantes ;
- permettent l'affichage des données à différents niveaux de granularité ;
- offrent une interface flexible et dynamique pour les modifications à la volée.

Les émetteurs peuvent également exporter des informations du tableau de bord vers divers formats pouvant être intégrés par des applications externes.

L'application d'analytique permet aux émetteurs d'avoir une meilleure connaissance de leur environnement de menaces. Ils peuvent ainsi prendre des décisions plus éclairées concernant la gestion des règles, les seuils de score de risque et d'autres variables configurables.

3-D SECURE 2.0 – LA NOUVELLE GÉNÉRATION

Le protocole 3-D Secure est en constante évolution. EMVCo, l'organisme de normalisation chargé du développement du nouveau protocole, a lancé la nouvelle génération de 3-D Secure (EMV 3-D Secure, 3-D Secure 2.0, ou simplement « 3DS 2.0 ») en octobre 2016. Le protocole 3DS 2.0 vise à promouvoir une expérience d'achat fluide pour les détenteurs de cartes en tirant parti des technologies d'authentification basées sur le risque, une approche dont RSA a été le précurseur en 2008. En tant qu'associé technique d'EMVCo, RSA a fourni à 3DS 2.0 les données d'entrée intégrées dans les spécifications.

RSA se réjouit de pouvoir activer de nouvelles fonctionnalités sur sa plate-forme. Nous continuerons à travailler directement avec nos clients et EMVCo sur des initiatives qui fournissent une authentification transparente et sans mot de passe aux émetteurs de cartes.

À PROPOS DE RSA

Les solutions RSA® Business-Driven Security™ offrent aux organisations une approche unifiée de la gestion du risque numérique qui repose sur une visibilité intégrée, des informations automatisées et des actions coordonnées. Avec des solutions permettant une détection et une réponse rapides, un contrôle d'accès des utilisateurs, une protection du consommateur contre les fraudes et une gestion intégrée des risques, les clients de RSA peuvent se développer et s'adapter en permanence au changement transformationnel. Pour plus d'informations, accédez au site rsa.com/fr-fr.