Foire aux questions

Observatoire
de la sécurité
des cartes de paiement

Quel intérêt ai-je à identifier les transactions à risque ?

Les transactions à risque sont les transactions les plus exposées à la fraude (du fait de la nature du produit vendu par exemple) ou celles à l'origine du plus fort taux de fraude. L'identification des transactions à risque permet de prendre des mesures destinées à lutter contre la fraude et à réduire le coût supporté à l'occasion de chaque fraude subie.

Comment puis-je identifier les transactions à risque ?

Le pré-requis pour sécuriser les paiements reçus à l'occasion de ventes par Internet est de faire preuve de bon sens, toute opération atypique devant pousser à redoubler de vigilance. Il est essentiel, en outre, de parfaitement connaître son activité, ses produits et ses clients. Toute action inhabituelle ou incohérence dans la décomposition de l'acte d'achat ou dans les modalités de livraison/réception est susceptible d'éveiller le soupçon.

Des outils de détection des transactions les plus risquées ont été développés par le e-commerce, les prestataires techniques ou prestataires de solutions de paiement et les systèmes de paiement par carte. Ils analysent en temps réel les caractéristiques d'une transaction sur Internet pour déterminer son niveau de risque induit. Pour ce faire, ils mettent en relation différents critères comme, par exemple, les produits commandés, l'origine géographique de la commande et sa compatibilité avec l'adresse IP du client, le pays d'émission de la carte de paiement, le lieu de livraison des produits, le montant de la commande. Dans certains cas, ces outils de détection peuvent être paramétrés pour immédiatement bloquer la transaction analysée comme particulièrement risquée. Ces outils s'enrichissent automatiquement avec l'historique des analyses et sont confrontés, à des fins d'amélioration de la précision du filtrage, aux fraudes réellement constatées.

Comment puis-je sécuriser les transactions à risque ?

Les transactions peuvent être sécurisées par la mise en place d'un outil d'authentification renforcée du porteur de la carte, tel que 3D-Secure, pour s'assurer que ce dernier est bien le porteur légitime.

Qu'est-ce que 3D-Secure ?

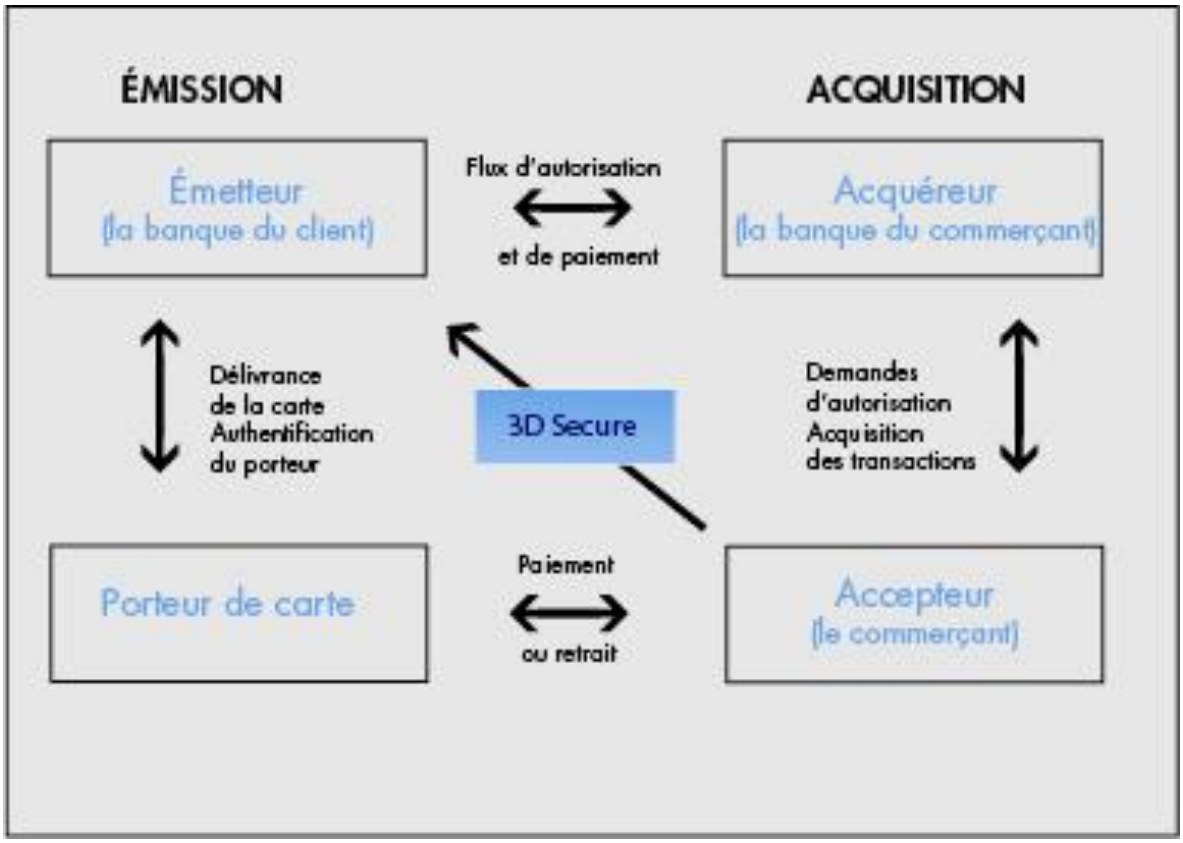
3D-Secure est un protocole de sécurité proposé par VISA, MasterCard, le GIE Cartes bancaires et par American Express (qui déploiera SafeKey, son moyen d'authentification renforcée du porteur, à compter du deuxième semestre 2013)

Son objectif est d'augmenter le niveau de sécurité des paiements à distance en ajoutant au processus actuel du paiement par formulaire une étape d'authentification réalisée par la banque du porteur, et selon la méthode d'authentification de son choix.

Lorsqu'une opération de paiement met en œuvre 3D-Secure, elle est éligible au transfert de responsabilité de l'acquéreur vers l'émetteur, parfois désigné sous son expression anglophone « *Liability shift* ».

Un commerçant est dit 3D-Secure lorsque son site de vente à distance (VAD) propose ce moyen d'authentification renforcée des acheteurs.

Comment 3D-Secure fonctionne-t-il?



3D-Secure : VERIFIED by VISA MasterCard SecureCode. et, à compter du deuxième semestre 2013, AMERICAN EXPRESS SafeKey

NOTA : le système ci-dessus est un système dit à « quatre coins », c'est-à-dire, qu'il s'agit d'un système où l'émetteur et l'acquéreur sont différents. Il existe aussi des systèmes « trois coins » où l'émetteur et l'acquéreur sont identiques.

Le système de paiement par carte met en relation le porteur de la carte, le commerçant, l'émetteur de la carte et l'acquéreur. Il gère notamment les demandes d'autorisation et les flux financiers lors du dénouement des opérations. Il gère les règles du système carte (voir *infra*).

L'émetteur de la carte (la banque du client) est généralement un établissement de crédit, de paiement ou de monnaie électronique qui propose des cartes de paiement à sa clientèle en vue de lui permettre de régler des achats de biens ou de services ou de procéder à des retraits d'espèces à un distributeur automatique de billets.

Dans le cadre du protocole 3D-Secure, l'émetteur enrôle les porteurs (enregistrement du numéro de téléphone mobile) et authentifie ces derniers lors de la transaction avec un code non-rejouable.

L'acquéreur (la banque du commerçant) est généralement un établissement de crédit, de paiement ou de monnaie électronique qui collecte les transactions de paiement par carte qui lui sont présentées par son client commerçant et qui en crédite le montant (net de commissions) au compte du commerçant.

Dans le cadre du protocole 3D-Secure, l'acquéreur fournit au commerçant les briques techniques à installer sur son site de vente à distance. Au-delà, son rôle est identique à celui qui serait le sien dans le cadre d'une opération non 3D-Secure.

L'accepteur de la carte est un commerçant qui accepte la carte comme instrument de paiement. Il est en relation avec une banque, un établissement de paiement ou de monnaie électronique qui le crédite du montant (net de commissions) des transactions carte.

Dans le cadre du protocole 3D-Secure, l'accepteur redirige automatiquement le porteur vers sa banque pour que celui-ci soit authentifié.

Le porteur de la carte (le client ou l'acheteur) dispose d'un compte auprès d'une banque, d'un établissement de paiement ou de monnaie électronique qui gère le compte bancaire ou de paiement auquel sa carte est associée.

Dans le cadre du protocole 3D-Secure, dans le cas des envois d'OTP (one-time-password) par SMS, le porteur de la carte saisit un code à usage unique qui permet à sa banque émettrice de l'authentifier.

Qui sont les prestataires de solution de paiement ?

Il peut s'agir d'une banque ou d'une société de service en ingénierie informatique qui fournit au commerçant en ligne une solution lui permettant d'accepter les paiements en contrepartie de la vente d'un bien ou d'un service.

Quelles sont les règles de transfert de responsabilité liées à 3D-Secure?

L'objectif de 3D-Secure est de tendre vers une garantie similaire à celle du paiement de proximité à travers la mise en place du transfert de responsabilité.

En cas de contestation pour motif de fraude dans le cadre d'une transaction de vente à distance, le transfert de responsabilité garantit le commerçant dont la responsabilité financière est alors transférée vers le banquier émetteur.

Cartes CB : Dans le cas d'un commerçant sous contrat d'acceptation CB « VADS » et de la carte d'un porteur présentant le logo CB, si le commerçant a respecté toutes les obligations liées à son contrat d'acceptation (à titre d'exemple, obtention d'une réponse positive de l'émetteur à une demande d'autorisation 3D-Secure), il n'y a pas de restrictions au transfert de responsabilité en fonction du type de la carte.

Réseaux MasterCard et Visa : Pour ce qui est des opérations réalisées avec des cartes ne présentant par le logo CB, les réglementations des réseaux internationaux MasterCard et Visa s'appliquent et des particularités sur le « non transfert de responsabilité » peuvent être identifiées, même si le processus de paiement 3D-Secure a abouti avec succès. Ainsi, par exemple, le transfert de responsabilité peut ne pas s'appliquer pour toutes les cartes « *corporate* », « *business* » ou « *purchasing* » émises hors Europe, lorsque la région d'émission de la carte et la région d'acquisition du paiement sont différentes. **Pour de plus amples informations concernant les limites du transfert de responsabilité, vous pouvez vous rapprocher de votre banque acquéreur.**

Quel pourrait être l'apport de 3D-Secure lors des paiements fractionnés ou récurrents ?

Bien que le paiement par carte n'ait pas vocation à se substituer au prélèvement avec signature d'un mandat, des cas de paiement fractionné ou récurrent par carte de paiement ont été relevés. Dans ces cas très spécifiques et non souhaitables, 3D-Secure permet d'assurer la sécurisation et le transfert de responsabilité sur la première opération réalisée avec mise en œuvre de 3D-Secure. Le statut des paiements suivants ne change pas par rapport à la situation sans mise en œuvre de 3D-Secure. Néanmoins, la réalisation d'une première opération authentifiée par le porteur permet au commerçant d'avoir un degré d'assurance et de confiance sur les paiements suivants bien supérieur à celui qui serait le sien dans le cadre d'un paiement sans 3D-Secure sur le premier paiement.

3D-Secure est il adapté au paiement sur mobile ?

L'architecture de paiement 3D-Secure peut être mise en œuvre dans le cadre d'un paiement par téléphone mobile, mais peut se révéler d'un usage difficile pour le porteur selon l'ergonomie de saisie des données cartes adoptée et la méthode d'authentification utilisée par la banque.

Que faire en cas de fraude ?

La fraude ne doit pas être confondue avec le litige commercial (contestation du client par rapport au produit commandé, livré ou non livré).

Les systèmes de pré-plainte en ligne comme https://www.pre-plainte-en-ligne.gouv.fr/ permettent d'effectuer une déclaration pour des faits d'atteinte aux biens (vols, dégradations, escroqueries...) dont les particuliers ou les professionnels sont les victimes et pour lesquels ils ne connaissent pas l'identité de l'auteur. Cette démarche vise essentiellement à faire gagner du temps ; mais, pour qu'elle soit enregistrée comme une plainte, la déclaration doit être signée dans l'unité de gendarmerie ou le service de police choisi.

Dans ce cadre, il est important que les commerçants victimes d'une fraude fournissent un maximum de renseignements qui concourront à l'enquête, à savoir, aussi bien les informations sur les commandes litigieuses/suspectes (et donc notamment toutes les informations sur la livraison comme l'adresse, le numéro de suivi, etc.), que les informations techniques, en particulier les adresses IP au moment des différentes étapes de la transaction (depuis l'éventuelle création d'un compte, même si celle-ci est ancienne, jusqu'à la transaction frauduleuse). Enfin, il est essentiel de préciser les coordonnées des contacts avec le prestataire chargé de traiter les paiements électroniques.

Par ailleurs, la notion de suivi des incidents « importants » est essentielle. Il est utile aux forces de l'ordre de disposer, dans un tableau, par exemple, de l'ensemble des actions entreprises dans le cadre du suivi de l'incident (un incident étant, par exemple, une série de faits corrélés et pas uniquement une transaction). Cela permet d'avoir un journal de bord qui aide au dialogue avec les enquêteurs ; ceci peut également servir à évaluer de façon plus exhaustive le préjudice subi ou encore à tirer des leçons pour l'avenir (ce qui aurait dû être fait, comment la détection en amont aurait pu intervenir, etc.).

Qui contacter pour de plus amples renseignements ?

Secrétariat de l'Observatoire de la sécurité des cartes de paiement

oscp@banque-france.fr


BANQUE DE FRANCE
EUROSYSTÈME