Commerçants, comment renforcer la sécurité des paiements sur Internet ?

Observatoire
de la sécurité
des cartes de paiement

La fraude au paiement à distance : une réalité

Créée à l'origine pour les paiements en face-à-face, la carte de paiement s'est rapidement affirmée comme l'outil le plus utilisé pour payer sur Internet.

Or, les statistiques montrent que ce canal de paiement est particulièrement touché par la fraude.
En effet, la rapidité et la faculté d'adaptation des fraudeurs touchent tous les secteurs et tous les acteurs.

Au-delà de son impact sur les résultats des commerçants, la fraude représente un coût pour tous : celui qui assume la perte, celui ou ceux qui assument les démarches, etc.

Dans ce contexte, la Banque de France, l'Observatoire de la sécurité des cartes de paiement et les acteurs qu'il représente recommandent la mise en œuvre de mesures de sécurité appropriées.

Cette brochure présente des moyens et des outils permettant aux commerçants de sécuriser les paiements par carte qu'ils reçoivent sur Internet.

Pour en savoir plus

Lien vers le site de l'Observatoire de la sécurité des cartes de paiement
Lien vers l'action de la Banque de France dans le domaine de la sécurité des paiements à distance
Lien vers le site de la Fédération du E-commerce et de la Vente à distance (FEVAD)

Comment sécuriser les paiements par carte sur Internet ?

Les pré-requis

Connaître son activité

Connaître ses produits, ses clients, la décomposition de leur acte d'achat, leurs modalités de livraison/réception…

Identifier les transactions à risque

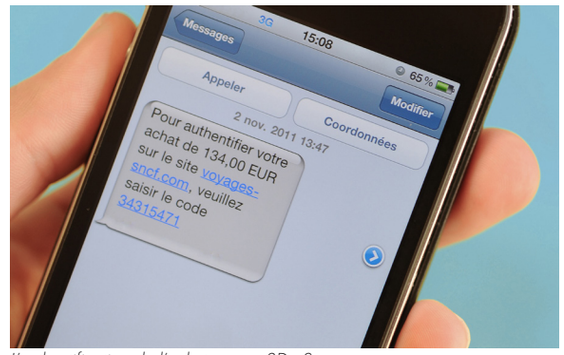
Mettre en place des outils adaptés afin de détecter les transactions les plus risquées (origine géographique de la transaction, informations de livraison, type de produit, montant de la transaction, etc.)

Les dispositifs de protection

Sécuriser ces transactions

L'une des solutions consiste à authentifier de manière renforcée le porteur de la carte, particulièrement pour les transactions les plus risquées, comme le permet par exemple 3D-Secure, le mécanisme le plus répandu aujourd'hui en France et à l'étranger.

D'autres solutions, comme les portefeuilles électroniques peuvent contribuer à renforcer l'authentification du porteur sur les nouveaux canaux de paiement (notamment le canal mobile…).



L'authentification de l'acheteur par 3D - Secure

Pour en savoir plus

Lien vers la FAQ
Lien vers le rapport annuel 2011 de l'Observatoire

Un exemple de solution pour renforcer l'authentification du porteur : 3D-Secure

à partir du 2e semestre 2013

3D-Secure est un dispositif permettant d'authentifier le porteur d'une carte de paiement de manière renforcée à l'occasion, par exemple, d'un achat sur Internet.

L'acheteur doit saisir un code d'authentification à usage unique, reçu le plus souvent par SMS, pour valider le paiement de ses achats.

TÉMOIGNAGES DE COMMERCANTS

Voyages-SNCF.com

« Pour contenir l'augmentation des impayés reçus suite à l'achat de billets sur www.voyages-sncf.com, 3DS s'est avéré être une 1ère solution efficace et rapide à mettre en place. Nous avons déployé l'authentification 3DS prudemment, à partir de certains montants d'achats dans un 1er temps, avec beaucoup de pédagogie et d'accompagnement de nos clients pour les aider à se familiariser avec cette nouvelle étape dans leur parcours d'achat.» Lire la suite

Delamaison.fr

« Fin 2010, Delamaison.fr a mis en place une solution visant à lutter plus efficacement contre la fraude des paiements.
Notre système analyse le risque en temps réel lors du paiement. Si un risque est détecté, une transaction 3D Secure est déclenchée. Dans le cas contraire le client effectue son paiement sans 3D Secure.
Cette mise en œuvre a l'avantage de nous garantir le paiement pour les transactions risquées et de limiter les tentatives de fraude sur notre site.
Enfin la mise en œuvre sélective de 3D Secure sur une partie des transactions limite les risques d'abandon de paiement.
Après 2 ans d'utilisation, le bilan de la solution mise en œuvre est positif. »

Pour en savoir plus

sur 3D-Secure :
Lien vers le site de l'Observatoire de la sécurité des cartes de paiement
Lien vers la FAQ

Pourquoi mettre en oeuvre un mécanisme d'authentification renforcée ?

Vous réduisez la fraude que vous subissez et vous participez à la réduction générale de la fraude

L'authentification renforcée est un moyen de faire baisser votre taux de fraude. C'est la raison pour laquelle certains grands sites particulièrement exposés ont mis en place avec succès un mécanisme d'authentification renforcée.

Vous ne supportez plus le coût de la fraude

Les dispositifs d'authentification renforcée du porteur de la carte comme 3D Secure sont pour la plupart assortis d'une clause de transfert de responsabilité (également appelé « liability shift ») garantissant le commerçant en cas de contestation pour motif de fraude. Le marchand continue en revanche à assumer les éventuelles répercussions financières liées aux transactions contestées par ses clients pour d'autres motifs (litige commercial par exemple).

Il convient de noter que ce transfert de responsabilité peut ne pas s'appliquer à certaines cartes (« corporate » ou certaines cartes émises en dehors des frontières européennes) et à certaines modalités de paiement (notamment paiements récurrents ou fractionnés).

83 % des acheteurs sur Internet indiquent avoir entendu parler des dispositifs d'authentification renforcée pour sécuriser les paiements par carte en ligne.

L'authentification renforcée des porteurs se généralise

- **Plus de la moitié des commerçants en ligne** ont sécurisé leur processus d'achat en permettant à l'émetteur de la carte d'authentifier le porteur via le protocole 3D-Secure.
- L'adoption de 3D-Secure par certains grands commerçants et les efforts de communication déployés notamment par les émetteurs de cartes ont permis de familiariser les acheteurs sur Internet avec l'authentification renforcée du porteur et d'augmenter la progression du taux de succès des transactions sécurisées à plus de **80 %.**

Pour en savoir plus

Lien vers la FAQ

Les dispositifs d'authentification renforcée vont progressivement être étendus aux paiements sur Internet au niveau européen où certains marchés, comme la Belgique ou le Royaume Uni, ont déjà adopté 3D-Secure de manière généralisée.

Dans ce contexte, le déploiement progressif de l'authentification renforcée pourrait conduire à un report de la fraude vers les sites non protégés, y compris vers ceux actuellement épargnés.

Des dispositifs qui renforcent le sentiment de sécurité pour vos clients

- Près de **90 %** des consommateurs estiment que les dispositifs d'authentification du porteur renforcent significativement la sécurité des paiements par carte sur Internet ;
- **84 %** des acheteurs en ligne disent se sentir en sécurité lorsqu'ils utilisent un dispositif d'authentification renforcée ;
- **57 %** des acheteurs sur Internet déclarent qu'ils favoriseront les sites d'e-commerce présentant de tels dispositifs.

Les associations de consommateurs soutiennent la généralisation de tels dispositifs.

Ainsi, certaines associations de consommateurs conseillent aux consommateurs d'utiliser de préférence les sites qui proposent un paiement sécurisé, notamment par le procédé « 3D Secure ».

Pour en savoir plus

Lien vers la brochure de l'Association Force Ouvrière Consommateurs (AFOC)

Qui vous aide à sécuriser vos paiements par carte sur Internet ?

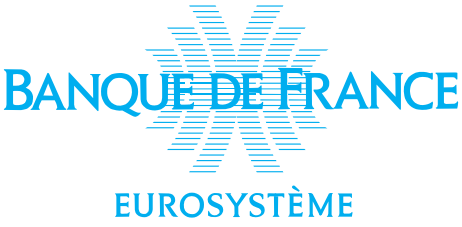
- votre prestataire de solution de paiement : pour déterminer et mettre en place les moyens techniques adéquats, le cas échéant, en lien avec vos équipes informatiques ou avec votre prestataire technique, pour identifier et sécuriser les transactions les plus risquées ;
- votre banque : pour mettre en place ou faire évoluer votre contrat d'acceptation des paiements par carte.

Comment réussir la mise en œuvre de l'authentification renforcée ?

- Déterminez la stratégie de déploiement la mieux adaptée à votre contexte, par exemple en authentifiant de manière prioritaire les transactions les plus risquées ;
- Sensibilisez vos clients à la mise en œuvre d'un dispositif d'authentification renforcée ;
- Communiquez en amont sur votre site Internet ;
- Formez votre assistance clientèle à ce dispositif pour qu'elle soit en mesure de répondre aux questions éventuelles de vos clients ;
- Suivez l'évolution de la fraude sur vos transactions pour réagir de manière adaptée. Restez attentif au risque de report de la fraude vers les paiements effectués sur d'autres canaux (mobile, téléphone, courriel, etc.) ;
- Pour le canal mobile, des solutions spécifiques comme, par exemple, les portefeuilles électroniques peuvent être envisagées afin de renforcer l'authentification de vos clients.

Pour en savoir plus

Lien vers le rapport annuel 2011 de l'Observatoire


BANQUE DE FRANCE
EUROSYSTÈME