BANQUE ET ASSURANCES

E-transactions

Les " bonnes pratiques" 3D Secure

AVERTISSEMENT

Les informations contenues dans ce document n'ont aucune valeur contractuelle. Elles peuvent faire l'objet de modification à tout moment. Elles sont à jour en date de rédaction au 06/07/2016.

E-transactions est une solution de paiement à distance dans un environnement sécurisé, distribuée par les Caisses régionales de Crédit Agricole.
Renseignez-vous auprès de votre conseiller sur les conditions générales et tarifaires de cette solution.

TABLE DES MATIERES

1. PRINCIPE

La plupart des sites de commerce électronique, qui proposent de faire du paiement en ligne, utilisent les protocoles SSL pour chiffrer les informations sensibles telles que le numéro de carte bancaire. Ces protocoles ont été conçus pour assurer la confidentialité des informations échangées entre deux entités et s'avèrent insatisfaisants par rapport aux exigences requises pour des paiements sécurisés.

Dans ce contexte, MasterCard et VISA ont conçu l'architecture 3D-Secure dont la finalité est de permettre aux banques d'authentifier leurs porteurs par le moyen de leur choix, via un mécanisme technique mis en place à la fois par les banques des commerçants et des porteurs de cartes.

3D-Secure permet de :

- **s'assurer que l'internaute qui réalise la transaction est bien le titulaire de la carte utilisée pour le paiement,**
- **garantir au commerçant les transactions et d'introduire en cas de contestation du porteur de carte, un transfert de responsabilité vers la banque de ce dernier**

L'authentification du porteur est gérée par la banque du porteur de carte. Le porteur visualise donc toujours la même page d'authentification. La Banque de France préconise une authentification forte non rejouable (ANR) : code envoyé par SMS ou SVI, calculette …

Remarque :

Le dispositif 3D Secure ne concerne que les paiements à l'acte sur Internet, effectués par une carte bancaire Visa (programme « Verified by Visa ») ou MasterCard (programme « MasterCard SecureCode).

Les paiements ci-dessous sont exclus du programme 3DS :

- récurrents,
- fractionnés (le premier paiement est 3D Secure),
- de vente à distance classique (téléphone, courrier…),
- créés directement par le commerçant sur un outil de back-office (création, duplication de transactions) car le porteur n'est pas présent.- réalisés avec les cartes privatives.

Rmq : American Express dispose de son propre programme équivalent : Safekey

En France, toutes les banques émettrices de cartes adhèrent au programme 3D-Secure.

Légalement vu du porteur

Lors d'achat internet sans 3DSecure, à aucun moment, l'identité du porteur n'est prouvée.
En paiement de proximité, elle est prouvée par la saisie du code PIN ou par la signature.

Il suffit que le porteur conteste un paiement auprès de sa banque pour que cette dernière le rembourse. La banque du porteur se retournera alors vers la banque du commerçant pour lui réclamer la somme.

Lors d'un achat en mode 3DSecure, si l'authentification est un succès, il y a un transfert de responsabilité vers la banque du porteur, puisqu'elle a affirmé que c'était bien le porteur qui était en train de payer. Elle ne peut donc plus contester et doit régler le paiement à la banque du commerçant.

La banque du porteur transfèrera cette responsabilité vers son client qui lui-même ne pourra plus contester un paiement 3DSecure et donc se faire rembourser.

Si l'authentification 3DS a échoué et que la banque du commerçant réclame le recouvrement de la somme, la banque du porteur est censée refuser. Si elle l'accepte malgré tout, le porteur pourra contester ce débit et se faire rembourser (puisque rien n'aura prouvé que c'est le porteur qui a effectué le paiement).

Si un porteur ne dispose pas de l'option Internationale dans son abonnement mobile, il ne pourra pas effectuer un achat par Internet pendant un déplacement à l'étranger (ex: réservation d'hôtel ou location de véhicule).
De même, il lui sera impossible d'effectuer un achat à distance s'il se trouve dans une zone non couverte par le réseau de téléphonie portable (campagne, montagne, voire dans certains lieux de grandes villes).

2. ILLUSTRATION

1. Lors du paiement de sa commande, le porteur saisit son numéro de carte, la date de fin de validité et le cryptogramme visuel (le code à trois chiffres au dos de la carte)
2. E-transactions vérifie si le client est enregistré **3D Secure**, auprès d'un annuaire Visa ou Mastercard. Si le BIN du commerçant est référencé dans l'annuaire, la demande est transmise à la banque du porteur.
3. La banque du porteur vérifie si ce dernier dispose d'un moyen d'authentification (enrôlé).
4. Si le porteur est enrôlé, E-transactions renvoie le porteur vers le site d'authentification de sa banque.
5. Le client s'authentifie auprès de sa banque.
6. La banque renvoie le client vers E-transactions avec la preuve d'authentification.
7. Une demande d'autorisation est effectuée en utilisant la preuve **3D Secure**.
8. Si l'autorisation est accordée, dans un deuxième temps, E-transactions envoie la remise en banque et la preuve du paiement **3D Secure**.
9. La preuve du paiement **3D Secure** est archivée et visible dans le Back Office Vision

3. AUTHENTIFICATION

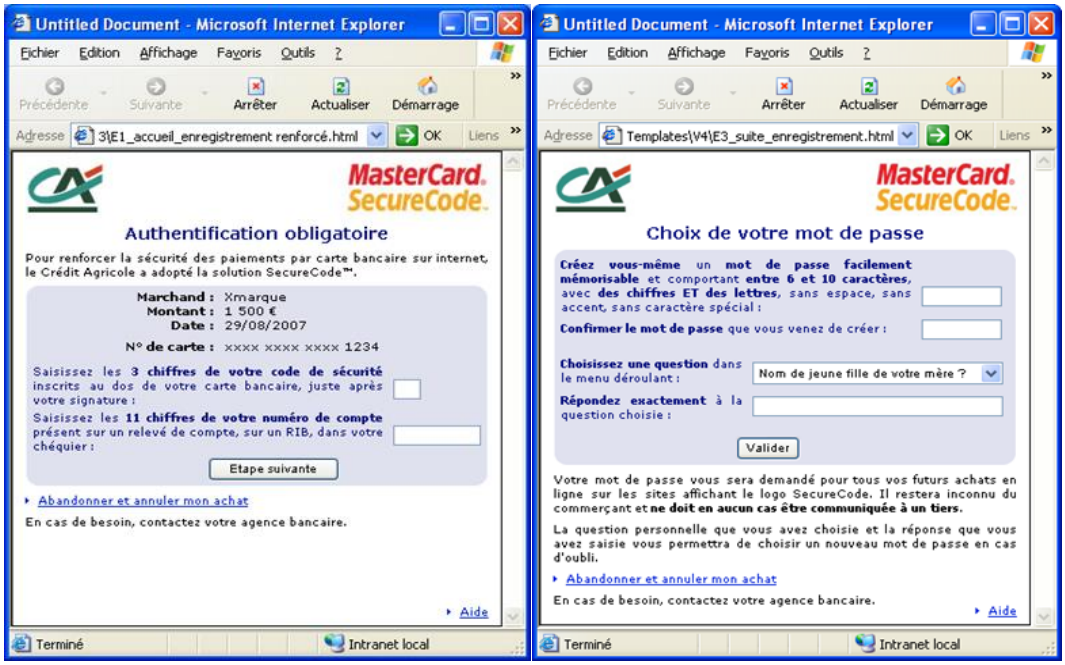
Comment se passe l'authentification ?

La technologie 3D Secure permet à la banque du porteur de s'assurer que l'acheteur est bien le titulaire de la carte en introduisant une étape spécifique dans le processus d'achat : **L'authentification**.

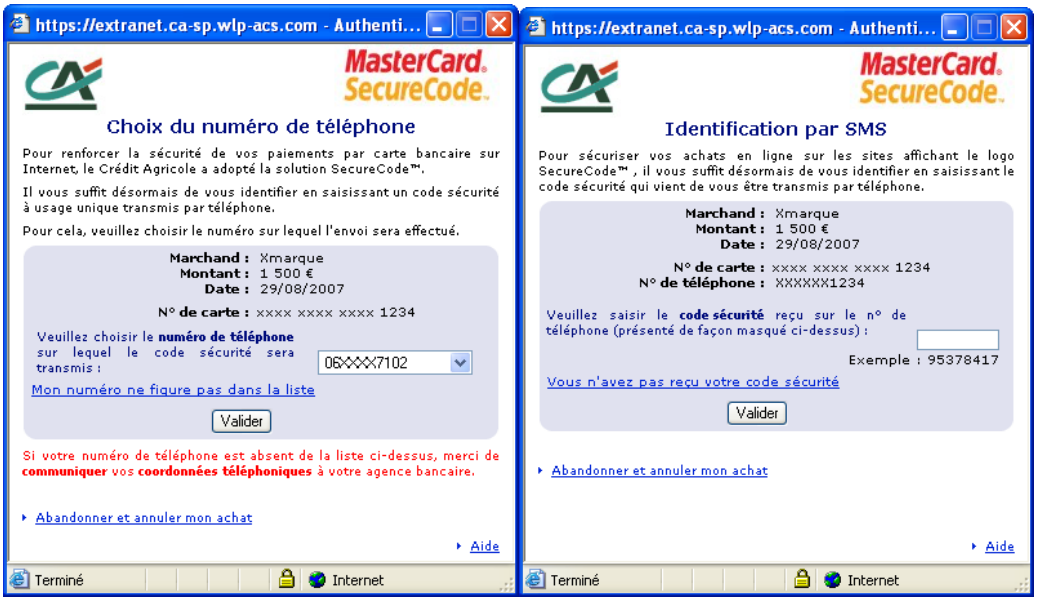
Chaque banque émettrice de cartes décide du ou des moyens d'authentification qu'elle fournit à ses porteurs de carte. Si dans un premier temps, certaines banques françaises ont choisi la date de naissance du porteur, ou demandent au client de choisir un identifiant personnel alphanumérique, suivant les directives de la Banque de France, les banques ont migré progressivement vers des solutions d'authentification forte (code secret par SMS, Token…).

Qu'est-ce qu'une authentification faible ? Une authentification forte ?

Une authentification faible est une authentification "**re-jouable**" : elle est basée sur un élément statique comme une date de naissance, un code non aléatoire ou une question secrète utilisable pour les paiements sur Internet.



Une authentification forte est une authentification **non "re-jouable"**, à usage unique. Elle se différencie par l'association de plusieurs éléments en vue d'assurer son inviolabilité : carte matricielle (carte "bataille navale"), code secret aléatoire à usage unique envoyé par SMS ou par SVI (téléphone fixe), un code unique fourni par une calculette ou une clé USB (boitier d'authentification), fonctionnant en liaison ou pas avec la carte de paiement.



L'authentification forte est le choix par défaut du Crédit Agricole

4. INDICATEUR DE GARANTIE 3D SECURE

Le commerçant E-transactions visualise dans son back-office si la transaction est ou non garantie 3DSecure. Les indicateurs suivant sont disponibles :

- **Paiement 3D-Secure : Indique si la transaction a été exécutée avec un contrôle 3DSecure**
  - « OUI » Avec 3D-Secure
  - « NON » Sans 3D-Secure

- **Porteur authentifié : Indique si la carte de l'acheteur est enrôlée à 3D-Secure et s'il a réussi à s'authentifier**

  - **Y** : L'authentification s'est déroulée avec succès

  - **N** : Le porteur n'est pas parvenu à s'authentifier, la transaction est interdite : le banquier émetteur refuse le paiement (ex : plus d'argent sur le compte, le code n'a pas été saisi dans le délai imparti ou mal saisi, le code n'a pas été reçu : zone téléphonique « blanche »)

  - **U** : L'authentification n'a pu être finalisée suite à un problème technique : impossible de saisir le code
    Exemple : L'authentification n'a pu être finalisée suite à un problème technique ➔ Problème technique qui ne bloquerait pas la transaction (sauf si le commerçant a demandé un paramétrage dans E-transactions pour n'accepter que les transactions full 3DS) ➔ **Le commerçant reste garanti**

- **A** : L'authentification n'était pas disponible, mais une preuve de tentative d'authentification a été générée
  Exemple : L'authentification n'était pas disponible, mais une preuve de tentative est disponible ex le porteur n'a pas de portable, ou n'a pas déclaré de numéro de mobile ➔ **Le commerçant reste garanti**

- **Garantie : Indique l'état de la garantie de la transaction selon les règles 3D-Secure**
  - « OUI » Garantie
  - « OUI expirée » Non Garantie car remise en banque au-delà du délai maxi de 7 Jours
  - « NON » Non Garantie

Seules les transactions marquées « OUI » font l'objet d'une garantie 3D-Secure

Par conséquent, au moment de l'implémentation de la solution de paiement dans sa boutique, pour bénéficier de la protection que propose le 3DS, le commerçant doit veiller avec son intégrateur à :

- S'il est équipé d'E-transactions Premium et de la gestion automatisée des encaissements :

  Ne finaliser les parcours d'achats et donc de livraison de marchandise que lorsque la garantie est à OUI

- S'il est équipé d'E-transactions Access et/ ou qu'il n'a pas mis en œuvre la gestion automatisée des encaissements :

  Annuler les transactions « garantie à Oui expirée » ou « garantie à NON » et ne pas livrer la marchandise.

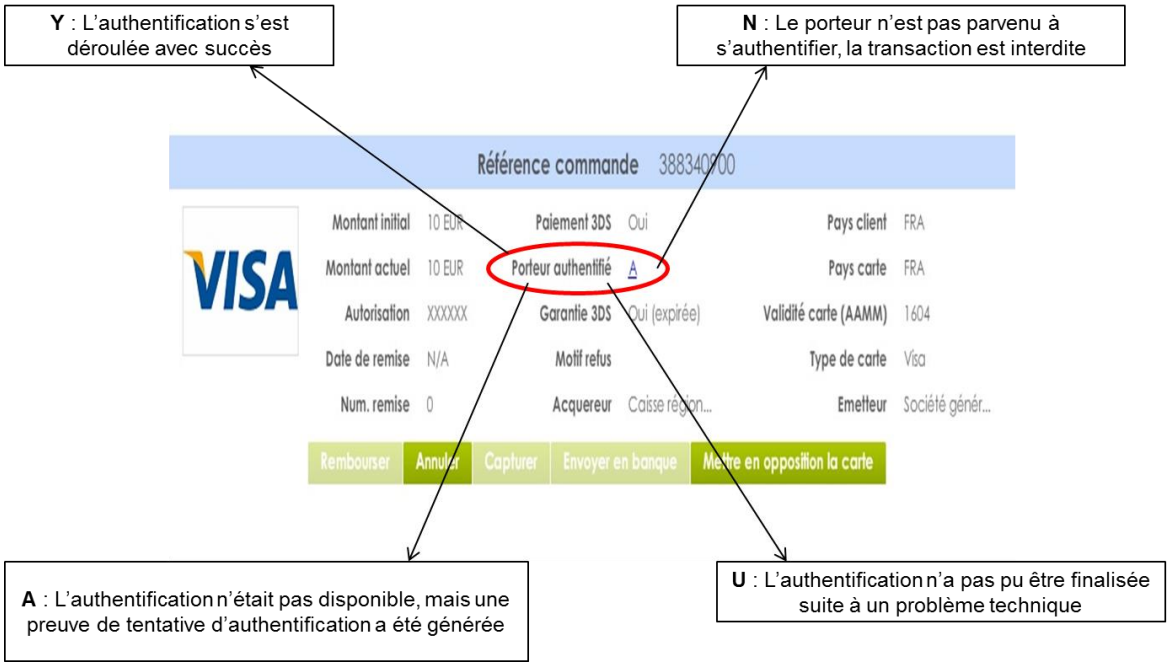
  Le cas échéant, le commerçant **ASSUME** le risque lié à la non utilisation du 3DS (contestation du porteur : « ce n'est pas moi qui ait fait cet achat »)

C'est au commerçant de piloter la remise en banque de la transaction et la livraison de la commande. C'est du domaine de son activité e-commerce et non du banquier, qui lui met à disposition les moyens et l'information pour le faire.

Si une transaction garantie 3DSecure (indicateur à « OUI ») est contestée par le porteur, l'impayé sera supporté par la banque émettrice.

Par contre, si le commerce laisse partir en banque une transaction non garantie, il prend le risque d'assumer le coût des impayés en cas de contestation du porteur.

Les échéances postérieures au 1er paiement lors d'un paiement en plusieurs fois ou d'un abonnement ne sont pas garanties 3DS, car elles ne sont pas réalisées par l'internaute en mode 3DSecure mais générées automatiquement.



5. 3D SECURE PARAMETRABLE

Le mode 3D SECURE paramétrable permet au commerçant de configurer lui-même les mesures de sécurité souhaitées : par exemple, activer l'authentification 3DS du porteur à partir d'un certain montant.

Le commerçant a plusieurs possibilités pour débrayer le contrôle 3D Secure :

1. Si le commerçant a choisi l'offre Premium, il peut avec le chargé d'affaires de sa Caisse régionale, demander la mise en place de règles de débrayage

2. Avec son intégrateur, le commerçant peut également gérer le débrayage du 3DS via la variable PBX_3DS qu'il renseigne à NON dans son appel à E-transactions.

6. AVANTAGES CLIENTS

Vous bénéficiez de la garantie du paiement si le 3D Secure est actif

Dans la plupart des cas*, vous n'aurez plus à supporter les impayés dans le cas où l'internaute nie être l'auteur de la transaction.

**Le Crédit Agricole pourra contrepasser le montant des opérations non garanties (exemple : défaut de réception d'un justificatif 3D Secure) qui n'ont pu être imputées au compte sur lequel fonctionne la carte, sous réserve du respect des toutes les mesures de sécurités prévues à votre contrat d'acceptation.*

7. MISE EN ŒUVRE

Le 3D Secure est activé par défaut dans l'offre E-transactions Access et Premium afin de vous offrir la sécurité du 3DS.

8. IMPORTANT

Même s'il a souscrit à 3D Secure, le commerçant doit toujours rester vigilant lorsque la transaction lui semble frauduleuse.

9. BON A SAVOIR

Le 3DS est un protocole mondial :

La Banque Centrale Européenne avec la Directive sur les Services de Paiement (DSP) va également demander que les cartes émises en Europe soient toutes enrôlées. Plus précisément, la DSP2 exige une authentification forte. Aujourd'hui c'est une incitation de Visa / MasterCard qui poussent les banques à enrôler leurs cartes pour des aspects de transfert de risque, mais sans obligation.

Pour les banques émettrices du reste du monde il n'y a pas d'obligation mais une incitation des réseaux Visa / MasterCard

En France, à la demande de la Banque de France, le 3DS est utilisé **par l'ensemble des banques et concerne les cartes CB / Visa et CB / Mastercard** : cela garantit le paiement aux commerçants, sous réserve que le parcours 3DS se soit déroulé normalement.
A la marge, si un client n'est pas enrôlé 3DS, le commerçant est alors couvert puisque ce n'est pas de son fait.

Si un commerçant est 3DS, qu'il utilise le 3DS pour les paiements de ses clients, il bénéficie de la garantie 3DS (cf tableau à la fin).

Les exceptions à la garantie

- L'e-Carte bleue n'est pas concernée, puisqu'un nouveau numéro, unique et temporaire, servant à régler les achats, est émis à chaque tentative de paiement : cela consiste un soit un système d'identification du porteur et élimine toute contestation du type « ce n'est pas moi qui ai fait la transaction »

- Les cartes American Express (American Express a un système similaire dénommé Safekey), JCB, toutes les cartes privatives.

Un commerçant est 3D Secure lorsqu'il procède à l'authentification de ses acheteurs et qu'il a un contrat VADs. Le système 3DS le dégage des risques de paiements contestés :

> Le commerçant 3D Secure ne reçoit plus d'impayés pour les contestations du type « ce n'est pas moi qui ai fait la transaction » (motif 45). qui représentaient 80% des impayés avant la mise en place du programme 3DS et 0,70% du volume total des paiements sur Internet. *(source Fevad 2015)*

D'autre part cela le dispense en partie des audits de sécurité de plus en plus draconiens imposés par Visa et Mastercard.

Attention cependant !

Le transfert de responsabilité ne protège pas contre les litiges commerciaux (mauvaises livraisons, produits non conformes.
Par conséquent des impayés pour litiges commerciaux peuvent être émis.
Si l'impayé est justifié le commerçant sera débité.

Une transaction 3-D Secure ne doit jamais être modifiée, de facto dès que le commerçant fait du débit partiel ou une duplication de la demande pour un débit supérieur, la protection 3-D Secure n'est plus garantie.

Bien garder à l'esprit :

L'enrôlement 3DS du commerçant auprès de Visa / Mastercard prend environ 15 jours.

Si le commerçant passe une transaction avant que l'enrôlement 3DS ne soit effectif, il ne peut évidemment pas en bénéficier.
Pour savoir s'il est bien enrôlé et que c'est actif, plusieurs solutions :

- Faire un test sur sa boutique
- Consulter le back office E-transactions dans la rubrique Paramétrage / Contrats
- Appeler le SAV E-transactions

Bien vérifier avec votre intégrateur, que le 3DS sera systématiquement utilisé pour tout règlement et qu'il n'a programmé aucune règle sans vous en parler.

Vous pouvez a contrario décider de débrayer (d'accepter des transactions de paiement SANS le parcours 3DS) : ex petit montant, client connu/fidèle (information détenue dans la base client du commerçant) …

Vous prenez alors le risque de vous voir imputer des impayés liés à des contestations d'achat faites par les porteurs (« ce n'est pas moi qui ai fait cet achat »)

3DS et demande d'autorisation :

En VAD, tout paiement par carte fait l'objet d'une demande d'autorisation qui, si elle est acceptée par la banque émetteur au moment de la transaction, vous garantit le paiement du règlement **si vous la remettez avant 7 jours en banque.**
Le cas échéant, une remise tardive pourra faire l'objet d'un rejet de la banque émetteur.

Par conséquent, la demande d'autorisation seule ne suffit pas à garantir le règlement des achats.

En France, le Groupement Carte Bancaire garantit tout paiement, dès lors que le commerçant à fait une demande d'autorisation, qu'elle a été acceptée et que la remise en banque s'est faire dans un délai maximum de 7 jours.
Le cas échéant, le commerçant s'expose à un impayé.

Hors de France, le système de demande d'autorisation ne fonctionne ainsi :

- Mastercard : idem : 7 Jours pour présenter en compensation
  Exception : Les préautorisations (Type PLBS) où on passe à 30 Jours

- Visa : 180 jours

Le 3DS quant à lui, permet simplement de vérifier l'identité du client et d'écarter les fraudeurs : ce n'est qu'une garantie **d'authentification du porteur**.

Le commerçant doit satisfaire à ses autres obligations comme :

- Effectuer une demande d'autorisation : obligatoire en vente à distance (elle gère, la validité de la carte et l'état du compte bancaire)
- Remettre une transaction en banque :
  - dans un délai de 6 jours maximum pour garder le bénéfice du 3DS,
  - dans un délai de 7 jours maximum, pour garder le bénéfice de l'accord sur la demande d'autorisation
  - pour un montant <= à la demande d'autorisation obtenue

MAIS, le banquier émetteur peut rejeter la demande de paiement au motif que :

- Le Siret du commerçant est invalide
- L'opération a été dupliquée : (erreur de traitement à éviter)
- L'accepteur est suspendu ou radié (ex : procédure de liquidation …)

Par conséquent, une transaction garantie 3DS n'est pas forcément réglée par la banque « émetteur »

Rappel :

Le client a 13 mois pour contester un achat.
Si le client conteste (je n'ai pas fait cet achat), **alors qu'il a été authentifié 3DS**, sa contestation est rejetée.
Si le client conteste (je n'ai pas fait cet achat), **et qu'il n'a pas été authentifié 3DS**, sa contestation est acceptée.

C'est ce système qui a permis de créer la confiance dans l'éco-système d'achats sur internet : le consommateur sait qu'il est protégé des achats frauduleux réglé avec sa carte.

En France 90 % des contestations étaient liées au porteur : le 3DS couvre le commerçant sous réserve que le commerçant l'ait utilisé (non débrayé) et que le 3DS se soit déroulé correctement

Quels sont nos conseils ?

- Utilisez le 3DS que les solutions de paiement sur internet E-transactions Access ou Premium intègrent systématiquement

Si la transaction 3DS n'est pas à OUI, ne pas finaliser la vente, ne pas envoyer ce paiement en banque : le supprimer

- Vérifier bien avec votre intégrateur ce qu'il fait et que ce soit conforme à vos choix : ex : accepter des transactions sans 3DS dans certains cas commerciaux que vous aurez définis avec lui.

- Livrer votre client :

  - ✓ une fois que votre transaction a été remise en banque dans les délais (< 7 jours)
  - ✓ et sous réserve bien sûr, que le 3DS se soit déroulé normalement.

  Rappel : cela n'exclut pas les contestations pendant 13 mois

- En cas de livraisons successives pour une même commande (produit qui n'est pas en stock par exemple) : refaire une demande d'autorisation pour procéder à l'encaissement suivant (possible exclusivement sur Premium avec la Gestion Automatisée des Encaissements)

  En revanche il ne peut y avoir d'authentification 3DS puisque le client n'est plus là : il existe donc un risque de contestation.

  Vous disposez cependant d'un faisceau de preuves démontrant la mauvaise foi du consommateur. Ce cas sera à régler entre le commerçant et son acheteur.

Commerçant enrôlé 3DS et utilisant le 3DS = commerçant protégé !

Commerçant 3DS et garantie de paiement 3DS *	Client enrôlé 3DS / Banquier 3DS	Client non enrôlé 3DS / Banquier 3DS	Banquier non 3DS
FRANCE			
CB/Visa/Mastercard détenue par un particulier	OUI	OUI	Cas de figure inexistant
CB/Visa/Mastercard détenue par un « pro »	OUI	OUI	Cas de figure inexistant
CB/Visa/Mastercard fournie par un employeur à son personnel	OUI	OUI	Cas de figure inexistant
EUROPE			
Visa/ Mastercard détenue par un particulier	OUI	OUI	OUI
CB/Visa/Mastercard détenue par un « pro »	OUI	OUI	OUI
CB/Visa/Mastercard fournie par un employeur à son personnel	OUI	OUI	OUI
MONDE			
Visa/ Mastercard détenue par un particulier	OUI	OUI	OUI
CB/Visa/Mastercard détenue par un « pro »	OUI	OUI	OUI
CB/Visa/Mastercard fournie par un employeur à son personnel	OUI	OUI	OUI

*** Garantie de paiement 3DS = impossibilité de recevoir un impayé pour une contestation du porteur motif 45 « ce n'est pas moi qui ai fait la transaction ».**