

MARCHANDS

3-D Secure : ce que couvre le transfert de responsabilité et ce qu'il ne couvre pas

Publié le 11 septembre 2026

Authentifier un paiement par carte transfère le coût de la fraude du marchand à l'émetteur, mais seulement pour certains paiements et certaines contestations. Où la protection commence et où elle s'arrête.

3-D Secure est l'étape d'un paiement par carte en ligne où la banque du porteur confirme qu'il s'agit bien de lui, généralement via son application bancaire ou un code à usage unique. Les réseaux de cartes le commercialisent sous leurs propres noms, Visa Secure et Mastercard Identity Check, et en Europe c'est ainsi que la plupart des marchands satisfont à l'obligation légale d'authentification forte du client.

Pour un marchand, son principal attrait est le transfert de responsabilité. C'est aussi la partie la plus souvent mal comprise.

Ce qu'est le transfert

Sans authentification, un marchand en ligne supporte le coût de la fraude. Si un porteur dit « ce n'était pas moi », l'argent repart et le marchand perd la vente et la marchandise.

Lorsqu'un paiement a été authentifié par 3-D Secure, cette responsabilité passe à l'émetteur de la carte. Si une contestation pour fraude survient, l'émetteur l'absorbe et le marchand garde l'argent.

Ce qu'il couvre

Uniquement les contestations pour fraude. C'est tout.

Ce qu'il ne couvre pas

- **Tout autre type de contestation.** Marchandise non reçue, non conforme à la description, abonnement résilié encore facturé, remboursement non traité : l'authentification ne dit rien de tout cela, et le marchand reste responsable.

- **Les paiements suivants d'un abonnement.** Le premier paiement, effectué en présence du client, peut être authentifié. Les renouvellements qui suivent sont initiés par le marchand, sans porteur pour s'authentifier, et ne bénéficient d'aucun transfert.
- **Les paiements pour lesquels le marchand a demandé à éviter le contrôle.** Les règles européennes autorisent des exemptions, pour les petits montants ou pour les transactions que le prestataire du marchand juge à faible risque. Si c'est le marchand qui demande l'exemption, il conserve la responsabilité.
- **Certains marchands et certaines catégories.** Un marchand placé dans un programme de surveillance de la fraude ou des chargebacks d'un réseau peut perdre le transfert, et certaines catégories ne le reçoivent jamais entièrement.
- **Les paiements tentés mais pas correctement aboutis.** Le transfert dépend du résultat d'authentification renvoyé, et les règles applicables à une tentative diffèrent d'un réseau à l'autre.

Sans friction et avec challenge

Le 3-D Secure moderne n'arrête pas toujours le client. Le marchand envoie à l'émetteur des données sur le paiement, et l'émetteur soit l'approuve en silence, ce qu'on appelle sans friction, soit demande au porteur de confirmer, ce qu'on appelle un challenge. Les deux valent authentification, et les deux emportent normalement le transfert.

C'est important, car la vieille objection à 3-D Secure tenait aux ventes perdues à l'écran de challenge. Meilleures sont les données envoyées par le marchand, plus nombreux sont les paiements qui passent sans challenge.

Ce que cela vous coûte

- **De la conversion.** Certains clients abandonnent face à un challenge, et l'authentification de certains émetteurs échoue pour des raisons techniques.
- **Des frais.** De nombreux prestataires facturent chaque authentification.
- **Pas forcément rien dans le décompte des contestations.** Une contestation pour fraude sur un paiement authentifié peut ne rien coûter au marchand, mais demandez à votre prestataire si elle compte tout de même dans le taux de surveillance du réseau.

Bien s'en servir

1. **Authentifiez là où se trouve le risque de fraude.** Les commandes de montant élevé, les nouveaux clients et les comportements inhabituels sont les cas où le transfert justifie son coût.
2. **Utilisez les exemptions de façon délibérée.** Éviter le contrôle pour un client régulier à faible risque améliore la conversion, mais vous choisissez alors de porter le risque de fraude sur ce paiement.

3. **Envoyez des données complètes.** L'adresse de facturation, l'e-mail, les informations sur l'appareil et l'historique des commandes aident l'émetteur à approuver sans challenge.
4. **Conservez le résultat.** Le résultat de l'authentification est la preuve si une contestation pour fraude est tout de même déposée.
5. **N'y voyez pas un remède aux chargebacks.** Si la plupart de vos contestations portent sur la livraison ou les résiliations, l'authentification ne les réduira pas.

La question à poser à votre prestataire

Pour chaque type de paiement que vous acceptez, premier achat, renouvellement, achat répété en un clic et paiement exempté, demandez qui supporte une contestation pour fraude. La réponse diffère pour chacun, et le marchand qui suppose une seule réponse pour tous l'apprend par un chargeback.

Sources

- [Checkout.com : les transferts de responsabilité dans les paiements](#) (en anglais)
- [Ravelin : le transfert de responsabilité pour les chargebacks](#) (en anglais)
- [PCI Proxy : le transfert de responsabilité 3-D Secure expliqué](#) (en anglais)

Lire en ligne : <https://payments-marketplace.com/fr-FR/insights/3d-secure-liability-shift/>

Payments Marketplace Ltd

Registered in England & Wales No. 17424288

Garden Ctg, Dereham Road, Dereham, Norfolk, NR19 2PW, UK

connect@payments-marketplace.com · +44 1366 727140