WORLDLINE

Payments to grow your world

Bonnes pratiques 3-D Secure

7 conseils pour les commerçants en ligne

Dans le cadre de la deuxième directive européenne sur les services de paiement DSP2, les organisations de cartes exigent que tous les commerçants en ligne de l'UE et de la Suisse se conforment à la norme de sécurité 3-D Secure (3DS) pour le traitement des paiements dans le commerce électronique. Suivez nos 7 conseils pour prévenir la fraude, augmenter les taux de conversation et réduire les coûts.

#1 Demander des exemptions par l'intermédiaire de 3DS Server pour sauter des étapes de sécurité supplémentaires

Comment ça fonctionne	Parfois, vous pouvez vous passer du contrôle de sécurité supplémentaire lorsque les clients effectuent un achat. Cette action est appelée exemption. Vous demandez ces exemptions par l'intermédiaire de votre 3-D Secure Server, qui vous aide à déterminer quelles transactions sont suffisamment sûres pour ne pas nécessiter d'étapes de sécurité supplémentaires.
Exemple concret	Imaginez qu'un client passe une commande de repas en ligne. Au lieu de leur demander d'entrer un code spécial ou un mot de passe, votre système peut reconnaître qu'il s'agit d'un achat à faible risque et le laisser passer sans autre forme de procès.
Avantages	**Augmentation des ventes :** avec moins de frictions, davantage de personnes sont disposées à effectuer leurs achats. **Des économies de coûts :** la diminution des contrôles de sécurité peut réduire les coûts de transaction. **Des caisses plus rapides :** les clients effectuent leurs achats plus rapidement, ce qui permet de leur offrir une expérience agréable et d'améliorer les performances de l'entreprise.
Disponibilité	Mastercard et Visa

#2 Utiliser les demandes « Information Only » pour Mastercard Insights

Comment ça fonctionne	Envoyez une demande 3DS à Mastercard avec tous les détails de paiement habituels, mais au lieu de demander une authentification complète, demandez uniquement des informations. Mastercard fournit alors une évaluation du risque qui aide la banque à décider si la transaction est sûre sans coûts supplémentaires.
Exemple concret	Imaginez qu'un client achète un livre dans votre boutique en ligne. Au lieu de passer par un contrôle de sécurité complet, vous demandez à Mastercard un score de risque basé sur les détails de la transaction. Mastercard renvoie un score que la banque utilise pour approuver ou refuser le paiement.
Avantages	**Des décisions éclairées :** la banque reçoit des informations utiles pour prendre de meilleures décisions concernant l'approbation des transactions. **La flexibilité :** utilisez cette approche pour les transactions qui ne nécessitent pas de contrôles de sécurité stricts. **Des coûts moins élevés :** évitez les frais supplémentaires en évitant le contrôle de sécurité complet.
Disponibilité	Mastercard

#3 Utiliser 3DS pour Merchant Initiated Transactions (MIT)

Comment ça fonctionne	Lorsqu'un client effectue un premier achat, enregistrez les détails d'authentification tels que le montant, l'horodatage et l'identifiant de la transaction. Pour les paiements ultérieurs, envoyez ces informations à votre 3DS Server. Si le paiement est approuvé, vous recevez un code spécial à inclure dans la demande de paiement.
Exemple concret	Imaginez qu'un client s'abonne à un service mensuel sur votre site. Pour le premier paiement, vous enregistrez les données de sécurité. Pour les mensualités suivantes, vous utilisez ces données enregistrées pour vous assurer que les paiements sont sécurisés et pour transférer la responsabilité à la banque.
Avantages	**Protection supplémentaire :** vous bénéficiez d'une protection de la responsabilité pour les paiements futurs. **Des économies de coûts :** évitez les frais supplémentaires en utilisant les données de sécurité enregistrées. **Des paiements sans heurts :** assurez un traitement fluide des paiements futurs sans avoir à ré-authentifier le client.
Disponibilité	Mastercard

#4 Améliorer la qualité des données

Comment ça fonctionne	EMV 3DS vous permet d'envoyer de nombreuses informations détaillées sur le client et la transaction. Plus ces données sont précises et complètes, mieux la banque peut évaluer le risque de la transaction.
Exemple concret	Imaginez qu'un client achète un ordinateur portable dans votre boutique en ligne. En envoyant des informations détaillées telles que le nom, l'adresse, l'adresse électronique et l'historique des achats du client, la banque peut mieux évaluer le risque et probablement approuver la transaction sans demander de contrôles de sécurité supplémentaires.
Avantages	**Des paiements sans heurts :** les clients sont moins interrompus, ce qui augmente leur satisfaction. **Protection de la responsabilité :** de meilleures données permettent de transférer la responsabilité à la banque, ce qui vous protège contre la fraude. **Des taux d'approbation plus élevés :** les banques peuvent prendre de meilleures décisions, ce qui se traduit par un plus grand nombre de transactions approuvées.
Disponibilité	Mastercard et Visa

#5 Utiliser la redirection hors bande

Comment ça fonctionne	Lorsqu'un contrôle de sécurité 3DS est nécessaire, votre application peut automatiquement rediriger le client vers l'application de sa banque pour l'authentification. Cela simplifie le processus pour le client.
Exemple concret	Imaginez qu'un client achète des chaussures dans votre boutique en ligne. Lorsqu'il arrive à l'étape du paiement et doit vérifier son identité, votre application ouvre automatiquement l'application de sa banque où il peut approuver la transaction. Après approbation, il est renvoyé vers votre application pour finaliser l'achat.
Avantages	**Des taux de réussite plus élevés :** plus de clients effectuent leurs achats avec succès et sans erreur. **Une meilleure expérience client :** le processus est plus fluide et moins déroutant, en particulier pour ceux qui ne sont pas familiarisés avec les paiements en ligne. **Moins d'échecs :** réduit les problèmes tels que les échecs d'authentification ou les dépassements de délai, ce qui rend le processus de paiement plus fiable.
Disponibilité	EMV 3DS 2.2

#6 Utiliser Method URL pour la collecte des données

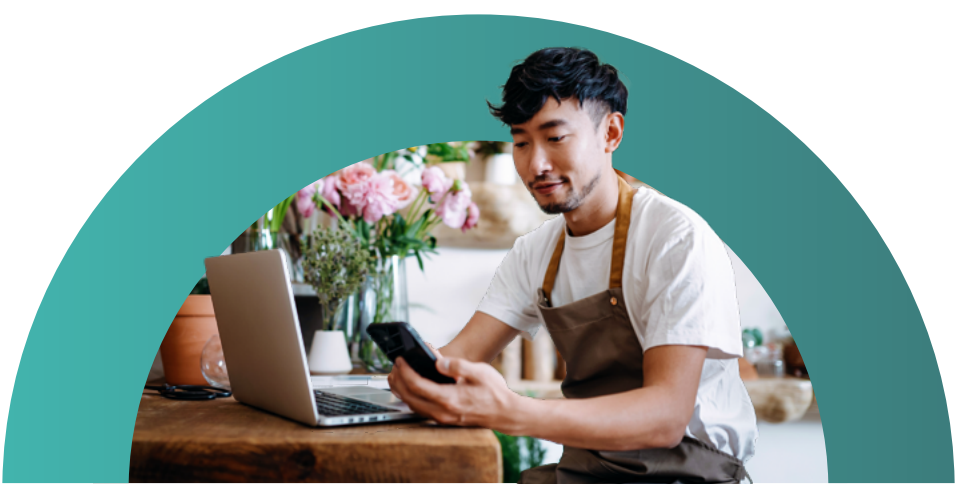
Comment ça fonctionne	Avant l'étape d'authentification, le système ACS (le système de sécurité de la banque) fournit une URL par l'intermédiaire du 3DS Server qui collecte de manière transparente des données supplémentaires à partir du navigateur du consommateur. Cette étape permet de rassembler les informations nécessaires à l'évaluation du risque de la transaction.
Exemple concret	Imaginez qu'un client achète un nouveau gadget en ligne. Avant qu'il n'ait besoin d'authentifier un achat, une étape cachée collecte des données à partir de son navigateur. Ces données permettent à la banque de décider que l'achat est sûr, de sorte que le client n'a pas besoin de passer par des étapes supplémentaires.
Avantages	**Une expérience utilisateur transparente :** les consommateurs bénéficient d'un processus de paiement fluide sans être soumis à des messages de sécurité supplémentaires. **Une amélioration de l'évaluation des risques :** les émetteurs peuvent effectuer des évaluations de risque plus précises en utilisant les données collectées, ce qui réduit le nombre de contestations inutiles. **Une augmentation des taux de conversion :** en réduisant le nombre de problèmes d'authentification, davantage de transactions sont effectuées avec succès, ce qui stimule les ventes.
Disponibilité	Émetteurs de cartes Mastercard et Visa pour le flux de navigation 3DS

#7a Utiliser l'authentification forte du client (Strong Customer Authentication SCA) – option Mastercard

Comment ça fonctionne	Avec la délégation SCA, si votre entreprise dispose d'une solution SCA conforme, vous pouvez contourner le processus 3DS. Cela signifie que l'authentification est gérée par vous, le commerçant, plutôt que par l'émetteur. Toutefois, étant donné que l'émetteur n'effectue pas l'ACS, il n'y a pas de transfert de responsabilité. La délégation de l'ACS doit être demandée pour chaque autorisation par l'intermédiaire du Network Tokens Service et s'applique aux clients connus, mais pas aux clients invités.
Exemple concret	Imaginez qu'un client régulier achète un abonnement mensuel sur votre site Web. Comme vous disposez d'un système SCA conforme, vous pouvez gérer vous-même l'authentification, ce qui rend le processus transparent pour le client. Vous demandez la délégation de l'ACS pour cette transaction et l'émetteur l'autorise, sautant ainsi l'étape 3DS. Le client effectue l'achat rapidement, sans contrôle de sécurité supplémentaire.
Avantages	**Des paiements sans heurts :** les clients bénéficient d'une expérience de paiement fluide et rapide, sans étapes d'authentification supplémentaires. **Des relations de confiance :** pour les clients connus, le processus est plus rapide et plus efficace. **Une plus grande satisfaction des clients :** un processus transparent pour les clients connus, offrant une expérience d'achat plus rapide et plus efficace.
Disponibilité	Mastercard

#7b Utiliser l'authentification forte du client (Strong Customer Authentication SCA) – option Visa

Comment fonctionne Digital Authentication Framework (DAF)	Le DAF authentifie un justificatif de paiement spécifiquement pour un commerçant, plutôt que d'authentifier l'autorisation elle-même. Si le commerçant dispose d'une solution SCA conforme, il peut demander à utiliser le DAF par transaction. Cette demande peut être faite par l'intermédiaire du service de jetons de réseau ou du 3DS Server, généralement après l'authentification initiale par l'émetteur. La DAF peut être appliquée pour les clients connus, mais pas pour les passages à la caisse des invités.
Exemple concret	Un client régulier effectue un achat dans votre boutique en ligne en utilisant les informations d'identification de paiement qu'il a enregistrées. Votre application gère l'authentification de manière transparente dans l'environnement du commerçant à l'aide de DAF, ce qui permet d'éviter des étapes 3DS supplémentaires et de garantir une transaction rapide et sécurisée.
Avantages	**Une expérience de paiement sans friction :** si votre application peut exécuter le SCA, vous pouvez ignorer le 3DS pour les transactions éligibles, ce qui facilite le processus de paiement pour les clients. **Un déplacement potentiel de la responsabilité :** contrairement à la délégation de l'ACS, la DAF offre la possibilité d'un transfert de responsabilité sous certaines conditions, ce qui renforce la protection financière des commerçants. **Applicabilité aux MIT :** à partir de 2024, le DAF sera également disponible pour les transactions initiées par les marchands (MIT), ce qui permettra de rationaliser davantage les transactions sécurisées.
Disponibilité	Visa



Veuillez discuter de ces options avec votre partenaire PSP.
Pour toute autre question, n'hésitez pas à contacter notre service clientèle par e-mail : cs.ecom@worldline.com

Votre point de contact local se trouve à l'adresse suivante : **worldline.com/merchant-services/contacts**

110.1159.03 INT_FR/09.2024