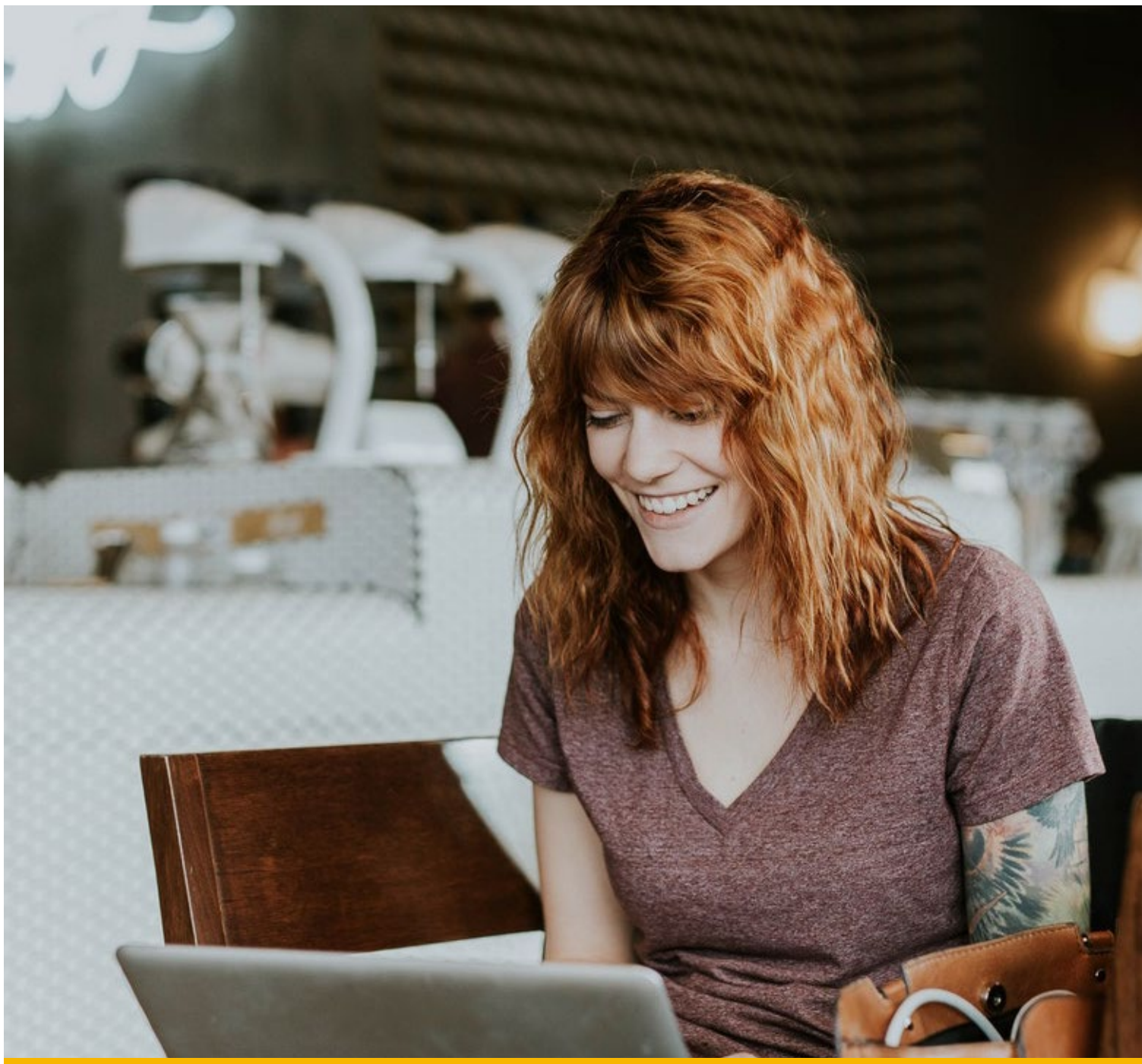


La prévention de la fraude à l'ère de l'authentification forte du client





L'authentification forte du client, Strong Customer Authentication (SCA) en anglais, deviendra une exigence réglementaire en septembre 2019. Le présent guide explique quand et comment celle-ci s'appliquera ; à qui incomberont les responsabilités et pourquoi l'authentification forte du client ne remplace pas les programmes de prévention de la fraude des commerçants.

Bien que la directive révisée sur les services de paiement (DSP2) soit entrée en vigueur en janvier 2016, avec des règles s'appliquant à partir de janvier 2018,¹ un certain nombre de mesures liées à la sécurité des transactions ne prendront effet que le 14 septembre 2019. L'une d'entre elles est l'authentification forte du client, une authentification à plusieurs facteurs conçue pour lutter contre les transactions frauduleuses.

L'authentification forte ne remplace pas la prévention de la fraude

L'introduction de l'authentification forte ne signifie pas que les commerçants peuvent arrêter d'analyser les risques de fraude. En empruntant cette voie, il est fort probable que vos taux de fraude augmentent, que vous soyez responsable ou non de la fraude pour une transaction donnée. En effet, la capacité d'un commerçant à influencer le recours à une analyse de risques en temps réel (permettant à certaines transactions d'être exemptées d'authentification forte) dépend du fait que son taux de fraude global soit inférieur à des seuils spécifiques. Si vous augmentez le taux de fraude moyen de votre acquéreur, vous pouvez vous attendre à ce qu'un plus grand nombre de transactions soit refusé ou soumis à une procédure d'authentification, et vous pourriez même faire l'objet de pénalités pour avoir enfreint les règles des réseaux de cartes.

¹ https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en

Introduction à l'authentification forte

Lorsque l'authentification forte du client entrera en vigueur, elle s'appliquera à toutes les transactions électroniques, à l'exception des transactions hors champ d'application et des transactions exemptées.

Les transactions situées hors du champ d'application de l'authentification forte

Les transactions suivantes se trouvent hors du champ d'application de l'authentification forte :

- Les transactions du canal MOTO² (commandes par e-mail et par téléphone)
- Les transactions initiées par les commerçants, telles que les prélèvements automatiques
- Les transactions « one leg out » (OLO)
- Les transactions récurrentes d'un même montant, après une première transaction réussie avec authentification forte

L'introduction de l'authentification forte n'affecte en rien ce type de transactions. Vous devrez non seulement maintenir un programme de prévention de la fraude efficace, mais aussi garder à l'esprit que lorsque la fraude deviendra plus difficile sur l'un de vos canaux, les fraudeurs migreront certainement vers un autre. Préparez-vous donc à expérimenter une augmentation du taux de fraude sur le canal MOTO lorsque l'authentification forte prendra effet.



Qu'est-ce que l'authentification forte du client ?

L'authentification forte, mesure de sécurité associée à la DSP2, permet de sécuriser le paiement d'une transaction électronique en demandant au consommateur de présenter au moins deux des éléments suivants :



Quelque chose qu'il connaît
(mot de passe, code PIN...)



Quelque chose qu'il possède
(générateur de tokens, téléphone portable, carte...)



Quelque chose qui le définit
(empreinte digitale, voix...)

² Voir glossaire en fin de document pour en savoir plus concernant les acronymes utilisés.

Cas d'exemptions de l'authentification forte

Les transactions situées dans le champ d'application de l'authentification forte peuvent parfois en être exemptées. Selon la DSP2, seuls les acquéreurs (PISP) et les émetteurs (ASPSP) peuvent exempter une transaction d'authentification forte. Les commerçants peuvent cependant influencer la décision de l'acquéreur (voir chapitre suivant).

Le tableau 1 présente trois exemptions clés de l'authentification forte.³

Tableau 1. Principaux cas d'exemptions de l'authentification forte

Exemption autorisée si	Exemption appliquée par
La valeur de la transaction est inférieure à 30 €. L'émetteur doit toutefois annuler cette exemption lorsqu'une carte : <ul style="list-style-type: none">• accumule cinq transactions sans authentification forte (l'authentification forte sera obligatoire lors de la sixième transaction)ou• atteint un montant cumulé de plus de 100 € sans authentification forte (une authentification forte remettra le compteur de la carte à zéro)	L'acquéreur (PISP), de sa propre initiative ou au nom du commerçant ou L'émetteur (ASPSP)
Le bénéficiaire a été inscrit sur une liste blanche par le client et sa banque.	L'émetteur (ASPSP)
Après analyse de risques en temps réel, l'acquéreur ou l'émetteur décide que l'authentification forte n'est pas nécessaire. L'analyse des risques ne peut s'appliquer qu'aux transactions de moins de 500 €.	L'acquéreur (PISP) ou L'émetteur (ASPSP)

Qu'est-ce que l'analyse de risques en temps réel ?

L'analyse des risques en temps réel, Transaction Risk Analysis (TRA) en anglais, ne s'applique qu'aux transactions de moins de 500 €. Les acquéreurs (PISP) et les émetteurs (ASPSP) ne peuvent appliquer une analyse de risques en temps réel que si leur niveau d'exposition global est inférieur à des taux de fraude spécifiques.

Valeur de la transaction (euros)	Taux de fraude maximal toléré pour bénéficier d'une exemption (%)	
	Paiements par carte à distance	Virements
250–500	0,01	0,005
100–250	0,06	0,010
0–100	0,13	0,015

L'analyse de risques en temps réel est déjà mise en œuvre par la plupart des fournisseurs 3D Secure au moment de déterminer si une transaction doit être soumise ou non à la procédure d'authentification 3D Secure.

³ Nous n'avons pas traité tous les cas d'exemption de l'authentification forte. Pour en consulter la liste exhaustive, voir : Directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication <https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1523371602118&uri=CELEX%3A32018R0389>

Comment influencer l'application d'exemptions ?

Selon la DSP2, seuls les acquéreurs (PISP) et les émetteurs (ASPS) peuvent appliquer des exemptions de l'authentification forte. Pour autant vous disposez de deux options pouvant potentiellement influencer les actions de votre acquéreur et de votre émetteur.

1. Décidez d'une stratégie d'exemption en collaboration avec votre acquéreur

Mettez-vous d'accord sur une stratégie d'exemption avec votre acquéreur afin de vous assurer que celui-ci respectera vos choix. Déterminez ensemble ce qui se passera non seulement lorsque vous voudrez qu'une exemption soit appliquée, mais aussi lorsque vous choisirez de ne pas bénéficier d'une exemption autorisée (par exemple, pour bénéficier d'un transfert de responsabilité).

Gardez à l'esprit que si votre acquéreur vous autorise à prendre des décisions en matière d'exemption, vous deviendrez probablement responsable des transactions concernées. Assurez-vous donc de maintenir un programme de détection de la fraude efficace. Il s'agit en quelque sorte du même scénario que celui de l'autorisation des transactions et du renoncement au transfert de responsabilité de 3D Secure : un programme de détection de la fraude efficace est le seul moyen de minimiser à la fois la fraude et la responsabilité pour ces transactions.

2. Prenez des responsabilités en matière d'analyse de risques en temps réel

Si vous disposez d'un programme de gestion de la fraude efficace, vous pouvez proposer à votre acquéreur de vous sous-traiter ses responsabilités en matière d'analyse de risques en temps réel. Si votre acquéreur accepte et qu'il respecte les seuils de fraude tolérés pour bénéficier d'une exemption et appliquer une analyse de risques en temps réel (voir ci-dessous), vous pourrez directement contrôler quand appliquer ou non une exemption à vos transactions.

Qu'en est-il de l'émetteur ?

Même lorsque votre acquéreur exempte une transaction, l'émetteur est en mesure d'annuler cette exemption (uniquement s'il existe une bonne raison de le faire). En pratique, les émetteurs peuvent toujours annuler l'exemption ; ils peuvent même mener leur propre analyse de risques en temps réel afin de prendre cette décision. Il est toutefois très peu probable que les émetteurs soumettent systématiquement et sans raison apparente les transactions à une procédure d'authentification forte étant donné que la perturbation de l'expérience client n'est pas dans leur intérêt non plus.

Le rôle d'un programme de détection de la fraude efficace

Bien que votre influence sur le comportement de l'émetteur soit indirecte, celle-ci est bien réelle. Il est très peu probable que vous rencontriez des difficultés imprévues liées à l'émetteur si :

- vous disposez d'un programme de détection de la fraude efficace, avec des taux de fraude faibles
- vous garantissez (en collaboration avec votre acquéreur) que les transactions à risque ne seront jamais exemptées

L'authentification forte et la responsabilité en matière de fraude

La DSP2 n'a pas le dernier mot en ce qui concerne l'assignation de la responsabilité en matière de fraude dans les différents scénarios potentiels. En effet, la spécification des conditions de responsabilité repose sur des accords entre les systèmes de cartes, les acquéreurs, les émetteurs et les commerçants.

Il est toutefois possible de formuler des hypothèses concernant le fonctionnement de la responsabilité en matière de fraude étant donné que les acquéreurs et les émetteurs utiliseront certainement 3D Secure en tant que processus d'analyse de risques en temps réel. Nos hypothèses sont présentées ci-dessous. Veuillez noter que ces informations ne visent en aucun cas à fournir de conseils juridiques.

Les transactions situées hors du champ d'application de l'authentification forte

Dans le cas des transactions hors champ d'application, 3D Secure restera une option pour le transfert de responsabilité.

Les transactions situées dans le champ d'application de l'authentification forte

La responsabilité pourra appartenir à l'acquéreur, à l'émetteur ou même au commerçant en fonction de la situation. Voir tableau 2.

Tableau 2. La responsabilité en matière de fraude pour les transactions situées dans le champ d'application de l'authentification forte

Situation	Qui est responsable ?	Explication
L'authentification forte du client a lieu (l'émetteur soumet la transaction à une procédure d'authentification forte)	L'émetteur	L'émetteur sera responsable étant donné que celui-ci est chargé de la mise en œuvre de l'authentification du client.
L'acquéreur n'applique pas d'exemption : <ul style="list-style-type: none">• passant outre la demande d'exemption du commerçant• à la demande du commerçant• de sa propre initiative si le commerçant n'exprime aucune préférence	L'émetteur	L'émetteur sera responsable qu'il soumette la transaction à une procédure d'authentification forte ou qu'il exempte cette transaction en raison d'une analyse des risques, d'une liste blanche ou autre.
L'acquéreur exempte une transaction	L'acquéreur déléguera probablement toute responsabilité au commerçant, à moins d'une entente contraire dans le contrat	Selon les règles du système, l'acquéreur choisira l'une des options suivantes : <ul style="list-style-type: none">• Exempter + autoriser⁴• Exempter + authentifier Dans les deux cas, si l'émetteur accepte sans soumettre la transaction à une procédure d'authentification forte, l'acquéreur sera responsable.

⁴ Si l'émetteur refuse, l'acquéreur formulera une nouvelle demande via l'option « exempter + authentifier ».

Analyser la fraude pour protéger votre marque

L'introduction de la DSP2 et de l'authentification forte du client ne changent en rien la nécessité pour les commerçants de protéger la réputation de leur marque ainsi que leur expérience client. Il est essentiel de maintenir un programme d'analyse de la fraude efficace à la fois pour les transactions situées dans et hors du champ d'application de l'authentification forte.

En bref, si vous n'examinez pas les risques de fraude, vous vous exposez à une augmentation de la fraude. Confier l'analyse de risques en temps réel aux acquéreurs et aux émetteurs ne sera pas plus efficace que le recours à 3D Secure. En réalité, vous restez le mieux placé pour mettre en œuvre une stratégie pertinente pour votre entreprise en tenant compte du comportement de vos clients sur tous vos canaux.

À l'ère de l'authentification forte, même lorsque vous n'êtes pas responsable de la fraude, votre taux de fraude jouera toujours en votre défaveur. D'ailleurs, les émetteurs

et les acquéreurs seront encore plus hostiles à l'égard des commerçants dont le taux de fraude augmente étant donné que leur capacité à utiliser l'analyse de risques en temps réel pour bénéficier d'une exemption dépend du maintien de taux de fraude faibles chez l'ensemble de leurs clients.

Si vous arrêtez d'analyser les risques de fraude, vous observerez très vite une augmentation du nombre de transactions refusées ou soumises à une procédure d'authentification forte. Les commerçants qui s'engagent sur cette voie ne pourront pas non plus s'étonner de perdre des clients.

Glossaire de termes clés

ASPSP prestataire de services de paiement gestionnaire de comptes (émetteur)

MOTO canal des commandes par e-mail et par téléphone

OLO « one leg out » une transaction est dite OLO lorsque l'une des conditions suivantes s'applique :

- La carte a été émise en dehors de l'UE
- La banque du client se trouve en dehors de l'UE (pour les virements)
- Le commerçant n'est pas domicilié dans l'UE

PISP prestataire de services d'initiation de paiement (acquéreur)

DPS2 directive révisée sur les services de paiement de l'UE, en vigueur depuis le 13 janvier 2018

Plus d'informations concernant l'authentification forte du client dans le cadre de la DSP2

Les informations contenues dans ce document concernant l'authentification forte du client dans le cadre de la DSP2 sont exactes en date du [insérer la date une fois le contenu finalisé]. Pour plus de détails, voir : Directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

Contactez-nous

Email. fr@cybersource.com www.cybersource.com

CyberSource est une plateforme de gestion des paiements internationale et modulaire intégrée aux infrastructures sécurisées de Visa et qui bénéficie des avantages et de l'expertise d'un réseau de traitement international d'une valeur de 427 milliards de dollars. Cette solution aide les entreprises à faire preuve d'agilité et à atteindre leurs objectifs en matière de commerce numérique en améliorant l'expérience client, en augmentant les revenus et en atténuant les risques. CyberSource offre à ses partenaires acquéreurs une plateforme technologique, une expertise en matière de paiements et un service d'assistance permettant à ces derniers de développer et de gérer leur portefeuille de commerçants afin d'être en mesure de tenir leurs promesses en tant que marques. Pour plus d'informations, rendez-vous sur www.cybersource.com

© 2018 CyberSource Corporation. Tous droits réservés.

CyberSource®
A Visa Solution