



VOS SERVICES AU QUOTIDIEN

Information PSD2

Services de paiement

Ce document d'information a pour objectif de vous expliquer simplement le fonctionnement et les apports de « PSD2 », acronyme faisant référence à la deuxième Directive¹ européenne traitant des services de paiement au sein de l'Union Européenne, et d'une manière générale à tout texte législatif ou réglementaire qui en découle.

Ce document a une portée exclusivement informative et vous êtes tenu de vous reporter à votre Contrat, en particulier aux Documents Annexes pertinents, pour connaître le détail des règles qui vous sont applicables. En particulier, des définitions, listées dans le Glossaire, viennent compléter votre Contrat et des développements ont été introduits dans les Documents Annexes concernés (ex : Opérations de Paiement, Banque en ligne, Cartes, etc.).

Vocabulaire

	anglais	français	concrètement
AISP	account information service provider	prestataire de services d'information sur les comptes	Banque ou fintech
ASPSP	account servicing payment service provider	prestataire de services de paiement gestionnaire du compte	Votre banque
PISP	payment initiation service provider	prestataire d'initiation de service de paiement	Banque ou fintech
PSU	payment service user	utilisateur de services de paiement	Vous
PSP	payment service provider	prestataire de services de paiement	Banque ou fintech
SCA	strong customer authentication	authentification forte du client	Moyen sécurisé

Personnes concernées

La PSD2 s'applique à ceux qu'on appelle les PSP, qui sont majoritairement des banques fournissant des services de paiement à leurs clients (ex : POST Finance avec vous). Cependant, d'autres prestataires sont également concernés par les exigences de la PSD2 comme les PISP, les AISP ou encore les établissements de monnaie électronique et les institutions de paiement. L'applicabilité de PSD2 dépend uniquement de la fourniture de service(s) de paiement et non de la nature des activités, du type de clients servis ou encore de la taille de l'institution.

Contenu

Informations : la PSD2 impose aux PSP d'être d'avantage transparents sur les informations qui sont communiquées aux PSU à propos des frais, des délais d'exécution des transactions, de l'utilisation d'instruments de paiement, des réclamations, de vos droits au remboursement, etc.

Transactions : grâce à l'entrée en vigueur de la PSD2, l'ensemble des PSP en Europe doivent, en principe, exécuter en un jour ouvrable (à compter de la date de réception de l'Ordre de Paiement) les paiements qui ont lieu exclusivement au sein de l'Union Européenne et dans une monnaie européenne. De façon générale, les délais d'exécution et de mise à disposition des fonds sont réduits.

Responsabilité : la PSD2 renforce la responsabilité des PSP vis-à-vis de la bonne exécution des opérations de paiement.

Remboursements : les PSU voient leurs conditions de remboursement d'opérations de paiement améliorées.

Incidents : tout incident considéré comme étant majeur devra être reporté directement à l'autorité compétente (pour le Luxembourg, il s'agit de la CSSF²) et le PSP concerné devra avertir le PSU dans le cas où l'incident pourrait avoir des répercussions sur ses intérêts financiers.

Fraudes : en imposant de nouvelles obligations relatives au risque, à la sécurité, la surveillance et la notification de statistiques liées aux fraudes, la PSD2 a pour but d'aider les PSP à mieux vous protéger contre les fraudes. Afin de les limiter, PSD2 impose également aux ASPSP de mettre en place une authentification forte de leur PSU pour tout accès à distance aux informations au compte ou initiation de paiement.

L'authentification forte

L'authentification forte est un moyen de d'authentifier le PSU qui se base sur au moins deux des trois éléments d'authentification suivants :

¹ Directive UE 2015/2366 du 25 novembre 2015

² [Commission de Surveillance du Secteur Financier](#)

- la possession (ex : une clef électronique/token);
- la connaissance (ex : un mot de passe);
- l'inhérence (ex : l'empreinte digitale, tout élément biométrique).

Ces éléments doivent être indépendants afin que la compromission de l'un n'affecte pas la fiabilité de l'autre. La combinaison de deux de ces éléments donne lieu à la génération d'un code d'authentification qui n'est accepté qu'une seule fois.

Lorsque l'authentification forte est utilisée à des fins d'initiation de paiement, le code d'authentification est dynamiquement lié au montant et au bénéficiaire du paiement.

POST Finance fournit une authentification forte grâce à la solution LuxTrust.

L'authentification forte est requise lorsqu'un PSU (ou un PISP ou AISP qu'il a mandaté):

- accède à son compte de paiement en ligne;
- initie une opération de paiement électronique ; ou
- exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

Sous certaines conditions, certains accès ou initiations d'opérations de paiement peuvent néanmoins être exemptés d'authentification forte, comme par exemple :

- L'accès au solde d'un ou plusieurs comptes de paiement et à l'historique des transactions datant de moins de 90 jours ;
- L'initiation d'un paiement vers un bénéficiaire de confiance ;
- L'initiation d'un paiement à faible valeur ;
- L'initiation d'un paiement vers un compte propre ;
- L'initiation d'un paiement considéré comme étant à faible risque.

Nouveaux acteurs

La PSD2 introduit principalement deux nouveaux types d'acteurs (les PISP et AISP) régulés et supervisés (par la CSSF ou par une autre autorité compétente de l'UE) sur le marché des paiements, qui peuvent initier des paiements à partir de ou accéder à des informations sur les comptes de PSU détenus auprès d'un autre PSP (qui est alors désigné comme un ASPSP) :

Ce sont des prestataires qui, avec le consentement explicite et préalable du PSU :

- (**PISP**) initie des opérations de paiement à partir d'un compte de paiement détenu auprès d'une autre entité (ex. une banque) ; ou
- (**AISP**) collectent des informations sur un ou plusieurs comptes de paiement détenu(s) auprès d'une ou plusieurs autres entités (ex : les agrégateurs de comptes).

Révocation d'un ordre de paiement

Le PSU ne peut révoquer un ordre de paiement après la réception de celui-ci par un PSP. Lorsque l'ordre de Paiement est initié par un PISP ou via le bénéficiaire, un PSU ne peut révoquer l'ordre de paiement :

- une fois son accord donné au PISP pour initier l'opération de Paiement, ou
- après avoir transmis l'ordre de paiement au bénéficiaire dudit ordre de paiement, ou
- donné son consentement à l'exécution de l'ordre de paiement directement au bénéficiaire dudit ordre.

Responsabilité en cas d'opérations de paiement non autorisées

Lorsque l'opération de paiement est directement initiée par le PSU et qu'elle ne peut pas être considérée comme ayant été autorisée par le PSU, y compris lorsqu'il a eu recours à un PISP, le PSP/ASPSP du PSU rembourse au PSU le montant de l'opération de paiement immédiatement après avoir pris connaissance ou après en avoir été informé, sauf s'il a de bonnes raisons de soupçonner une fraude et qu'il communique ces raisons à l'autorité compétente.

Le PSU pourra être tenu de supporter les pertes liées à l'opération de paiement non-autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé ou détourné dans la limite de 50 euros à moins que cette perte ou ce vol ne lui soit pas imputable ou que l'opération initiée se soit faite dans le cadre d'une violation de l'obligation légale de mettre en œuvre une authentification forte par le PSP/ASPSP. En tout état de cause, le PSU sera tenu de supporter toutes les pertes liées à l'opération de paiement en cas de fraude de sa part.

Si le PISP se trouvait être responsable de l'opération de paiement non-autorisée, il indemniserait le PSP/ASPSP conformément à la Loi, ce processus étant étranger au PSU et étant traité exclusivement entre le PISP et l'ASPSP.

Responsabilité en cas de non-exécution, de mauvaise exécution ou d'exécution tardive d'opérations de paiement

Lorsque l'opération de paiement n'a pas été exécutée ou a été mal exécutée (y compris tardivement), et que le PSU a initié l'ordre de paiement, y compris lorsqu'il a eu recours à un PISP, le PSP/ASPSP du PSU lui rembourse le montant de l'opération de paiement non-exécutée ou mal exécutée, à condition que :

- la non-exécution ou la mauvaise exécution ne soit pas due à la fourniture par le PSU d'un identifiant unique inexact ;
- la non-exécution ou la mauvaise exécution ne soit pas due à un cas de force majeure ; et
- le PSU ait notifié le PSP/ASPSP de la non-exécution ou la mauvaise exécution selon les procédures mises en place par le PSP/ASPSP.

Si le PSP/ASPSP du PSU prouve que le bénéficiaire de l'opération de paiement a reçu les fonds, c'est cependant le PSP du bénéficiaire qui est responsable.

Si le PISP se trouvait être responsable de l'opération de paiement non-exécutée ou mal exécutée, il indemniserait le PSP/ASPSP conformément à la Loi, ce processus étant étranger au PSU et étant traité exclusivement entre le PISP et l'ASPSP.

Les impacts sur vos Services

Initiation de paiement et information sur les comptes : nouveaux services ?

Non. Vous avez déjà accès à ces services d'initiation de paiement et d'information sur les comptes, puisque vous pouvez accéder aux informations de votre Compte POST Finance et initier des paiements via la Banque en ligne de POST Finance. La nouveauté vient du fait que désormais que POST Finance et des entités régulées peuvent également vous proposer ces services d'initiation et d'information en relation avec votre Compte détenu chez POST Finance et chez d'autres ASPSP / TPP utilisant les services de LUXHUB. Toutefois vous devez avoir activé votre accès à la Banque en ligne pour pouvoir bénéficier de ces services et POST Finance n'est pas responsable si tel n'est pas le cas.

Vous pouvez utiliser les services d'initiation de paiement et d'information sur les comptes fournis par des PISP ou AISP dûment autorisés à cet effet au Luxembourg ou dans un autre Etat Membre de l'UE en relation avec votre Compte dans les livres de POST Finance.

Vous avez le droit au même niveau de services que vous passiez directement par la Banque en ligne de POST Finance ou par les AISP/PISP.

Et vos comptes détenus ailleurs ?

POST Finance peut vous proposer une nouvelle fonctionnalité d'agrégation de comptes de paiement externes et d'initiation de paiement à partir de ces comptes. Elle agit alors elle-même en tant qu'AISP et/ou PISP. Vous pouvez alors bénéficier de deux nouveaux services : Service d'Initiation de Paiement et le Service d'Information sur les Comptes que vous détenez auprès d'autres établissements financiers. Ainsi, en vous connectant à votre application de Banque en ligne POST Finance et après donné votre consentement, vous pouvez depuis vos comptes de paiement détenus dans un autre établissement financier, initier des paiements et consulter des informations sur vos Comptes POST Finance et sur ceux dudit établissement financier. POST Finance peut décider de retirer un établissement bancaire de sa liste ou mettre fin au service d'agrégation de comptes sans avoir à s'en justifier. Afin d'améliorer le fonctionnement du service d'agrégation de comptes et d'en assurer la maintenance, POST Finance peut, par ailleurs, en suspendre l'accès pour une période déterminée et sans préavis.

Vous pouvez à tout moment modifier le paramétrage (afficher ou masquer les comptes de votre choix, supprimer les établissements financiers ajoutés, ou désactiver le service d'agrégation de comptes. La liste des établissements financiers concernés sera disponible dans votre application Banque en ligne de POST Finance.