POINT SUR LA DIRECTIVE SERVICES DE PAIEMENT (DSP2)

Date de publication : **27/12/2019 - Banque/argent**

La 2ème directive 2015/2366 du 25 novembre 2015 relative aux services de paiement dans le marché intérieur (DSP2) actualise le cadre règlementaire des paiements en Europe en renforçant le niveau de sécurité des paiements et la protection des clients. Elle intègre et abroge la première directive 2007/64 du 13 novembre 2007 sur les services de paiement (DSP1). **La directive DSP1 du 13 novembre 2007** avait permis 3 choses **:**

- **l'accélération du développement d'un espace unique de paiements en euros au sein de l'Union européenne (SEPA)** afin de faciliter l'exécution des paiements,
- l'introduction du **statut de prestataire de services de paiement (PSP)** qui a permis aux nouvelles sociétés non bancaires d'effectuer des transactions financières. Ces PSP ont pris la forme d'établissements de paiement, d'établissements de monnaie électronique ou d'établissements de crédit. Des établissements de paiement (Western Union, Compte Nickel...) ont ainsi pu effectuer des opérations de services de paiement (virements, prélèvement, transmission de fonds...). Avant, seules les banques et les banques centrales ou les agences gouvernementales fournissaient des services de paiement,
- **la transparence** des banques et des autres prestataires de services de paiement **sur leurs services et leurs frais** , y compris sur les délais maximum d'exécution des paiements, les taux de change.

Mais cela était insuffisant pour régir l'apparition de nouveaux types de services de paiement, et le développement des paiements électroniques et mobiles.

La directive DSP2 a comblé les lacunes et a instauré de nouvelles règles intéressant les consommateurs, notamment :

- **un abaissement de la franchise de 150 euros à 50 euros restant à la charge du client** en cas de paiement frauduleux par carte avant opposition pour perte ou vol de la carte,
- **l'obligation d'une authentification forte pour les paiements en ligne de plus de 30 euros,**
- la reconnaissance **de nouveaux services de paiement et de deux nouveaux acteurs** en charge de les assurer : les prestataires de services d'information sur les comptes, et les prestataires de services d'initiation de paiement ;
- l'ouverture du marché à de nouveaux acteurs en donnant **accès aux informations** sur les comptes par un canal de communication sécurisé ;
- **la légalisation du cash back** c'est-à-dire la possibilité de retirer des espèces chez un commerçant au moment d'un paiement par carte bancaire.

Les dispositions de la directive DSP2 s'appliquent aux services de paiement fournis sur le "territoire économique européen" c'est-à-dire celui des 28 Etats membres de l'Union européenne auxquels s'ajoutent l'Islande, le Liechtenstein et la Norvège par au moins un prestataire de services de paiement, et ce quel que soit la monnaie utilisée. Le rattachement avec ce territoire se définit par rapport à la situation du siège des prestataires et non par rapport au domicile ou à la résidence des utilisateurs.

La directive a été transposée en droit français, de manière échelonnée, par la loi n°2016-1321 du 7 octobre 2016 pour une république numérique et par l'ordonnance n°2017-1252 du 9 août 2017. Elle est entrée en vigueur le 13 janvier 2018, mais un délai de 18 mois - jusqu'au 14 septembre 2019 - a été accordé aux établissements de crédit pour mettre au point des interfaces de programmation (API - application programming interface). Cette date a été reportée au 31 décembre 2020.

Cet article fait le point sur la mise en oeuvre de la directive.

1 - Un abaissement de la franchise restant charge du client
Depuis janvier 2018, pour les opérations frauduleuses effectuées par carte bancaire avant opposition, à la suite du vol ou de la perte de la carte, **une franchise de 50 euros** reste à la charge du client si le code confidentiel a été utilisé. Cette franchise était auparavant de 150 €.

Cette franchise ne s'applique pas :

- s'il n'y a pas eu utilisation du code confiidentiel,
- si la perte, le vol ou l'utilisation frauduleuse de la carte ne pouvait pas être détecté avant le débit frauduleux.

Des délais plus courts de remboursement et un droit au remboursement inconditionnel pour les prélèvements en euros sont prévus. La banque doit rembourser au plus tard **un jour ouvré** après la notification de l'utilisation frauduleuse, sauf si elle suppose une fraude de la part de l'utilisateur.
Pour en savoir plus, consultez la fiche pratique INC "La carte bancaire".

2 - l'obligation d'une authentification forte pour les paiements en ligne de plus de 30 euros
Il est constaté une croissance du nombre de risques : le nombre de cyberattaques a augmenté de 32 % en 2018 (source F-Secure mars 2019). La sécurité est une préoccupation majeure et essentielle au fonctionnement des activités économiques et du commerce électronique.

Aussi, de nouvelles solutions concernant le renforcement de la sécurité des moyens de paiement en ligne sont prévues, et ont pour objet de généraliser une authentification forte du client pour les paiements électroniques de plus de 30 euros afin de limiter les risques de fraude.

L'authentification forte repose **sur deux éléments** ou plus d'authentification parmi les 3 suivants :

- **connaissance** (quelque chose que seul l'utilisateur connait) : mot de passe, information personnelle,
- **possession** (quelque chose que seul l'utilisateur possède) : un ordinateur, un téléphone,
- **inhérence** (quelque chose que l'utilisateur est) : reconnaissance faciale, rétinienne ou vocale (empreinte digitale).

L'authentification forte est requise pour :

- l'accès au compte de paiement en ligne,
- une opération de paiement électronique (virement, paiement par carte),
- une action exécutée par un mode de communication à distance qui présente un risque de fraude.

Des dérogations à l'authentification forte sont limitativement prévues par la directive car considérés comme peu risquées, notamment le paiement aux automates de transport et de parking, le paiement de faible montant sans contact ou à distance.

Les dispositions relatives à la sécurité de cette directive sont entrées en vigueur depuis le 14 septembre 2019. Cette date d'échéance a été reportée et l'Observatoire de la sécurité des moyens de paiement a élaboré un plan de migration national en deux temps.

Dans un premier temps, d'ici décembre 2020, il est prévu de remplacer de manière progressive, le recours aux codes SMS à usage unique par des solutions plus sûres comme la saisie d'un code confidentiel ou d'une empreinte biométrique à travers l'application mobile de banque en ligne.
L'Autorité bancaire européenne a fixé au 31 décembre 2020 la date butoir pour disposer de la mise en conformité des solutions d'authentification pour les paiements en ligne.

Dans un deuxième temps, d'ici mars 2021, une mise a jour de l'infrastructure 3d secure est prévue.

3 - l'apparition de deux nouveaux acteurs et services de paiement
La directive DSP2 amplifie la démonopolisation du système bancaire, amorcée avec la DSP1, et autorise **l'apparition de deux nouveaux acteurs** (article L. 314-1, II, 7° et 8° du code monétaire et financier) : **les prestataires de services d'information sur les comptes (PSIC**), et les prestataires de services d'initiation de paiement (PSIP) regroupés sous le terme TPP ("Third party providers").

Les premiers (PSIC) sont des agrégateurs rassemblant les informations bancaires des utilisateurs ayant plusieurs comptes de paiement sur une même plateforme et ayant pour mission de collecter des données et de les consolider : cela permet à l'utilisateur d'avoir une vue globale et actualisée de ses comptes, et d'améliorer la gestion de ses finances (article D.314-2-7° du code monétaire et financier).

Ils devront adresser une procédure d'enregistrement à l'Autorité de contrôle prudentiel.

Les seconds (PSIP) sont des initiateurs de paiement procédant à des opérations de paiement à la demande de l'utilisateur concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement et en faveur d'un bénéficiaire, tel qu'un paiement par virement sur internet. Il s'agit d'un paiement direct de compte à compte permettant de faire des achats en ligne sans passer par l'intermédiaire de la carte de paiement (article D. 314-2 du code monétaire et financier).

Ils devront obtenir **un agrément préalable**.

Les contrôles sont opérés par le pays où les nouveaux acteurs ont leur siège statutaire. En France, c'est l'Autorité de contôle prudentiel et de résolution (ACPR) qui est en charge de contrôler ces nouveaux acteurs.

Ces nouveaux services de paiement se greffent à un contrat déjà existant entre le client et son banquier.

L'utilisateur doit donner son consentement au libre accès à son compte à des prestataires autres que le banquier. **Le consentement devra être explicite à l'égard du PSIP** (article L. 133-40-I du code monétaire et financier) **et exprès à l'égard du PSIC**

(article L. 133-41-II-1° du code monétaire et financier). Le consentement sera donné via les conventions de compte.

Le prestataire de services de paiement gestionnaire du compte (le banquier) peut refuser à un prestataire de services de paiement fournissant un service d'information sur les comptes ou d'initiation de paiement l'accès à un compte de paiement **pour des raisons objectivement motivées ou documentées** liées à un accès non autorisé ou frauduleux au compte de paiement de la part de ce prestataire.

Le banquier ne pourra imposer un prestataire avec lequel il aurait établi un partenariat : **l'utilisateur peut s'adresser au prestataire de services de paiement de son choix**. L'article L. 112-13 du code monétaire et financier indique que lorsque le prestataire de services de paiement applique des frais pour l'utilisation d'un instrument de paiement donné, il en informe l'utilisateur de services de paiement avant l'initiation de l'opération de paiement.

La Banque de France s'assurera de la sécurité de l'accès aux comptes de paiement et à leurs informations dans le cadre de la fourniture des services des paiements (article L. 521-8 du code monétaire et financier). La CNIL et l'ACPR participeront aussi à la sécurité.

4 - L'accès aux informations

La DSP 2 oblige les prestataires de service de paiement gestionnaires de compte (les banques) à fournir l'accès aux données de leurs clients (avec leur accord) à des acteurs tiers tels que les initiateurs de services de paiement (appelées PSIP) ou les prestataires de services d'information sur les comptes (les agrégateurs). **Les clients devront consentir à l'accès, à l'utilisation et au traitement de ces données**.

Auparavant, les clients devaient transmettre leurs codes d'accès et leurs identifiants à ces TPP : il y avait donc un risque dans la circulation des données bancaires et identifiants.

Les données du compte bancaire doivent être protégées et leur utilisation est encadrée : elles ne doivent pas être utilisées, consultées ou stockées à des fins autres que la fourniture du service d'initiation de paiement ou la fourniture du service d'information sur les comptes expressément demandés par l'utilisateur de service de paiement.

Les données transmises doivent l'être via des canaux sécurisés (API) et ne doivent concerner que les données nécessaires pour fournir le service d'initiation de paiement (article L. 133-40, II, 6° du code monétaire et financier). Le PSIC n'accède qu'aux informations provenant des comptes de paiement désignés par l'utilisateur et des opérations de paiement associées (article L. 133-40, II, 4° du code monétaire et financier). Ces API doivent permettre aux entreprises fournissant certains services de paiement (fintechs) d'accéder aux données des clients des établissements de crédit de manière contrôlée et sécurisée.

Les données des comptes de paiement des clients seront accessibles gratuitement dans le cadre du service d'information sur les comptes (service d'agrégation de données), et du service d'initiation de paiement (transmission de paiement).

5 - la légalisation du cash back

Il s'agit de la possibilité de retirer des espèces chez un commerçant au moment d'un paiement par carte bancaire.

Les articles L. 112- 14 et D. 112-6 du code monétaire et financier prévoient que le montant minimum du cash back est fixé à 1 € et le montant maximum est de 60 €. Un **affichage obligatoire** est prévu au niveau du lieu d'encaissement pour informer le consommateur de cette possibilité et du caractère gratuit ou non de l'opération. Si cela est payant, il doit indiquer les frais et commissions perçus.

Le non-respect de ces prescriptions peut avoir pour effet une contravention de la 5e classe (1 500 €).

Pour en savoir plus, consultez l'article "Le cash back, comment cela marche ?"

Corinne Lamoussière-Pouvreau

Juriste à l'Institut national de la consommation