L’actualité juridique du secteur du paiement

+ Mise en perspective

(période 1er trimestre 2023)

Plénière *France Payment Forum* – 20 avril 2023

SOMMAIRE

01

ACTUALITÉ JURISPRUDENTIELLE

A. Qu’est ce qu’une opération autorisée?

B. Devoir de vigilance du PSP

I\ Actualité jurisprudentielle

A - Arrêt de la Cour de cassation du 30 novembre 2022 – revue ch. com. mars 2023

Problématique: une banque est-elle tenue de rembourser le porteur d'une carte de paiement si, après que celui-ci a introduit sa carte dans un DAB et composé son code confidentiel, un tiers saisit à son insu le montant du retrait et s'empare des billets ?

Une opération de paiement initiée par le payeur, qui donne un ordre de paiement à son PSP, est **réputée autorisée uniquement si le payeur a consenti au montant de l'opération**

Casse l'arrêt d'appel qui avait considéré qu'introduire la carte dans le DAB et composer le code secret ne permettait pas au porteur de la carte de solliciter le remboursement (*pas un cas d'exemption de la responsabilité du payeur*)

Pour mémoire, sur l'opération non autorisée (article 73 DSP2)

- Droit au remboursement (principe)
- A moins que :
  - Preuve que l'opération a été dûment autorisée et/ou
  - Client gravement négligent :
    - Preuve du lien de causalité entre la négligence et les pertes occasionnées :
      - l'émission de l'ordre de paiement a été rendue possible par la sa négligence grave
      - l'opération n'a pas été affectée par une déficience technique ou autre

Devoir de vigilance du PSP

B – La jurisprudence française sur le devoir de vigilance du PSP

- Une position historique de la Cour de cassation plutôt contre le devoir de vigilance du banquier sur les transferts de fonds à des personnes sur listes noires (ex: Diamants, Forex, CFD, FX, PSP, assurance, etc.) – Com 28 avril 2004: *la victime d'agissements frauduleux ne peut se prévaloir de l'inobservation des obligations de vigilance et de déclaration [LCB-FT] pour réclamer des dommages-intérêts à l'établissement financier*

- Confirmation avec Civ/Com 21 septembre 2022
- Résistance de CA Paris du 14 décembre 2022

la banque en sa qualité de teneur de compte de [son client] est tenue d'une obligation de vigilance la contraignant à vérifier les anomalies apparentes, matérielles ou intellectuelles, notamment d'un ordre de virement

- **A rapprocher** de CA Versailles du 4 avril 2023, dans lequel la cour considère que la banque *a manqué à son obligation générale de prudence en créditant le montant des virements frauduleux […] bien avant l'expiration du délai de 24 heures dont elle disposait contractuellement pour effectuer cette opération* [à une personne qui n'avait jamais été bénéficiaire et dont le statut de bénéficiaire a été contesté dans les 24 heures]

Les juges d'appel considèrent aussi que la banque n'a pas apporté la preuve que la fraude résulterait d'une intervention de la personne chargée des virements au sein de la société utilisatrice

02

ACTUALITÉ DSP2

A. RTS « Authentification forte » applicables au 25 juillet 2023
B. FAQs Commission (janvier 2023)
C. Etude d’impact du 2 février 2023

A- Modifications RTS - dérogation à l'authentification forte

Pour mémoire, les RTS finalement publiées en décembre 2022 et applicables au 25 juillet 2023 rendent:

(i) obligatoire la dérogation à l'authentification forte pendant 180 jours (au lieu de 90) en cas d'accès au compte via un prestataire d'information sur les comptes

(ii) optionnelle ladite authentification au client accédant directement à son compte pour exécuter des opérations de paiement vers des personnes déjà bénéficiaires d'opérations de paiement au cours des 90 jours précédents

La première évolution vient donner un coup d'accélérateur bienvenu aux agrégateurs de données alors que la seconde va révéler aux clients la volonté de simplification de leurs banques

B – FAQs Commission (janvier 2023)

Thématique sur l'authentification forte du client (la SCA) (1/2)

date question	date réponse	Solution
16/11 2020	31/01 2023	En commençant par l'inscription d'une carte de paiement à un portefeuille numérique, le processus conduit à la création d'un jeton ou d'une version numérisée de la carte de paiement qui nécessite l'application de la SCA, car il s'agit d'une action qui peut impliquer un risque de fraude ou d'autres abus. Le PSP vérifie ainsi que le PSU est l'utilisateur légitime de la carte de paiement et associe le PSU et la version numérisée de la carte de paiement à l'appareil concerné
24/05 2022	31/01 2023	L'émission d'un nouveau jeton, en remplacement d'un jeton existant, et sa liaison à un appareil/utilisateur nécessitent d'appliquer la SCA
31/08 2021	31/01 2023	Le déverrouillage d'un téléphone mobile à l'aide de données biométriques (par exemple, une empreinte digitale) ou à l'aide d'un code PIN/mot de passe ne doit pas être considéré comme un élément SCA valide pour l'ajout d'une carte de paiement à un *wallet* si le mécanisme de de l'appareil mobile n'est pas sous le contrôle de l'émetteur ou si le payeur n'a pas été associé précédemment, par l'intermédiaire d'un SCA, au justificatif utilisé pour déverrouiller le téléphone
12/05 2021	27/01 2023	Le PSP du bénéficiaire ne peut pas appliquer une exemption de la SCA lorsque le payeur initie un virement, même si l'opération est initiée par l'intermédiaire du bénéficiaire

B – FAQs Commission (janvier 2023)

Thématique sur l’authentification forte du client (la SCA) (2/2)

date question	date réponse	Solution
15/12 2021	06/01 2023	Lorsqu'un payeur demande à son PSP d'exécuter une opération de paiement par email, cette action est similaire à un paiement par correspondance. Le payeur ne procède pas à l'initiation du paiement proprement dit. Il ordonne seulement à son PSP d'initier et de traiter le paiement, en fournissant des instructions comprenant les informations nécessaires à la transaction. Le paiement est ensuite traité par un employé du PSP. Le payeur n'est donc pas dans la situation où il initie une transaction électronique qui devrait déclencher l'authentification forte
20/12 2021	27/01 2023	Toutes les procédures d'authentification mises à la disposition des utilisateurs par l'ASPSP dans les canaux de communication directe avec ses clients doivent être prises en charge (*supported*) lorsqu'un TPP intervient
06/10 2020	06/01 2023	Le paiement de factures par courrier postal n'entre pas dans la définition de l'exigence DSP2 relative aux moyens de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse et n'est donc pas soumis aux exigences de l'authentification forte
01/09 2021	27/01 2023	Le fait d'exiger des TPP qu'ils fournissent un numéro de téléphone mobile aux ASPSP pour l'envoi du mot de passe de décryptage par SMS est un obstacle répréhensible

B – FAQs Commission (janvier 2023)

Autres thématiques (1/2)

date question	date réponse	Solution
27/01/2020	06/01/2023	Différence entre le service d'acquisition d'ordres et la transmission de fonds dans le contexte du service de règlements de factures (*bill paying services*): • transmission de fonds: A la demande de payeurs, le PSP collecte puis remet leurs fonds à un créancier bénéficiaire sans jamais contracter avec ce dernier • acquisition: A la demande d'un créancier bénéficiaire (sur une base contractuelle), le PSP collecte et transmet à celui ci, sur une base quotidienne, le montant cumulé des fonds de divers payeurs sans contracter avec ceux-ci
19/05/2020	06/01/2023	L'EP peut protéger les fonds en combinant les deux méthodes de protection (50% par l'assurance et 50% par un compte de cantonnement). L'EP peut par exemple obtenir une assurance sur un montant de base et faire transiter le surplus par un compte de cantonnement
08/02/2021	06/01/2023	La Commission reconnait la possibilité pour un PSP d'intervenir dans un Etat C à partir d'une succursale ou d'un agent enregistrés dans un Etat B (passeport triangulaire) mais la responsabilité ultime de l'exécution du service revient au PSP (et non à l'agent ou à la succursale) et cela doit être également clairement indiqué aux utilisateurs finaux

B – FAQs Commission (janvier 2023)

Autres thématiques (2/2)

date question	date réponse	Solution
06/12/2021	06/01/2023	Même si le payeur n'a pas été en mesure de détecter la perte, le vol ou le détournement de son instrument avant qu'il ne soit utilisé (ex *phishing, skimming, hacking*), il n'est pas acceptable de considérer qu'il n'encoure aucune responsabilité s'il a agi avec négligence grave
23/02/2021	06/01/2023	Un compte de cantonnement doit être considéré comme un compte de paiement et ainsi être accessible via l'API de l'ASPSP dans la mesure où il concoure à la réalisation d'une opération de paiement. Le PSP qui utilise ce compte de cantonnement (mais pas les utilisateurs du PSP) peut donc y accéder via un TPP utilisant l'API de l'ASPSP. L'ASPSP a donc tort de s'opposer à cette demande du TPP (agissant pour le compte du PSP)
07/09/2020	06/01/2023	La DSP2 ne prévoit aucune exigence formelle sur les modalités de formalisation du consentement du payeur à un mandat de prélèvement (et sa modification correspondante). La possibilité pour le créancier bénéficiaire de modifier ce mandat résulte exclusivement des stipulations contractuelles
19/10/2021	06/01/2023	Au moment où les fonds propres sont calculés, généralement en fin de mois, l'"*année précédente*" visée dans la DSP2 est une période complète de douze mois précédant le moment du calcul (plutôt que l'année comptable précédente)

C - Analyse d’impact Commission Européenne

Début février 2023, la Commission européenne a rendu publique son analyse d’impact de la DSP2, notamment sur les sujets expressément visés par la clause de réexamen (article 108)

Attendue depuis le 13 janvier 2021, l’analyse comprend 4 parties:

- Une approche méthodologique
- Un aperçu des tendances de marché du secteur du paiement
- Les 6 sujets spécifiquement visés par la clause de réexamen
- Les résultats de l’évaluation de la DSP2 (analyse d’impact) fondés sur la pertinence, l’effectivité, l’efficacité et la cohérence de la DSP2

La Commission conclue cette analyse en formulant des recommandation autour de **trois piliers:**

- **Le champ d’application et les exclusions**
- **L’*open banking***
- **La protection des données / du consommateur**

C - Analyse d’impact Commission Européenne

Champ d’application et exclusions

- Volonté de combattre l’arbitrage règlementaire, en revisitant la gouvernance des autorités sur les divergences d’application
- Assurer la nécessaire coordination avec MICA, DORA et DMA en faisant cohabiter les nouveaux services avec ceux issus de la DSP2
- Fusionner la DSP2 et la DME2 pour éviter les situations où des services identiques sont alternativement couverts dans un EM sous la DSP2 et dans un autre EM sous la DME2, selon l’interprétation divergente conduite par les acteurs (EP, EME, autorités de supervision)
- Afin d’éviter les ambiguïtés tirées des composantes actuelles des « services de paiement », privilégier une description des principales caractéristiques de ces services par rapport à d'autres services financiers, ainsi que les services auxiliaires à l'exécution des paiements qui ne sont pas couverts par la DSP2
- Lever certaines ambiguïtés sur certains régimes d’exclusion (notamment sur l’agent commercial) et les conditions d’accès des EP/EME aux infrastructures de paiement

C - Analyse d’impact Commission Européenne

L’*open banking*

- Conférer à l’EPC une capacité normative pour établir des standards de marché rendus obligatoires (ex: normalisation des Codes QR ou encore des standards API, afin d’éviter la fragmentation du marché européen observée)

- Modifier l'article 97 de la DSP2 (sur la SCA) pour préciser que lorsqu’un PSU autorise un agrégateur à accéder à ses comptes, l’autorisation est valable en permanence jusqu'à ce que l'utilisateur révoque l'accès (l’autorisation ne devrait donc plus être soumise à une nouvelle authentification forte tous les 90 ou 180 jours)

- Définir un concept de "service de paiement" à trois niveaux basé sur i) le transfert et la garde d'actifs monétaires (c'est-à-dire de fonds) ainsi que ce qui est nécessaire pour envoyer ou recevoir des fonds, ii) le transfert et la garde de données associées aux transactions de paiement, iii) la gestion de plateformes de paiement;
- Cette nouvelle définition pourrait:
  - assimiler l'émission de monnaie électronique aux services de paiement; ou encore
  - inclure les prestataires de services de cryptoactifs dans le champ d'application de la DSP3

C - Analyse d'impact Commission Européenne

La protection des données / du consommateur

- Selon la Commission, la protection des consommateurs pourrait passer par:
  - La fixation de différents niveaux de protection et de responsabilité en fonction du degré de vulnérabilité du PSU (ex: les personnes âgées ou vulnérables)
  - Le traitement du fournisseur d'une licence en tant que service (mode SAAS) comme responsable de la garde/du transfert de fonds/données dans la relation avec l'autorité de supervision et la LCB-FT en tant qu'il a rendu possible l'activité commerciale en ligne du PSP utilisateur de sa licence
- La Commission entend également que soit assurée une meilleure coordination entre l'EBA et les autorités nationales en charge de la protection des données personnelles

Focus régime responsabilité

La Commission souligne que :

- les situations révélant la notion de **négligence grave** peuvent être comprises et appliquées différemment selon les sensibilités nationales
- Les acteurs du marché réclament un traitement différencié des paiements effectués par les **grandes sociétés**
- Il peut y avoir une confusion dans ce qui peut être considéré comme une **opération non autorisée**, ce qui donne un faux sentiment de sécurité au PSU qui croit que toute opération qu'il considère comme non autorisée sera remboursée quel que soit ses diligences sur la transaction
- Les données de l'EBA révèlent que les PSU ont supporté 68 % des pertes dues aux virements frauduleux

03

AUTRES ACTUALITÉS

Autres grands chantiers législatifs européens

Transpositions françaises (loi d’habilitation du 9 mars 2023), notamment de DORA & MiCA

Autres grands chantiers législatifs européens

Loi DDADUE

La **loi du 9 mars 2023** portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture (dite **DDADUE**) a été publiée au Journal officiel du 10 mars 2023.

Le secteur du paiement suivra les mesures législatives que Gouvernement est habilité à prendre pour prendre en compte de nombreux textes européens:

- le Règlement MiCA, avec l'ajustement nécessaire concernant les « PSAN » français (et un régime d'enregistrement renforcé pour les nouveaux entrants à compter du 1er juillet 2023)
- les différents textes associés au Règlement sur la résilience opérationnelle numérique du secteur financier (dit « DORA ») – le 6 février 2023, les Autorités européennes de supervision ont d'ailleurs traité des implications de DORA dans la perspective des normes techniques de réglementation (RTS) attendues
- la Directive sur l'accessibilité des produits et services, notamment financiers (2019/882), avec notamment l'obligation nouvelle imposée aux PSP de s'assurer que les méthodes d'authentification fournies à ses clients (ex: choix SCA) respectent les exigences d'accessibilité découlant de cette Directive

La Tour *International*

ALEXANDRE MARION

Avocat associé

alexandre.marion@latourinternational.com

+33 (0)1 42 25 91 69