CLUBBANQUE

REVUE BANQUE

« CLUB BANQUE » DU 29 février 2024

Paiements, fraudes, partage de données : la DSP3 rebat les cartes

Introduction

Florence GIULIANO, EMEA Financial Crimes Analytics Director, SAS

Le régime de responsabilités doit concerner tous les acteurs

Maya ATIG, Directrice générale, Fédération Bancaire Française

De la DSP2 à la DSP3, de nouveaux apports

Julien LASALLE, Secrétaire Général, Observatoire de la sécurité des moyens de paiement

Projecteurs sur le calendrier : s'investir et s'engager

Emmanuelle CHOUKROUN, Directrice des relations interbancaires, Société Générale

Table Ronde « Quel partage des données entre établissements financiers ? »

Richard EUDES, Directeur Data, Technology & Analytics, Deloitte

Questions/Réponses

INTRODUCTION

Florence GIULIANO, EMEA Financial Crimes Analytics Director, SAS

Bienvenue à la conférence de ce Club Banque. Je suis en charge des sujets liés à la fraude et à la criminalité financière au niveau européen. Nous explorerons les évolutions et les défis actuels dans le paysage financier. Nous nous concentrerons sur la directive des services de paiement et en particulier sur sa dernière version : la DSP3. Cette dernière représente une mise à jour significative des règlements précédents visant à promouvoir l'innovation, la compétitivité et la sécurité des paiements électroniques dans l'Union européenne. Nous verrons comment cette directive rebat les cartes et affecte nombre d'éléments. Le 28 juin 2023, la Commission européenne a présenté son projet de refonte de la DSP2 avec plusieurs objectifs :

- améliorer la lutte contre la fraude ;
- accroître la compétitivité des services d'*open banking* ;
- harmoniser les règles applicables au secteur bancaire pour favoriser la concurrence ;
- préserver le droit des consommateurs.

La révision prévoit deux textes de référence : la directive en elle-même (DSP3) et le règlement des services de paiement (RSP).

Il est procédé à un tour de présentation.

LE REGIME DE RESPONSABILITES DOIT CONCERNER TOUS LES ACTEURS

Maya ATIG, Directrice générale, Fédération Bancaire Française

Nous constatons sur les questions de fraude et de paiement que nous avons renforcé considérablement le plan technique. La DSP2 a mis en place l'authentification renforcée et les établissements s'imposent eux-mêmes des obligations. Par conséquent, les investissements informatiques et humains sont très nombreux, car la technologie doit relever le niveau de sécurité en permanence.

Les criminels déplacent ainsi le terrain de jeu. Ils ne peuvent plus utiliser des outils techniques. Ils utilisent donc l'ingénierie sociale à travers la manipulation.

De plus, les opérateurs télécoms constituent aujourd'hui un élément de la chaîne très utilisé par le monde de la fraude. Cet élément n'est pas suffisamment appréhendé aujourd'hui. Des initiatives sont néanmoins menées au niveau national. La loi Naegelen a été votée il y a quelques années. La DSP3 ne produit aucune incitation dans ce domaine. Cette faille constitue un élément manquant de la chaîne. En effet, la sécurisation des appels est indispensable.

Le deuxième élément insuffisamment appréhendé concerne la responsabilisation des clients. Les clients doivent être protégés et nous dépensons beaucoup d'énergie, d'argent et de moyens humains pour les protéger. Nous avons au niveau de la profession engagé une campagne relayée par beaucoup d'acteurs privés et certains acteurs associatifs.

Nous appliquons pleinement les dispositions de la DSP2 sur le remboursement. Les notions de négligence grave et les mécanismes de remboursement autorisé ne permettent pas de nous diriger vers une juste répartition et responsabilisation des clients dans la DSP3. Aujourd'hui, les cas de remboursements automatiques sont nombreux.

Il ne s'agit pas de revenir en arrière. Toutefois, si la DSP3 persiste à ne pas suffisamment préciser la notion de négligence grave et à augmenter certains cas de remboursement automatique, nous ne nous dirigerons pas vers une vigilance renforcée. Une personne insuffisamment vigilante peut être vulnérable à toute sorte d'escroquerie. Il s'agit de définir le plus précis équilibre entre un remboursement juste pour ne pas couvrir le cas de la négligence grave et ne pas créer une sorte de franchise de remboursement qui conduirait à une forme d'industrie organisée de la recherche de remboursement.

La DSP3 comporte de nombreux éléments positifs. Cependant, elle témoigne d'une insuffisante compréhension des mécanismes profonds de la fraude.

DE LA DSP2 A LA DSP3, DE NOUVEAUX APPORTS

Julien LASALLE, Secrétaire Général, Observatoire de la sécurité des moyens de paiement

Je souhaite vous présenter le point de vue du régulateur par rapport à la réglementation de la sécurité des paiements.

La DSP2 laisse deux héritages majeurs :

- la sécurisation des paiements électroniques, notamment des paiements en ligne : l'authentification forte et le recours à deux facteurs d'authentification ont contribué à renforcer la sécurité des transactions. Dans la mesure où l'authentification forte génère des frictions et des contraintes pour l'utilisateur, la DSP2 avait prévu d'adopter une approche en fonction du niveau de risque de façon systématique. Quand le niveau de risque d'une transaction est jugé suffisamment faible, il est possible de se passer d'authentification forte. L'émetteur assumera alors le risque associé à cette transaction. Les cas d'exemption sont strictement encadrés. La responsabilité reste confiée à la banque qui tient le compte et c'est elle seule qui peut déterminer si le niveau de risque est acceptable ;
- l'*open banking* : les banques sont aujourd'hui les premières consommatrices de ces solutions d'*open banking*. Il s'agissait de sortir du *web scraping* sauvage dans lequel des acteurs tiers collectaient les identifiants personnels. Aujourd'hui, des interfaces d'accès spécialisées sont en place avec des certificats qualifiés qui permettent de vérifier que l'entité qui se connecte dispose de l'autorisation nécessaire pour fournir ce type de service. Une dose d'authentification forte a été injectée pour s'assurer que l'utilisateur donne réellement son consentement à l'accès à son compte par le TPP. Le but était de créer un environnement de confiance pour l'échange de données.

Nous constatons que la mise en place de l'authentification forte a permis de réenclencher la baisse du taux de fraude des paiements par carte sur internet. Dans les années 2010, la baisse était très nette avec l'introduction de 3D Secure et de l'authentification par mot de passe (reçu par SMS principalement). Après 2018, nous sommes entrés dans une période de stagnation. La DSP2, avec l'introduction de l'authentification forte, le renforcement des mécanismes de suivi des taux de fraude et le *scoring,* a réamorcé de manière spectaculaire la baisse du taux de fraude en 2022. Ainsi, les gains en matière de lutte contre la fraude ont été significatifs.

Que pouvons-nous attendre aujourd'hui ? En matière de sécurité, cinq axes nous intéressent :

- le partage de données entre PSP : le projet de réglementation est flou à ce sujet. Les PSP ne doivent pas être isolés dans leur capacité à traiter des données, mais ils doivent pouvoir s'appuyer sur les enseignements des profils de fraude, par exemple des IBAN utilisés par les fraudeurs pour alimenter leur moteur de *scoring* ;
- qui est responsable de quoi ? : le prestataire de service de banque qui tient les comptes a un niveau de responsabilité très fort. Que supportent comme responsabilité les autres acteurs qui contribuent à la chaîne de paiement (prestataires techniques tiers, fournisseurs de *wallets*, opérateurs de téléphonie, etc.) quand la fraude relève de leur fait ? ;
- le remboursement des consommateurs en cas de manipulation par un tiers : la DSP2 était un peu floue sur cette question. L'Observatoire de la sécurité des moyens de paiement en France a recommandé aux établissements d'établir une introspection pour préciser la part de responsabilité de la victime et celle de l'établissement, et ce, pour déterminer si le mécanisme de remboursement doit être mis en œuvre. Nous souhaitons que les pratiques deviennent homogènes avec la DSP3 ;
- la clarification des notions d'autorisation et de négligence grave ;
- un tableau de bord des consentements accordés aux TPP et possibilité de radiation : l'utilisateur doit pouvoir avoir la main et révoquer ses consentements.

Les autres apports attendus sont :

- l'accès aux systèmes de paiement pour les établissements de paiement ;
- l'intégration de la monnaie électronique dans les services de paiement : le développement des services de paiement entraînait des difficultés à expliquer dans quels cas la qualification penchait vers la monnaie électronique et dans quels cas elle penchait vers un compte de paiement ;
- le développement des retraits d'espèces en point de vente : les acteurs qui souhaiteraient mutualiser leurs réseaux de points de distribution d'espèces chez des commerçants font aujourd'hui face à une incapacité juridique à le faire dans des conditions viables ;
- l'essor des services d'*open banking* : la future réglementation ouvre la porte à un *open banking* plus équilibré qui permettrait de proposer des services à valeur ajoutée via les API tout en assurant une juste rémunération des acteurs qui fournissent l'effort de proposer ces services.

Par ailleurs, la réglementation sur les paiements instantanés a été adoptée formellement par les colégislateurs. Elle comporte des dispositions en matière de sécurité, dont le service de confirmation d'IBAN qui relève d'un partage de données interbancaire.

PROJECTEURS SUR LE CALENDRIER : S'INVESTIR ET S'ENGAGER

Emmanuelle CHOUKROUN, Directrice des relations interbancaires, Société Générale

Le calendrier constitue une question très importante. Le calendrier a des chances de prendre du retard. Parmi les amendements déposés (plus de 400) et les propositions formulées, un certain nombre méritent des clarifications.

En mars 2024, nous saurons si la proposition du Parlement est adoptée. Les élections européennes se dérouleront en juin 2024. Aujourd'hui, les délais de mise en œuvre pour la partie la plus contraignante sont de l'ordre de 18 mois. Des normes techniques réglementaires avec leurs lots de contraintes interviendront respectivement un an et 18 mois après l'entrée en vigueur de PSR.

Parmi les normes techniques réglementaires figurent :

- le droit au compte ;
- une disposition sur l'obligation de disposer d'une interface spécifique sur l'accès aux données ;
- des règles relatives à l'authentification et les mécanismes de contrôle des opérations ;
- des obligations de *reporting* sur la partie *open banking* ;

Dans la DSP3, un pack concernera les sanctions. Nous sommes intrigués par l'article relatif aux astreintes. Il indique qu'en tant qu'acteur régulé par la DSP3, des astreintes peuvent monter jusqu'à 3% du chiffre d'affaires pendant six mois si l'établissement ne se met pas assez vite en conformité.

La partie la plus importante du calendrier est celle qui se joue en ce moment. En effet, c'est maintenant que nous posons les règles qui régiront l'industrie des paiements avec des enjeux communs pour les consommateurs et tous les acteurs qui dépendent des paiements.

Dans les dispositions de la DSP3 nous pourrions voir le risque de substituer une dépendance à une autre. Aujourd'hui, les particuliers utilisent de plus en plus leur mobile pour payer avec une utilisation de paiement mobile ou avec l'authentification forte. Cependant, notre niveau de souveraineté sur les constructeurs mobiles n'est pas très fort.

L'article 88 obligera les constructeurs de *device* à ajouter des éléments *software* ou *hardware* sur leurs appareils. Les enjeux sont doubles : l'enjeu utilisateur et l'enjeu commerçant.

Il faut également gérer les dépendances des avis des prestataires de service *cloud*.

De plus, il est nécessaire de ne pas réaliser des investissements qui se révèlent improductifs, et ce, dans le cas d'une contrainte de développement d'offres coûteuses et faiblement utilisées. Par exemple, en Pologne, nous avons développé une API DSP2 sur laquelle aucun TPP ne s'est *on-boardé.* Très souvent, nous observons des exigences qui imposent de développer une solution alors qu'il serait possible de se baser sur une expression de besoins et trouver une solution peu frugale et plus performante.

La coordination avec les différents intervenants de la chaîne transactionnelle interroge. Aujourd'hui, nous avons besoin d'inventer la manière dont ces acteurs coopéreront. Il faut vraiment attribuer les bonnes responsabilités aux bons acteurs.

Enfin, quelle stratégie de modération ? Nous observons à ce sujet deux grands axes :

- l'élaboration du texte et des normes techniques réglementaires : pour la DSP3, il est important de réaliser des études d'impact, car force est de constater qu'elles ont été peu nombreuses jusqu'à présent. Il est également nécessaire d'évaluer la viabilité des dispositions trans-sectorielles ;
- la phase de mise en œuvre : des questions se poseront inévitablement et des dispositions auront besoin d'être interprétées. Cela suppose une coopération agile entre l'Autorité Bancaire Européenne, les superviseurs des Etats membres et les acteurs de la chaîne de paiement.

TABLE RONDE : « QUEL PARTAGE DE DONNEES ENTRE ETABLISSEMENTS FINANCIERS ? »

Florence GIULIANO

Quels sont les ingrédients qui permettent l'établissement d'un calendrier performant de la DSP3 ?

Emmanuelle CHOUKROUN

Un calendrier est toujours trop juste. Il me paraît important d'instruire les points critiques. Il est essentiel de travailler sur un cadre protecteur pour l'échange de données. Il faut donc poser des règles claires et protectrices. Il n'est pas souhaitable d'exempter certains acteurs dans le cadre de questions industrielles par exemple.
Ainsi, la DSP3 est très riche. Pour chaque sujet, il est nécessaire de prendre le temps de l'instruction, laquelle doit également être proactive et suffisamment précise.

Florence GIULIANO

Le régulateur comprend-il ce point de vue ?

Julien LASALLE

En matière d'échange de données et de protection, de nombreuses attentes ont déjà été formulées par l'Observatoire des moyens de paiement. Les fondamentaux des établissements en matière de gestion des données et de traitement sont très bons au niveau des banques.

Quid des autres acteurs de la chaîne de paiement ? Ces acteurs agréés sont sujets à un certain nombre de contrôles préalables. Le traitement de la chaîne des paiements

transite par de nombreux acteurs non régulés. Quelque part, derrière l'ensemble des établissements régulés par la DSP2 se trouvent tout un tas d'acteurs sur lesquels il est nécessaire de porter une attention.

Florence GIULIANO

La mise en responsabilité des opérateurs de communication électronique vous paraît-elle positive ?

Emmanuelle CHOUKROUN

C'est un élément très positif. Dès lorsqu'ils interviennent dans la chaîne transactionnelle, les opérateurs ont une responsabilité. Cependant, la version du Parlement projette d'étendre la responsabilité des banques, quelle que soit l'entité concernée. Si le fraudeur usurpe l'identité d'une entité publique ou privée et que l'utilisateur du service de paiement est un consommateur, alors la banque doit rembourser. Un enjeu concerne donc la sécurisation. Pourquoi, en raison d'un défaut de sécurité, les banques paieraient-elles ? Il faut aller plus loin et s'assurer d'attribuer le bon niveau de responsabilité à chaque acteur.

Julien LASALLE

Nous avons mis entre les mains des consommateurs et des entreprises des moyens de paiement extrêmement sécurisés. Mais dans le même temps, nous évoluons dans un environnement où il n'est plus possible de faire confiance à l'origine des mails et aux SMS. Nous avons découvert que même la ligne téléphonique peut être également sujette à usurpation. Dans un environnement qui manque de confiance, les établissements bancaires et les prestataires de service de paiement sont devenus en quelque sorte un ilot de sécurité. Il faut étendre cela pour que les autres contributeurs au paiement puissent apporter le même niveau de sécurité. Des projets encourageants sont réalisés en ce sens. Dans le domaine de la communication, nous travaillons avec la Fédération française des Télécoms. Nous nous dirigeons vers une authentification des numéros d'appelants. Un travail a également été mené par les opérateurs pour nettoyer les mauvaises pratiques en ce qui concerne les SMS.

Florence GIULIANO

Quelles sont les difficultés dans l'instruction des dispositions de la DSP3 ?

Emmanuelle CHOUKROUN

Il faut prendre le temps d'instruire les obligations qui pèseront sur les banques et les acteurs qui interviennent dans la chaîne transactionnelle, et ce, de façon détaillée. Nous sommes allés très vite entre la proposition de la Commission européenne et l'extension de responsabilité.

Florence GIULIANO

Quelles sont les grandes tendances de la fraude post-DSP2 ?

Julien LASALLE

La fraude s'est engouffrée dans les angles morts de la DSP2. Le moyen de paiement papier tel que le chèque, n'étant pas couvert par la DSP2, reste le moyen de paiement

préféré des fraudeurs. C'est un ilot pour lequel la DSP3 ne changera pas la donne. Mais les pouvoirs publics français et l'Observatoire s'y attaquent fort heureusement.

Les fraudeurs ont constaté qu'il était difficile d'attaquer les mécanismes d'authentification moderne. Ils se sont donc attaqués aux porteurs avec des techniques de manipulation. Les fraudeurs doivent fournir beaucoup plus d'efforts pour un chiffre d'affaires plus faible.

Les proportions de fraudes sont très élevées sur les transactions émises par le bénéficiaire du paiement pour les paiements par carte (MIT) et les ordres de paiement passés par supports papier (MOTO). Ces paiements génèrent un bruit médiatique assez modeste, car il est difficile de démontrer que le paiement a été autorisé. Ces ilots ne sont pas couverts par la DSP2, car elle ne visait que les paiements électroniques émis par les payeurs. Nous attendons que la DSP3 sécurise les opérations qui s'apparentent à des prélèvements. Ces paiements n'ont pas un poids important dans les flux, mais représentent un poids disproportionné dans la fraude.

Florence GIULIANO

Les constructeurs mobiles sont-ils exclus de la DSP3 ?

Emmanuelle CHOUKROUN

L'article 88 impose aux constructeurs mobiles de permettre aux PSP de stocker des éléments logiciels ou matériels, et ce, pour permettre des transactions *off-line* et faire en sorte que certains acteurs ne s'arrogent pas un monopole.

Le taux de fraude sur les paiements mobiles de proximité est trois fois plus élevé que sur les paiements par carte de proximité. Cela est lié à un problème d'enrôlement frauduleux de la carte. Si nous utilisons ces terminaux mobiles comme des solutions d'acceptation, il faudra dès lors instruire ce volet dans la DSP3.

Florence GIULIANO

Comment les régulateurs discutent-ils avec les constructeurs américains ou chinois ?

Julien LASALLE

En pratique, un acteur comme Apple est facile à identifier et son pouvoir de traction sur le marché est connu. Dans le passé, la Banque de France a été amenée à convoquer l'entreprise américaine pour recevoir des explications sur Apple Pay. Aujourd'hui, Apple a anticipé cet aspect et a présenté la technologie associée à son service d'acceptation. Quand l'acteur est identifié et qu'il est possible d'échanger, la situation est rassurante d'autant plus que dans la négociation entre Apple et un PSP, le pouvoir de négociation du prestataire de service paiement, même quand il s'agit d'une grande banque, n'est pas aussi fort que ce que prévoit la réglementation pour les PSEE (prestataires de services essentiels externalisés). Il existe une asymétrie de marché sur ce type d'acteur. C'est pourquoi les régulateurs doivent avoir la capacité d'échanger avec eux.

La situation se complique quand l'authentification forte s'externalise vers des solutions biométriques sous Android. Les acteurs sont alors multiples. En ce sens, il est

important que les établissements bancaires soient capables d'effectuer du *monitoring* relativement poussé. Dans le monde du mobile, ce n'est pas parce que la version de l'Android est très moderne que la biométrie est très sécurisée. Il n'appartient pas aux établissements de faire la police. Mais les établissements doivent être capables de piloter ce sujet et de cesser d'utiliser des terminaux pour l'acceptation de la biométrie par exemple si des dérives sont observées.

Florence GIULIANO

L'intelligence artificielle permettra de réaliser des progrès et de mieux appréhender les nouvelles typologies de fraude. Quel type d'innovation peut nous aider à répondre aux exigences de la DSP3 ?

Richard EUDES

Il faut s'interroger sur le type d'IA et sur les données qui nourrissent l'IA. Le temps réel présente une véritable contrainte technologique. En effet, la capacité de l'IA à ingurgiter très vite de l'information et à détecter un comportement de fraude implique une surenchère technologique.

La promesse de valeur du temps réel est de détecter des anomalies très fines. Une exploitation classique de la donnée entraîne rapidement des limites. L'ouverture aux données autres que la partie transaction classique peut en effet offrir de nombreuses possibilités.

L'analyse comportementale peut intégrer des variables exogènes comme la vitesse de navigation ou de frappe sur un clavier qui peuvent enrichir les scénarii de fraude.

Ainsi, il est nécessaire de se diriger vers la dynamique du temps réel. Nous sommes dans une course technologique. Il faut reconsidérer l'ensemble des problèmes et ne pas les considérer selon un seul cas d'usage. Il s'agit de s'approprier l'ensemble des possibles et les différentes typologies de modélisation pour raisonner sur son système d'information et sur sa performance.

Florence GIULIANO

Comment appréhendez-vous l'évolution du *data management* par rapport aux nouvelles exigences réglementaires et typologies de fraude ?

Richard EUDES

Le sujet de la gouvernance de la *data* est clé dans les entreprises. Tous les métiers sont concernés. Ce sujet reste clé notamment pour le partage interbancaire.

L'extension du périmètre de données pouvant être disponibles constitue une bonne nouvelle. Tout ce qui enrichit l'IA peut en effet être bénéfique.

Le sujet de la *cyber security* est également essentiel. DSP3 introduit la notion de modèle de compensation pour le partage de données. C'est un sujet d'intérêt, car il donne la possibilité aux banques et assureurs de réclamer des compensations pour la mise à disposition et le partage des données.

Emmanuelle CHOUKROUN

Il me semble que ce dernier point est inscrit dans la directive FIDA. Mais il est en effet important de travailler sur des cas d'usage précis et de ne pas confondre un service pour un client bancaire et un service pour un marchand qui nécessite des fonctionnalités différentes.

Florence GIULIANO

Au niveau de la Banque de France, des groupes de travail ont été mis en place sur le partage des données. Existe-t-il déjà une manne de données quelque part ?

Julien LASALLE

Nous disposons d'un fichier national des chèques irréguliers et d'un fichier central des chèques. Dans le cadre de DSP3, il s'agit de s'interroger sur la valeur ajoutée du partage de données entre établissements.

Aujourd'hui, l'architecture des cartes est d'une grande complexité, mais elle a l'avantage d'une gouvernance et d'infrastructures de traitement de données centralisées par les opérateurs des réseaux de paiement par carte. Ainsi, nous avons été capables dans la DSP2 d'enrichir les informations fournies qui ont permis d'alimenter des bases de *scoring*. Par exemple, à travers le protocole 3D Secure version 2, un commerçant peut demander une exemption en fournissant des informations à l'appui. La banque pourra prendre sa décision en conséquence. Ce processus ne crée pas du point de vue du client de la latence et de la friction.

Sommes-nous capables d'étendre ce fonctionnement à d'autres moyens de paiement électroniques comme le virement ? Il faut pouvoir permettre à l'établissement qui valide le paiement d'avoir un minimum d'assurance. Dans le cadre du service d'initiation de paiement, le TPP a-t-il les moyens d'envoyer à la banque des informations complémentaires pour la rassurer ? Les API doivent en ce sens permettre d'enrichir l'information disponible pour l'émetteur.

Pour le virement plus classique de compte à compte, il s'agirait de savoir si le compte destinataire est connu pour de mauvaises raisons par les autres établissements.Dans une approche expérimentale, une réflexion sur un éventuel fichier des IBAN frauduleux est en cours. Le dossier a été présenté à la CNIL. Toutefois, dans le cadre législatif français, il ne serait pas possible de mettre en place ce dispositif sans une nouvelle loi.

Est-il possible de partager des données entre établissements financiers et autres acteurs ? Aujourd'hui, une API développée par les opérateurs de télécom permet de savoir s'il y a eu une réémission récente de carte SIM sur une ligne. En effet, la technique du *SIM swapping* est telle que le fraudeur reçoit une carte SIM sur la ligne de sa victime et reçoit les SMS d'authentification à sa place.

Ne serait-il pas intéressant d'avoir une API qui permettrait de savoir si le client est au téléphone au moment où il valide sa transaction ? Cela existe dans certains pays comme au Royaume-Uni. Nous réfléchissons à cette piste avec les opérateurs.

Il est donc possible d'alimenter les moteurs de *scoring* avec des données issues d'un autre secteur.

Florence GIULIANO

L'EBA doit développer des *guidelines* sur les outils de *monitoring*. N'est-ce pas contraignant ?

Emmanuelle CHOUKROUN

Il s'agit d'une RTS. Ce processus prendra un peu de temps. Si l'autorité bancaire a mal calibré certains points, la disposition deviendra contraignante. Mais ne pas mettre en place cette norme réglementaire permettrait à des PSP d'avoir des modèles un peu moins robustes.

Julien LASALLE

Nous avons aujourd'hui des bases très élémentaires qui indiquent que les taux de fraude doivent être inférieurs à des valeurs cibles pour effectuer des exemptions sur des tranches définies. Mais si chacun devenait plus performant, les cibles fixées pourraient être plus basses tout en incitant les établissements à baisser la fraude.

Le RTS impliquera forcément une consultation de marché. La Banque de France portera auprès de l'EBA ses revendications lors de l'élaboration des RTS.

Florence GIULIANO

La DSP3 permet-elle un ROI supplémentaire sur la data et l'IA ?

Richard EUDES

Oui via les éléments de promesse de valeur évoqués. Les IA présentent un apport de valeur sur les processus métier. Elles renforceront les dispositifs de fraude et les capacités de typologie de lutte anti-fraude.

Potentiellement, elles permettront une meilleure compréhension des mécanismes de fraude et ouvriront à tout un écosystème de données. Dans cette logique, il sera nécessaire de se diriger vers une personnalisation accrue des services à proposer aux différents clients.

Emmanuelle CHOUKROUN

Tout se joue en ce moment. L'enjeu est de mettre les bonnes responsabilités face aux bons acteurs en se coordonnant avec des secteurs autres que ceux des paiements.

Julien LASALLE

Sans doute sommes-nous capables d'estimer ce qu'a coûté la DSP2, mais il est impossible de dire quel aurait été le niveau de fraude si la DSP2 n'avait pas été mise en place. Le ROI gagné dans la DSP2 est d'avoir réussi à maintenir un certain niveau de confiance dans les paiements sur internet. Aujourd'hui, nous devons contribuer à injecter de la confiance dans le développement des nouveaux moyens de paiement. Le ROI de la DSP3 se mesurera sur les angles morts qui resteront après les quatre à cinq années d'implémentation nécessaires.

QUESTIONS/REPONSES

Un intervenant

Comment pouvons-nous protéger nos clients non équipés de téléphone mobile contre la fraude ?

Julien LASALLE

A titre d'exemple, il est possible de payer en ligne via une authentification forte par un serveur vocal interactif et un mot de passe personnel. Une attention est portée par les établissements en ce qui concerne l'accessibilité des solutions d'authentification. Nous nous intéressons également aux solutions pour les personnes malvoyantes. Il est en effet nécessaire d'être inclusif pour toutes les catégories d'utilisateur.

Emmanuelle CHOUKROUN

Nous sommes également convaincus que l'inclusion fait partie de notre chaîne de valeur dans les paiements.

Julien LASALLE

Nous devons équiper tout le monde. Face à un utilisateur qui a le choix, il est important d'attirer son attention sur le fait que toutes les solutions d'authentification ne se valent pas.

Une intervenante

Un des enjeux du marché était que les règles du jeu devaient être identiques pour tous les acteurs confrontés aux mêmes situations. Les règles du jeu sont-elles plus équitables à l'aune de ce qui se prépare ?

Emmanuelle CHOUKROUN

Lors de notre travail sur la DSP2 et la DSP3, la notion de discrimination est revenue dans deux domaines : l'accès aux systèmes de paiement et les API.

Dans la DSP3, il semble important d'expliquer la responsabilité de chacun. Quand un candidat se présente, les systèmes de paiement doivent déterminer si l'acteur remplit les règles. Si un régulateur décide d'autoriser un établissement de paiement ou de monnaie électronique à participer en direct à un système de paiement, il doit s'assurer qu'il a mis en place les éléments qui permettront de pouvoir agir ainsi.

En ce qui concerne l'*open banking*, nous n'avons pas les mêmes activités avec les TPP. Parfois, il nous est demandé de mettre en place des services qui ne correspondent pas à des services pour nos clients, mais à des services pour les TTP qui souhaitent développer leur offre. Il me paraît judicieux de développer de tels services sur une base contractuelle et rémunérée.

Des marges de progrès restent à mener sur la discrimination d'IBAN.

Julien LASALLE

Nous traitons la discrimination d'IBAN au Comité national des moyens de paiement. Par ailleurs, il est nécessaire de distinguer la discrimination à l'IBAN des mesures conservatoires prises en réponse à un risque de fraude aggravé vis-à-vis de certains établissements, sans que cela n'ait un rapport avec leur pays d'établissement.

Un intervenant

Dans le cadre des paiements sur internet, l'une des difficultés rencontrées réside dans l'écart entre la DSP2, les recommandations de l'Observatoire et les schémas des programmes soumis à FISE. Cet étau est-il mieux pris en compte ? Des discussions sont-elles en cours avec eux ?

Julien LASALLE

Il faut être attentif à ce que les règles de fonctionnement des réseaux de paiement par carte ne soient pas contre-productives par rapport à ce qui est souhaité dans la réglementation. Une délégation d'authentification forte doit être contractualisée avec la banque. Il n'est pas possible pour les schemes de décréter des règles qui touchent à l'authentification et à la gestion de la fraude. Cela amènerait les établissements participants aux schemes à choisir entre être en infraction avec la réglementation ou aux règles de participation du scheme, ce qui n'est pas satisfaisant. Nous sommes très attentifs avec l'ACPR aux remontées que les établissements pourraient nous formuler à ce sujet.

Un intervenant

Comment se situe la DSP3 par rapport à des réglementations similaires en Grande-Bretagne, voire aux Etats-Unis ?

Julien LASALLE

Il n'y a pas de réglementations aux Etats-Unis. D'ailleurs, peu de zones géographies dans le monde possèdent des directives similaires à la DSP2.

Le Royaume-Uni possédait dans son corpus de règles la DSP2 et il n'est pas revenu dessus. Les autorités continuent à l'affiner. Des mesures ont été annoncées sur la protection du consommateur et le remboursement en cas de fraude qui différeront peut-être de la DSP3.

La fraude fait partie du business aux Etats-Unis. Les régulateurs regarderont si le consommateur est suffisamment protégé. Mais les mécanismes techniques comme l'authentification forte ou le *scoring* n'existent pas dans la réglementation. C'est à la charge du commerçant de se créer une marge suffisante pour faire face à ses obligations.

Un intervenant

Il me semble que toutes les banques ne sont pas au même niveau et ont pris des choix technologiques et pratiques avec une utilisation des informations différentes. Des recommandations peuvent-elles être formulées à destination des établissements de crédit pour les encourager à modifier leurs systèmes d'information et à améliorer leurs pratiques ?

Emmanuelle CHOUKROUN

La loi est la même pour tout le monde. Toutes les banques ne pourraient-elles pas offrir la même qualité de service ? Nous restons un marché concurrentiel. Certaines banques sont meilleures que d'autres. C'est l'enjeu de l'exécution. En cas de manquements graves, des sanctions contraignantes sont néanmoins prévues dans le cadre de la DSP3.

Julien LASALLE

La DSP2 nous a dotés d'outils comme les *reportings* statistiques obligatoires qui nous permettent d'identifier les bons et mauvais élèves. Nous mesurons si le taux de fraude des établissements est homogène. Si des établissements subissent beaucoup de fraudes, cela nous donne l'occasion de les contrôler et d'émettre in fine des recommandations.

En ce qui concerne la fraude entrante, nous savons vers où part la fraude et nous partageons ces informations avec l'ACPR.

Un intervenant

La DSP3 demandera probablement des développements supplémentaires par rapport à des TPP. Les lignes pourraient-elles changer en modulant l'implémentation par rapport à la typologie des établissements ?

Emmanuelle CHOUKROUN

Nous ferons tout pour. Un enjeu autour de l'allocation efficace des ressources est présent dans les traités européens. Contraindre des établissements à mettre durablement en place des infrastructures qui ne seront jamais utilisées irait à l'encontre du traité. Il est important de montrer dans l'élaboration de la DSP3 cet aspect de la DSP2 qui a pu être mal calibré.

Julien LASALLE

Il existe un besoin de simplicité sur l'*open banking*. Il n'est pas non plus confortable pour un superviseur de vérifier qu'une interface est conforme en termes de disponibilité et de performance, alors qu'elle ne reçoit aucune transaction.

Un intervenant

Pouvez-vous nous confirmer qu'un client qui se voit refuser le remboursement d'une opération de paiement à la suite de sa contestation est éligible à déposer une réclamation ? Il est parfois difficile de distinguer ce qui relève de la contestation d'une opération de paiement de ce qui relève d'une réclamation portant sur un service de paiement. Est-il prévu une clarification ou des FAQ de la part de l'Observatoire ?

Julien LASALLE

Il me semble qu'il existe une publication de référence de l'ACPR sur les modalités de réclamation de contestation.

CLUB BANQUE

Le rendez-vous mensuel
des professionnels
de la banque et de la finance

Paiements, fraudes, partage de données : la DSP 3 rebat les cartes

29 février 2024

18 h 00 à 20 h 00
Auditorium de la FBF
18, rue La Fayette
75009 Paris

REVUE BANQUE

sas

TNP
Partenaire officiel

Programme

CLUB BANQUE

Introduction

Florence GIULIANO

EMEA Financial Crimes Analytics Director

sas

Présentation des intervenants

Maya Atig

Directrice générale

Fédération bancaire française

Julien Lasalle

Secrétaire Général

Observatoire de la sécurité des moyens de paiement

Emmanuelle Choukroun

Directrice des relations interbancaires

Société Générale

Richard Eudes

Directeur Data, Technology & Analytics

Deloitte

Florence Giuliano

EMEA Financial Crimes Analytics Director

SAS

Programme

Paiements, fraudes, partage de données : la DSP 3 rebat les cartes

Président de séance - Introduction

Florence GIULIANO
EMEA Financial Crimes Analytics Director
SAS

« Le régime de responsabilités doit concerner tous les acteurs »

Maya ATIG, Directrice générale, Fédération Bancaire Française

« De la DSP2 à la DSP3, de nouveaux apports »

Julien LASALLE, Secrétaire Général, Observatoire de la sécurité des moyens de paiement

« L'angle mort du calendrier pour les banques : comment investir et s'engager ?»

Emmanuelle CHOUKROUN, Directrice des relations interbancaires, Société Générale

Table ronde « Quel partage des données entre établissements financiers ? »

Modérée par Florence GIULIANO

Questions / Réponses

CLUB BANQUE

Programme

Le régime de responsabilités doit concerner tous les acteurs

Maya ATIG
Directrice générale

FÉDÉRATION BANCAIRE FRANÇAISE

CLUB BANQUE

Programme

De la DSP2 à la DSP3, de nouveaux apports.

Julien LASALLE
Chef du service de surveillance des moyens de paiement scripturaux

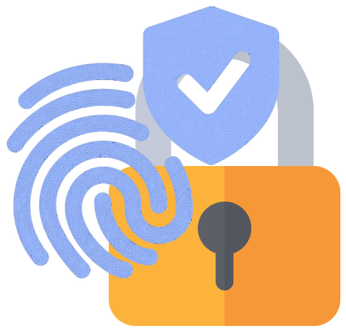
BANQUE DE FRANCE
EUROSYSTÈME

CLUB BANQUE

SÉCURITÉ DES PAIEMENTS : DES ACQUIS DE LA DSP2 À PRÉSERVER

Règle générale : application de l'**authentification forte** du payeur

- Sécurité assurée par le recours à deux facteurs d'authentification de nature différente (SCA)
- Lien assuré entre les éléments d'authentification utilisés et la transaction



Paiement **exempté** d'authentification forte en raison d'un faible niveau de risque

- Mise en place de mécanismes d'analyse de risques des transactions (*scoring*)
- Cas d'exemption définis de façon limitative par la réglementation
- Application de l'exemption soumise à la validation de l'émetteur du moyen de paiement

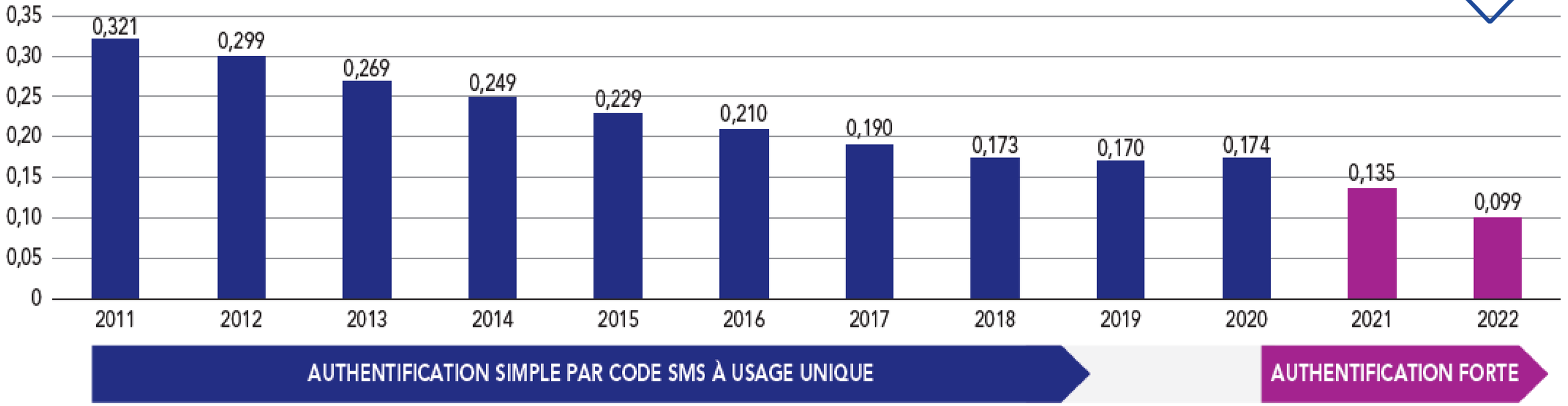
Instauration d'un environnement de confiance entre acteurs pour les services d'open banking

- Utilisation de certificats eIDas par les PSP pour se reconnaitre mutuellement
- Application de la SCA lors de la connexion via un TPP

SÉCURITÉ DES PAIEMENTS : DES RÉSULTATS SIGNIFICATIFS OBSERVÉS

Baisse de 33% du taux de fraude sur les cartes émises en France, **et même de 42%** pour les paiements domestiques

Évolution du taux de fraude sur les paiements domestiques par carte sur Internet (en %)



Source : Observatoire de la sécurité des moyens de paiement.

FUTUR RÈGLEMENT SUR LES SERVICES DE PAIEMENT (RSP)
DE NOUVEAUX AXES DE RENFORCEMENT DE LA SÉCURITÉ

Instauration d’un cadre de partage inter-PSP de données relatives à la fraude

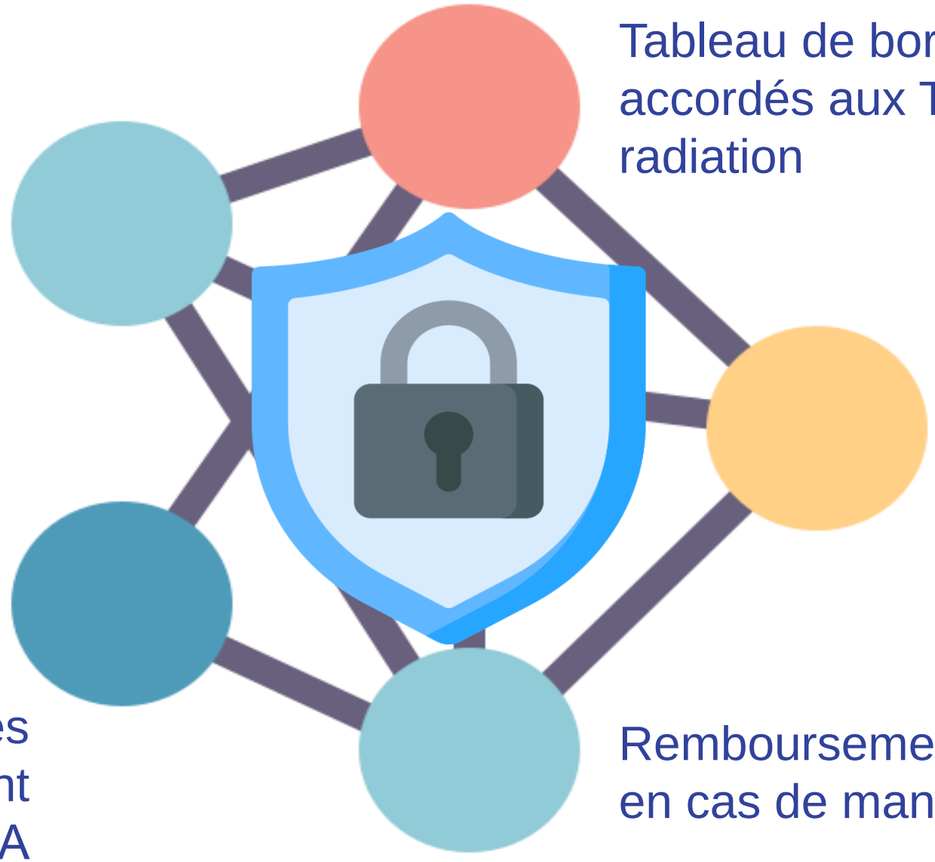


Tableau de bord des consentements accordés aux TPP et possibilité de radiation

Clarification des notions d’autorisation et de négligence grave

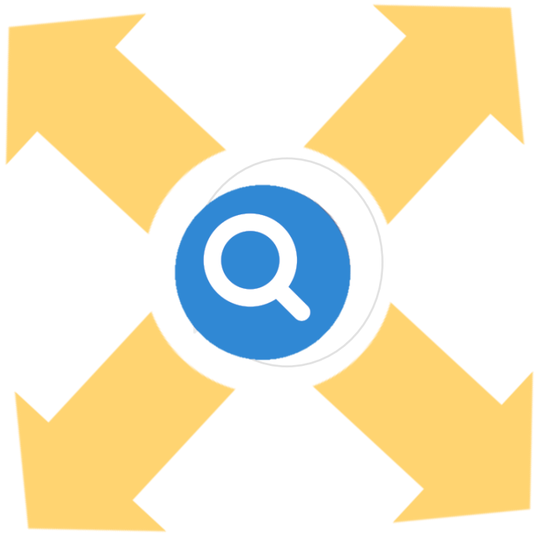
Responsabilité des prestataires techniques et schemes de paiement dans la mise en œuvre de la SCA

Remboursement des consommateurs en cas de manipulation par un tiers

AUTRES APPORTS ATTENDUS DE LA DSP3 ET DU RSP

Accès aux systèmes de paiement pour les établissements de paiement

Intégration de la monnaie électronique dans les services de paiement

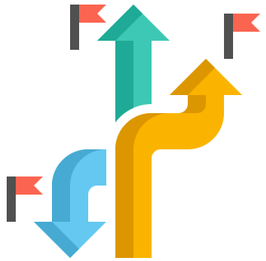


Développement des retraits d'espèces en point de vente

Stimuler l'essor des services d'open banking, y.c. à valeur ajoutée

MISE EN ŒUVRE ET CALENDRIER

UNE ARTICULATION AVEC LE RÈGLEMENT SUR LE VIREMENT INSTANTANÉ



Juin 2023 — **Novembre 2023** — **Février 2024** — **Fin 2025**

DSP3 + RSP

Présentation du projet de révision de la DSP2

Négociations au niveau de co-législateurs

IPR

Accord politique → Adoption → Entrée en application progressive

Service de confirmation d'IBAN

Programme

L'angle mort du calendrier pour les banques : comment investir et s'engager ?

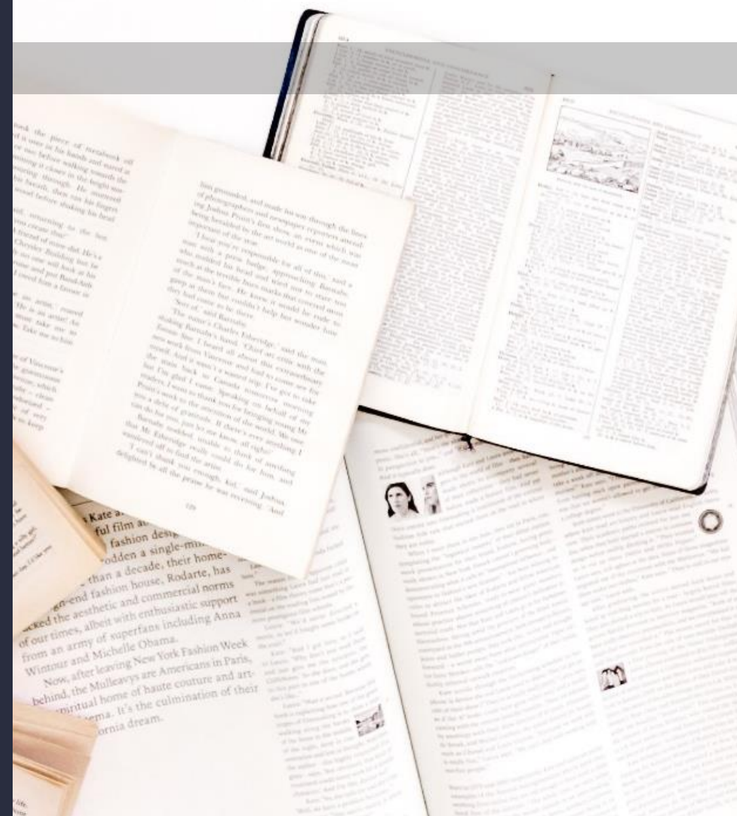
Emmanuelle CHOUKROUN
Directrice des relations interbancaires

SOCIETE GENERALE

CLUB BANQUE

AU SOMMAIRE...

→



SOCIETE GENERALE

LE CALENDRIER DE LA DSP3

	REGLEMENT - PSR	DIRECTIVE - PSD
Proposition initiale	28 juin 2023	
Vote parlement	Mars 2024	
Elections européennes	6 – 9 juin 2024	
Hypothèse d'accord politique	Fin 2024/Début 2025	
Entrée en vigueur *Si adoption en Janvier 2025*	Immédiate - 20 jours après publication au J.O *Février 2025*	
Délai de mise en oeuvre	18 mois	18 mois
Publication des Normes Techniques réglementaires (NTR)	▪ Mai 2026* ▪ Novembre 2026*	

SOCIETE GENERALE

* *Détail ci-après pour PSR.*

LE CALENDRIER DE LA DSP3

Focus sur les NTR de PSR affectant les PSP

MAI 2026

- **Art. 32.5** : Informations harmonisées devant figurer dans la notification et la motivation de refus d'ouverture ou de clôture de compte à un EP/EME
- **Art. 39.2** : Dérogation à l'obligation de disposer d'une interface spécifique pour l'accès aux données
- **Art. 82.2** : Données statistiques sur la fraude à fournir à l'Autorité Compétente
- **Art. 89.1** : Authentification, communication et mécanismes de contrôle des opérations

NOVEMBRE 2026

- **Art. 48.8** : Reporting à fournir par les banques aux autorités compétentes sur l'activité Open Banking

SOCIETE GENERALE

LES ASTREINTES, UN GAGE D'EFFICACITÉ ?

Article 98

1. Les autorités compétentes sont habilitées à infliger des astreintes aux personnes physiques ou morales pour non-respect de toute décision, injonction, mesure provisoire, demande, obligation ou autre mesure adoptée conformément au présent règlement. L'astreinte visée au premier alinéa est effective et proportionnée et consiste en un **montant journalier** à payer jusqu'au rétablissement de la conformité. Les astreintes sont infligées pour une durée n'excédant pas **six mois** à compter de la date indiquée dans la décision infligeant l'astreinte.

   Les autorités compétentes sont habilitées à infliger des astreintes d'un montant maximal **d'au moins 3 % du chiffre d'affaires journalier moyen** dans le cas d'une personne morale;

2. Les États membres peuvent prévoir des **montants de sanctions pécuniaires plus élevés** que ceux prévus au paragraphe 1.

SOCIETE GENERALE

INVESTIR POUR LE BIEN COMMUN : RISQUES ET ENJEUX

- **Substituer une dépendance à une autre**
  - Constructeurs de mobiles (article 88) / Prestataires de services cloud
- **Affaiblir la capacité des banques à accompagner leurs clients en les contraignants à réaliser des investissements improductifs ou peu créateurs de valeur**
  - Développement d'offres coûteuses et faiblement utilisées
  - Imposer des solutions et freiner toute forme d'innovation susceptible de naître à partir d'une expression de besoins
- **Définir des exigences purement fonctionnelles**
  - Ne tenant pas compte du risque
  - Faisant abstraction de toute considération économique (outil de lutte contre la fraude plus cher que le coût de la fraude…)
- **Coordination efficiente des différents acteurs intervenant dans la chaine transactionnelle**
  - Des opérateurs de communication électronique aux banques en passant par les EP/EME, les PSIC, les PSIP et leurs agents
  - Attribuer les bonnes responsabilités aux bons acteurs

SOCIETE GENERALE

QUELLE STRATÉGIE DE MODÉRATION ?

- **Dans la phase d'élaboration du texte et des normes techniques réglementaires**
  - Etudes d'impact
  - Evaluation de la viabilité des dispositions trans-sectorielles proposées
    - Articles 59 et 88
  - Se donner le temps

- **Dans la phase de mise en œuvre**
  - Des questions vont inévitablement se poser
  - Certaines dispositions auront besoin d'être interprétées, y inclus pour les dispositions de PSR
  - Cela suppose une coopération agile entre l'Autorité Bancaire Européenne, les superviseurs des Etats membres et les acteurs de la chaine de paiements
    - Afin d'éviter les désagréments constatés lors de la mise en place de la DSP2 : manque de clarté entre les NTR, les guidelines et les précisions sur les exigences qui se sont ajoutées au fil de l'eau

SOCIETE GENERALE

Table ronde:
« Quel partage des données entre établissements financiers ? »

Julien Lasalle

Secrétaire Général

Observatoire de la sécurité des moyens de paiement

Emmanuelle Choukroun

Directrice adjointe des relations interbancaires

Société Générale

Richard Eudes

Directeur Data, Technology & Analytics

Deloitte

Florence Giuliano

EMEA Financial Crimes Analytics Director

SAS

CLUBBANQUE

sas

Questions / réponses

CLUB
BANQUE

à venir

Les prochains événements REVUE BANQUE

CLUB BANQUE

Quelle place pour l'euro numérique ?

21 mars 2024

CLUB BANQUE

Open Finance : vers la transformation du modèle bancaire ?

4 avril 2024

LES DÉBATS DE REVUE BANQUE

Adoption de l'IA au sein des banques, de l'innovation aux processus métiers

23 avril 2024

LES DÉBATS DE REVUE BANQUE

L'intelligence artificielle au service des moyens de paiement digitaux

30 avril 2024

CLUB BANQUE

à venir

Profitez du Club Banque toute l'année avec l'adhésion !

Inscription et renseignements :

clubbanque@revue-banque.fr

01.48.00.54.04

CLUB BANQUE

CLUBBANQUE