Observatoire de la sécurité des moyens de paiement

www.observatoire-paiements.fr

Publication initiale le 10 juin 2024
Dernière mise à jour le 18 avril 2025

Mesures de prévention de la fraude sur les paiements par carte à distance hors *3-D Secure*

1. Contexte des travaux

La directive UE n° 2015/2366 du 25 novembre 2015 sur les services de paiement, dite DSP2[1], transposée en droit français dans le code monétaire et financier[2], prévoit le recours à un dispositif d'authentification forte du payeur pour les paiements électroniques ainsi que pour les opérations exécutées par le biais d'un moyen de communication à distance susceptibles de comporter un risque de fraude[3]. Le règlement délégué UE n° 2018/389 du 27 novembre 2017 (ou *RTS* pour *regulatory technical standard*) prévoit toutefois des exemptions[4] concernant notamment les opérations effectuées en faveur d'un bénéficiaire de confiance, les opérations récurrentes, les opérations de faible montant ou encore les opérations qui présentent un faible niveau de risque.

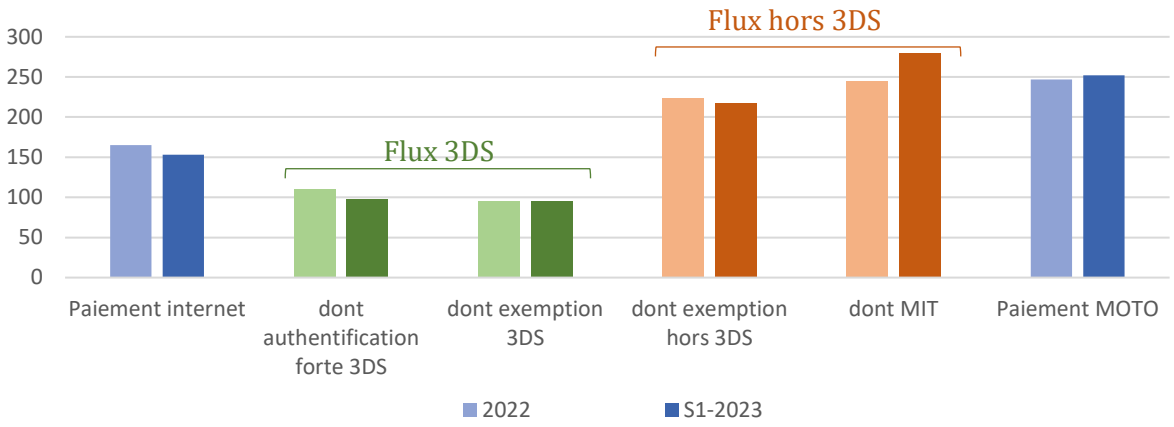
En France, la mise en œuvre progressive de l'authentification forte pour les paiements à distance effectués par carte bancaire s'est effectuée dans le cadre du plan de migration adopté par l'Observatoire[5].

Cette mise en œuvre a été rendue possible par le déploiement de la deuxième version du protocole *3-D Secure*, destiné à la gestion des échanges entre le commerçant, le porteur de la carte et leurs prestataires de services de paiement (PSP), en vue de l'authentification des paiements par internet. La version 2.0 du protocole permet la gestion de l'authentification forte des paiements à distance à l'aide des différentes solutions actuellement proposées aux porteurs de cartes par les PSP émetteurs, et prend également en charge les demandes d'exemption à l'authentification forte.

La mise en œuvre de l'authentification forte a permis la réduction du taux de fraude sur les paiements à distance effectués via *3-D Secure*. Le taux de fraude apparaît aujourd'hui maîtrisé sur l'ensemble de ces paiements, y compris sur ceux bénéficiant d'une exemption à l'authentification forte (figure n° 1).

[1] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur
[2] Articles L. 133-1 et suivants
[3] Article L. 133-4, I du code monétaire et financier
[4] Articles 11 à 18 du règlement UE n° 2018/389
[5] Chapitre 1 du rapport annuel 2018 de l'Observatoire

Figure n° 1 : taux de fraude sur la carte *(en € de fraude / 100.000 € de paiements)*



À l'inverse, le taux de fraude reste aujourd'hui structurellement plus élevé sur les paiements effectués à distance hors *3-D Secure*, parmi lesquels les paiements de type *MIT (Merchant Initiated Transaction)* ainsi que les paiements *MOTO* (pour *Mail Order – Telephone Order*).

Par nature, ces paiements, qui ne donnent lieu à aucune authentification au moment de leur émission, sont beaucoup plus exposés à la fraude que les paiements transitant par le protocole *3-D Secure* :

- de tels paiements peuvent être initiés par toute personne ayant pu prendre connaissance des données inscrites sur la carte bancaire (numéro et date d'expiration pour les paiements *MOTO*, et cryptogramme visuel en sus pour les paiements *MIT*), sans même que cette personne ait besoin d'être en possession de la carte ou d'avoir accès au dispositif d'authentification forte des paiements à distance ;
- en particulier, un commerçant peut transmettre à son PSP des paiements qui ne correspondent en réalité à aucun produit ou service délivré au porteur de la carte, par exemple en réutilisant les données de cartes de paiement précédemment utilisées dans le cadre de transactions légitimes ;
- s'agissant en particulier des paiements *MOTO*, ceux-ci reposent sur la communication par le client payeur du numéro de sa carte bancaire et de sa date d'expiration par un canal non sécurisé (conversation téléphonique, courriel, envoi postal, télécopie…) puis sur leur manipulation par un opérateur qui assure la saisie sur le terminal de paiement du commerçant. Cette situation favorise la fraude interne ou externe par détournement des données de paiement.

Si les standards techniques en vigueur incluent théoriquement la possibilité de mettre en place une solution d'authentification des paiements *MOTO*, cette possibilité est en pratique inutilisée et aucune solution uniforme pour l'authentification de ces paiements n'a été identifiée à ce jour.

De plus, les paiements *MOTO* et les paiements internet hors *3-D Secure* sont parfois détournés de leur finalité originelle pour permettre à un commerçant d'accepter des paiements par internet initiés par le client (*CIT* pour *Customer Initiated Transaction*) en contournant l'obligation d'authentification forte pourtant imposée par la DSP2.

Ces constats conduisent l'Observatoire à adopter des recommandations qui visent à prévenir la fraude sur les paiements à distance effectués hors *3-D Secure*.

Ces recommandations, publiées le 10 juin 2024 dans leur version initiale, ont fait l'objet d'ajustements intégrés dans les versions publiées les 13 et 27 août 2024. La présente version

prend également en compte les apports de la feuille de route pour l'année 2025, validée lors de la réunion plénière du 19 décembre 2024 de l'Observatoire.

2. Périmètre des recommandations

Les présentes recommandations s'appliquent à l'ensemble des paiements à distance sans authentification forte effectués hors *3-D Secure*, à savoir :

- d'une part, les paiements *MOTO* ;
- d'autre part, les paiements internet hors *3-D Secure*, au nombre desquels les paiements de type *MIT* (pour lesquels seule l'authentification forte effectuée lors de la validation du mandat utilise le canal *3-D Secure*), ainsi que les paiements *CIT* demandant le bénéfice d'une exemption sans transiter par le protocole *3-D Secure* (on parle alors de paiement *DTA* pour *direct to authorisation*).

Par exception, ces recommandations ne s'appliquent pas :

- aux paiements internet hors *3-D Secure* reconnus comme authentifiés fortement par le PSP émetteur, tels que les paiements effectués à l'aide d'une solution mobile de type *wallet* intégrant une solution d'authentification forte reconnue comme conforme à la DSP2 par le PSP émetteur de la carte ;
- aux paiements électroniques initiés par des personnes morales au moyen de procédures ou de protocoles de paiement dédiés qui sont uniquement mis à la disposition de payeurs qui ne sont pas des consommateurs, lorsque les autorités compétentes ont acquis la certitude que lesdits procédures et protocoles garantissent des niveaux de sécurité au moins équivalents à ceux prévus par la DSP2[6] ;
- aux paiements pour lesquels le PSP acquéreur est situé dans un État qui n'est pas partie à l'accord sur l'Espace économique européen (EEE) à l'exception du Royaume-Uni et de la Suisse.
    - **[Nouveau]** À compter du 12 mai 2025, ces recommandations s'appliquent pleinement aux paiements pour lesquels le PSP acquéreur et le commerçant accepteur sont situés au Royaume-Uni ou en Suisse dans la mesure où les PSP acquéreurs situés dans ces deux pays ont mis en œuvre les mécanismes techniques permettant l'authentification forte via *3-D Secure* des paiements sur internet, au même titre que les PSP acquéreurs situés dans les États membres de l'Espace économique européen.

Les présentes recommandations ont vocation à être mises en œuvre par les commerçants qui acceptent de tels paiements, par leurs prestataires d'acceptation techniques, par les différents schémas de cartes ainsi que par l'ensemble des PSP, qu'ils soient émetteurs et/ou acquéreurs.

3. Recommandations applicables aux paiements à distance hors *3-D Secure*

3.1 Utilisation des paiements *MOTO* et des paiements par internet hors *3-D Secure* seulement lorsque le recours à un autre mode de paiement n'est pas possible

Le taux élevé de fraude sur ces paiements impose de limiter les paiements *MOTO*, ainsi que les paiements par internet hors *3-D Secure* (autres que ceux reconnus comme authentifiés par le PSP

[6] Ces paiements sont exemptés de l'obligation d'authentification forte en application de l'article 17 du règlement UE n° 2018/389.

émetteur, par exemple lors de l'utilisation d'un *wallet*) aux seuls cas d'usage auxquels ces modes de paiements sont destinés.

En particulier, les paiements par internet pouvant bénéficier d'une exemption à l'authentification forte ont vocation à être présentés via *3-D Secure*. En effet, ce protocole permet la gestion des demandes d'exemption, et la demande d'authentification forte du client lorsque la demande d'exemption est rejetée via *soft decline*.

Le PSP émetteur doit conserver, en tout état de cause, la faculté d'imposer l'authentification forte du payeur, même lorsqu'une demande d'exemption est présentée. La fonctionnalité *Data Share Only* proposée par le protocole *3-D Secure* n'est donc pas conforme à la présente recommandation.

Afin de favoriser l'exemption à l'authentification forte, lorsqu'un paiement peut relever de plusieurs catégories d'exemption distinctes (par exemple, exemption pour paiement de faible montant et exemption pour faible niveau de risque[7]), le commerçant et le PSP acquéreur sont invités à demander l'exemption qui est la mieux prise en compte par les PSP émetteurs, par exemple l'exemption pour faible niveau de risque ou *TRA (Transaction Risk Analysis)* dans la version 2.2, aujourd'hui majoritairement déployée, du protocole *3-D Secure*.

Recommandation n° 1 : limitation des paiements *MOTO* et *MIT* aux seuls cas d'usage ou le recours à un autre mode de paiement n'est pas possible

Les commerçants veillent :

- **à n'accepter des paiements par carte de type *MOTO* que pour les contrats souscrits à distance par un canal (téléphone, courrier…) autre qu'internet. Ils veillent à recourir à un paiement de proximité ou à un paiement sécurisé par internet chaque fois que la nature d'un contrat et les modalités de sa souscription ainsi que de la livraison des biens ou services commandés sont compatibles avec un tel paiement (par exemple, paiement de proximité lors de la livraison, effectuée directement par le commerçant, de biens commandés par téléphone) ;**
- **à n'accepter des paiements par internet que via le canal sécurisé *3-D Secure*, en dehors des cas où le paiement est reconnu comme authentifié par l'émetteur (par exemple lors de l'utilisation d'un *wallet* intégrant l'authentification forte) et des cas d'usage qui ne permettent pas le recours à *3-D Secure*, tels que les paiements de type *MIT*.**

En particulier, les commerçants ne doivent jamais recourir à des paiements par internet hors *3-D Secure* et des paiements de type *MOTO* lorsque le paiement s'effectue par internet et a été initié par le client *(CIT)*.

Les prestataires d'acceptation technique et les prestataires de services de paiement acquéreurs veillent au respect de cette recommandation par les commerçants avec lesquels ils ont conclu un contrat d'acceptation.

3.2 Chainage valide des paiements *MIT*

Le recours au protocole *3-D Secure* pour l'ensemble des paiements par internet initiés par le client *(CIT)* devrait conduire à réserver les paiements par internet hors *3-D Secure* autres que ceux reconnus comme authentifiés par le PSP émetteur (par exemple lors de l'usage d'un *wallet*

[7] Voir paragraphe 4.1.3 du rapport de l'Observatoire de la sécurité des moyens de paiement scripturaux pour l'année 2022

intégrant une solution d'authentification forte) aux seuls paiements initiés par le commerçant *(MIT)*.

Chaque paiement *MIT* doit être associé à une référence de chainage valide permettant à l'émetteur de la carte de s'assurer du consentement de son porteur au paiement présenté ou, lors du traitement d'une contestation formulée par le porteur, de procéder au rapprochement entre le paiement et le mandat préalablement validé par authentification forte.

Si l'absence de chainage peut être détectée lors de l'acceptation du paiement par le PSP émetteur, l'analyse de la validité du chainage (c'est-à-dire s'assurer que le chainage présenté correspond à une authentification préalable) ne peut être réalisée en temps réel par celui-ci. De ce fait, les chainages invalides, c'est-à-dire ne correspondant pas à un mandat de paiement dûment validé par le porteur au moyen d'une authentification forte, ne pourront être détectés qu'en réalisant un rapprochement *a posteriori* que les PSP émetteurs sont invités à mettre progressivement en œuvre.

Recommandation n° 2 : chainage valide des *MIT*

Lors de toute émission d'un paiement *MIT*, les commerçants communiquent à leur PSP la référence de chainage issue de la validation par authentification forte du mandat de paiement autorisant le paiement.

Les PSP émetteurs sont invités :

- **à mettre en œuvre progressivement un mécanisme de rapprochement entre le chainage des paiements *MIT* et les mandats de paiement validés par authentification forte ;**
- **à notifier aux commerçants et aux prestataires d'acceptation techniques les anomalies relevées dans les chainages présentés dans les transactions *MIT* qu'ils émettent afin que ces derniers mettent en place un plan d'action visant à y remédier ;**
- **à défaut de remédiation, à appliquer la limite de vélocité définie par la recommandation n° 3 aux paiements *MIT* présentés par les commerçants et/ou les prestataires d'acceptation techniques concernés par le recours à des références de chainage invalides.**

3.3 Limitation de la vélocité des paiements *MOTO* et des paiements par internet hors *3-D Secure* et mesures spécifiques applicables aux commerçants prioritaires pour la lutte contre la fraude

La prévention de la fraude sur les paiements *MOTO* et sur les paiements par internet hors *3-D Secure* (en dehors des cas, tels que l'usage d'un *wallet* intégrant une solution d'authentification forte, où l'opération est considérée comme authentifiée par le PSP émetteur) imposent de limiter la vélocité, c'est-à-dire le montant cumulé des achats effectués avec une même carte auprès d'un même commerçant durant une période de 24 heures (glissante).

Vélocité = montant cumulé des achats / carte / commerçant / 24 heures

La vélocité est mesurée de manière indépendante pour les paiements *MOTO* d'une part, et pour les paiements par internet hors *3-D Secure* d'autre part.

L'Observatoire invite les PSP émetteurs à rejeter toute opération conduisant au dépassement de cette limite, par *soft decline* lorsque les caractéristiques de l'opération permettent ce mode de rejet.

Cette limite de vélocité ne concerne pas :

– les secteurs d'activité pour lesquels le recours au mode de paiement considéré (*MOTO* et/ou *MIT*) apparaît justifié et pour lesquels le taux de fraude est maîtrisé. Ces secteurs sont intégrés à la « liste d'exemptions » définie en annexe 2 ;

– les paiements *MIT* associés à une référence de chainage techniquement valide et pour lesquels le commerçant et le prestataire d'acceptation technique n'ont pas été identifiés comme émettant des paiements associés à des références de chainage présentant des anomalies.

En outre, des dérogations individuelles pourront être accordées, en fonction du taux de fraude observé pour chaque commerçant[8] et selon les modalités prévues par la procédure définie en annexe 3.

À l'inverse, l'exemption pourra être levée, sur décision du PSP émetteur et pour la durée de son choix, pour un commerçant dont le *MCC* bénéficie d'une exemption, mais qui réalise un usage inapproprié des paiements *MOTO* ou des paiements par internet hors *3-D Secure*, ou encore dont le taux de fraude sur ces paiements apparaît insuffisamment maîtrisé au regard des critères définis par le PSP émetteur.

Recommandation n° 3 : limite de vélocité et mise en place d'un mécanisme de *soft decline*

Les PSP émetteurs rejettent, par *soft decline* lorsque cela est possible, les paiements *MOTO* et les paiements par internet hors *3-D Secure* reconnus comme non authentifiés par l'émetteur, dès lors que le montant du paiement conduirait au dépassement de la limite de vélocité définie par la présente recommandation.

La vélocité est mesurée sur une période de 24 heures glissantes et de manière distincte :

– **d'une part, pour les paiements *MOTO* ;**

– **d'autre part, pour les paiements internet hors *3-D Secure*. Pour cette catégorie de paiement, la mesure de la vélocité ne prend en compte ni les paiements *CIT* authentifiés par l'émetteur (notamment par *wallet* mobile), ni les paiements *MIT* associés à une référence de chainage valide.**

Pour les paiements *MOTO*, la limite de vélocité est définie à 500 euros à compter depuis le 10 juin 2024.

Pour les paiements internet hors *3-D Secure*, la limite de vélocité est définie à 100 euros depuis le 14 octobre 2024.

Cette limite sera abaissée :

– **à 50 euros le 10 février 2025 ;**

– **à 30 euros le 10 mars 2025 ;**

– **[Mise à jour] à 10 euros le 10 avril 2025 ;**

– **[Mise à jour] à 1,01 euro le 12 mai 2025 : à compter de cette dernière date, les paiements internet hors 3-D Secure d'un montant strictement supérieur à 1 euro ne seront donc plus admis. Cela ne concerne (i) ni les CIT reconnus par l'émetteur comme authentifiés fortement, (ii) ni les MIT associés à une référence de chainage valide, (iii)**

[8] Un commerçant est identifié, lors de l'émission d'un paiement par carte, par la valeur renseignée dans le champ *Merchant ID* inclus dans les données de ce paiement.

ni les demandes de renseignement à 0 euro et (iv) ni les demandes de pré-autorisation à 0€.

- **[Nouveau] Les commerçants sont invités à bien vérifier la qualification de leurs demandes d'autorisation ≤ 1 euro, afin de distinguer les cas d'usage des différents services utilisés (vérification de compte/carte, vérification de solde, pré-autorisation etc.) car cette limite de vélocité pourrait être abaissée à 0,01 euro à partir du 1er janvier 2026.**

Sont exclus de l'application de cette recommandation :

- **les paiements acceptés par des commerçants qui bénéficient d'une exemption (pour le type de paiement concerné) accordée dans les conditions définies en annexes 2 ou 3 ;**
- **les paiements *MIT* qui sont associés à une référence de chainage valide ;**
- **les paiements *MOTO* qui ont fait l'objet d'une authentification forte.**

La mise en œuvre des limites de vélocité sera supervisée par un comité de pilotage placé sous l'égide du groupe de travail authentification forte de l'Observatoire.

Ce comité de pilotage aura la charge :

- de vérifier que l'ensemble des cas d'usage légitimes des paiements *MOTO* et des paiements par internet hors *3-D Secure* ont été pris en compte et que la mise en œuvre de la limite de vélocité ne conduit pas au rejet d'opérations légitimes ;
- de proposer tout ajustement nécessaire des modalités de mise en œuvre de la présente recommandation et en particulier de modifier la liste des secteurs d'activités exclus de son champ d'application ou de différer les dates et conditions d'entrée en vigueur des 2e et 3e paliers.

Par dérogation à la recommandation n° 3, les commerçants bénéficiant d'une exemption sectorielle pour les paiements *MOTO* mais acceptant un volume important de tels paiements et présentant pour ces paiements une exposition à la fraude régulièrement supérieure à la moyenne de l'ensemble des commerçants, seront identifiés comme prioritaires et assujettis à une limite de vélocité à défaut de plan d'action présenté par le commerçant et validé par la Banque de France. Ces modalités visent à inciter à la mise en œuvre d'un dialogue entre les commerçants concernés et les PSP émetteurs.

L'identification de ces commerçants prioritaires est effectuée par les PSP émetteurs en association avec la Banque de France et selon les critères définis en annexe n° 4.

Cette démarche s'inscrit dans la perspective d'un remplacement progressif des exemptions sectorielles par des dérogations individuelles, accordées selon les critères et les modalités définis en annexe n° 3.

Recommandation n° 3 *bis* : mesures spécifiques applicables aux commerçants identifiés comme prioritaires pour la réduction de la fraude sur les paiements *MOTO*

Les commerçants qui bénéficient d'une exemption sectorielle pour les paiements *MOTO* mais acceptent un volume important de paiements *MOTO* et présentent pour ces paiements une exposition à la fraude régulièrement supérieure à la moyenne, selon les critères définis en annexe n° 4, sont identifiés comme prioritaires et se voient appliquer des mesures spécifiques.

Les commerçants identifiés comme prioritaires sont informés par leurs PSP acquéreurs ainsi que par l'intermédiaire des schémas de cartes, et doivent présenter un plan d'action à la Banque de France.

À défaut de plan d'action validé par la Banque de France dans un délai d'un mois suivant l'identification d'un commerçant comme prioritaire, celui-ci se voit appliquer, pour les paiements MOTO qu'il accepte, une limite de vélocité diminuée progressivement jusqu'au seuil de 500 euros, selon un calendrier communiqué par la Banque de France.

De même, les commerçants acceptant un volume important de paiements *MIT* et présentant pour ces paiements une exposition à la fraude régulièrement supérieure à la moyenne de l'ensemble des commerçants, feront l'objet, à défaut de plan d'action présenté par le commerçant et validé par la Banque de France, de mesures individuelles mises en œuvre par les PSP émetteurs (refus des demandes de renseignement à 0 euro sans authentification forte, rejet des transactions identifiées comme présentant un risque de fraude élevé…). Ces modalités visent à supprimer les tout usage manifestement impropre des *MIT* au regard du modèle d'affaire (par exemple, achat sur internet effectué en présence du porteur) et incitent à la mise en œuvre d'un dialogue entre les commerçants concernés et les PSP émetteurs.

L'identification de ces commerçants prioritaires est effectuée par les PSP émetteurs en association avec la Banque de France et selon les critères définis en annexe n° 4.

[Nouveau] Recommandation n° 3 *ter* : mesures spécifiques applicables aux commerçants identifiés comme prioritaires pour la réduction de la fraude sur les paiements *MIT*

Les commerçants qui acceptent un volume important de paiements *MIT* et présentent pour ces paiements une exposition à la fraude régulièrement supérieure à la moyenne, selon les critères définis en annexe n° 4, sont identifiés comme prioritaires et se voient appliquer des mesures spécifiques.

Les commerçants identifiés comme prioritaires sont informés par leurs PSP acquéreurs ainsi que par l'intermédiaire des schémas de cartes, et doivent présenter un plan d'action à la Banque de France.

À défaut de plan d'action validé par la Banque de France dans un délai d'un mois suivant l'identification d'un commerçant comme prioritaire, celui-ci se voit appliquer des mesures spécifiques proposées par les PSP émetteurs et validées par la Banque de France.

3.4 Sécurité des données de paiement transmises par le payeur lors d'un paiement *MOTO*

Les commerçants qui acceptent des paiements *MOTO* doivent apporter une attention particulière à la sécurité des données de paiements qu'ils manipulent, afin de prévenir leur détournement.

S'agissant des paiements de type *Telephone Order*, le recours à un système informatisé permet d'éviter la manipulation des données par un opérateur : le client payeur saisit ses données de paiement directement sur le clavier de son téléphone à fréquences vocales (qu'il s'agisse d'un téléphone fixe, d'un téléphone mobile ou d'un *smartphone*) et le système transmet automatiquement ces données vers le terminal de paiement, pour permettre l'acceptation du paiement.

Selon le cas d'usage, le client peut soit être en relation directement avec un serveur vocal (par exemple pour le paiement d'une facture : le client saisira alors la référence de la facture avant de

saisir ses données de paiement), soit être en relation avec un opérateur auquel il indique les caractéristiques des biens ou services qu'il souhaite commander, avant d'être mis en relation avec un serveur vocal au moment de procéder au paiement, soit saisir ses données de paiement sur le clavier du téléphone pendant l'échange avec l'opérateur.

Recommandation n° 4 : sécurisation des données de paiement

Les commerçants qui acceptent des paiements *MOTO* veillent à garantir la sécurité des données de paiement communiquées par les clients. Les commerçants qui acceptent des paiements par téléphone *(Telephone Order)* veillent dans la mesure du possible à ce que les clients communiquent leurs données de paiement à un automate ou par saisie directe sur le clavier du téléphone plutôt qu'oralement à un opérateur.

Les prestataires de services de paiement acquéreurs veillent au respect de cette recommandation par les commerçants avec lesquels ils ont conclu un contrat d'acceptation.

3.5 Expérimentation de l'authentification des paiements *MOTO*

La mise en œuvre d'un mécanisme d'authentification, même simple (un seul facteur d'authentification), pour les paiements *MOTO* permettrait l'amélioration du niveau de sécurité puisque ces paiements ne font pour l'instant l'objet d'aucune authentification.

Dans certains cas, cette authentification pourrait s'effectuer à l'aide des dispositifs déjà existants, tels que l'authentification par application mobile des paiements effectués par téléphone, pour les porteurs de cartes enrôlés à la solution d'authentification forte par application mobile proposée par leur PSP, ou par la saisie d'un mot de passe à usage unique reçu par SMS.

Certaines solutions d'authentification forte conçues pour les paiements par internet apparaissent à l'inverse incompatibles avec les paiements par téléphone, qui ne permettent pas la saisie d'un mot de passe alphanumérique. La typologie particulière de la clientèle qui recourt aux paiements par téléphone (par exemple, clients ne disposant pas d'un accès à internet et/ou d'une ligne de téléphone mobile) devrait par ailleurs être prise en compte.

Recommandation n° 5 : expérimentation de l'authentification des paiements *MOTO*

Les commerçants et les prestataires de services de paiement (PSP) sont encouragés à proposer pour les paiements de type *MOTO* des solutions d'authentification adaptées à chaque canal de paiement et à la typologie de clientèle concernée.

L'Observatoire appelle par ailleurs l'ensemble des acteurs de la chaîne des paiements (schémas de cartes de paiement, prestataires de services de paiement, prestataires techniques, prescripteurs de normes monétiques…) à œuvrer pour le déploiement d'une solution d'authentification forte des paiements par téléphone *(TO)* à l'horizon du 4e trimestre 2025.

ANNEXE 1: Glossaire

PSP : prestataire de services de paiement.

PSP acquéreur : PSP du bénéficiaire, c'est-à-dire du commerçant qui accepte des paiements par carte.

PSP émetteur : PSP du payeur, c'est-à-dire PSP qui émet la carte.

CIT : *Customer Initiated Transaction*, opération initiée par le client. Cette catégorie couvre la majorité des paiements par carte effectués directement par le porteur de la carte sur les sites de e-commerce.

MIT : *Merchant Initiated Transaction*, opération initiée par le commerçant. Cette catégorie correspond notamment aux paiements dont le montant exact n'est pas connu à l'avance, aux paiements récurrents (abonnements) ou encore aux paiements fractionnés (paiement en plusieurs fois), selon un fonctionnement comparable à celui d'un prélèvement SEPA : le client souscrit à un mandat, validé par authentification forte, par lequel il autorise le commerçant à initier un ou plusieurs paiements ultérieurs dans des conditions prédéfinies (montant unitaire, plafond, périodicité…).

MOTO : *Mail Order – Telephone Order*, paiements pour lesquels le porteur de la carte communique au commerçant par téléphone, courrier postal, courriel, télécopie… le numéro de sa carte et la date d'expiration, données que le commerçant saisit ensuite sur son terminal de paiement électronique. Ce mode de paiement est destiné au paiement d'achats effectués par téléphone (par exemple : réservation de voyage ou d'hôtel) ou par l'envoi d'un bon de commande sur support papier.

Chainage : référence cryptographique d'authentification, sous forme d'une chaîne de caractères alphanumériques, communiquée par le PSP émetteur à la suite de l'authentification forte du client lors de la validation du mandat *MIT*. Cette référence permet aux PSP d'identifier le mandat authentifié fortement au titre duquel un ou plusieurs paiements sont ensuite émis par le commerçant.

Soft decline : mécanisme par lequel le PSP acquéreur ou émetteur rejette un paiement par carte avec demande d'exemption tout en permettant au commerçant (ou à son prestataire d'acceptation technique) de présenter à nouveau la demande de paiement via le protocole *3-D Secure* (opération dite de *retry*). Le rejet est transparent pour le porteur de la carte qui n'a pas à saisir de nouveau ses données de paiement ; en revanche, le porteur devra valider le paiement par authentification forte[9].

Vélocité : montant cumulé des paiements effectués à l'aide d'une même carte auprès d'un même commerçant durant la même période glissante de référence (24 heures).

[9] Voir sur le sujet la note « Trajectoire de mise en œuvre du *soft decline* pour finalisation du plan de migration pour l'authentification forte des paiements en ligne » publiée par l'Observatoire le 18 février 2021 : https://abc-economie.banque-france.fr/sites/default/files/media/2021/12/21/210218_osmp-trajectoire-soft-decline.pdf

ANNEXE 2 : Procédure pour les exemptions au mécanisme de limitation de la vélocité par secteur d'activité et liste actualisée des exemptions sectorielles en vigueur

Une liste des activités exemptées de l'application de la limite de vélocité est définie, pour chaque catégorie de paiements (paiements *MOTO* et paiements par internet hors *3-D Secure*), en fonction du *MCC (Merchant Category Code)* attribué aux commerçants de ce secteur d'activité.

La liste ci-après peut être modifiée, en fonction des taux de fraude et cas d'usage observés, par le comité de pilotage placé sous l'égide du groupe de travail (GT) authentification forte de l'Observatoire. La liste actualisée des exemptions en vigueur est disponible sur le site internet de l'Observatoire.

Motif d'une demande d'exemption d'un secteur d'activité

Conformément aux présentes recommandations, l'objectif est d'identifier les secteurs d'activité pour lesquels le recours au mode de paiement considéré (*MOTO* et/ou paiement par internet hors *3-D Secure*) apparaît justifié et pour lesquels le taux de fraude est maîtrisé. Un secteur d'activité qui subirait une dégradation importante de son taux d'acceptation à la suite de la mise en œuvre du plan, tout en présentant un taux de fraude limité, peut demander une exemption.

Procédure à suivre

Pour qu'une exemption soit accordée à un secteur d'activité, une demande mentionnant la raison ainsi que les éléments énumérés ci-dessous doit être transmise au secrétariat de l'Observatoire (2323-OSMP-ut@banque-france.fr). La demande peut être présentée par un des représentants du secteur d'activité, un représentant des commerçants, un schéma de cartes de paiement ou un PSP acquéreur. L'exemption d'un secteur d'activité peut également être proposée directement par le secrétariat de l'Observatoire.

Liste des éléments à fournir

- Description de l'activité
- Donnée technique : *MCC*
- Catégorie de paiements sur laquelle porte la demande d'exemption : paiements *MOTO* ou paiements par internet hors *3-D Secure*
- Volume des opérations en nombre et en montant pour le *MCC* et la catégorie de paiements concernée
- Nombre et montant des refus liés à la mise en œuvre du plan et la phase en cours (seuil de 500, 250 ou 100 euros)

Critères d'éligibilité

Afin d'être éligible à une exemption, le *MCC* doit respecter les critères suivants (de manière cumulative) :

1. Critère lié à la fraude

Le taux de fraude observé pour le *MCC* sur les paiements à distance internet hors *3-D Secure* ou *MOTO* inférieur à 0,13 % en montant, sur une période idéalement annuelle (et dans tous les cas d'au minimum six mois pour éviter les effets de saisonnalité).

2. Critère lié à la gêne client et commerçant

Le taux de refus en nombre ou en montant sur les opérations du *MCC* liés à la mise en œuvre des recommandations doit être supérieur à 10 %. Ce taux est calculé à partir de la date de début de

mise en œuvre des recommandations (le 7 juin 2024) ou de l'un de ses jalons intermédiaires liés à l'abaissement successif de la limite de vélocité.

Après avoir recueilli l'analyse des schémas de cartes de paiement et des PSP émetteurs, le comité de pilotage placé sous l'égide du GT authentification forte de l'Observatoire accorde ou refuse la demande d'exemption, et informe le demandeur de la décision. La liste des exemptions mise à jour est publiée sur le site internet de l'Observatoire.

Liste des *MCC* bénéficiant actuellement d'une exemption

Paiements par internet hors *3-D Secure*

Néant

Paiements *MOTO*

1771 BÉTON
2741 PRESSE
3000 à 3299 COMPAGNIES AERIENNES *(MCC attribués individuellement)*
3350 à 3449 ENTREPRISES DE LOCATION DE VOITURES *(MCC attribués individuellement)*
3500 à 3999 CHAINES HOTELIERES *(MCC attribués individuellement)*
4011 TRANSPORT FERROVIAIRE
4112 TRANSPORT FERROVIAIRE DE PASSAGERS
4411 TRANSPORTS MARITIMES
4511 TRANSPORTS AERIENS
4722 AGENCES DE VOYAGES
4814 SERVICES DE TELECOMMUNICATION
4900 SERVICES ELECTRIQUES, GAZ, EAU, SANITAIRE
5965 VENTE SUR CATALOGUE
6010 DISTRIBUTION DE CREDIT
6012 INSTITUTIONS FINANCIÈRES
6300 ASSURANCES
6513 LOCATION DE LOGEMENT (bailleurs sociaux)
7011 HEBERGEMENT HOTELS MOTELS
7032 COLONIES ET CAMPS DE VACANCES OU ACTIVITES SPORTIVES
7033 AUTRE HEBERGEMENT TOURISTIQUE
7322 RECOUVREMENT DE CREANCES
7512 LOCATION ET LOCATION BAIL DE VOITURES
8111 SERVICES JURIDIQUES ET AVOCATS
8220 ENSEIGNEMENT SUPÉRIEUR
8398 ŒUVRES SOCIALES ET CARITATIVES
9405 ACHATS ENTRE AGENCES D'UNE MEME ADMINISTRATION

ANNEXE 3 : Procédure de dérogation d'un commerçant au mécanisme de limitation de la vélocité

Conformément aux présentes recommandations, des dérogations individuelles peuvent être accordées, en fonction du taux de fraude observé pour chaque commerçant. La présente annexe précise le processus de dérogation d'un commerçant pour les paiements par internet hors *3-D Secure* ou les paiements *MOTO*.

Motif d'une demande de dérogation pour un commerçant

Un commerçant qui subirait une dégradation importante de son taux d'acceptation à la suite de la mise en œuvre de la recommandation peut demander une dérogation auprès du secrétariat de l'Observatoire (2323-OSMP-UT@banque-france.fr), directement ou par l'intermédiaire de son PSP acquéreur ou de tout autre membre du comité de pilotage. Il est fortement recommandé aux commerçants de solliciter leur prestataire technique d'acceptation et/ou leur PSP acquéreur pour demander une telle dérogation.

Procédure à suivre

Pour qu'un commerçant puisse bénéficier d'une dérogation, la demande présentée doit préciser la raison ainsi que la durée de cette dérogation et comporter un engagement du commerçant pour la sécurisation et la mise en conformité de ses opérations de paiement. Cette dérogation, incluant sa durée de validité, devra être validée par la Banque de France après recueil des avis des représentants des PSP émetteurs et des schémas de cartes de paiement membres du comité de pilotage.

Liste des éléments à fournir

- Description de l'activité du commerçant
- Données techniques : *BIN* acquéreur/*ICA*, *MCC*, *Merchant ID/Card acceptor ID*, *Card acceptor name*
- Catégorie de paiements sur laquelle porte la demande : paiements *MOTO* ou paiements par internet hors *3-D Secure*
- Volume des opérations en nombre et en montant liées à l'activité du commerçant pour la catégorie de paiements concernée
- Actions déjà mises en œuvre en matière de prévention et de détection de la fraude
- Actions planifiées pour se mettre en conformité et lutter contre la fraude
- Durée de dérogation demandée

Critères d'éligibilité

1. Critères liés à la fraude ou à la gêne

Pour bénéficier d'une dérogation, le commerçant doit justifier qu'il se trouve dans l'une des situations suivantes :

- Le taux de fraude du commerçant sur les paiements par internet hors *3-D Secure* ou *MOTO* doit être inférieur à 0,13 % en montant, sur une période idéalement annuelle (et dans tous les cas d'au minimum six mois pour éviter les effets de saisonnalité) ;
- **Ou** le taux de refus en nombre ou montant sur les opérations du commerçant liés à la mise en œuvre des recommandations doit être supérieur à 20 %. Ce taux est calculé à partir de la date de début de mise en œuvre des recommandations (le 7 juin 2024) ou de l'un de ses jalons intermédiaires liés à l'abaissement successif de la limite de vélocité.

2. Critères liés aux actions de lutte contre la fraude

En outre, la délivrance de la dérogation est conditionnée :

- aux actions déjà mises en œuvre par le commerçant en matière de prévention et de détection de la fraude ;
- aux actions planifiées par le commerçant pour se mettre en conformité et lutter contre la fraude.

Après avoir recueilli l'analyse et l'avis des schémas de cartes de paiement et des PSP émetteurs représentés au comité de pilotage, la Banque de France accorde ou refuse la demande de dérogation, et informe de sa décision les parties concernées. Ces dérogations ne sont pas publiées.

Nouveau

ANNEXE 4 : Critères de ciblage des commerçants prioritaires pour la lutte contre la fraude

Le montant total de la fraude liée à un commerçant donné, et le taux de fraude qui découle de ce montant, sont calculés pour chaque type de paiement (*MOTO* d'une part et *MIT* d'autre part) et pour l'ensemble des PSP acquéreurs de ce commerçant (dans le cas où le commerçant dispose de plusieurs PSP acquéreurs).

Paiements *MIT*

- Le commerçant est dit « en incident » s'il présente, chez un émetteur :
  - soit un montant total de fraude supérieur à 5 000 euros / mois et un taux de fraude en montant supérieur à 0,13 % ;
  - soit un montant total de fraude supérieur à 10 000 euros / mois et un taux de fraude en montant supérieur à 0,05 % ;
- Le commerçant devient prioritaire s'il est « en incident » durant au moins 4 des 6 derniers mois, chez 3 des 7 principaux émetteurs français.
- Le commerçant cesse d'être prioritaire si, durant 3 mois consécutifs, il n'est plus « en incident » chez 3 des 7 principaux émetteurs français.

Ces deux sous-ensembles alternatifs de critères permettent de cibler d'une part, les commerçants qui ne maîtrisent pas suffisamment leur taux de fraude (premier sous-ensemble) et d'autre part, les commerçants qui, malgré un faible taux de fraude, présentent une fraude significative en valeur absolue (second sous-ensemble).

Paiements *MOTO*

- Le commerçant est dit « en incident » s'il présente, chez un émetteur, un montant total de fraude supérieur à 5 000 euros / mois et un taux de fraude en montant supérieur à 0,13 %.
- Le commerçant devient prioritaire s'il est « en incident » durant au moins 4 des 6 derniers mois, chez 3 des 7 principaux émetteurs français.
- Le commerçant cesse d'être prioritaire si, durant 3 mois consécutifs, il n'est plus « en incident » chez 3 des 7 principaux émetteurs français.