Observatoire de la sécurité des moyens de paiement
www.observatoire-paiements.fr

Feuille de route approuvée lors de la réunion plénière du 19 décembre 2024 de l'Observatoire, et intégrée dans la version mise à jour le 21 janvier 2025 du plan de prévention de la fraude sur les paiements à distance hors *3-D Secure*

Adaptation du plan de l'OSMP sur la prévention de la fraude sur les paiements par carte à distance hors *3-D Secure*

1. Les transactions MOTO

a. Contexte

En 2023, sur le périmètre des cartes émises en France, les paiements MOTO représentaient 2% du montant total des paiements par carte mais 9% du montant total de la fraude (16 milliards d'euros échangés, 42 millions d'euros de fraude). Le taux de fraude des transactions MOTO était ainsi 1,7 fois supérieur à celui des transactions internet (0,266% pour les transactions MOTO contre 0,160% pour les transactions internet).

C'est au vu de ces chiffres que le plan de l'OSMP, adopté en juin 2024, visait à réduire la fraude sur les transactions MOTO, en agissant sur trois leviers :

1. D'une part, en limitant ce canal de paiement aux seules transactions légitimes, c'est-à-dire en forçant la mise en conformité de transactions qui ne correspondent pas à des achats de produits ou de services effectués par téléphone ou par correspondance (par exemple des transactions internet ou des transactions de proximité catégorisées à tort comme des transactions MOTO) ;

2. D'autre part, en sécurisant mieux les transactions MOTO, par la mise en œuvre des recommandations n^{os} 4 et 5 du plan de l'OSMP, portant respectivement sur la sécurisation des données de paiement lorsque la transaction est effectuée par téléphone (par exemple saisie directe du numéro de la carte sur le clavier du téléphone) et sur l'expérimentation de l'authentification des paiements MOTO ;

3. Enfin, en invitant les commerçants et les utilisateurs à recourir à d'autres canaux de paiement plus sécurisés (exemples : paiement par lien, ou transaction sur un terminal de paiement mobile lorsque la transaction se fait en proximité).

Par son action, l'OSMP cherche à conforter le positionnement de « niche » des transactions MOTO, qui doivent être circonscrites aux seuls modèles d'affaires légitimes (par exemple vente par correspondance, vente sur catalogue papier…) et à certaines populations ciblées (par exemple, dépourvues d'internet ou de *smartphone*).

Pour inciter à la prise en compte de ces recommandations, le plan de l'OSMP a prévu une limite de vélocité (vélocité = montant cumulés des achats / carte / commerçant / période

de 24 heures glissantes), qui avait vocation à être progressivement abaissée. Les prestataires de services de paiement (PSP) émetteurs sont ainsi invités à rejeter les paiements MOTO dès lors que le montant du paiement conduit au dépassement de la limite de vélocité.

Depuis le 10 juin 2024, cette limite de vélocité est fixée à 500 euros pour les paiements MOTO.

Sont cependant exclus de cette limite de vélocité les paiements MOTO qui ont fait l'objet d'une authentification forte, ainsi que les secteurs – définis par leur MCC (*Merchant Category Code*) – bénéficiant d'une exemption sectorielle, qui est formalisée en annexe 2 du plan de l'OSMP.

b. Constats

Le seuil de 500 euros a été mis en œuvre par les PSP émetteurs à partir du 10 juin 2024. D'après les statistiques recueillies par la Banque de France auprès des principaux PSP émetteurs de la Place, l'application de cette limite de vélocité a motivé un rejet sur 0,45% des transactions MOTO reçues en autorisation.

Le Comité de pilotage a décidé de suspendre l'abaissement de la limité de vélocité sur les paiements MOTO, qui était initialement prévue à 250 euros le 9 septembre et à 100 euros le 14 octobre 2024, et de réajuster le plan sur ce périmètre de transactions.

Trois facteurs ont, en effet, plaidé en faveur d'une telle temporisation :

1. D'une part, les transactions catégorisées comme MOTO mélangent à la fois des usages légitimes (une transaction à distance par téléphone ou courrier) et des usages illégitimes (une transaction par carte sur internet ou en proximité catégorisée à tort comme MOTO), et il est impossible pour le PSP émetteur de distinguer avec certitude les uns des autres ;

2. D'autre part, les commerçants, qui acceptent aujourd'hui des paiements MOTO, ont besoin de temps pour déployer des parcours alternatifs et pour accompagner leurs clients (par exemple page internet, paiement par lien, sécurisation des données de la carte par saisie sur clavier, équipement en TPE mobile ou *softPOS* etc.) ;

3. Enfin, même si une expérimentation d'authentification forte des paiements MOTO a été conduite à l'automne 2024, confirmant la faisabilité de cette authentification, les commerçants ne peuvent encore pas y recourir, dans l'attente de sa mise en œuvre opérationnelle.

Par ailleurs, le Comité de pilotage a constaté qu'une part significative de la fraude sur les transactions MOTO provenait de commerçants bénéficiant d'une exemption sectorielle. Sur la base de données mensuelles collectées à partir du mois d'avril auprès des PSP émetteurs, le Comité de pilotage a en effet relevé que les paiements MOTO, bénéficiant d'une exemption sectorielle, représentaient une part significative des flux (59% des montants échangés par MOTO) et de la fraude (58 % des montants de fraude).

Cela étant, le Comité de pilotage relève **les premiers effets positifs** de l'application d'une limite de vélocité sur les paiements MOTO :

- Si les données demandent à être confirmées dans le temps et que leur analyse appelle la plus grande prudence en raison du caractère cyclique de la fraude, le taux de fraude sur les paiements MOTO sur des MCC soumis au plan de l'OSMP est passé de 0,357% au 2e trimestre 2024 à 0,297% au 3e trimestre 2024.

- Les commerçants, accompagnés par leurs PSP acquéreurs et leurs prestataires, ont également été encouragés à évaluer le bien-fondé de leurs usages, à déployer des solutions alternatives au MOTO et/ou à mieux sécuriser ces transactions (saisie des données de la carte sur clavier pour les transactions passées par téléphone, recours à des prestataires certifiés PCI-DSS etc.)

- Des acteurs de la Place ont également expérimenté le 10 octobre 2024 l'authentification forte des paiements MOTO avec utilisation du protocole *3-D Secure*. Avant de pouvoir être commercialisée, cette solution demande encore des développements, des échanges avec les PSP pour prendre en compte la diversité des solutions d'authentification forte proposées aux porteurs (notification sur application mobile, « SMS renforcé » etc.) et des évolutions de standards pour que les transactions MOTO fortement authentifiées soient catégorisées et reconnues comme telles tout au long de la chaîne monétique.

c. Propositions pour la continuation du plan en 2025

Au regard de ce qui précède, pour poursuivre le plan de sécurisation des transactions MOTO, le comité de pilotage propose de :

- **Maintenir la limite de vélocité à 500 euros pour les commerçants n'appartenant pas un secteur exempté, aussi longtemps qu'une solution d'authentification forte reposant sur le protocole 3-D Secure ne sera pas commercialisée et reconnue par les différents acteurs de la chaîne monétique ;**

- **Soutenir l'écosystème des paiements (*scheme*, prestataires de services de paiement, prestataires techniques, prescripteur de normes monétiques) dans le déploiement d'une solution d'authentification forte des paiements initiés par téléphone (TO) à l'horizon du T4-2025 ;**

- **Engager un dialogue avec une dizaine de commerçants prioritaires, appartenant à des secteurs (MCC) aujourd'hui exemptés de la limite de vélocité à 500 euros, présentant une activité MOTO importante avec une exposition à la fraude régulièrement supérieure à la moyenne de la Place.**

Ces premiers commerçants ont été identifiés par les PSP émetteurs en association avec la Banque de France. Ceux-ci seront avertis, par le biais de leurs acquéreurs et prestataires, ainsi qu'au travers des *schemes*. Par l'intermédiaire de leurs prestataires d'acceptation et de leurs acquéreurs, ces commerçants devront présenter un plan d'action à la Banque de

France d'ici fin février 2025, apportant les preuves de leur engagement à mieux sécuriser ces transactions MOTO (cf. recommandation n°4 sur la sécurisation des transactions passées par téléphone) et/ou à déployer des parcours de paiement alternatifs plus sécurisés (ex. paiement internet par lien). À défaut de plan d'action, après décision par le Comité de pilotage, une limite de vélocité pourrait leur être appliquée par les PSP émetteurs :

- à partir du **10 mars 2025** une limite de vélocité à **2000 euros**
- à partir du **10 avril 2025** une limite de vélocité à **1000 euros**
- à partir du **12 mai 2025** une limite de vélocité à **500 euros**

À partir de mars 2025, et en fonction des premiers résultats, le Comité de pilotage pourra décider d'adopter une démarche similaire à une liste plus élargie de commerçants appartenant toujours à des secteurs aujourd'hui exemptés de la limite de vélocité à 500 euros.

Si les exemptions sectorielles sont pour le moment maintenues, il est ainsi progressivement souhaité que les exemptions sectorielles disparaissent au profit au profit de **dérogations individuelles**, accordées selon les critères et la procédure déjà définis en annexe 3. Les commerçants effectuant un usage légitime du MOTO, ayant démontré une maîtrise de leur taux de fraude et apporté les preuves de leur engagement dans la sécurisation de leurs transactions (cf. recommandation n°4 sur la sécurisation des transactions passées par téléphone), ont spécialement vocation à bénéficier d'une exemption individuelle. **Ces dérogations individuelles peuvent être accordées sans limite de temps par le Comité de pilotage.**

2. Les transactions internet hors *3-D Secure*

a. Contexte

L'Observatoire constate une nette amélioration de la sécurité des paiements par carte sur internet lorsqu'ils transitent par *3-D Secure*, que ceux-ci débouchent sur une authentification forte ou non du porteur (taux de fraude de 0,095% en 2023). En revanche, les paiements hors *3-D Secure* sans authentification forte sont comparativement près de quatre fois plus fraudés avec un taux de fraude de 0,358%. Ainsi, parmi tous les paiements par carte sur internet, les paiements hors *3-D Secure* sans authentification forte représentent 24% des montants échangés mais 53% de la fraude (187 millions d'euros de fraude).

Si une minorité de ces flux (4% des montants) sont des transactions dites *one leg* avec des acquéreurs situés en dehors de l'espace économique européen (EEE), la grande majorité de ces flux est constituée de transactions initiées par le marchand (*Merchant Initiated Transaction*, MIT) et de transactions initiées par le porteur (*Customer Initiated Transaction*, CIT) au sein de l'EEE. Pour ces dernières, la demande d'exemption à l'authentification forte, si elle est bien présente et renseignée, est véhiculée dans les flux d'autorisation, en dehors de *3-D Secure*.

Le plan de l'OSMP adopté en juin 2024 visait donc à renforcer la sécurité des paiements par carte sur internet, en agissant sur trois leviers :

1. D'abord, en demandant aux commerçants, à travers leurs prestataires et leurs PSP acquéreurs, à systématiquement utiliser le protocole *3-D Secure* pour leurs transactions CIT (recommandation n°1)

2. D'autre part, en assurant un chaînage valide des transactions MIT, qui pour être valables doivent au préalable avoir fait l'objet d'un mandat validé par authentification forte systématique du porteur (recommandation n°2). Cette exigence de chaînage valide des MIT avait été formalisée par l'Autorité bancaire européenne (ABE) dans sa Q&A n°4031 publiée le 1er mars 2019.

Pour donner un caractère incitatif à ces recommandations, l'OSMP avait décidé d'introduire :

- un mécanisme de rapprochement entre les MIT et les mandats de paiements validés par authentification forte, de façon à ce que les PSP émetteurs puissent notifier les anomalies identifiées aux commerçants concernés ;

- une limite de vélocité spécifique sur ces transactions (vélocité = montant cumulés des achats / carte / commerçant / 24 heures glissantes) avec un seuil, qui avait vocation à être progressivement abaissé. Les PSP émetteurs sont ainsi invités à rejeter les paiements internet hors *3-D Secure*, dès lors que le montant du paiement conduit au dépassement de la limité de vélocité. Ce rejet se fait de préférence par *soft decline*, de façon à ce que le commerçant, toujours au travers de ses prestataires d'acceptation et PSP acquéreurs, puissent représenter la transaction avec un appel à 3-D Secure.

Cette limite de vélocité d'abord établie à 500 euros le 10 juin 2024 a ensuite été progressivement abaissée jusqu'à 100 euros depuis le 14 octobre 2024.

Les œuvres sociales et caritatives sont le seul secteur exempté de l'application de cette limite de vélocité. Par ailleurs, Paypal a aussi bénéficié d'une exemption temporaire jusqu'à la fin du mois d'août 2024, de façon à corriger certaines de ces pratiques.

b. Constats

Après plusieurs mois de mise en œuvre, il apparaît que la limite de vélocité touche essentiellement les transactions CIT qui sont exemptés de SCA en dehors de *3-D Secure*. Sur les mois de juin à septembre 2024 (avant l'abaissement du seuil à 100 euros), 7,25% de ces transactions reçues en autorisation ont été rejetées (*soft decline*) par les PSP émetteurs en application du plan de l'OSMP.

Ces transactions CIT exemptées de SCA hors *3-D Secure* représentent toujours près d'un tiers des flux CIT (en volume). Toutefois, et s'il convient encore d'associer la plus grande prudence à ces conclusions, le taux de fraude sur les transactions CIT hors *3-D Secure* est passé de 0,163% au T2-2024 à 0,137% au T3-2024.

En revanche, seulement 0,52% des transactions MIT reçues en autorisation ont été rejetées par les PSP émetteurs. En effet, les PSP émetteurs peuvent rejeter les MIT qui ne respectent manifestement pas les protocoles d'échange, par exemple en ne renseignant pas l'identifiant de chaînage. Dans de telles situations, les PSP émetteurs peuvent rejeter les MIT dès 0,01 euro.

Les PSP émetteurs ne sont toutefois pas encore parvenus à définir un ensemble de règles communes pour identifier *a posteriori* les chaînages invalides, en menant un travail de rapprochement des références de chaînage des authentifications préalables réalisées. Une proposition avait été formulée en juillet, mais deux principales difficultés avaient été mises à jour : (i) d'une part, cette procédure ne prenait en compte qu'un historique de 13 mois, ce qui aurait conduit à déclarer non-conformes des transactions MIT pourtant chaînées à des CIT fortement authentifiées plus vieilles de 13 mois et (ii) d'autre part, il est encore fréquent que les commerçants changent de prestataire d'acceptation, sans que le nouveau ne récupère les identifiants de chaînage de la CIT initiale.

Pour contourner ces difficultés sur les MIT, le Comité de pilotage a toutefois soutenu la démarche des PSP émetteurs de rejeter, par *soft decline*, les demandes de renseignement à 0 euros émanant de deux grands commerçants, dans la mesure où ces demandes de renseignement étaient suivies de MIT, sans jamais que le porteur ne soit fortement authentifié. Après une phase pilote chez SG, cela a été mis en place de façon concertée à partir du 18 novembre, de façon à convaincre ces deux grands commerçants, associés au même prestataire d'acceptation technique, à faire évoluer leurs pratiques.

c. Propositions pour la continuation du plan en 2025

Il est d'abord proposé de supprimer l'exemption sectorielle bénéficiant aux œuvres sociales et caritatives à partir du 15 janvier 2025.

Constatant qu'une part encore significative des flux CIT ne font pas d'appel au canal sécurisé *3-D Secure*, le Comité de pilotage suggère un futur abaissement des seuils pour l'application de la limite de vélocité sur les flux CIT sans SCA hors *3-D Secure*:

- **50 euros** à partir du **10 février 2025**
- **30 euros** à partir du **10 mars 2025**
- **0 euro** à partir du **10 avril 2025**

À tout moment, en fonction des retours d'expérience, le Comité de pilotage pourra ajuster les échéances de ce plan. Il est rappelé que les accepteurs recevant un *soft decline* sur des flux CIT hors 3-D Secure doivent resoumettre leur transaction CIT avec un appel *3-D Secure* avec une demande d'authentification forte (ou *challenge mandate*).

Pour augmenter les chances d'obtention d'une exemption, il est donc recommandé aux commerçants et aux prestataires d'acceptation technique de présenter directement leur transaction CIT via *3-D Secure* avec une demande d'exemption, et ce sans attendre la réception d'un premier *soft decline*.

En ce qui concerne les MIT, le comité de pilotage propose une action en trois paliers successifs :

1. **D'abord, au cours du T1-2025, agir sur une dizaine de commerçants ayant des pratiques de MIT douteuses au regard de leurs activités commerciales et exposées à la fraude.** Ces commerçants ont été identifiés par les PSP émetteurs en association avec la Banque de France. Les commerçants cités seront avertis par leurs acquéreurs et leurs prestataires d'acception, ainsi que par le biais des *schemes*.

    a. **À partir du 9 janvier 2025, élargir les rejets des demandes de renseignement à 0 euro à ces commerçants**. Il s'agit de cibler les demandes de renseignement immédiatement suivies de MIT, alors qu'il s'agit en réalité de situations de CIT[1].

    b. **À partir du 10 février 2025, appliquer une limite de vélocité en nombre de transactions aux transactions MIT de ces commerçants**, qui sont correctement chaînées à une CIT initiale, mais qui sont manifestement utilisées de manière impropre, compte tenu de leurs modèles d'affaires (achat sur internet en présence du porteur). Cette limite de vélocité sera individualisée pour chaque commerçant concerné, en fonction de son modèle d'affaires.

2. **Ensuite, à partir du T2-2025, en fonction des résultats obtenus sur ce premier palier, appliquer ces deux leviers d'action (rejet des demandes de renseignement à 0 euro <u>et</u> limite de vélocité individualisée en nombre de transactions) à une nouvelle liste élargie de commerçants.** Ceux-ci seront identifiés par les PSP émetteurs en association avec la Banque de France, en tenant toujours compte de critères de flux, de conformité et de fraude.

3. **Enfin, au cours du 2e semestre 2025 avec des dates restant à définir, bloquer les transactions MIT qui seraient chaînées avec une référence de chaînage invalide, c'est-à-dire une référence de chaînage sans lien technique ou économique avec un mandat de paiement validé par authentification forte**

    a. **Il s'agit, d'abord, de rejeter les transactions présentant des identifiants techniques dit de « *grandfathering* »**

Il s'agit de mettre fin à une tolérance appliquée aux MIT, dont les mandats avaient été consentis par les consommateurs à une date antérieure à la mise en application des nouvelles règles d'authentification de la DSP2 (officiellement le 14 septembre 2019, en pratique en 2021).

Le Comité de pilotage note que l'arrêt du *grandfathering* est déjà applicable ou planifié dans les trois principaux réseaux de paiement par carte en France.

- Pour le réseau CB, les MIT correspondant à des abonnements souscrits depuis le 1er janvier 2022 doivent être associés à un identifiant unique de transaction (champ CBAE 47-99), qui a été renvoyé par l'émetteur après une authentification forte du

[1] Il est précisé que les prochains protocoles CB2A/CBAE permettront désormais de distinguer les demandes de renseignement à 0 euro, par exemple utilisées pour vérifier la validité de la carte, des CIT servant à formaliser un mandat pour des MIT futures.

porteur. Pour les MIT correspondant à des abonnements souscrits avant le 1er janvier 2022, une tolérance existe pour un identifiant unique de transaction par défaut (*9999999999999*) jusqu'à fin décembre 2024. Le commerçant doit ainsi identifier son porteur au plus tard d'ici le 1er janvier 2025 de façon à recevoir un nouvel identifiant unique de transaction valide.

- Pour le réseau MASTERCARD, le recours à un identifiant par défaut (Trace ID *MCC9999991231*) pour les MIT n'est plus accepté depuis le 18 octobre 2024, avec un suivi de conformité qui sera réalisé en 2025.

- Pour le réseau VISA, l'identifiant de chaînage générique n'est plus conforme aux règles du *scheme* depuis le 31 octobre 2023.

b. Il s'agit, ensuite, de mieux contrôler *a posteriori* les transactions MIT en rapprochant leurs identifiants de chaînage avec les mandats de paiement préalablement validés par authentification forte

Certaines transactions MIT présentent l'apparence d'un chaînage correct, mais celui-ci ne serait pas lié à un mandat de paiement validé par une authentification forte. Conformément à la recommandation n°2 du plan de l'OSMP, les PSP émetteurs sont invités à finaliser au cours du 1er semestre 2025 une procédure de contrôle *a posteriori* reposant sur des critères communs. À défaut de remédiation, les commerçants identifiés avec des pratiques invalides de chaînage pourraient ensuite être soumis à une limite de vélocité individualisée.

3. Autres propositions du Comité de pilotage

Le plan de l'OSMP, ainsi mis à jour pour 2025, sera traduit et diffusé en anglais en janvier pour assurer sa bonne diffusion auprès des commerçants et des prestataires européens, ayant une activité commerciale en France.

Le Comité de Pilotage continuera d'associer FrenchSys aux côtés des émetteurs, acquéreurs et *schemes* pour assurer une application aussi homogène que possible du plan de l'OSMP dans les différents réseaux de paiement (en rappelant par exemple les modalités de rejeu en *3-D Secure* pour les commerçants après avoir reçu un *soft decline*, ou en spécifiant les standards pour l'authentification forte des paiements initiés par téléphone).