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

RECOMMANDATIONS DE L'OBSERVATOIRE

MODALITÉS DE REMBOURSEMENT DES OPÉRATIONS DE PAIEMENT FRAUDULEUSES

1- CONTEXTE DES TRAVAUX

1.1 La mise en place de l'authentification forte du porteur pour sécuriser les paiements électroniques

Le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique est une disposition clé en matière de sécurité des paiements, qui a été introduite par la deuxième directive européenne sur les services de paiement (DSP2)[1]. Pour ce qui concerne les paiements par carte sur internet, la mise en œuvre de cette disposition au niveau du marché français s'est appuyée sur un plan de migration adopté par l'Observatoire à l'automne 2019, et l'authentification forte a ensuite été déployée sur une période de deux ans environ.

Pour mémoire, l'authentification forte repose sur l'utilisation de deux éléments ou plus appartenant au moins à deux catégories différentes de facteurs d'authentification, parmi les trois catégories suivantes :

- « connaissance » : une information que seul l'utilisateur connaît, par exemple un code confidentiel, un mot de passe ou une information personnelle ;
- « possession » : un objet que seul l'utilisateur possède, et qui peut être reconnu sans risque d'erreur par le prestataire de services de paiement (PSP) comme par exemple une carte, un smartphone, une clé USB, un boîtier sécurisé, une montre ou un bracelet connecté, etc. ;
- « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique (empreinte digitale, visage, voix…).

Lorsque l'enrôlement d'un élément de possession, c'est-à-dire l'association à un utilisateur d'un objet que seul cet utilisateur possède et qui servira de facteur d'authentification forte, s'effectue à distance, alors cet enrôlement doit lui-même être validé par authentification forte.

La DSP2 dispose que ces éléments doivent être indépendants : la compromission de l'un ne doit pas remettre en question la fiabilité des autres, de manière à préserver la confidentialité des données d'authentification. En outre, concernant les paiements à distance, la DSP2 ajoute une exigence supplémentaire : les données d'authentification doivent être liées à l'opération de paiement, de sorte qu'elles ne peuvent être réutilisées pour une opération de paiement ultérieure. On parle de lien dynamique :

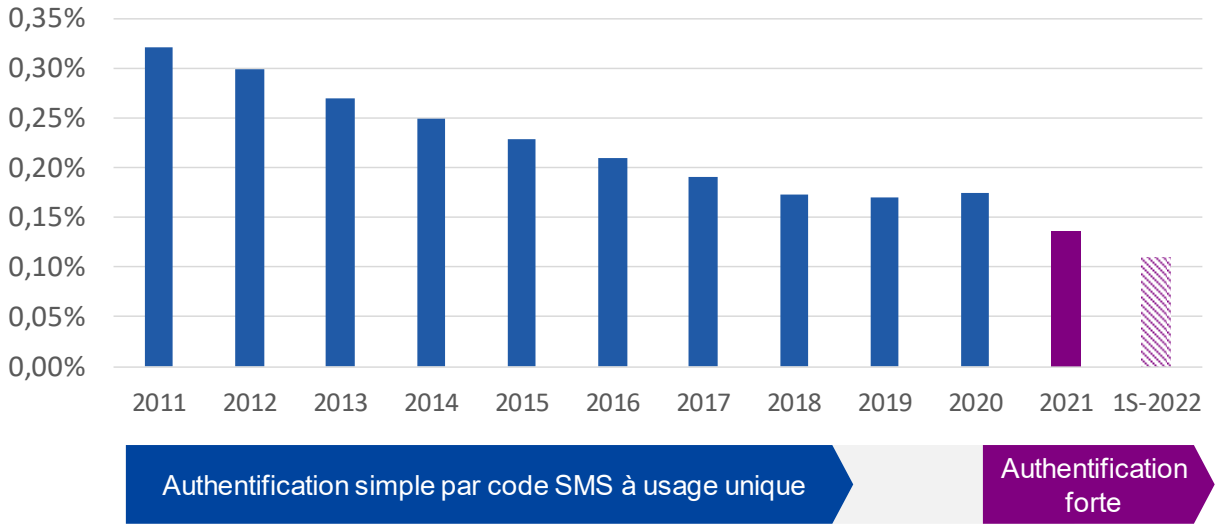
- le code d'authentification généré pour l'opération est spécifique au montant de l'opération et au bénéficiaire identifié ;
- toute modification du montant ou du bénéficiaire nécessite une nouvelle authentification.

[1] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur

Dans le cas du recours à un facteur biométrique, la clé de validation de l'opération de paiement générée après lecture de l'empreinte devra être également à usage unique.

S'il est encore trop tôt pour tirer un bilan définitif de la mise en place de l'authentification forte, l'Observatoire note d'ores et déjà qu'elle a contribué à faire baisser substantiellement le taux de fraude sur les paiements internet, après deux ans de stagnation qui soulignaient les limites atteintes en termes de sécurité par l'utilisation de l'authentification simple (SMS-OTP) déployée durant les années 2010. Les premières données disponibles concernant 2022 montrent que le taux de fraude devrait continuer à baisser de façon significative.

Graphique 1 – Évolution du taux de fraude sur les paiements domestiques par carte sur internet



Sur l'ensemble des paiements par carte sur internet (y compris les paiements réalisés auprès de sites étrangers par les porteurs français), le taux de fraude en montant sur les paiements en ligne est ainsi passé de 0,249 % en 2020 à 0,196 % en 2021, soit son plus bas niveau historique, alors que sur la même année, le montant des opérations de paiement par carte a cru de 21 % pour atteindre 177,1 milliards d'euros.

1.2 Le développement de nouvelles techniques de fraude basées sur la manipulation pour contourner l'authentification forte

Si la mise en place de l'authentification forte permet d'assurer un haut niveau de sécurité technologique sur l'ensemble de la chaîne des paiements, il rend d'autant plus nécessaire de renforcer la vigilance des utilisateurs, qui sont de plus en plus ciblés par des fraudeurs. À défaut de pouvoir émettre eux-mêmes des paiements frauduleux, les fraudeurs essayent en effet de manipuler leurs victimes par téléphone ou par messagerie instantanée pour les amener à valider à leur place des opérations frauduleuses, en se faisant généralement passer pour leur banque (par exemple, en prétextant des tests de sécurité, la lutte contre la fraude ou en annonçant une opération atypique sur le compte de la victime nécessitant un contrôle par authentification). Ils parviennent à convaincre leur victime de communiquer des informations leur permettant d'utiliser à distance leurs moyens de paiement. Ils récoltent d'abord des informations sur leur victime grâce aux attaques de type hameçonnage par SMS ou message électronique, au vol de données à des tiers mais aussi grâce aux réseaux sociaux et à différentes sources publiques, puis contactent directement la victime. Les fraudeurs ont également recours au *« spoofing »*, c'est-à-dire qu'ils parviennent à usurper le numéro de téléphone d'une agence bancaire afin de rassurer leur victime.

Si l'Observatoire constate que la proportion de paiements frauduleux avec authentification forte est restée contenue en 2021, soit 9 % du nombre total des paiements frauduleux par carte sur internet, leur proportion dans le montant total des opérations frauduleuses est bien plus significative (30 % du montant total de 103 millions d'euros).

Selon les associations de consommateurs, ce nouveau type de fraude entrainerait une augmentation du montant du préjudice financier supporté par les consommateurs, en dépit de la baisse globale de la fraude. En effet, avec la mise en œuvre de l'authentification forte, le risque de refus de remboursement des opérations frauduleuses par la banque à son client est susceptible d'avoir augmenté de manière significative.

À ce titre, la Banque de France et l'Observatoire de la sécurité des moyens de paiement ont été interpelés par les associations de consommateurs sur les difficultés rencontrées par leurs adhérents pour bénéficier du droit à remboursement en cas de fraude prévu par les textes, en particulier dans les cas où l'opération contestée a fait l'objet d'une authentification forte.

1.3 Les travaux conduits par l'Observatoire sur le traitement des contestations pour motif de fraude

L'Observatoire a décidé de mettre en place un groupe de travail chargé d'émettre des recommandations sur le traitement des demandes de remboursement d'opérations frauduleuses en vue d'assurer la bonne application des dispositions de la DSP2 en matière de protection des consommateurs victimes de fraude.

Le groupe de travail s'est réuni à cinq reprises entre octobre 2022 et février 2023. Les participants à ce groupe de travail représentent les associations de consommateurs, les prestataires de services de paiement, leurs fédérations professionnelles, les médiateurs et les autorités (police, gendarmerie, ACPR, Banque de France).

Le secrétariat du groupe de travail a défini les éléments en entrée ainsi que les livrables attendus en sortie.

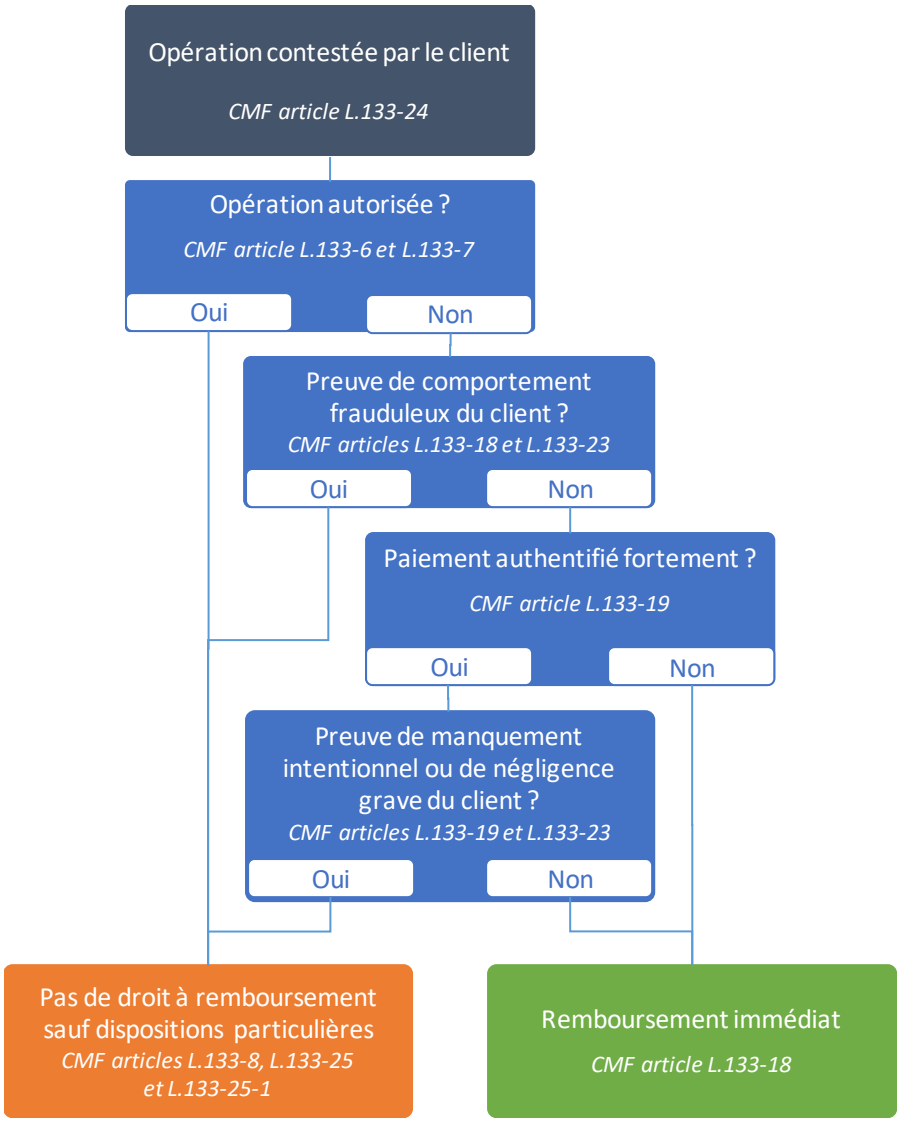
Éléments en entrée	Livrables attendus en sortie
▪ Réglementation et jurisprudence applicables au traitement des contestations ▪ Identification des développements récents en matière de typologie des cas de fraude ▪ Expérience des médiateurs bancaires et des associations de consommateurs sur des demandes non satisfaites de remboursement pour motif de fraude ▪ Synthèse des contrôles sur place conduits par l'ACPR concernant le traitement des demandes de remboursement des clients pour motif de fraude	▪ Rappel des règles applicables en matière de traitement des demandes de remboursement pour motif de fraude ▪ Grille d'analyse des demandes de remboursement (identifier les cas pour lesquels un remboursement immédiat devrait être systématique) ▪ Recommandations sur le traitement des demandes de remboursement pour motif de fraude ▪ Revue des motifs identifiés dans le cadre des déclarations à la Banque de France au titre de l'article L.133-18 du CMF *(à engager à l'issue de la publication des recommandations présentées dans ce document)*

2- RÉGLEMENTATION APPLICABLE AUX CONTESTATIONS D'OPÉRATIONS DE PAIEMENT

2.1 Le caractère « autorisé » de la transaction comme facteur déterminant

Selon le code monétaire et financier (CMF), le remboursement d'une opération contestée est conditionné par le fait qu'elle ait été autorisée ou non par le payeur[2], c'est-à-dire si celui-ci a explicitement donné son consentement à son exécution dans les conditions prévues par sa convention de compte, notamment par l'utilisation du moyen d'authentification forte mis à sa disposition.

Le schéma ci-dessous illustre l'articulation des textes relatifs aux opérations contestées dans le code monétaire et financier.



- **Si l'opération est reconnue comme « autorisée » et qu'elle n'a pas été affectée par une erreur d'exécution de la part du prestataire de services de paiement du payeur, la réglementation**

[2] Hors cas particulier du régime de remboursement applicable à certaines opérations autorisées, dont les prélèvements intervenus depuis moins de huit semaines (articles L.133-25 et L.133-25-1 du CMF)

relative aux moyens de paiement ne prévoit pas de droit à remboursement. C'est le cas notamment pour les demandes de remboursement pour cause de litige commercial entre le payeur et le bénéficiaire (par exemple : non livraison ou malfaçon d'un produit, souscription d'un produit d'épargne, de crédit ou d'un service financier auprès d'un intermédiaire malveillant…). **À défaut de droit à remboursement prévu par la réglementation, la qualification de l'opération comme « autorisée » n'empêche pas une réclamation à l'encontre du bénéficiaire, voire une action civile ou pénale**.

- **Si l'opération est reconnue comme « non autorisée », le payeur dispose en règle générale d'un droit à remboursement immédiat prévu par le Code monétaire et financier**, dont les modalités diffèrent toutefois en fonction de différents paramètres tels que la nature de l'instrument de paiement, le fait qu'il soit doté de données de sécurité personnalisées ou l'usage d'un dispositif d'authentification forte lors de la transaction. **Ce remboursement peut toutefois être refusé en cas de comportement frauduleux de l'utilisateur lui-même ou, pour les seules opérations authentifiées de manière forte dans les conditions prévues par la loi[3], en cas de négligence grave de l'utilisateur démontrée par le prestataire de services de paiement**.

L'appréciation du caractère autorisé ou non d'une opération est donc un critère déterminant pour le remboursement des clients qui contestent une opération de paiement pour motif de fraude. Cette question est particulièrement sensible dans le cas d'opérations ayant fait l'objet d'une authentification forte, où il convient de déterminer dans quelle mesure le succès de l'authentification forte peut être ou non assimilé à un consentement du porteur de l'instrument de paiement.

L'objectif des recommandations présentées ci-après est de réduire la « zone grise » sur l'appréciation du caractère « non autorisé » d'une opération contestée, au travers de l'examen de différents cas de contestation, du plus simple au plus complexe. Il s'agit de déterminer sous quelles conditions l'opération peut être présumée non autorisée et donner lieu à remboursement immédiat, à moins que le prestataire de service de paiement n'apporte la preuve de la fraude ou de la négligence grave de l'utilisateur.

2.2 Apports de la jurisprudence sur l'appréciation de la négligence grave de l'utilisateur de services de paiement

Les textes ne précisent pas explicitement quels sont les éléments qui caractérisent une négligence grave de l'utilisateur, qui est le principal motif invoqué par les prestataires de services de paiement pour refuser le remboursement d'un paiement non autorisé. En outre, il convient de noter qu'il n'existe pas encore de jurisprudence de la Cour de Cassation portant sur une contestation d'opération effectuée postérieurement à l'entrée en vigueur de la DSP2 et des textes pris pour sa transposition et son application. La jurisprudence actuelle (relative à des contestations d'opérations effectuées antérieurement à l'entrée en vigueur de la DSP2) repose sur le concept d'utilisateur « normalement attentif ». Dans ce contexte, il convient pour les prestataires de services de paiement qui souhaitent recourir à ce motif d'exclusion du droit à remboursement d'évaluer le cas au regard de la jurisprudence, qui sera vraisemblablement amenée à s'enrichir dans les prochaines années, certaines décisions étant néanmoins d'ores et déjà éclairantes.

[3] Article L.133-4, f) du CMF

3- RECOMMANDATIONS GÉNÉRALES APPLICABLES AU TRAITEMENT DES CONTESTATIONS D'OPÉRATIONS DE PAIEMENT

3.1 Délai pour la conduite des investigations

Lorsque des investigations doivent être conduites par le prestataire de services de paiement (par exemple, investigations liées à une opération de paiement authentifiée de manière forte, cf. paragraphe 4.3 ci-après), il apparaît nécessaire que la durée de ces investigations soit limitée dans le temps. En effet, il s'agit, d'une part d'éviter la disparition ou l'oubli des éléments d'information utiles au PSP, et d'autre part de permettre au client de disposer à une échéance suffisamment proche et connue d'une réponse claire et définitive à sa contestation.

Recommandation n° 1 : délai maximum des investigations

Les prestataires de services de paiement sont invités à mettre en œuvre les investigations dès la réception de la contestation, en prenant en compte les éventuels éléments de description fournis par l'utilisateur (tels que précisés par la recommandation n°8)**, et à en limiter la durée à 30 jours, sauf situation exceptionnelle.**

3.2 Modalités et délai de reprise des fonds

Il existe différents cas de figure dans lesquels une décision initiale de remboursement du client par le prestataire de services de paiement est susceptible d'être remise en cause *a posteriori*, par exemple en cas d'investigations complémentaires ou si l'utilisateur vient à être remboursé par un autre canal (par la contrepartie de l'opération, via un mécanisme d'assurance…), conduisant le prestataire à procéder à une reprise des fonds. Il apparait nécessaire que l'utilisateur soit informé le cas échéant de cette possibilité au moment de son remboursement initial.

Recommandation n° 2 : information du client en cas de reprise des fonds

En cas de remboursement susceptible de donner lieu à une reprise de fonds ultérieure en fonction du résultat d'investigations engagées, le prestataire de services de paiement informe son client de cette éventualité au moment du remboursement, et veille à ne pas procéder à la reprise des fonds dans un délai excédant 30 jours à compter de la date à laquelle le remboursement a été effectué, sauf situation exceptionnelle.

3.3 Information délivrée au client en cas de refus de remboursement ou de reprise des fonds

Recommandation n° 3 : justification du refus de remboursement

Lorsque le prestataire de services de paiement refuse le remboursement ou procède à la reprise des fonds, il veille à informer le client de cette décision et lui en communique le motif, en prenant soin le cas échéant de joindre les éléments qui la justifient (par exemple, mandat de prélèvement, éléments transmis par le commerçant, preuve de négligence grave…). En outre, il détaille dans cette même communication les modalités suivant lesquelles une réclamation peut être déposée.

4- RECOMMANDATIONS APPLICABLES AU TRAITEMENT DE CAS SPÉCIFIQUES

Les cas présentés ci-après excluent volontairement les demandes de remboursement ne relevant pas du périmètre de la fraude aux moyens de paiement, tels que les litiges commerciaux et les escroqueries (ex: faux produits d'épargne, investissements dans des crypto-actifs crapuleux, arnaques au crédit, etc.), lorsque les opérations concernées ont été autorisées.

De même, les recommandations sont centrées sur l'application du droit à remboursement prévu par la réglementation relative aux moyens de paiement, et excluent les autres mécanismes pouvant exister par ailleurs, tels que les assurances de moyens de paiement, ou encore les gestes commerciaux consentis par les prestataires de services de paiement.

4.1 Opérations de paiement effectuées sans authentification forte

Il convient de rappeler que toutes les opérations ne sont pas soumises à l'obligation d'authentification forte, la réglementation issue de la deuxième directive européenne sur les services de paiement (DSP2) prévoyant un ensemble de cas d'exclusion ou d'exemption à son application :

- Les **paiements en dehors de l'Union Européenne (transactions dites *one leg*)** ;
- Les **ordres de paiement émis par le bénéficiaire du paiement**, tels que les prélèvements ou les paiements par carte de type *Merchant Initiated Transactions* (**MIT**), c'est-à-dire émis par le commerçant sans connexion active de l'utilisateur correspondant notamment les paiements fractionnés ou différés, les abonnements et les paiements à l'usage ;
- Les **paiements éligibles à un motif d'exemption à l'authentification forte prévu par les normes techniques de règlementation (RTS)** arrêtées par l'Autorité Bancaire Européenne[4] :
    - Les paiements sur internet de faible valeur (article 16), soit moins de trente euros et dans la limite de cinq opérations consécutives ou d'un montant cumulé de cent euros ;
    - Les paiements présentant un faible niveau de risque (article 18), c'est-à-dire correspondant aux habitudes de paiement du porteur (achat depuis son terminal habituel, adresse de livraison connue, nature de l'achat, montant, etc.) et pour un montant n'excédant pas cinq cents euros ;
    - Les paiements récurrents (article 14), c'est-à-dire d'un montant et d'une périodicité fixes en faveur du même bénéficiaire, à compter de la deuxième transaction ;
    - Les paiements vers un bénéficiaire de confiance (article 13), c'est-à-dire vers un bénéficiaire désigné comme étant de confiance par le payeur, cette désignation ayant elle-même fait l'objet d'une authentification forte (cette authentification forte lors de l'ajout du bénéficiaire n'ayant ni pour objet ni pour effet d'authentifier de manière forte les opérations de paiement ultérieurement effectuées en faveur de ce bénéficiaire) ;
    - Les paiements initiés électroniquement via des processus ou protocoles de paiement sécurisés réservés à un usage entre professionnels (article 17).
- Les **paiements émis dans le cadre des mécanismes de continuité des infrastructures d'authentification**, en cas d'incident ne permettant pas de mettre en œuvre l'authentification

[4] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

forte du payeur, ainsi que les paiements par carte bancaire effectués durant la phase transitoire (du 14 septembre 2019 au 15 juin 2021) de déploiement de l'authentification forte.

Dans tous les cas listés ci-dessus, l'opération ne peut pas être considérée comme authentifiée de manière forte au sens de la règlementation, alors même que dans la plupart des cas l'absence d'authentification forte est autorisée ou tolérée.

Recommandation n° 4 : principes applicables aux opérations sans authentification forte

Lorsqu'un utilisateur du service de paiement conteste une ou plusieurs opérations qu'il nie avoir autorisées et que ces opérations n'ont pas été authentifiées de manière forte, le prestataire de services de paiement du payeur rembourse sans délai[5] le montant de ces opérations, sauf lorsqu'il a de bonnes raisons de soupçonner une fraude de l'utilisateur lui-même. Ce soupçon de fraude ne peut résulter de la seule utilisation de l'instrument de paiement.

Ce remboursement immédiat ne fait pas obstacle à la reprise ultérieure des fonds lorsque le prestataire de services de paiement réunit des éléments prouvant soit que l'opération a été autorisée (par exemple, par l'existence d'un mandat de prélèvement SEPA[6]), soit qu'une fraude a été commise par l'utilisateur lui-même. En revanche, la négligence, même grave, commise par le payeur ne peut fonder le refus de remboursement d'une opération qui n'a pas été authentifiée de manière forte.

Dans le cas particulier des paiements initiés par le bénéficiaire (prélèvement ou paiement par carte de type MIT - *Merchant Initiated Transaction*), le payeur bénéficie en outre d'un droit à remboursement immédiat dans un délai de 8 semaines qui suit le débit en compte :

- **pour le prélèvement, ce remboursement est sans condition, indépendamment de l'existence ou non d'un mandat de prélèvement ;**
- **pour le paiement par carte ordonné par le bénéficiaire, si l'autorisation donnée n'indiquait pas le montant exact de l'opération de paiement et si le montant de l'opération dépassait le montant auquel le payeur pouvait raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances propres à l'opération.**

Références : articles L133-19 V L133-18, L133-25 et L133-25-1 du CMF et SEPA Direct Debit Core Scheme Rulebook V1.1 section 4.3.4

Le prestataire de services de paiement doit être en mesure de justifier qu'une opération a été authentifiée, et doit à ce titre conserver les éléments techniques (piste d'audit) relatifs à cette authentification. Il en est de même pour la piste d'audit de l'authentification forte effectuée pour l'enrôlement d'un facteur d'authentification.

4.2 Paiement au moyen d'une application mobile se substituant à l'instrument de paiement

[5] La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la contestation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs…).

[6] Sauf pour les prélèvements contestés dans les huit semaines suivant le débit du compte, pour lesquels le payeur dispose d'un droit au remboursement inconditionnel.

Pour réaliser des paiements via une solution mobile disposant de son propre mode d'authentification (ce qui est le cas notamment des solutions mobiles « X-Pay » proposées par les fabricants de terminaux et les éditeurs de systèmes d'exploitation), l'utilisateur doit préalablement enrôler son instrument de paiement sur l'application de paiement de son terminal mobile. Cet enrôlement, considéré comme une opération sensible au sens de la réglementation, nécessite une authentification forte de la part de l'utilisateur (ABE Q&A 2021_6141). La responsabilité de la mise en œuvre de l'authentification forte repose sur le prestataire de services de paiement, à qui il appartient de justifier du respect de cette obligation.

Recommandation n° 5: principes applicables aux opérations réalisées avec une application mobile se substituant à l'instrument de paiement

Lorsque l'utilisateur du service de paiement conteste une opération de paiement qu'il nie avoir autorisée et qui a été réalisée au moyen d'une solution mobile pour laquelle l'enrôlement de l'instrument de paiement n'a pas donné lieu à authentification forte, le prestataire de services de paiement du payeur procède sans délai[7] au remboursement du montant de cette opération.

Références : article L133-18 du CMF et ABE Q&A 2021_6141

4.3 Paiement ayant fait l'objet d'une authentification forte

Comme mentionné précédemment, l'essentiel de la « zone grise » concerne les opérations contestées ayant donné lieu à une authentification forte. Le processus d'investigation des prestataires de services de paiement doit s'attacher à examiner les éléments et paramètres susceptible d'altérer l'authentification forte de l'utilisateur.

Les **éléments d'analyse à prendre en compte** sont notamment :

- **L'existence possible d'une prise de possession du moyen d'authentification forte par une tierce partie**, notamment en cas d'occurrence d'un ou plusieurs facteurs ci-après :
    - le transfert du moyen d'authentification forte en amont de la fraude (par exemple, enrôlement d'un nouveau mobile) ;
    - l'émission d'une nouvelle carte SIM par l'opérateur téléphonique dans le cas d'une solution d'authentification forte de type « SMS renforcé » ;
    - la saisie des identifiants par une tierce partie et/ou sur un terminal n'étant pas identifié comme appartenant à l'utilisateur (cas des solutions d'authentification forte nécessitant une saisie des données d'authentification sur la page de paiement).

- **Les paramètres de l'opération, visant à identifier dans quelle mesure l'utilisateur en est ou non à l'origine :** cette analyse est nécessaire afin de distinguer d'une part les cas de contestation qui pourraient relever d'un litige commercial plutôt que d'une fraude aux moyens de paiement (dans le cas d'un litige commercial, l'opération a été initiée par l'utilisateur), et d'autre part les cas où l'opération a manifestement été initiée par une personne distincte de l'utilisateur (l'utilisateur pouvant cependant être sollicité par le fraudeur au moment de l'authentification).

[7] La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la contestation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs…).

- Les **éléments relatifs au contexte de l'opération**, notamment **la qualité et l'exhaustivité des informations fournies par le prestataire de services de paiement** au moment de l'authentification de l'opération ou via des mécanismes d'alerte en temps réel, ainsi que **les éléments rapportés par l'utilisateur (cf. recommandation n°8)**.

Recommandation n° 6 : principes applicables aux opérations authentifiées de manière forte

Lorsqu'un client conteste une opération de paiement qu'il nie avoir autorisée et que cette opération a été authentifiée de manière forte, le prestataire de services de paiement doit procéder dans le délai d'un jour ouvré à une première analyse de cette opération. Cette analyse vise à apprécier, en prenant en compte les 3 familles de paramètres mentionnées ci-après, si l'utilisateur est susceptible d'avoir consenti à l'opération ou s'il s'agit d'une opération non autorisée :

- **les paramètres techniques associés à l'opération** (tels que l'origine de la transaction, le terminal utilisé pour l'achat ou la connexion à la banque en ligne, la localisation géographique…), pour évaluer la possibilité que l'utilisateur en soit à l'origine ;
- **les modalités de l'authentification forte mise en œuvre** (tel que le type de solution, intégrité des facteurs d'authentification et du canal de communication, la preuve d'une utilisation précédente de la solution par l'utilisateur ou au contraire caractère récent de l'enrôlement…), pour s'assurer du rôle effectif de l'utilisateur ;
- **les éléments de contexte dont il dispose** : tels que les informations délivrées à l'utilisateur lors de l'authentification (cf. recommandation n°11), les éventuelles alertes liées à l'opération et adressées à l'utilisateur par différents canaux de communication, les éléments rapportés par l'utilisateur (cf. recommandation n°8), tels que les procédés manipulatoires auxquels il a pu être confronté**.**

À l'issue de cette première analyse :

- **soit le prestataire de services de paiement constate que l'opération n'a pas été autorisée ou a un doute sur le consentement donné à l'opération, auquel cas il procède sans délai[8] au remboursement de la transaction ;**
- **soit le prestataire de services de paiement dispose de bonnes raisons de soupçonner une fraude de l'utilisateur[9] et qu'il communique ses raisons à la Banque de France, auquel cas il peut refuser de rembourser immédiatement la transaction dans les conditions prévues à la recommandation n°3 ;**
- **soit le prestataire de services de paiement a suffisamment d'éléments de preuves pour considérer que l'opération a été autorisée par l'utilisateur[10] ou que ce dernier a été gravement négligent[11] ou qu'il n'a pas satisfait intentionnellement à ses obligations, auquel cas il peut refuser le remboursement de l'opération contestée au client, dans les conditions prévues à la recommandation n°3.**

[8] La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la contestation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs…).

[9] Au sens de l'article L. 133-18

[10] Au sens de l'article L. 133-6

[11] Au sens des articles L.133-19 et L.133-23

Dans les deux premiers cas, et à partir notamment des mêmes critères susmentionnés et des éléments nouveaux qu'aurait pu rapporter l'utilisateur, le prestataire de services de paiement est invité à poursuivre si nécessaire les investigations dans les conditions prévues aux recommandations n° 1 à 3 en vue de déterminer le droit à remboursement de l'utilisateur.

Références : articles L133-18, L133-19 et L133-23 du CMF

5- RECOMMANDATIONS À L'ATTENTION DES CONSOMMATEURS ET DE LEURS REPRÉSENTANTS

5.1 Bonnes pratiques pour la sécurité des moyens de paiement

Face à l'ingéniosité des fraudeurs qui cherchent des moyens de contournement face à des dispositifs de sécurité de plus en plus sophistiqués, les consommateurs ont, par leur comportement vigilant et responsable, un rôle clé pour préserver la sécurité de leurs propres moyens de paiement.

En particulier en ce qui concerne leurs usages sur internet, il leur revient de veiller à la sécurité des données associées à leurs moyens de paiement en évitant leur divulgation à des tiers, ce qui est susceptible de permettre la réalisation d'attaques frauduleuses. En effet, ces données sont tout aussi sensibles que ne l'est le code confidentiel de leur carte de paiement, et le non-respect de ces bonnes pratiques peut être un facteur pris en compte dans la caractérisation d'une négligence de l'utilisateur.

Recommandation n° 7: bonnes pratiques pour la sécurité des moyens de paiement

Les consommateurs doivent s'efforcer de rester vigilants quant à la préservation de la sécurité des données de sécurité associées à un instrument de paiement (mot de passe, code confidentiel, cryptogramme…), en respectant les bonnes pratiques en la matière :

- **ne jamais communiquer ces données à un tiers ;**
- **ne pas conserver ces données de sécurité sur quelque support que ce soit, physique (carnet, *post-it*…) ou informatique (messagerie électronique, disque dur, portable…) ;**
- **ne pas répondre aux sollicitations de personnes se présentant comme des collaborateurs des prestataires de services de paiement (conseillers bancaires, service de lutte contre la fraude…). Toujours utiliser un canal sécurisé et connu pour établir un contact avec son prestataire de services de paiement. Ne jamais ouvrir un lien reçu par messagerie électronique ou SMS dont l'origine n'est pas sûre ;**
- **ne jamais confier son instrument de paiement à une tierce personne (proche, coursier...) :**
- **être attentif aux communications de son prestataire de services de paiement et des autorités en matière de sécurité.**

Il est rappelé que le personnel du prestataire de services de paiement ne sera jamais amené à demander ces informations en cas d'appel de son client et n'en a pas besoin pour annuler une opération frauduleuse.

En outre, les consommateurs sont invités à privilégier la solution d'authentification la plus sûre proposée par leur prestataire de services de paiement, dès lors qu'ils sont en capacité de l'utiliser. Il s'agit généralement des solutions reposant sur un élément matériel robuste comme l'application bancaire sur un *smartphone* (solution majoritaire en France) ou un dispositif physique autonome mis à disposition par le prestataire de services de paiement (lecteur de carte, clef USB…).

Références : article L133-16 du CMF

5.2 Transparence dans la déclaration des cas de fraude

La lutte contre la fraude, quel que soit le type d'opération, implique que toutes les parties prenantes, y compris les utilisateurs des moyens de paiement victimes des fraudeurs, coopèrent et fassent preuve de la plus grande transparence dans la description des faits relatifs à la fraude. La transmission d'une information exhaustive est nécessaire à l'instruction du dossier, mais aussi à l'identification des auteurs et à la mise en œuvre de poursuites pénales à leur encontre, ainsi qu'au renforcement des mécanismes de filtrage anti-fraude des professionnels des paiements. Elle est également indispensable pour enrichir de façon vertueuse les avis de mise en garde à l'attention des consommateurs et contribuer ainsi à la sensibilisation des utilisateurs de services de paiement.

Auprès des forces de l'ordre, les démarches sur les plateformes Perceval et Thésée[12] sont à privilégier pour faciliter leur travail d'enquête. Par ailleurs, **il est rappelé qu'un dépôt de plainte de l'utilisateur ne peut pas être exigé par le prestataire de services de paiement comme préalable à l'instruction de sa demande de remboursement**.

Recommandation n° 8 : devoir de transparence de la part des victimes de fraude

Lors des démarches de déclaration auprès de leur prestataire de services de paiement ou des forces de l'ordre (qu'il s'agisse d'une déclaration sur l'honneur ou des démarches en ligne sur les plateformes Perceval ou Thésée, voire du dépôt de plainte au commissariat de police ou dans une unité de gendarmerie)**, les consommateurs et leurs représentants veillent à fournir l'ensemble des éléments dont ils disposent concernant la fraude dont ils ont été victimes.**

Les utilisateurs veillent notamment à fournir tous les éléments connus sur:

- **La nature et le contexte de l'opération :** par exemple leur niveau de connaissance du bénéficiaire, les procédés techniques ou manipulatoires que le fraudeur est supposé avoir mobilisés, l'instrument et les terminaux utilisés pour l'opération de paiement, les messages ou appels reçus, les actions réalisées sous le coup d'une manipulation par le fraudeur, etc.
- **Les actions entreprises une fois la fraude découverte :** par exemple le blocage de l'instrument, le récépissé des démarches Perceval ou Thésée, ou le cas échéant ou le dépôt de plainte auprès des forces de l'ordres, etc.

Le traitement des contestations d'opérations frauduleuses auprès des PSP comprend habituellement plusieurs niveaux de recours :

- la contestation initiale doit être adressée auprès du chargé de clientèle de l'établissement teneur de compte, qui est le point de contact privilégié de l'utilisateur, ou selon la procédure de contestation spécialement prévue par l'établissement, par exemple sur l'espace de banque en ligne ;

[12] Perceval est le télé-service pour signaler aux forces de l'ordre les fraudes à la carte bancaire en ligne ; Thésée permet de porter plainte en ligne contre des arnaques ou des escroqueries sur internet, notamment dans le cas des fraudes aux virements.

- en cas de réponse insatisfaisante, l'utilisateur peut déposer une réclamation auprès de son prestataire de paiement[13] ;
- enfin, il peut saisir le médiateur désigné par son prestataire de service de paiement.

Par ailleurs, le client peut engager une action en justice, s'il l'estime utile, à tout moment après le rejet de sa contestation initiale.

6- RECOMMANDATIONS VISANT À PRÉVENIR LA FRAUDE

6.1 Consultation des comptes du client à l'aide de la banque en ligne ou de l'application mobile

L'un des scénarios de fraude actuellement observé consiste, pour le fraudeur, à récupérer par hameçonnage l'identifiant et le mot de passe de la banque en ligne, ainsi que les informations personnelles du client (nom et prénom, numéro de téléphone…).

Muni de ces informations, le fraudeur se connecte à l'espace de banque en ligne du client pour réunir des informations sur les produits détenus par le client et la situation des comptes (solde, dernières opérations effectuées…). Ainsi, le fraudeur peut contacter le client en usurpant l'identité du prestataire de services de paiement, cette usurpation étant rendue crédible par la détention d'informations bancaires précises le concernant et qu'un tiers n'est pas censé connaître. Mis en confiance, le client victime de la fraude sera incité à accéder à la demande du fraudeur de valider des opérations (ajout de bénéficiaire, ordres de virement…) par authentification forte.

Ce scénario de fraude peut être prévenu par la mise en place de l'authentification forte à chaque consultation de la banque en ligne, sauf si la consultation se fait à partir d'un terminal régulièrement utilisé par l'utilisateur et que la dernière connexion avec authentification forte date de moins de 180 jours.

Recommandation n° 9 : application d'une authentification forte lors de l'accès à la banque en ligne depuis un nouveau point d'accès à internet ou un nouveau terminal

Les prestataires de service de paiement sont invités à exiger une authentification forte en cas de consultation des comptes depuis la banque en ligne ou l'application mobile depuis un terminal et/ou un point d'accès à internet qui n'a pas été précédemment utilisé par le client.

6.2 Information délivrée au client lors de l'ajout d'un bénéficiaire de virement

La réglementation actuelle en matière de sécurité des paiements ne prévoit pas de contrôle systématique sur le nom du bénéficiaire d'un virement : un ordre de virement peut être exécuté dès lors que l'IBAN bénéficiaire est valide, que le compte bénéficiaire existe et n'a pas été clos, indépendamment de la concordance entre le nom du bénéficiaire fourni par le payeur et le nom du titulaire réel du compte.

[13] Si l'utilisateur engage une réclamation sur la décision finale du prestataire de services de paiement à la suite de sa contestation, il est rappelé que la recommandation 2022-R-01 du 9 mai 2022 de l'ACPR sur le traitement des réclamations serait alors pleinement applicable et complète les présentes recommandations. https://acpr.banque-france.fr/sites/default/files/media/2022/05/17/20220517_recommandation_2022-r-01_traitement_reclamations.pdf

Cette situation est exploitée par certains fraudeurs, notamment dans le cadre du scénario dit de « substitution d'IBAN » : le fraudeur transmet l'IBAN d'un compte dont il est titulaire (ou dont le titulaire est complice de la fraude) en l'associant à l'intitulé d'un bénéficiaire de confiance (par exemple, le Trésor public ou un notaire).

Or, lors de l'ajout d'un bénéficiaire, l'émetteur du virement est invité à saisir le nom du bénéficiaire. Une étape de « validation de l'IBAN », nécessitant un délai pouvant atteindre plusieurs jours, est même annoncée sur l'espace de banque en ligne et l'application mobile de certains établissements. L'émetteur du virement peut ainsi présumer, à tort, de l'existence d'un contrôle de concordance, et que le virement ne sera pas exécuté ou pourra être annulé par le payeur dans le cas où le véritable titulaire du compte bénéficiaire ne correspond pas au nom saisi lors de l'ajout de l'IBAN de ce compte.

Cette situation devrait toutefois évoluer au cours des prochaines années : dans sa proposition de révision du règlement SEPA[14], la Commission européenne prévoit notamment de renforcer la confiance dans les paiements instantanés avec l'obligation pour les prestataires de vérifier la concordance entre l'IBAN et le nom du bénéficiaire fournis par le payeur afin d'alerter celui-ci d'une éventuelle erreur ou fraude avant que le paiement ne soit effectué.

Recommandation n° 10 : modalités d'enregistrement des IBAN bénéficiaires de virements

Les prestataires de services de paiement sont invités à indiquer clairement, à chaque ajout d'un bénéficiaire de virement, si un contrôle de concordance entre IBAN et nom du bénéficiaire a été mis en œuvre. À défaut, il doit être précisé à l'utilisateur que le champ « Nom du bénéficiaire » est exclusivement destiné à faciliter le suivi des opérations par le client qui émet des virements, et que son contenu ne fait l'objet d'aucun contrôle de concordance avec l'identité du titulaire de l'IBAN du bénéficiaire.

Par ailleurs, les prestataires de services de paiement établis en France sont encouragés à explorer par anticipation la possibilité d'implémenter au plus tôt un service de confirmation du bénéficiaire tel qu'envisagé par la Commission européenne dans sa proposition de révision du règlement SEPA.

6.3 Information et options présentées à l'utilisateur du service de paiement au moment de l'authentification forte

Dans le cas de fraude par manipulation, le fraudeur s'appuie sur l'emprise qu'il exerce sur sa victime pour l'amener à passer outre l'ensemble des messages et alertes adressés par le prestataire de services de paiement. Cette manipulation est facilitée lorsque ces messages et alertes sont insuffisamment précis et exhaustifs sur la nature et les caractéristiques de l'opération en attente de validation. Le renforcement du caractère explicite et de l'exhaustivité de l'information présentée, mais aussi du choix donné à l'utilisateur durant son parcours d'authentification, constituent des mesures efficaces de prévention de la fraude par manipulation.

[14] Proposition du 26 octobre 2022 (2022/0341 (COD)) visant à rendre les paiements instantanés en euros accessibles à tous les particuliers et à toutes les entreprises qui possèdent un compte bancaire dans l'UE ou dans un pays de l'EEE

Recommandation n° 11 : information et options présentées à l'utilisateur au moment de l'authentification forte

Les prestataires de services de paiement veillent à présenter à l'utilisateur, à chaque étape du processus d'authentification, une information explicite quant à la nature de l'opération, et mentionnant notamment le montant, le bénéficiaire, le caractère unique ou récurrent de l'opération, la périodicité dans le cas d'une opération récurrente ainsi que le caractère irrévocable de la validation de l'ordre de paiement. Dans le cas d'un premier virement vers un compte donné, lorsque la concordance entre l'identité du bénéficiaire et l'IBAN fournis n'a pas fait l'objet d'un contrôle, le parcours d'authentification le rappelle explicitement.

Par ailleurs, les prestataires de services de paiement veillent à ce que le parcours d'authentification propose de manière explicite une option permettant de refuser l'opération.

6.4 Simplicité d'accès aux procédures de blocage des instruments de paiement

Dans le cas où l'utilisateur détecte une activité anormale sur ses comptes ou instruments de paiement ou identifie une faille dans la protection de ses données, il doit pouvoir mettre en opposition les instruments de paiement concernés auprès de son prestataire de services de paiement. Cette procédure doit être simple d'accès afin d'assurer la meilleure réactivité possible, à l'instar du centre de mise en opposition qui existe aujourd'hui pour les cartes de paiement.

Recommandation n° 12 : simplicité d'accès aux procédures de blocage des instruments de paiement

Les prestataires de services de paiement mettent à disposition de leurs utilisateurs des mécanismes de blocage pour chacun des instruments de paiement et veillent à ce qu'ils soient facilement accessibles, gratuits, et utilisables à tout moment.

Références : articles L133-15 et L133-17 du CMF

6.5 Rôle des fournisseurs de services et technologies de l'information dans la lutte contre la fraude

Les opérateurs de téléphonie et les fournisseurs de services numériques sont des parties prenantes centrales dans la sécurité des opérations de paiement effectuées à distance, pour lesquelles ils assurent la mise en relation entre les différentes parties et l'échange de données. Ils ont ainsi une responsabilité dans la lutte contre les techniques utilisées par les fraudeurs pour collecter des données de paiement à l'insu de l'utilisateur par des messages électroniques (hameçonnage) ou SMS (*smishing*) usurpant l'identité d'un expéditeur légitime, la mise en ligne de faux sites miroir, ou encore l'affichage, lors d'un appel entrant malveillant, du numéro de téléphone d'un interlocuteur légitime (*spoofing*).

Recommandation n° 13 : rôle des fournisseurs de services et technologies de l'information

Les acteurs du secteur des technologies de l'information (opérateurs de téléphonie, hébergeurs de contenu, éditeurs de sites de référencement, moteurs de recherche, fournisseurs de services de messagerie…) veillent à protéger les utilisateurs contre les risques d'usurpation d'identité et d'atteinte à l'intégrité et la confidentialité de leurs données. Ils œuvrent à empêcher l'utilisation de techniques frauduleuses telles que l'hameçonnage, le *spoofing* ou le *SIM-swapping*.

7- CONDITIONS D'APPLICATION DES RECOMMANDATIONS

Les treize recommandations de l'Observatoire constituent des pratiques de référence pour les acteurs du marché des paiements, qui précisent les attentes des autorités françaises au regard de la réglementation européenne. Elles n'ont pas vocation à se substituer à la réglementation applicable, ni à la jurisprudence en la matière.

Les prestataires de services de paiement s'engagent à prendre en considération les recommandations 1 à 6 dans leurs pratiques en matière de traitement des contestations d'opérations de paiement non autorisées, et l'ensemble des acteurs à jouer un rôle proactif dans la sécurité des paiements en veillant à appliquer les recommandations 7 à 13, pour celles qui les concernent, dans la gestion de leurs activités au quotidien.

Dans un contexte où les mécanismes de fraude évaluent rapidement, l'Observatoire s'engage à procéder à un bilan de ces recommandations et, le cas échéant, à leur révision sous un délai maximal de 18 mois à compter de leur adoption.