Mémoire

Les fraudes à la carte bancaire

Tara Bellaire

Master 2 Contentieux

Faculté de droit, sciences économiques et gestion de Nancy

Stage réalisé à l'Association de défense des consommateurs de France

3 avril – 30 juin 2023

Maître de stage : Monsieur Grandgirard

Mes plus sincères remerciements à Monsieur Grandgirard ainsi qu'à Madame Didier, Madame Techer et Monsieur Petropavlovsky pour m'avoir accompagnée durant l'écriture de ce mémoire ainsi que pour tout ce que j'ai appris à leurs côtés durant mon stage. Je remercie également Maître Delomel pour sa patience et sa bienveillance face à mes questions.

TABLE DES MATIERES

L'ASSOCIATION DE DEFENSE DES CONSOMMATEURS DE FRANCE

I. Présentation de l'Association de défense des consommateurs de France

L'association a vu le jour le 30 avril 1979. Il s'agissait au départ d'un réseau national d'association ; et c'est en octobre 2014 que l'Association de défense des consommateurs de Lorraine a été créée. Le nombre croissant de dossiers venant d'un peu partout en France a conduit l'association à se renommer Association de défense des consommateurs de France en avril 2019.

Si le siège de l'association se situe à Nancy, elle possède également des antennes à Pont-à-Mousson, Varangéville, Lunéville, Golbey et Vittel. Des permanences y sont assurées, permettant aux consommateurs d'échanger avec des bénévoles sur les problèmes qu'ils rencontrent.

L'ADC France œuvre dans tous les domaines du droit de la consommation, tant sur les litiges liés aux services qu'aux biens. Ainsi, elle est par exemple compétente en matière de logement, d'assurance, de véhicules, de banques et d'organismes de crédit, de travaux, d'énergies, d'eau… Son rôle est d'informer et d'aider les consommateurs victimes d'un litige non réglé à l'amiable. Les juristes et bénévoles de l'association sont joignables par téléphone et par courrier postal ou électronique. Il est également possible de les rencontrer lors des permanences.

Dans un premier temps, les juristes et bénévoles conseillent les consommateurs de manière à ce qu'ils soient en mesure de faire face à la difficulté qu'ils rencontrent. Mais si cela ne suffit pas, l'association intervient : après analyse du dossier, une lettre est adressée au professionnel avec qui le litige est en cours. Les connaissances juridiques des juristes et bénévoles permettent en effet d'appuyer les demandes d'arguments fondés ne laissant en général d'autre choix aux professionnels que d'accepter les réclamations en question.

L'association engage également des actions sur les arnaques financières et les pièges d'internet. Plus précisément, elle effectue des enquêtes puis les met en ligne. Elle organise également des regroupements de victimes pour des actions collectives et des actions pénales collectives avec Maître Arnaud DELOMEL, avocat spécialiste au barreau de Rennes. Ainsi, l'ADC France est par exemple

impliquée dans les affaires Aristophil et Artecosa ainsi que dans la découverte du réseau franco-israélien et du réseau bulgare. Le montant des préjudices pour les arnaques depuis le 1er janvier 2021 est de 110 millions d'euros.

En outre, l'ADC France a une activité de représentation des consommateurs à la Commission de surendettement de Meurthe-et-Moselle, à la Commission départementale d'aménagement commercial et aux réunions semestrielles de l'Autorité des marchés financiers.

L'association est aussi à l'origine d'une revue trimestrielle ANTIPAC qui contient toutes sortes d'informations utiles pour les consommateurs.

L'ADC France est présidée par M. Grandgirard et emploie trois juristes à temps plein, dont un est spécialisé dans les arnaques financières sur internet. Une cinquantaine de bénévoles vient également apporter son aide, que ce soit dans le traitement de dossiers ou pour des tâches administratives. Environ 1 200 dossiers sont traités par an, dont les deux tiers sont relatifs à des arnaques financières en ligne. 3 700 consommateurs sont actuellement adhérents à l'association.

II. Mon expérience au sein de l'Association de défense des consommateurs de France

Lors de mon stage, ma principale activité consistait à traiter des dossiers pouvant porter sur tous les domaines du droit de la consommation. Après analyse, mon objectif était de rédiger une lettre adressée à un professionnel et comportant une ou plusieurs demandes appuyées par des arguments juridiques. Cette tâche m'a notamment permis d'étudier de nombreux dossiers en rapport avec les fraudes à la carte bancaire, ce qui fut très enrichissant du point de vue de l'écriture de mon mémoire.

J'étais également chargée de répondre au téléphone afin d'apporter des renseignements et conseils à mes interlocuteurs. Si cela n'a pas toujours été simple car il arrivait que je ne maîtrise pas certains sujets, je pouvais toujours compter sur les juristes pour m'aider dans les réponses à apporter.

J'ai aussi pu assister à quelques permanences au cours desquelles juristes et bénévoles reçoivent les consommateurs, les écoutent puis les conseillent voire ouvrent de nouveaux dossiers afin que l'association se charge de la résolution du litige.

Ce stage m'a permis d'aborder le droit de la consommation de manière concrète et de mettre à l'épreuve mes connaissances juridiques acquises tout au long de mon parcours universitaire. Ce fut une expérience très enrichissante au cours de laquelle je me suis réellement sentie utile, que ce soit en aidant les gens par téléphone ou lorsqu'un professionnel cédait aux demandes d'une lettre que j'avais rédigée. J'ai de plus découvert le métier de juriste qui s'avère être très intéressant. Je remercie tout particulièrement M. Grandgirard ainsi que les juristes Léa, Roxane et Brian qui ont toujours été bienveillants envers moi et m'ont appris énormément de choses. Je ressors de ce stage avec de plus amples connaissances du droit de la consommation et une manière d'appréhender les litiges qui me seront utiles aussi bien pour ma future profession qu'au quotidien.

INTRODUCTION

L'Observatoire de la sécurité des moyens de paiement estime à 596 millions d'euros la fraude aux moyens de paiement au premier semestre 2022[1]. Et c'est la carte bancaire qui est le moyen de paiement le plus fraudé, avec 34,8% des montants de fraude ou encore 208 millions d'euros. De plus, la carte bancaire concentre 93,8% du total des transactions frauduleuses, bien devant le chèque, le retrait d'espèces et le virement.

La fraude à la carte bancaire est caractérisée lorsque les coordonnées d'une carte bancaire ont été utilisées afin d'effectuer une transaction dont le titulaire de la carte n'est pas à l'origine. On dit que l'opération est non autorisée. La carte en question peut être restée entre les mains de son titulaire ou lui avoir été subtilisée. Toutefois, la grande majorité des fraudes à la carte bancaire se fait à distance, ce qui est principalement dû à l'essor du commerce en ligne.

Si le chiffre d'affaires du e-commerce en France ne représentait que 0,7 milliard d'euros en 2000, il est en 2021 de 147 milliards d'euros[2]. Cette expansion des achats en ligne a pour conséquence d'offrir de nouvelles opportunités aux escrocs et donc d'augmenter la fraude dans ce domaine. Ce phénomène existe dans le monde entier, une étude de Juniper Research indiquant par exemple que le coût de la fraude dans l'e-commerce au niveau mondial s'élève à 17 milliards de dollars en 2020 et devrait dépasser les 25 milliards de dollars en 2023[3].

Face à ce constat, la législation n'a eu d'autre choix que d'évoluer. Au niveau européen, la deuxième directive sur les services de paiement (UE) 2015/2366 est venue abroger la première directive 2007/64/CE le 25 novembre 2015. Si cette première directive avait permis la création d'un ensemble de règles communes concernant les services de paiement pour l'Union européenne, elle s'est vite montrée insuffisante face aux progrès technologiques du secteur bancaire. Un des objectifs de la seconde directive sur les services de paiement fut alors de renforcer la protection de l'utilisateur de services de paiement, devenu la principale cible des fraudeurs. Le principal apport de cette directive

[1] Rapport « Chiffres-clés de l'Observatoire », 1er semestre 2022.
[2] Trustpair, « Les tendances de la fraude dans le secteur du e-commerce », 17 févrirer 2023.
[3] Juniper Research, « Online payment fraud : market forecasts, emerging threats & segment analysis 2022-2027 », 11 juillet 2022.

consiste en des règles d'authentification forte afin de valider des opérations de paiement, ce qui a effectivement permis de réduire le taux de fraude.

Toutefois, la fraude est toujours bien présente dans l'environnement bancaire, comme en atteste le nombre croissant de dossiers concernant des fraudes à la carte bancaire que traite l'ADC France. Et là n'est pas le seul ennui, puisque le constat est aussi celui d'une tendance des prestataires de services de paiement à refuser d'indemniser les victimes d'opérations non autorisées, le droit au remboursement étant pourtant le principe. Ces observations invitent donc à s'interroger sur la réelle efficacité de la récente législation en la matière.

Plusieurs problématiques se dégagent alors. Quels sont les apports de la deuxième directive sur les services de paiement quant au renforcement des droits de l'utilisateur de paiement en cas d'opération non autorisée ? La législation en vigueur est-elle réellement efficace dans la protection des consommateurs ? Quelles formes prend la fraude bancaire dans la pratique et de quels recours disposent les victimes ?

Ce mémoire traitera dans une première partie de l'évolution de la législation européenne en termes de protection du consommateur et de sa transposition en droit français. Il se penchera ensuite sur une étude de la fraude dans la pratique, avec le développement de nouvelles techniques par les escrocs ainsi que les solutions s'offrant aux victimes d'opérations non autorisées pour être indemnisées.

PARTIE 1 : L'EVOLUTION DE LA LEGISLATION EUROPEENNE EN TERMES DE PROTECTION DU CONSOMMATEUR ET SA TRANSPOSITION EN DROIT FRANÇAIS

Si la première directive sur les services de paiement, adoptée en avril 2007, a permis de renforcer la protection du consommateur en instaurant des obligations pesant sur les prestataires de services de paiement ainsi que sur les utilisateurs, les évolutions technologiques et des moyens de paiement ont vite montré ses limites.

C'est dans ce contexte que s'est fait ressentir le besoin de modifier la législation. Est alors née la seconde directive sur les services de paiement, adoptée en novembre 2015. Celle-ci a notamment instauré des règles d'authentification forte visant à sécuriser les transactions en ligne, ce mode de paiement étant de plus en plus utilisé par les consommateurs.

La transposition de cette deuxième directive dans le code monétaire et financier a conduit les banques et établissements de paiement à s'adapter aux exigences de la législation européenne. La mise en place de l'authentification forte s'est faite progressivement, de manière à laisser le temps aux professionnels de repenser leur fonctionnement.

Après avoir étudié en quoi la première directive sur les services de paiement protège l'utilisateur de services de paiement, il conviendra de se pencher sur les apports de la seconde et sur son impact sur le secteur bancaire.

Chapitre 1 : La DSP1 comme première étape dans le renforcement de la protection du consommateur

La directive 2007/64/CE, première directive européenne sur les services de paiement, dite « DSP1 », est adoptée en avril 2007. Avant son élaboration, chaque Etat membre de l'Union européenne appliquait ses propres règles en termes de services de paiement. Un tel système n'était pas judicieux et représentait notamment un coût important pour l'économie de l'Union européenne.

Cette directive a alors créé un ensemble de règles communes concernant les services de paiement et s'appliquant sur tout le territoire de l'Union européenne. Elle a également instauré un espace unique de paiement en euros afin de permettre des paiements transfrontaliers efficaces et à moindre coût. Elle a de plus mis un terme au monopole bancaire en prévoyant un accès sur le marché des paiements à de nouveaux entrants, les établissements de paiement.

La DSP1 est ainsi divisée en plusieurs titres. Le premier précise son objet, son champ d'application et les définitions afférentes. Le titre II porte quant à lui sur les prestataires de services de paiement. La transparence des conditions et les exigences en matière d'informations régissant les services de paiement sont évoquées au titre III.

Ce mémoire se penche sur les dispositions de la DSP1 en termes de protection de l'utilisateur de services de paiements. En 2007, la fraude aux paiements était déjà répandue et la directive se devait de renforcer la sécurité des paiements en ligne et de prévoir des règles en cas d'opérations de paiement non autorisées. A ce sujet, c'est le titre IV intitulé « Droits et obligations liés à la présentation et à l'utilisation de services de paiement » qui établit des règles relatives aux opérations de paiement et s'appliquant aux prestataires et utilisateurs de services de paiement.

I. Les obligations du prestataire de services de paiement

Dans un premier temps, la DSP1 vise à sécuriser les opérations de paiement que l'utilisateur de services de paiement souhaiterait effectuer. La directive prévoit ensuite les conséquences d'une opération de paiement qui n'aurait pas été autorisée par ce dernier.

A. La prévention du risque d'opérations non autorisées par le prestataire de services de paiement

D'abord, le prestataire de services de paiement doit recueillir le consentement de l'utilisateur. C'est en effet ce que prévoit l'article 54 paragraphe 1 de la directive[4] qui dispose que « les États membres veillent à ce qu'une opération de paiement ne soit réputée autorisée que si le payeur a donné son

[4] Les articles de la DSP1 cités sont reproduits au sein de l'annexe n°1.

consentement à l'exécution de l'opération de paiement ». L'article poursuit en précisant que l'opération de paiement peut être autorisée avant, ou, s'il en a été convenu ainsi, après son exécution.

Dès lors, un prestataire de services de paiement se doit de mettre en place un système permettant de s'assurer de la volonté du payeur de réaliser l'opération de paiement en question. Ce système doit faire l'objet d'un accord entre le prestataire et l'utilisateur de services de paiement.

Une telle règle permet également de prévenir l'utilisateur de services de paiement qu'une tentative de paiement dont il n'est pas à l'origine a lieu, ce qui lui donne ensuite l'occasion de mettre en œuvre les mesures nécessaires pour assurer la protection de son compte bancaire.

Le paragraphe 2 in fine de l'article 54 de la directive prévoit ensuite qu'en l'absence de consentement, l'opération de paiement est considérée comme non autorisée. Ainsi, les conséquences d'un défaut de consentement ne sont pas négligeables, puisqu'on le verra plus tard, une opération non autorisée peut entraîner d'importantes répercussions à la fois sur le prestataire et sur l'utilisateur de services de paiement.

En outre, l'article 57 paragraphe 1 a) dispose que le prestataire de services de paiement délivrant un instrument de paiement doit s'assurer que « les dispositifs de sécurité personnalisés de tout instrument de paiement ne sont pas accessibles à d'autres parties que l'utilisateur de services de paiement autorisé à utiliser cet instrument ».

Un dispositif de sécurité est un moyen technique, le plus souvent un code, qui est mis à la disposition du payeur par le prestataire de services de paiement et qui permet d'assurer une utilisation sécurisée d'un mode de paiement. Dès lors, seul l'utilisateur de services de paiement doit connaître le dispositif de sécurité dont il bénéficie et la directive insiste sur le fait que le prestataire de services de paiement veille à la confidentialité d'un tel dispositif.

Mais cette précaution ne suffit pas toujours à éviter les opérations non autorisées, notamment lorsqu'un utilisateur de services de paiement divulgue son code à une personne mal intentionnée. Il s'agit d'une hypothèse assez fréquente en pratique sur laquelle nous aurons l'occasion de revenir.

Malgré les précautions prises par l'utilisateur et le prestataire de services de paiement, des opérations irrégulières peuvent apparaître. La DSP1 soumet alors le prestataire de services de paiement à des règles visant à éviter qu'une opération non autorisée ne passe.

D'abord, l'article 55 paragraphe 2 de la directive dispose que « si le contrat-cadre le prévoit, le prestataire de services de paiement peut se réserver le droit de bloquer l'instrument de paiement ». Une telle option est possible « pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument de paiement, à la présomption d'une utilisation non autorisée ou frauduleuse de l'instrument de paiement ou, s'il s'agit d'un instrument de paiement doté d'une ligne de crédit, au risque sensiblement accru que le payeur soit dans l'incapacité de s'acquitter de son obligation de paiement ».

Ainsi, cet alinéa permet à la banque ou à l'établissement de paiement d'empêcher l'utilisation d'un instrument de paiement lorsqu'il suspecte notamment une utilisation frauduleuse ou allant à l'encontre de la volonté de son client. Cela suppose un rôle actif du prestataire de services de paiement qui ne se contente pas simplement d'autoriser les opérations de paiement mais qui veille à ce que ces dernières soient bel et bien réalisées par le payeur.

Dans l'hypothèse d'un blocage de l'instrument de paiement, l'article 55 paragraphe 3 poursuit en précisant que l'utilisateur de services de paiement doit immédiatement être informé de ce blocage, « à moins que le fait de donner cette information ne soit pas acceptable pour des raisons de sécurité objectivement motivées ou soit interdite en vertu d'une autre législation communautaire ou nationale pertinente ».

Enfin, l'article termine en précisant que l'instrument de paiement doit être débloqué ou remplacé dès qu'il n'y a plus de raison de penser qu'un blocage est nécessaire.

En plus de laisser au prestataire de services de paiement cette possibilité de bloquer l'instrument de paiement, la DSP1 met en place un système de notification permettant à l'utilisateur de services de paiement de prévenir la banque ou l'établissement de paiement en cas de perte, vol, détournement ou toute utilisation non autorisée de l'instrument de paiement. Nous aurons l'occasion de revenir sur cette obligation de notification pensant sur l'utilisateur prévue à l'article 56 paragraphe 1 b) de la directive.

S'agissant du prestataire de services de paiement, l'article 57 paragraphe 1 c) prévoit qu'il veille « à la disponibilité, à tout moment, de moyens appropriés permettant à l'utilisateur de services de paiement

de procéder à la notification ». En effet, dans l'hypothèse d'une potentielle mauvaise utilisation de son instrument de paiement, un utilisateur doit pouvoir réagir rapidement et prévenir facilement sa banque ou son établissement de paiement qu'un tel risque est encouru. Dès lors, le prestataire se doit d'établir un système de notification disponible et relativement simple d'accès.

Cette notification a pour objectif d'éviter toute mauvaise utilisation de l'instrument de paiement de l'utilisateur. Dès lors, l'article 57 paragraphe 1 d) poursuit en précisant qu'une fois notifié, le prestataire de services de paiement doit empêcher toute utilisation de l'instrument de paiement. Cela permet de réduire le risque que des opérations non autorisées ne soient effectuées. Toutefois, l'utilité de la mesure va dépendre de la rapidité avec laquelle l'utilisateur de services de paiement a connaissance du problème et procède à la notification.

B. Les conséquences d'une opération de paiement non autorisée

Malgré les précautions étudiées ci-dessus, des opérations de paiement non autorisées peuvent tout de même apparaître. Cela risque d'avoir d'importantes conséquences pour les banques et les établissements de paiement et ces derniers vont alors essayer de se décharger de toute responsabilité.

La DSP1 prévoit alors des éléments de preuve permettant aux prestataires de services de paiement de démontrer qu'une opération peut être considérée comme autorisée. En effet, l'article 59 paragraphe 1 de la directive énonce que « lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre ».

Ainsi, une opération qui ne serait a priori pas autorisée mais qui aurait été authentifiée, enregistrée, comptabilisée et qui n'aurait pas subi de déficience technique permet alors à la banque ou à l'établissement de paiement de ne pas être tenu pour responsable de cette opération.

Toutefois, l'objectif n'est pas de favoriser les banques en les exonérant de toute responsabilité et notamment, le second paragraphe de l'article 59 ajoute que « l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement en tant que

telle à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs obligations qui lui incombent ».

Cette règle fait sens puisqu'un moyen de paiement peut très bien être utilisé malgré la volonté d'un utilisateur, en cas de fraude par exemple, et alors même qu'il n'aurait pas manqué à une de ses obligations.

Comme évoqué précédemment, une opération non autorisée n'est pas sans incidence pour la banque ou l'établissement de paiement concerné. L'article 60 de la directive prévoit en effet qu'en cas de paiement non autorisé, « le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de cette opération de paiement non autorisée et, le cas échéant, rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu ».

Cette règle peut avoir de grosses conséquences pour les prestataires de services de paiement, notamment lorsque le montant de l'opération non autorisée est important. Dès lors, elle incite les banques à mettre en place les conditions prévues à l'article 59 de la directive : chaque opération doit être authentifiée, enregistrée, comptabilisée et ne doit pas avoir été affectée par une déficience technique ou autre, auquel cas l'opération pourrait être considérée comme non autorisée.

Ce système peut sembler sévère envers les banques et établissements de paiement contraints de rembourser l'utilisateur de services de paiement alors même qu'ils ne sont pas directement responsables de la survenance de l'opération non autorisée. Toutefois, un tel système est indispensable pour assurer la protection de l'utilisateur qui est de plus en plus victime de fraudes aux moyens de paiement.

Mais le prestataire de services de paiement n'est pas le seul à être soumis à des obligations et la directive prévoit également un rôle à l'utilisateur de services de paiement.

II. Les obligations de l'utilisateur de services de paiement

Les prestataires de services de paiement ne sont pas les seuls à être soumis à des règles renforçant la sécurité du consommateur. En effet, ce dernier doit également respecter certaines obligations permettant de réduire le risque d'opérations non autorisées. Et comme précédemment, la directive se penche sur les conséquences qu'une opération non autorisée aurait pour un utilisateur de services de paiement.

A. La prévention du risque d'opérations non autorisées par l'utilisateur de services de paiement

Comme mentionné antérieurement, la DPS1 prévoit au sein de son article 54 que l'utilisateur de paiement doit donner son consentement pour qu'une opération de paiement puisse être exécutée par la banque ou l'établissement de paiement.

Cette règle vise à éviter qu'une opération dont l'utilisateur n'est pas à l'origine soit réalisée. Toutefois, il se peut qu'un fraudeur réussisse à manipuler l'utilisateur en invoquant par exemple une urgence et/ou en se faisant passer pour un professionnel digne de confiance. Dans ces hypothèses, l'utilisateur pourrait alors donner son consentement à une opération dont il ne connait pas la vraie nature ou les conséquences. Dès lors, recueillir le consentement d'un utilisateur de paiement ne suffit pas toujours à éviter qu'une opération non autorisée soit exécutée.

L'article 56 de la directive prévoit ensuite les obligations de l'utilisateur de services de paiement liées aux instruments de paiement. D'abord, ce dernier doit utiliser l'instrument de paiement « conformément aux conditions régissant la délivrance et l'utilisation de cet instrument de paiement ».

Plus particulièrement, l'utilisateur se doit de prendre « toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés ». Si le prestataire de services de paiement a la charge de mettre en place des dispositifs permettant de valider les opérations de paiement, c'est à l'utilisateur de veiller à ce que ces derniers restent confidentiels. En effet, une banque ou un établissement de paiement qui aurait respecté son obligation ne peut être tenu responsable d'une

opération frauduleuse validée par le biais d'un dispositif de sécurité divulgué intentionnellement par l'utilisateur de services de paiement.

De plus, l'article 56 prévoit également que « lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement, l'utilisateur de services de paiement en informe sans tarder son prestataire de services de paiement ou l'entité désignée par celui-ci ». Cette notification permet en effet au prestataire d'empêcher toute utilisation de l'instrument de paiement afin de bloquer des opérations de paiement dont l'utilisateur ne serait pas à l'origine.

En outre, l'emploi de l'expression « sans tarder » montre l'urgence de la situation et invite l'utilisateur de services de paiement à faire preuve de vigilance et de réactivité lorsqu'il se retrouve dans un tel contexte.

B. Les conséquences d'une opération de paiement non autorisée pour l'utilisateur de services de paiement

Les précautions prises à la fois par l'utilisateur de services de paiement et par le prestataire ne suffisent pas toujours à éviter que des opérations non autorisées aient lieu. Dès lors, la directive prévoit ce qu'il en est de la responsabilité de l'utilisateur de services de paiement dans cette hypothèse.

Lorsque l'utilisateur de services de paiement constate qu'une opération qu'il n'a pas autorisée a eu lieu, l'article 58 de la directive prévoit qu'il doit la signaler « sans tarder » à son prestataire de services de paiement et « au plus tard dans les treize mois suivant la date de débit ». Cet avertissement de la part de l'utilisateur permet alors la « correction de l'opération » de la part de la banque ou de l'établissement de paiement.

Ainsi, si l'utilisateur dispose d'un délai de treize mois pour s'apercevoir de l'opération frauduleuse, une fois le problème détecté, il ne doit pas attendre pour en informer son prestataire. Ce délai peut sembler long mais dans la pratique, certaines personnes ne sont pas très attentives à leurs comptes bancaires. Il serait alors injuste de les priver de la possibilité d'être remboursées, un des principaux objectifs de la directive étant, rappelons-le, de veiller à la protection des utilisateurs de services de paiement.

C'est ensuite l'article 61 qui évoque la responsabilité du payeur en cas d'opérations de paiement non autorisées. Dans un premier temps, son paragraphe 1 nous apprend que l'utilisateur de services de paiement « supporte, jusqu'à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou, si le payeur n'est pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, au détournement d'un instrument de paiement ».

Ainsi, si les prestataires de services de paiement doivent rembourser le montant des opérations non autorisées, cet alinéa est un tempérament à ce principe qui laisse à la charge de l'utilisateur une partie de la somme prélevée frauduleusement. Le reproche que l'on peut alors faire à cette règle est qu'elle est générale et qu'elle ne s'adapte ni aux ressources de l'utilisateur concerné, ni au montant débité. De plus, si pour de nombreux clients, 150 euros peut représenter une somme importante, cela est moins vrai s'agissant des banques et établissements de paiement qui ont plus de fonds à leur disposition et qui seraient donc moins impactés par la prise en charge de ce montant.

Toutefois, la portée de cette règle est à relativiser en raison des paragraphes 4 et 5 du même article. D'abord, le paragraphe 4 prévoit qu'il ne faut pas pénaliser un utilisateur victime qui a agi conformément à ce qui lui était demandé par la directive. En effet, sans agissement frauduleux de sa part, « le payeur ne supporte aucune conséquence financière résultant de l'utilisation d'un instrument de paiement perdu, volé ou détourné, survenue après la notification prévue à l'article 56 ». Cela est cohérent : une victime d'opérations non autorisées n'a pas à supporter le coût de ces dernières alors que le prestataire de services de paiement était informé de la situation et avait l'obligation de bloquer l'utilisation du moyen de paiement en question.

De même, le paragraphe 5 dispose qu'un utilisateur ne pouvant respecter son obligation de notification en raison du prestataire qui « ne fournit pas de moyens appropriés permettant, à tout moment, la notification de la perte, du vol ou du détournement d'un instrument de paiement (…), n'est pas tenu, sauf agissement frauduleux de sa part, de supporter les conséquences financières résultant de l'utilisation de cet instrument de paiement ».

A l'inverse, le deuxième paragraphe de l'article 61 prévoit que le payeur « supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou du fait que le payeur n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent » ; à savoir l'obligation

d'utiliser l'instrument de paiement conformément aux conditions régissant la délivrance et l'utilisation de ce dernier et l'obligation d'informer sans tarder le prestataire en cas de perte, vol, détournement ou toute utilisation non autorisée de cet instrument de paiement.

Ainsi, en cas de fraude, mauvaise foi ou négligence grave de l'utilisateur, ce dernier est entièrement responsable de l'opération et ne peut se voir remboursé par le prestataire de services de paiement. Cette règle permet donc aux banques et établissements de paiement de s'exonérer de leur obligation de remboursement. Mais pour cela, ils doivent démontrer une faute lourde du payeur. Nous verrons qu'en pratique, la négligence grave est souvent invoquée.

Toutefois, la notion de négligence grave est appréciée différemment selon les juridictions et il peut parfois être difficile pour les banques de se décharger de toute responsabilité. Il faut en effet remettre chaque situation dans son contexte et ne pas permettre aux professionnels bancaires de s'exonérer trop facilement. Certaines victimes sont plus susceptibles de se faire manipuler que d'autres, en raison par exemple des capacités du fraudeur à les mettre en confiance et/ou à créer une situation d'urgence. Ainsi, parfois, la négligence grave peut être compliquée à caractériser.

Dans la même idée, le paragraphe 3 prévoit que « lorsque le payeur n'a pas agi de manière frauduleuse ni n'a manqué intentionnellement aux obligations qui lui incombent », il est possible de « limiter sa responsabilité (…) en tenant compte notamment de la nature des dispositifs de sécurité personnalisés de l'instrument de paiement et des circonstances dans lesquelles celui-ci a été perdu, volé ou détourné ».

En effet, les dispositifs de sécurité personnalisés varient selon les banques (il peut s'agir par exemple d'un code spécifique servant uniquement à valider des opérations ou simplement du mot de passe du compte de l'utilisateur) et ils ne protègent donc pas forcément de la même manière. Dès lors, cet aspect est à prendre en compte et il semble cohérent de ne pas pénaliser un utilisateur qui aurait à sa disposition un dispositif peu sécurisant.

De plus, comme évoqué précédemment, les circonstances dans lesquelles intervient la prise de possession frauduleuse de l'instrument de paiement ont leur importance. Parfois, les faits font que la victime ne pouvait pas ou alors très difficilement éviter la situation. Dès lors, il faut remettre les éléments dans leur contexte pour déterminer le niveau de responsabilité du payeur et les conséquences que l'opération doit avoir sur ce dernier.

Pour conclure, si la DSP1 a contribué à améliorer la sécurité des opérations de paiement et à limiter les risques de fraudes, les évolutions techniques ont fait qu'elle s'est rapidement montrée insuffisante pour assurer la protection du consommateur. C'est dans ces circonstances qu'intervient la DSP2, deuxième directive sur les services de paiement, qu'il convient maintenant d'étudier.

Chapitre 2 : Les apports de la DSP2 et sa transposition dans le droit français

Les apports de la DSP1 en termes de protection de l'utilisateur de services de paiement n'ont pas permis d'éradiquer la fraude. Pire encore, le développement des nouvelles technologies n'a fait qu'augmenter le risque, notamment en raison de l'essor du commerce en ligne. Jean-Michel Chanavas, délégué général de Mercatel, relève auprès de l'AFP que « le taux de fraude est vingt fois plus élevé en e-commerce que dans les commerces de proximité ».

Cette récente manière de réaliser des transactions par internet a de fait permis aux fraudeurs de développer de nouvelles techniques d'escroquerie. Les offres proposées par les services financiers en ligne nécessitant du client qu'il partage ses coordonnées bancaires, la sécurité des transactions électroniques s'en est inévitablement trouvée menacée.

Dès lors, la nécessité d'encadrer ce domaine par des règles juridiques internationales s'est rapidement montrée indispensable. C'est donc dans ce contexte qu'a été adoptée le 25 novembre 2015 la directive (UE) 2015/2366, seconde directive sur les services de paiement, qui vient abroger la DSP1. Cette nouvelle directive a deux objectifs principaux, à savoir favoriser l'innovation pour un marché européen des paiements compétitif et lutter contre la fraude en renforçant la protection des consommateurs et la sécurité des paiements.

Elle est structurée de la même manière que la DSP1 et reprend un grand nombre de ses points. Après avoir étudié les divergences existant tout de même entre la première directive sur les services de paiement et la deuxième, il conviendra de se pencher sur leur transposition et leur impact sur les prestataires de services de paiement français.

I. Le renforcement de la protection du consommateur par la DSP2

La deuxième directive sur les services de paiement abroge et remplace la première. Elle reprend les dispositions de cette dernière, en modifie certaines et en crée de nouvelles. L'apport majeur de la DSP2 est l'obligation pour les prestataires de services de paiement de mettre en place un dispositif d'authentification forte afin de valider la majorité des transactions.

A. Les modifications et ajouts apportés par la DSP2

Si la DSP2 vient abroger la première directive sur les services de paiement, seuls quelques points qu'il conviendra d'étudier diffèrent réellement de cette dernière. C'est afin de protéger de manière adéquate les utilisateurs contre les risques de sécurité liés aux paiements électroniques que des règles ont été modifiées ou spécialement créées.

Tout d'abord, l'apport majeur de la DSP2 est la nécessité pour les prestataires de services de paiement de mettre en place une authentification forte afin de vérifier doublement l'identité de l'utilisateur avant d'autoriser une opération d'un montant supérieur à trente euros. C'est en effet l'article 74 paragraphe 2 de la directive[5] qui prévoit que « lorsque que le prestataire de services de paiement du payeur n'exige pas une authentification forte du client, le payeur ne supporte aucune perte financière éventuelle à moins qu'il ait agi frauduleusement ».

Du temps de la DSP1, l'authentification forte n'était que facultative et un seuil d'authentification faible était acceptable. Il n'y avait donc pas de condition quant au niveau de vérification d'une identité dans l'hypothèse d'un paiement en ligne. L'authentification forte étant alors peu pratiquée, le risque qu'un fraudeur réalise une opération au détriment du payeur était important.

Désormais, cette exigence de double vérification afin de confirmer l'identité du payeur avant de valider une transaction électronique réduit le risque qu'une autre personne que le payeur soit à l'origine de l'opération. Et ainsi, un prestataire de services de paiement qui ne respecterait pas cette obligation se verrait dans l'obligation de rembourser un client victime d'une opération non autorisée. Cela se comprend : s'il ne met pas en place un moyen telle que l'authentification forte qui permet de fortement

[5] Les articles de la DSP2 cités sont reproduits au sein de l'annexe n°2.

réduire le risque de fraude, le prestataire engage sa responsabilité. Il doit dans ce cas assumer les conséquences d'un paiement frauduleux qui aurait pu être évité en respectant les dispositions de la directive.

Une autre modification apportée par la DSP2 est l'abaissement du montant de la franchise restant à la charge de l'utilisateur de services de paiement en cas d'opération non autorisée avant opposition. Pour rappel, la DSP1 prévoyait que le payeur devait dans cette hypothèse supporter jusqu'à 150 euros du paiement frauduleux.

Dorénavant, l'article 74 paragraphe 1 de la seconde directive dispose que « le payeur peut être tenu de supporter, jusqu'à concurrence de 50 euros, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou au détournement d'un instrument de paiement ».

Ce nouveau montant vient renforcer les droits du consommateur, d'autant plus qu'il n'a plus lieu d'être lorsque « la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur a agi frauduleusement » ou lorsque « la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ». Ainsi, dans ces hypothèses, le payeur n'est tenu de supporter aucune conséquence de l'opération non autorisée et c'est alors à son prestataire de services de paiement de lui rembourser la totalité de la somme en question.

Enfin, la DSP2 raccourcit le délai de remboursement auquel le prestataire de services de paiement est soumis. En effet, si comme la DSP1, la nouvelle directive prévoit qu'« en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur rembourse au payeur le montant de cette opération immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé », une échéance est dorénavant à respecter car le texte continue en disposant que ce remboursement doit se faire « en tout état de cause au plus tard à la fin du premier jour ouvrable suivant ». Ainsi, les banques et établissements sont dorénavant soumis à un devoir de diligence accru renforçant les droits du consommateur qui se voit garantir un remboursement quasiment immédiat.

B. Une mise au point sur l'authentification forte

Si l'on se concentre sur le renforcement de la protection des consommateurs, l'authentification forte que doivent mettre en place les prestataires de services de paiement pour les transactions électroniques est l'apport le plus significatif de la DSP2. Il convient donc de l'étudier plus en détail afin de comprendre son fonctionnement et ses enjeux.

Comme le considérant 95 de la directive[6] le prévoit, « tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude ». Ainsi, cette authentification sûre de l'utilisateur ne peut se faire que grâce à la mise en œuvre d'un système d'authentification forte par les banques et autres acteurs de l'écosystème de paiement.

Nous l'avons vu précédemment, c'est l'article 74 de la directive qui oblige les prestataires de services de paiement à respecter cette condition d'authentification forte. Toutefois, l'article 98 laisse à l'Autorité bancaire européenne ainsi qu'à la Banque centrale européenne le soin d'élaborer les projets de normes techniques de règlementation à l'intention des prestataires de services de paiement, cela incluant les exigences relatives à l'authentification forte. Ainsi, c'est le règlement délégué (UE) 2018/389 publié au Journal officiel de la Commission européenne du 13 mars 2018 qui spécifie les dispositifs d'authentification forte.

L'authentification forte permet de vérifier que la personne à l'origine de l'opération de paiement est bien le payeur. Pour ce faire, la directive dispose article 97 paragraphe 2 que les éléments à prendre en compte doivent établirent un lien dynamique entre l'opération, le montant et le bénéficiaire donné.

Plus particulièrement, le considérant 6 du règlement délégué (UE) 2018/389 de la Commission européenne[7] prévoit que l'identification se fait par le biais de deux facteurs minimum (et non plus un seul comme le prévoyait la DSP1). Ces derniers appartiennent à trois catégories différentes, à savoir :

- La catégorie « connaissance », qui correspond à quelque chose que seul l'utilisateur connaît, comme un mot de passe ou une information personnelle ;

[6] Le considérant 95 est reproduit au sein de l'annexe n°3.
[7] Les extraits du règlement délégué (UE) 2018/389 sont reproduits au sein de l'annexe n°4.

- La catégorie « possession », qui correspond à quelque chose que seul l'utilisateur possède, comme un téléphone ou un ordinateur ;
- La catégorie « inhérence », qui correspond à quelque chose que l'utilisateur est, comme une empreinte digitale ou une reconnaissance faciale.

La mise en place de l'authentification forte peut se faire selon un modèle de redirection ou un modèle intégré. Dans le cadre du premier modèle, l'utilisateur souhaitant valider un paiement en ligne est redirigé vers sa banque afin qu'il s'identifie. Quant au second modèle, il permet à l'utilisateur de s'identifier directement sur l'interface où se déroule la transaction.

La directive considère dans son article 97 paragraphe 1 qu'un prestataire de services de paiement doit appliquer l'authentification forte du client lorsque le payeur « accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute une action, grâce à un moyen de communication à distance susceptible de comporter un risque de fraude ».

Toutefois, des exceptions sont prévues aux articles 10 et suivants du règlement de la Commission européenne. L'authentification forte n'est notamment pas requise lorsque l'utilisateur est limité dans son accès à des éléments qui ne divulguent pas de données de paiement sensibles, en cas de paiement sans contact au point de vente, lorsqu'il s'agit de frais de transport et de parking ou de paiement à un bénéficiaire de confiance, pour des opérations récurrentes, des virements entre comptes détenus par la même personne ou des opérations de faible valeur (inférieures ou égales à 30 euros).

De plus, les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsqu'ils considèrent que l'opération présente peu de risque, notamment concernant le taux de fraude lié à l'opération en question.

Notons que l'Observatoire de la sécurité des moyens de paiement indique que ce dispositif d'exemption se révèle efficace en pratique car au premier semestre 2022, le taux de fraude des paiements exemptés d'authentification forte (0,115%) est très proche de celui des paiements avec authentification forte (0,108%)[8].

[8] Rapport « Chiffres-clés de l'Observatoire » de l'OSMP, 1er semestre 2022.

Pour le reste, l'authentification forte est rendue obligatoire depuis le 14 septembre 2019. Malgré tout, le risque de fraude demeure présent car les fraudeurs se sont adaptés en trouvant de nouvelles techniques afin de contourner le mécanisme.

Mais pour que les règles prévues par la DSP2 s'appliquent en droit interne, encore faut-il que les Etats membres transposent la directive. Concernant la France, c'est l'ordonnance n°2017-1252 du 9 août 2017 qui est venue prévoir des dispositions permettant la transposition de la DSP2 dans le code monétaire et financier.

II. L'impact de la DSP2 sur le droit national français

En France, les première et deuxième directives sur les services de paiement ont toutes deux été transposées au sein du code monétaire et financier. Notamment, l'authentification forte prévue dans le CMF à l'article L133-44[9] est venue modifier en profondeur le fonctionnement des prestataires de services de paiement qui se sont progressivement adaptés aux nouvelles exigences.

A. Une transposition des directives au sein du code monétaire et financier

Une directive est un texte communautaire adopté par les institutions européennes et qui fixe des objectifs à atteindre pour les Etats membres. Un tel texte doit donc être transposé au sein de ces pays afin d'adapter le droit national aux exigences de la législation européenne.

En France, le mécanisme de transposition d'une directive passe d'abord par le Conseil des ministres qui prend une ordonnance visant à transposer la directive. Cette ordonnance est ensuite signée par le président de la République et promulguée. Puis une loi de ratification est adoptée par le Parlement après débats et l'ordonnance prend alors force de loi.

Afin de connaître l'impact de la transposition de la DSP2 dans le code monétaire et financier, il convient de s'interroger sur les dispositions qui existaient auparavant. Ces dernières résultent de la transposition de la première directive sur les services de paiement par l'ordonnance n°2009-866 du 15 juillet 2009 et sont entrées en vigueur le 1er novembre 2009.

[9] Les articles du CMF cités sont reproduits au sein de l'annexe n°5.

Cette transposition de 2009 a permis de mettre le code monétaire et financier en accord avec les mesures prévues par la DSP1. Les articles modifiés ou créés reprenaient sensiblement les termes de la directive, ce qui a permis au droit national de respecter les exigences européennes. Ont donc été introduites les nouvelles obligations reposant sur les prestataires et utilisateurs de services de paiement, afin de renforcer la protection du consommateur.

Dans ces circonstances, les modifications apportées par la transposition de la DSP2 n'ont pas eu pour effet un quelconque assouplissement des règles en vigueur mais ont bien amélioré les droits de l'utilisateur de services de paiement.

La DSP2 a été transposée dans le droit national français par l'ordonnance n°2017-1252 du 9 août 2017, complétée par deux décrets et cinq arrêtés du 31 août 2017. La loi n°2018/700 du 3 août 2018 est ensuite venue ratifier cette ordonnance.

Cette transposition vient comme la première modifier le code monétaire et financier. S'agissant du renforcement de la protection du consommateur, les principaux changements se situent dans le chapitre III « Les règles applicables aux autres instruments de paiement et à l'accès aux comptes », tiré du titre III « Les instruments de la monnaie scripturale ».

A la lecture des articles modifiés ou créés par l'ordonnance du 9 août 2017, le constat est celui d'une transposition presque parfaite du texte européen. La rédaction des articles rappelle en effet ceux de la directive, comme c'était le cas s'agissant de la transposition de la DSP1.

Ainsi par exemple, l'article L133-17 du code monétaire et financier évoque la notification à la charge de l'utilisateur de services de paiement « lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées ».

Autre exemple, l'authentification forte est définie article L133-4 en reprenant les trois catégories citées par le règlement délégué de la Commission européenne ; à savoir la possession, la connaissance et l'inhérence. Il est ensuite prévu article L133-44 que l'authentification forte est applicable lorsque le payeur « accède à son compte de paiement en ligne, initie une opération de paiement électronique, exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse », comme en disposait la directive dans son article 97.

Ainsi, le législateur a respecté les exigences de la DSP2 et le droit français est donc en accord avec le droit communautaire. Nous noterons en outre que le législateur n'a pas souhaiter réaliser de surtransposition, un Etat membre ayant en effet la possibilité d'instaurer une norme plus contraignante que ce que prévoit une directive.

Cependant, nous pouvons relever que la Commission des finances du Sénat avait par exemple apporté une proposition de transposition visant à assurer une protection du consommateur sur l'ensemble des services proposés par les prestataires de services de paiement[10].

La DSP2 a en effet un champ d'application limité couvrant le périmètre des comptes de paiement et non les autres supports de bancarisation et d'épargne. Dans ces circonstances, l'authentification forte n'est par exemple pas requise pour les comptes hors périmètre de la DSP2 et les utilisateurs ne sont pas assez protégés en cas de fraude, le risque étant supporté par ces derniers et la possibilité d'un remboursement n'étant pas prévue par la loi.

L'idée était alors de garantir aux victimes une possibilité de remboursement par le prestataire même en cas de fraude sur un compte hors périmètre de la DSP2, tel que sur un compte épargne par exemple. Toutefois, cette proposition n'a pas été retenue, les parlementaires ayant estimé que cet enjeu devait être abordé au niveau européen pour des raisons de concurrence[11].

B. La mise en place progressive de l'authentification forte par les prestataires de services de paiement

La date d'application de la DSP2 par les Etats membres était prévue au 13 janvier 2018. Toutefois, le règlement européen relatif aux normes techniques réglementaires chargé de spécifier les dispositifs d'authentification forte n'a été publié au Journal officiel de la Commission européenne que le 13 mars 2018. De plus, s'en est suivie une période transitoire au cours de laquelle les normes de sécurité n'étaient pas encore appliquées. Ce n'est en effet qu'à partir du 14 septembre 2019 que ces dernières se sont progressivement vues être mises en pratique par les Etats membres.

[10] Le projet de loi de la Commission des finances est reproduit au sein de l'annexe n°6.
[11] Un extrait du rapport de l'Assemblée nationale est reproduit au sein de l'annexe n°7.

Ainsi, l'obligation pour les prestataires de services de paiement de mettre en place l'authentification forte est arrivée bien plus tard que la directive elle-même. Cela est regrettable, la DSP2 ayant notamment été élaborée dans l'urgence causée par l'augmentation des fraudes visant les paiements en ligne. Or, il aura fallu attendre au minimum quatre ans après l'adoption de la directive pour que soient enfin appliquées par les Etats membres les mesures de sécurité permettant de renforcer la protection des consommateurs.

Depuis 2008, en France, le système permettant de sécuriser les paiements en ligne est une procédure d'authentification 3-D Secure, élaboré conjointement par Visa et Mastercard. Il est aujourd'hui automatiquement proposé par la quasi-totalité des cartes. Un tel mécanisme a nécessairement dû évoluer en raison des nouvelles exigences européennes et nationales.

Avant la mise en place de l'authentification forte, après avoir rentré ses informations bancaires sur le site d'achat, le consommateur était redirigé vers une fenêtre provenant de sa banque et devait alors fournir un code unique reçu par SMS. Ainsi, ce mécanisme chargé de vérifier l'identité de la personne à l'origine du paiement en ligne ne reposait que sur un facteur d'authentification, à savoir la possession du téléphone sur lequel était envoyé le code.

Un tel système s'est donc rapidement montré insuffisant face au développement du commerce en ligne et au nombre élevé de fraudeurs qui contournaient facilement ce protocole d'authentification simple. C'est dans ce contexte qu'est intervenue la nécessité de mettre en œuvre l'authentification forte, celle-ci reposant sur deux éléments d'authentification et assurant ainsi une plus grande sécurité des transactions.

La mise en place de l'authentification forte s'est faite progressivement car les prestataires de services de paiement ont eu besoin de temps afin de repenser leur fonctionnement pour s'adapter aux nouvelles exigences. Et ainsi, il aura fallu attendre mai 2021 pour que le protocole 3-D Secure demande une authentification forte des utilisateurs.

Dorénavant, le consommateur doit d'abord télécharger l'application d'authentification de la banque et activer le service grâce à un code unique reçu par SMS. Avant un paiement, il est ensuite demandé à l'utilisateur de s'authentifier, par saisie de son code personnel, par son empreinte biométrique ou par une caractéristique personnelle. On retrouve bien les critères de l'authentification forte définis par la directive et par le code monétaire et financier : une fenêtre qui redirige vers l'application de la banque

renvoie à la catégorie « possession », un code personnel à la catégorie « connaissance » et une empreinte à la catégorie « inhérence ».

Notons que les banques et établissements de paiement peuvent également fournir des alternatives pour les personnes qui ne seraient pas dotées de téléphone portable, tels que des lecteurs QR-Code, des clés USB ou des boîtiers.

Enfin, les procédures peuvent varier selon les prestataires de services de paiement car ils sont libres de mettre en place le système de leur choix tant que ce dernier permet une authentification forte du client. Par exemple, en cas de paiement en ligne, Boursorama renvoie à son application et demande ensuite à l'utilisateur de s'identifier grâce au mot de passe de son compte ou à la reconnaissance facile ou digitale. Autre exemple, la Banque Postale et la Caisse d'épargne renvoient également à leur application mais exigent quant à elles un code personnel à 5 chiffres créé spécifiquement pour valider les opérations risquées.

Mais malgré le respect des règles d'authentification forte par les prestataires de services de paiement, la risque de fraude est encore présent et pèse sur les consommateurs victimes de nouvelles techniques de fraude.

PARTIE 2 : UN RISQUE DE FRAUDE MAINTENU ET ACCOMPAGNE DE LA DIFFICULTE POUR LES VICTIMES A SE FAIRE REMBOURSER LES OPERATIONS NON AUTORISEES

Selon l'Observatoire de la sécurité des moyens de paiement[12], la proportion de paiements frauduleux avec authentification forte est restée contenue en 2021 avec 9% du nombre total des paiements frauduleux par carte sur internet. Toutefois, leur poids dans le montant total des opérations frauduleuses est bien plus significatif puisqu'il représente 30% du montant total de 103 millions d'euros. Les associations de consommateurs déplorent en outre une augmentation du préjudice financier supporté par les consommateurs, en dépit de la baisse globale de la fraude.

Les escrocs disposent de nombreux moyens pour arriver à leurs fins. Il y a par exemple le skimming, qui consiste à dupliquer les données bancaires stockées sur la bande magnétique de la carte et parfois le code secret à l'aide d'une caméra ou d'un clavier numérique détourné. Autre exemple, la demande de rançon informatique : un message alarmant s'affiche sur un ordinateur qui semble ne plus fonctionner et le paiement d'une somme d'argent est alors demandé afin de le débloquer. Et n'oublions pas le cas classique ; l'utilisation frauduleuse d'une carte bancaire volée ou perdue. En clair, les possibilités de fraude sont variées.

Mais la mise en place de l'authentification forte afin de valider les opérations en ligne a en outre conduit les fraudeurs à développer d'autres techniques permettant de contourner cet obstacle. Et s'il existe plusieurs manières de frauder, deux d'entre elles se distinguent des autres de par leurs taux d'utilisation et de réussite : il s'agit du spoofing et du phishing, qui sont des formes d'usurpation d'identité destinées à manipuler les cibles des escrocs.

La loi prévoit un droit au remboursement du montant des opérations non autorisées à la charge des prestataires de services de paiement. Toutefois, il arrive régulièrement que ces derniers tentent de se décharger de cette obligation en remettant la faute sur les victimes. Dans de telles circonstances, les utilisateurs peuvent se tourner vers la médiation et/ou vers un tribunal afin d'obtenir gain de cause.

[12] Rapport annuel de l'Observatoire de la sécurité des moyens de paiement, édition 2021, Banque de France.

Il conviendra dans un premier temps d'étudier les techniques de fraude les plus utilisées ainsi que la tendance des prestataires de services de paiement au refus du remboursement des victimes. Puis, nous verrons quels sont les recours mis à la disposition de ces dernières pour obtenir un tel remboursement.

Chapitre 1 : Le remboursement des opérations non autorisées souvent refusé face aux capacités des fraudeurs à contourner l'authentification forte

Les techniques dorénavant utilisées par les fraudeurs permettent de récolter des informations confidentielles sur de potentielles victimes, de manière à les manipuler afin de leur faire valider des opérations frauduleuses par le biais de l'authentification forte.

Si la loi oblige normalement les prestataires de services de paiement à rembourser le montant des opérations non autorisées, ces derniers ont cependant tendance à refuser les demandes en ce sens. Un des arguments avancés pour justifier ce refus est le fait que les opérations contestées ont fait l'objet d'une validation par authentification forte. Ainsi, non seulement la mise en place de l'authentification forte ne stoppe pas la fraude, mais elle sert en plus de motif aux banques et établissements de paiement pour ne pas indemniser leurs clients.

Nous le verrons, l'autre argument le plus utilisé par les professionnels pour refuser les demandes de remboursement est d'accuser les victimes de négligence grave, celle-ci faisant en effet obstacle à une quelconque indemnisation. L'étude des réponses des prestataires de services de paiement aux réclamations permet de constater qu'elles se ressemblent toutes et que la tendance est de violer au maximum le droit au remboursement des opérations non autorisées.

C'est dans ces circonstances que sont intervenus l'Autorité de contrôle prudentiel et de résolution et l'Observatoire de la sécurité des moyens de paiement au travers de recommandations destinées aux professionnels du secteur bancaire. Des précisions ont ainsi été apportées quant au traitement des réclamations et aux modalités de remboursement des opérations de paiement frauduleuses.

Après avoir étudié le spoofing et le phishing, techniques de fraude ayant émergé face à la mise en place de l'authentification forte, il conviendra de se pencher sur les réponses apportées par les professionnels aux demandes de remboursement des opérations non autorisées.

I. L'émergence de techniques de fraude permettant de contourner l'obstacle de l'authentification forte

Si la mise en place de l'authentification forte a certes réduit le taux de fraude, elle a également poussé les escrocs à innover dans leurs techniques. Désormais les victimes valident elles-mêmes des opérations frauduleuses dont les montant peuvent être très importants.

A. Le spoofing

Le spoofing est une technique qui s'est énormément développée ces dernières années, notamment du fait de la DSP2 et de la mise en place de l'authentification forte sécurisant les paiements en ligne. Le terme « spoofing » provient de l'anglais et plus particulièrement du verbe « to spoof » qui signifie usurper, le spoofing correspondant en effet à une usurpation d'identité de la part de l'escroc.

La nécessité pour les prestataires de services de paiement de demander une authentification forte du consommateur pour ses achats en ligne a permis de réduire les risques qu'un escroc effectue directement un paiement à la place du payeur. Mais la fraude ne disparait pas pour autant, ce sont simplement les procédés des escrocs qui évoluent.

Comme l'explique Julien Lasalle, responsable du service de surveillance des moyens scripturaux à la Banque de France, « les fraudeurs, plutôt que d'essayer la technologie, vont s'attaquer au porteur de la carte lui-même ». Plus particulièrement, c'est en manipulant ce dernier que les escrocs parviennent à lui faire valider lui-même et par le biais de l'authentification forte les opérations frauduleuses.

Pour y parvenir, le fraudeur usurpe l'identité d'une source fiable, le plus souvent un professionnel, et contacte sa potentielle victime par appel téléphonique, courrier électronique ou même SMS. L'escroc dispose alors de plusieurs moyens afin de gagner la confiance de son interlocuteur.

En cas d'appel par exemple, il est en général capable de personnaliser le numéro apparaissant pour le consommateur, de manière à afficher le numéro de la personne ou de l'établissement usurpé et non le sien. De la même façon, un e-mail frauduleux va reproduire à l'identique le type d'e-mails qu'envoie habituellement la personne ou l'établissement usurpé.

Notons que les escrocs ont tendance à préférer les appels aux e-mails ou SMS car une personne est plus facilement manipulable lorsqu'il est possible de lui parler directement. Celle-ci a en effet du mal à prendre du recul sur la situation et n'a pas ou très peu d'éléments lui permettant de détecter la fraude. C'est moins le cas dans l'hypothèse d'un e-mail ou d'un SMS dans lequel il est possible de rechercher des fautes d'orthographe ou de s'interroger sur la réelle provenance du message.

Une fois la conversation engagée, le fraudeur va tenter d'établir une relation de confiance avec son interlocuteur. Pour ce faire, il va rassurer la victime en lui exposant des informations la concernant et que seul le professionnel qu'il prétend être est censé connaître. Cela demande un travail en amont de l'escroc qui va devoir se procurer des données confidentielles sur les gens qu'il souhaite arnaquer. Pour y parvenir, il peut notamment faire du piratage informatique, parcourir les réseaux sociaux ou encore acheter des données sur le Dark Web, ce dernier étant un ensemble caché de sites internet permettant de préserver l'anonymat et la confidentialité de ses utilisateurs.

Lorsque la personne est rassurée sur l'identité de son interlocuteur, celui-ci va chercher à lui faire peur afin de la perturber et de l'amener à faire ce qu'il lui demande. En sa qualité de professionnel, il indique à sa victime avoir remarqué des mouvements frauduleux sur son compte bancaire. Celle-ci va alors paniquer et vouloir remédier à la situation au plus vite, et ce avec l'aide de l'escroc qu'elle pense professionnel et fiable.

Le fraudeur propose alors à sa victime de bloquer les opérations frauduleuses en cours. Il a pour cela besoin d'elle et lui demande soit de valider directement des opérations censées éviter la fraude, soit de lui transmettre les codes qu'elle reçoit afin qu'il les valide lui-même. Mais pendant que la victime pense permettre à un professionnel d'empêcher une tentative de fraude, en réalité l'escroc lui fait autoriser des opérations ne profitant qu'à ce dernier.

En général, la technique du spoofing nécessite du fraudeur un piratage du compte bancaire de sa victime afin qu'il puisse initier les opérations de son choix. Comme il ne peut aller au bout en raison de la nécessité d'une authentification forte pour les valider, il manipule alors sa victime car elle seule peut autoriser les opérations en question. Cela remet donc en cause l'efficacité de l'authentification forte qui certes complique quelque peu le travail des fraudeurs, mais n'empêche pas pour autant la fraude d'avoir lieu.

Bien souvent, les victimes réalisent qu'elles se sont fait avoir trop tard. Il ne leur reste plus qu'à contacter l'établissement de paiement afin de leur signaler la situation et faire opposition. On retrouve ici l'obligation de notification prévue par la DSP2 et le code monétaire financier. Elles doivent également porter plainte, bien que qu'un dépôt de plainte ne soit pas nécessaire pour demander le remboursement des opérations non autorisées. Notons que ce type de fraude ne touche pas que des personnes naïves mais bien tout type de gens ; les fraudeurs étant doués pour amener leurs interlocuteurs à leur faire confiance.

Les opérations frauduleuses correspondent à des ajouts de bénéficiaires sur le compte bancaire, à des virements et/ou à des achats en ligne. Les sommes prélevées peuvent être très importantes et les effets dévastateurs pour les victimes. Il arrive qu'elles parviennent à récupérer leur argent mais la tâche n'est pas toujours simple, notamment du fait que les opérations ont été validées par le biais de l'authentification forte.

Afin de contrer ce phénomène, les banques font de la prévention et rappellent sur leurs sites ou applications mobiles qu'elles ne contacteraient jamais leurs clients pour leur faire valider une opération et qu'elles ne leurs demanderaient jamais des données de connexion ou d'informations bancaires. Elles appellent également leurs utilisateurs à ne jamais répondre aux communications qui n'auraient pas été sollicitées et à contacter leurs banques par leurs propres moyens.

Mais le spoofing est malgré tout très utilisé dans la pratique et l'ADC France reçoit énormément de dossiers de victimes de cette technique. Quelques-uns de ces dossiers ont été sélectionnés afin d'illustrer les propos ci-dessus.

Le premier exemple concerne une adhérente de l'association qui reçoit un appel téléphonique d'une personne prétendant être un policier. Celui-ci aurait constaté des opérations suspectes sur le compte bancaire de son interlocutrice, qui n'en est bien sûr pas à l'origine. L'escroc lui indique qu'en tant que policier, il peut remédier à la fraude en cours et la met en confiance en lui donnant des informations personnelles telles que sa date de naissance et sa banque.

Elle reçoit alors deux messages lui demandant de confirmer les opérations censées bloquer les paiements. Suivant les instructions de l'escroc, elle valide ces dernières. L'escroc raccroche, et lorsque la victime vérifie l'état de son compte, elle réalise que deux paiements de 308,32 euros et 751,24 euros ont été réalisés.

Le second exemple est semblable au premier sauf que cette fois, l'escroc se fait passer pour un salarié de Boursorama Banque et explique à sa victime que des paiements frauduleux sont en cours sur le compte commun du couple. Il contacte d'abord la femme et lui demande de transmettre les codes qu'elle reçoit afin qu'il puisse bloquer les paiements. Puis il l'informe qu'il va devoir contacter son mari. Ce dernier, mis au courant par sa femme de la situation, répond à l'appel et transmet également à l'escroc les codes qu'il reçoit. Il finit par se rendre compte de l'arnaque mais raccroche trop tard, deux virements de 6 500 euros et 10 000 euros ainsi que des achats pour un total de 15 629,84 euros ayant déjà été effectués.

Ce dernier cas est d'autant plus intéressant que la femme devient sans le vouloir la complice de l'escroc. Comme elle prévient son mari qu'il va recevoir un appel de sa banque, ce dernier est moins méfiant que s'il n'avait pas été averti par sa femme et le travail du fraudeur en est facilité. Nous remarquons également l'énorme montant des sommes prélevées et l'importance du préjudice subi par les victimes. Une telle fraude est d'autant plus étonnante qu'elle a abouti en raison de l'absence de réaction de la banque sur des opérations aussi importantes. Qu'en est-il du devoir de vigilance auquel sont pourtant soumis les prestataires de services de paiement ?

Un récent cas de spoofing a également attiré notre attention : en plus des étapes habituelles, l'escroc se faisant passer pour un conseiller bancaire a informé sa victime qu'il devait récupérer sa carte bancaire compromise dans le but de lui en envoyer une nouvelle. Pour ce faire, il a prévenu son interlocuteur qu'un taxi allait venir à son domicile chercher sa carte. Cela a réellement eu lieu, une voiture se faisant passer pour un taxi s'étant effectivement rendue chez la victime afin que celle-ci lui donne son instrument de paiement. Des retraits d'espèces frauduleux ont par la suite été effectués à l'aide de la carte bancaire en question.

B. Le phishing

Le phishing est une forme de manipulation qui, comme le spoofing, est de plus en plus appréciée des fraudeurs. Le terme provient de la contraction des mots anglais « fishing » qui veut dire « pêche » et « phreaking » qui signifie « piratage de lignes téléphoniques ». Il correspond en français à la technique de l'hameçonnage : les escrocs trompent leurs victimes de manière à leur soustraire des informations confidentielles et à voler leur argent.

D’abord, les fraudeurs contactent leurs potentielles victimes par des moyens variés : il peut s’agir de SMS, courriers électroniques, appels voire de documents papier. Le message transmis est alarmiste ou au contraire attrayant, afin qu’un maximum de personnes soit intéressé par son contenu. Pour ce faire, l’escroc usurpe l’identité d’une entité ou d’un organisme connu et copie à l’identique son style et ses codes pour tromper le destinataire.

Après avoir exposé la prétendue situation à ce dernier, le message l’invite à cliquer sur un lien ou une pièce jointe. Généralement, le consommateur est alors renvoyé vers un site reproduisant celui de l’organisme dont l’identité a été usurpée. Il lui est demandé de rentrer des informations personnelles tels que son identifiant et mot de passe de compte bancaire ou ses données de carte bleue. Si la victime pense bénéficier d’une offre ou s’acquitter d’une dette, elle est en réalité en train de fournir à l’escroc des données confidentielles depuis un site pirate. Elle peut même parfois sans le savoir valider une opération frauduleuse par le biais de l’authentification forte.

En cliquant sur un lien ou une pièce jointe, le risque est que la victime installe malgré elle un logiciel malveillant capable de voler des renseignements personnels et financiers. L’objectif de l’escroc est en effet d’obtenir des données confidentielles sur ses victimes de manière à pouvoir se connecter sur leurs comptes bancaires et détourner leurs fonds. La technique du phishing permet également de récolter des informations s’avérant être précieuses lors d’une tentative de spoofing ; la connaissance de celles-ci par le fraudeur étant un moyen efficace de mettre son interlocuteur en confiance.

Comme pour le spoofing, les victimes de phishing constatent des opérations non autorisées sur leurs comptes bancaires, tels que des virements, achats ou ajouts de bénéficiaires frauduleux. Les fraudeurs ayant accès à leurs comptes, elles doivent impérativement modifier l’accès à ces derniers et nettoyer leurs ordinateurs au cas où un logiciel malveillant y aurait été installé.

Si les escrocs peuvent atteindre un nombre important de personnes par le biais des e-mails ou SMS, cette technique n’est pas toujours efficace puisqu’un consommateur prudent va prendre le temps d’analyser le message. Notamment, l’arnaque est souvent détectable au regard de fautes d’orthographe ou d’une syntaxe inhabituelle. La provenance du message peut aussi alerter. De plus, ce type d’arnaque ne vise pas une personne en particulier et le contenu du message peut alors ne pas correspondre à la situation du destinataire. Par exemple, quelqu’un qui recevrait une prétendue amende suite à une infraction routière alors qu’il ne conduit pas va se douter du subterfuge.

Plusieurs exemples permettent d'illustrer le spoofing. D'abord, l'ADC France s'est penchée sur le fishing contre la Banque Postale. Un mail s'adressant aux clients de la Banque Postale et reprenant les caractéristiques de cette dernière (logo et style professionnel) informe ses clients du fait qu'ils n'ont pas encore reconfirmé leur numéro de mobile dans leur profil. Le courrier poursuit en précisant qu'à partir du 15 novembre 2022 et conformément à la DSP2, l'identifiant et le code secret de connexion ne suffiront plus pour accéder à l'espace client. Les destinataires sont alors conviés à suivre le lien « ACTIVEZ VOTRE SERVICE », censé permettre de confirmer le numéro de mobile.

Ici, le fraudeur instaure un sentiment d'urgence pour le lecteur qui ne souhaite pas perdre l'accès à son espace client. De plus, une simple confirmation de son numéro de téléphone ferait tout rentrer dans l'ordre. La tentation de suivre les instructions et de cliquer sur le lien fourni dans le mail est alors présente.

Toutefois, une lecture attentive du message permet de constater des fautes d'orthographe ainsi que des tournures de phrases peu habituelles. Le doute est donc permis. De plus, une analyse plus poussée réalisée par l'association permet d'établir la provenance de l'e-mail, totalement étranger à la Banque Postale. En effet, le code source indique que l'envoyeur est passé par une société de prestations de services internet japonaise ; il n'a donc rien à voir avec la Banque Postale. Toutefois, rares sont les personnes enquêtant de la sorte et un consommateur moyen est susceptible de se faire avoir, l'e-mail reprenant avec habileté les codes d'une banque.

Et pour cause, l'ADC France traite de nombreux dossiers de phishing. Un de ses adhérents a par exemple été victime de phishing par e-mail. Celui-ci affichait l'entête de Canal+ et proposait de profiter d'un chèque cadeau d'une valeur de 100 euros. Un lien pour en « profiter maintenant » était présent. Le consommateur, pensant que l'offre provenait réellement de Canal+ en raison de l'habillage du mail, a suivi le lien et a rentré ses coordonnées bancaires afin de régler la modique somme de 1,99 euros permettant de profiter du chèque cadeau. Mais en consultant son compte bancaire, la victime a alors découvert un achat de 699 euros dans une grande enseigne, achat dont elle n'était bien sûr pas à l'origine. Les escrocs ont ainsi réussi manipuler le consommateur pour qu'il valide par le biais de l'authentification forte un achat frauduleux de 699 euros. Ils ont de plus très certainement collecté ses données personnelles.

Enfin, la technique des faux procès-verbaux de stationnement mérite d'être soulignée. Un document papier signalant qu'une infraction à la réglementation du stationnement a été relevée est déposé sur un

véhicule stationné. L'automobiliste est alors invité à régler la contravention en scannant un QR code. Ce dernier renvoie à une contrefaçon du site « antai.gouv.fr », sur lequel la personne rentre ses coordonnées personnelles et bancaires et règle une amende inventée de toute pièce. Si un consommateur normalement avisé émet généralement un doute lorsqu'il reçoit un e-mail ou un SMS frauduleux, il aura tendance à moins se méfier face à une telle arnaque, encore peu connue du grand public.

Là encore, les sommes prélevées frauduleusement peuvent avoir des conséquences désastreuses pour les victimes. Certaines se retrouvent à découvert, ce qui engendre souvent des frais supplémentaires et augmente donc l'importance du préjudice financier voire moral qu'elles subissent. Mais comme pour le spoofing, tout espoir n'est pas systématiquement perdu car les établissements de paiement ont le devoir de rembourser à leurs clients le montant des opérations non autorisées.

Toutefois, la pratique montre que les professionnels du secteur bancaire cherchent à se décharger de toute responsabilité en exploitant les exceptions dans lesquelles le remboursement n'est pas dû.

II. La nécessaire élaboration de recommandations face aux réticences des prestataires de services de paiement à rembourser les opérations non autorisées

Les prestataires de services de paiement refusent régulièrement les demandes de remboursement, au motif que la victime a fait preuve de négligence grave ou que l'opération a été validée par le biais de l'authentification forte. L'Autorité de contrôle prudentiel et de résolution et l'Observatoire de la sécurité des moyens de paiement sont alors intervenus afin de limiter les abus de la part des professionnels, le droit au remboursement des opérations non autorisées devant rester le principe.

A. La tendance au refus d'indemnisation des victimes de fraude par les prestataires de services de paiement et comment l'aborder

1. L'habitude pour les prestataires de services de paiement d'invoquer les exceptions au devoir de remboursement afin d'y échapper

Les règles en matière de remboursement sont prévues par les articles L133-18 et suivants du code monétaire et financier. Selon ces derniers, le prestataire de services de paiement rembourse immédiatement et en tout état de cause à la fin du jour ouvrable suivant la victime qui a signalé l'opération non autorisée dans les treize mois.

Ce n'est que si l'utilisateur de services de paiement a agi frauduleusement ou n'a pas respecté, intentionnellement ou par négligence grave, ses obligations, que la banque est en droit de refuser le remboursement. Ainsi, si la victime n'a pas préservé ses données de sécurité personnalisées, n'a pas utilisé l'instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation ou a tardé à informer le prestataire de services de paiement de la situation, celui-ci peut tenter de se décharger de sa responsabilité et éviter un remboursement.

Notons qu'une franchise de 50 euros peut rester à la charge du payeur lorsque l'opération non autorisée a eu lieu avant le signalement de la perte ou du vol de l'instrument de paiement et avec l'utilisation des données de sécurité personnalisées. Toutefois, les hypothèses dans lesquelles ce montant est mis à la charge de l'utilisateur sont rares. Par exemple, il n'aura rien à payer s'il est toujours resté en possession de son instrument de paiement ou lorsque la perte ou le vol ne pouvait être détecté avant l'opération non autorisée.

De même, le payeur ne supporte aucune conséquence financière d'une opération non autorisée dans le cas où son prestataire de services de paiement n'exigeait pas une authentification forte de sa part.

En pratique, les banques et établissements de paiement cherchent à éviter le remboursement des opérations non autorisées de leurs clients. Une étude des dossiers de l'ADC relatifs aux fraudes

bancaires permet de constater une certaine concordance dans les réponses aux demandes de remboursement des victimes[13].

L'argument qui ressort presque systématiquement est le fait que l'opération a été validée par le biais de l'authentification forte. Dans de telles circonstances, le prestataire de services de paiement estime qu'il a fait son devoir en permettant une telle authentification et que le payeur était suffisamment protégé pour éviter qu'une opération frauduleuse puisse avoir lieu. Les exigences de la DSP2 étant respectées, il se décharge de toute responsabilité. En outre, la banque ou l'établissement de paiement fait une lecture a contrario de l'article L133-19 V du code monétaire et financier : comme une authentification forte est exigée, c'est au payeur de supporter les conséquences financières de l'opération non autorisée.

À cet argument de l'authentification forte est généralement associé celui de la négligence grave du payeur. Pour rappel, seule la fraude ou la négligence grave de l'utilisateur l'empêche d'être indemnisé. S'il est très rare que le client soit accusé d'agissements frauduleux par la banque ou l'établissement de paiement, sa négligence grave est pratiquement systématiquement invoquée. Cette notion signifie que la victime n'a pas agi comme une personne raisonnablement prudente face à la situation et que si elle avait fait preuve de plus de vigilance, elle aurait pu éviter la fraude.

Enfin, les banques et établissements de paiement peuvent se justifier en indiquant qu'aucun incident technique n'a eu lieu au cours de l'opération. Cet argument fait écho à l'article L133-23 du code monétaire et financier qui prévoit que le prestataire de services de paiement doit prouver que l'opération a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

Parfois, les banques et établissements de paiement demandent un retour des fonds, mais cela aboutit rarement. De plus, il arrive qu'ils conditionnent le remboursement à un dépôt de plainte préalable. Toutefois, cette règle n'est pas prévue par la loi et l'on peut imaginer qu'il s'agit d'une manière de décourager la victime ou de gagner du temps.

En plus de refuser le remboursement, il arrive que les prestataires de services de paiement menacent leurs clients d'une clôture de compte, d'une restitution des moyens de paiement, d'une interdiction

[13] Des exemples de réponses des banques sont reproduits au sein de l'annexe n°8.

bancaire voire d'une inscription au FICP[14] de la Banque de France. De telles sanctions risquent en effet de se voir appliquer lorsque la victime a perdu tellement d'argent qu'elle se retrouve à découvert sans pouvoir rembourser le solde débiteur. Les conséquences sont alors déplorables pour la victime qui, en plus de la fraude, doit surmonter les décisions de sa banque.

Puis, les prestataires de services de paiement terminent généralement leur réponse par un paragraphe de mise en garde ; indiquant qu'ils ne demanderaient jamais d'informations confidentielles à leurs clients et les invitant donc à faire preuve de prudence dans la conservation de leurs données personnelles.

2. Les justifications permettant de faire céder les prestataires de services de paiement dans l'obtention d'une indemnisation

Souvent, la première réaction des banques face à une demande de remboursement de la part de leur client victime d'une fraude est donc le refus. Toutefois, avec les bons arguments, il arrive régulièrement que les prestataires de services de paiement se plient à la demande des victimes et acceptent de les indemniser.

Ainsi, si les banques et établissements de paiement connaissent la loi et donc l'obligation de remboursement pesant sur eux, il faut généralement leur apporter de solides justifications pour ne pas leur laisser le choix. Mais cela n'est pas à la portée de la majorité des victimes et beaucoup se découragent face au refus d'indemnisation de leur banque.

C'est dans ce contexte qu'intervient l'ADC France, composée de juristes et bénévoles habitués à ce genre de dossiers et sachant quels arguments invoquer[15].

Si l'utilisateur supporte toutes les pertes occasionnées par des opérations non autorisées en cas de fraude ou de négligence grave de sa part, encore faut-il prouver ces dernières. La jurisprudence est en effet constante sur le sujet : c'est à la banque de prouver que l'utilisateur du service a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations[16].

[14] Fichier National des Incidents de remboursement des Crédits aux Particuliers.
[15] Des exemples de lettres rédigées par un juriste de l'ADC France sont reproduits au sein de l'annexe n°9.
[16] Com., 21 novembre 2018, n°17-18.888 et Com., 26 juin 2019, n°18-12.581.

Or, la plupart du temps, les banques se contentent d'accuser leurs clients de négligence grave sans prendre la peine de démontrer cette dernière. Et quand elles s'y essaient, les faits qu'elles relatent ne sont en général pas assimilables à de la négligence grave. Il ne faut pas oublier qu'une personne ayant fait preuve de négligence grave commet une faute lourde. Une telle notion entraîne donc d'importantes conséquences et ne peut être employée à la légère et pour tous les cas.

Ce n'est pas parce qu'un fraudeur est parvenu à arnaquer une personne que celle-ci a nécessairement été gravement négligente. Nous l'avons déjà évoqué, les escrocs peuvent être remarquables dans leur capacité à manipuler leurs victimes afin que celles-ci ne se doutent de rien. L'objectif du juriste est alors de justifier le comportement du consommateur au vu des faits, en se penchant notamment sur les moyens employés par les fraudeurs pour arriver à leurs fins.

Il faut se mettre à la place de la victime : pouvait-elle douter de la nature du message et de la véritable intention de l'escroc ? La jurisprudence prévoit en effet que la négligence grave s'apprécie au regard d'indices permettant à un utilisateur normalement attentif de douter, peu importe qu'il soit ou non avisé des risques de fraude[17].

Les juges indiquent également qu'il faut prendre en compte les circonstances dans lesquelles la fraude a eu lieu[18]. Dès lors, différentes victimes d'un même type d'arnaque peuvent ne pas être responsables au même degré, tout dépendant des particularités de chaque affaire.

Ainsi, citer de la jurisprudence dans la lettre adressée au prestataire de services de paiement est un moyen efficace de faire céder ce dernier. Il sait que si la victime devait aller en justice, il aurait de grandes chances d'être condamné. Il va alors préférer régler la situation à l'amiable, d'autant plus que des juges ont déjà condamné les banques à des dommages et intérêts au profit de la victime accusée à tort de négligence grave[19].

Enfin, il faut s'interroger sur la part de responsabilité du prestataire de services de paiement dans la fraude. Il arrive parfois que la fraude ait été facilitée en raison d'une faute de la banque ou de l'établissement de paiement. Une déficience technique de sa part peut par exemple mener à une fuite de données des utilisateurs, permettant ensuite des opérations de phishing et de spoofing. De plus,

[17] Com., 28 mars 2018, n°16-20.018.
[18] CA de Versailles, 28 mars 2023, n°21/07299.
[19] CA de Versailles, 28 mars 2023, n°21/07299.

l'article 33 du règlement général sur la protection des données prévoit que le prestataire est dans l'obligation de déclarer à ses clients qu'une telle fuite a eu lieu. Il commettrait donc une faute dans le cas où il ne dirait rien.

En outre, les prestataires de services de paiement ont un devoir de vigilance qui leur impose de veiller à la bonne tenue des comptes et de détecter les anomalies. Or, les opérations non autorisées sortent généralement de l'ordinaire, de par leur montant, leur fréquence et/ou leur destination. Dans ces circonstances, de tels mouvements sont censés alerter les banques et établissements de paiement et permettre le blocage des transactions suspectes, au moins le temps d'en discuter avec le payeur. C'est alors parfois à se demander de qui provient la réelle négligence.

B. Les recommandations de l'ACPR et de l'OSMP sur le traitement des réclamations et les modalités de remboursement des opérations de paiement frauduleuses

1. La recommandation 2022-R-01 du 9 mai 2022 de l'ACPR[20]

Face au peu de considération de la part de certains prestataires de services de paiement quant aux contestations d'opérations de leurs clients, il a fallu agir.

En premier lieu, l'Autorité de contrôle prudentiel et de résolution, organe de supervision français de la banque et de l'assurance, est intervenue au travers de la recommandation 2022-R-01 du 9 mai 2022 applicable à compter du 31 décembre 2022. Elle y invite les professionnels à se doter d'une organisation simple et efficace afin d'apporter à leur clientèle des réponses adaptées, claires et surtout justifiées dans un court délai de temps.

Cette organisation du traitement des réclamations doit d'abord permettre aux professionnels d'identifier et de transmettre les demandes à l'interlocuteur ou au service compétent. L'ACPR insiste aussi sur le fait que les réclamations doivent se faire sur un support écrit, durable et daté.

Mais ce n'est pas tout : une fois la réclamation écrite reçue, le professionnel a l'obligation d'en accuser réception par écrit et dans un délai maximal de 10 jours ouvrables à compter de son envoi. Si cette

[20] La recommandation de l'ACPR est reproduite au sein de l'annexe n°10.

règle permet à l'utilisateur de s'assurer que sa demande a bien été réceptionnée, elle empêche surtout le prestataire de services de paiement d'ignorer la réclamation. Et puisqu'il l'a reçoit, cela implique aussi qu'il va devoir l'étudier et y apporter une réponse.

S'agissant de la réponse du prestataire de services de paiement, l'ACPR prévoit qu'elle doit se faire par écrit pour toute réclamation écrite. Elle doit être claire, de manière à ce que l'interlocuteur en comprenne facilement le sens et n'ait pas de doute quant à la position de la banque ou de l'établissement de paiement.

La réponse doit de plus être adaptée au cas d'espèce. Ainsi, les prestataires de services de paiement ne peuvent pas se contenter d'une réponse générale pouvant s'appliquer à la majorité des cas rencontrés. Ils doivent prendre en compte les éléments propres à chaque affaire et les intégrer à leurs explications afin d'apporter une solution personnalisée à chaque client. Toutefois, la lecture des réponses fournies en pratique permet de douter du respect de cette règle ; les mêmes arguments étant quasiment systématiquement invoqués sans que soit réellement étudié le contexte d'espèce.

En outre, l'ACPR prévoit que la réponse à une réclamation doit être argumentée. Mais comme nous l'avons déjà évoqué, ce sont toujours les mêmes motifs qui sont allégués ; à savoir le fait qu'il y ait eu authentification forte pour valider l'opération et la négligence grave du client. Ainsi, la qualité de l'argumentaire laisse souvent à désirer, d'autant plus que souvent les banques ne vont pas au bout de leur réflexion : elles ne démontrent pas la négligence grave et omettent le fait que ce n'est pas parce qu'il y a eu authentification forte que l'utilisateur donnait réellement son consentement à l'opération. L'auteur d'une réclamation doit obtenir une réponse dans un délai cohérent avec l'objet du mécontentement et dans la limite de deux mois. L'étude de la demande doit donc se faire rapidement afin de ne pas laisser la victime dans l'incertitude, d'autant plus que les investigations sont plus faciles à mener rapidement après la survenue des faits.

L'ACPR continue sa recommandation en précisant que l'organisation du traitement des réclamations doit être simple : elle ne doit pas reposer sur une multitude de circuits de traitement ou d'intervenants distincts. Un tel fonctionnement rallongerait en effet le délai de réponse. De plus, les collaborateurs en relation avec la clientèle ou pouvant recevoir des réclamations doivent être formés et compétents et l'organisation formalisée.

La recommandation précise également que les modalités pratiques pour effectuer une réclamation doivent être portées à la connaissances des utilisateurs de manière claire et compréhensible. Il ne faudrait pas qu'une victime de fraude renonce à son droit au remboursement parce qu'elle n'a pas connaissance de ce dernier ou parce qu'elle ne connaît pas la démarche à suivre.

Pour finir, l'ACPR invite les professionnels à identifier les dysfonctionnements, manquements à la réglementation et mauvaises pratiques commerciales et à prendre les mesures correctives pour y remédier. Ils sont également chargés d'analyser la qualité du dispositif de traitement des réclamations. Ainsi, répondre aux réclamations n'est qu'une étape dans la mission des prestataires de services de paiement qui doivent, une fois le problème identifié, trouver une solution pour qu'il ne se reproduise plus.

Lorsqu'un professionnel ne respecte pas une telle recommandation, il est possible de le signaler à l'ACPR. Un tel manquement est en premier lieu sanctionné par une mise en garde individuelle, dont le non-respect pourra ensuite donner lieu à une procédure disciplinaire.

2. La recommandation de l'OSMP du 16 mai 2023[21]

A cette recommandation de l'ACPR est venue s'ajouter celle de l'Observatoire de la sécurité des moyens de paiement. Ce dernier est une instance destinée à favoriser l'échange d'informations et la concertation entre les parties concernées par le bon fonctionnement des moyens de paiement et la lutte contre la fraude. C'est face aux difficultés rencontrées par les victimes de fraude pour bénéficier de leur droit à remboursement que l'OSMP a décidé d'intervenir.

Dans un premier temps, l'OSMP invite les prestataires de services de paiement recevant des contestations d'opérations de paiement à mettre en œuvre les investigations dès la réception de la contestation et dans un délai de trente jours maximum. Ils doivent en outre informer leurs clients quant à une éventuelle reprise des fonds remboursés lorsque les circonstances la rendent possible. Cette reprise doit avoir lieu dans les trente jours du remboursement initial.

[21] La recommandation de l'OSMP est reproduite au sein de l'annexe n°11.

L'OSMP prévoit également qu'en cas de refus de remboursement, les prestataires de services de paiement expliquent leur décision à l'aide du motif de refus ainsi que des éléments justifiant ce refus. L'OSMP rejoint ici la recommandation de l'ACPR : les réponses doivent être motivées et adaptées à chaque cas. Il était en effet nécessaire de le rappeler aux professionnels puisqu'on l'a vu, ces derniers se contentent souvent de réponses types mal argumentées pour refuser un remboursement.

L'OSMP se concentre ensuite sur la question de l'authentification forte. Les banques et établissements de paiement ont pris l'habitude de refuser le remboursement d'opérations non autorisées lorsque celles-ci ont fait l'objet d'une authentification forte. Or, les techniques employées par les escrocs conduisent le payeur à valider des opérations frauduleuses par le biais de l'authentification forte. Dès lors, refuser systématiquement le remboursement en cas d'authentification forte est injuste envers les victimes qui se voient supprimer leur droit au remboursement des opérations non autorisées. L'OSMP est donc intervenu afin d'éviter les abus de refus d'indemnisation de la part des prestataires de services de paiement.

D'abord, l'Observatoire rappelle qu'une opération non autorisée validée sans authentification forte est remboursée sans délai, et ce même en cas de négligence grave du payeur. Seule une fraude de sa part pourrait en effet faire obstacle au remboursement. Dans le même registre, l'OSMP prévoit que doit être remboursée sans délai toute opération contestée et réalisée au moyen d'une solution mobile pour laquelle l'enregistrement de l'instrument de paiement a été réalisé sans authentification forte.

A l'inverse, lorsque l'opération contestée a fait l'objet d'une authentification forte, l'OSMP demande au prestataire de services de paiement de procéder dans le délai d'un jour ouvré à une première analyse afin de déterminer si l'opération a été ou non autorisée par le payeur. L'Observatoire indique quels sont les paramètres à prendre en compte, à savoir :

- Les paramètres techniques associées à l'opération, permettant d'évaluer si l'utilisateur est ou non à l'origine de l'opération ;
- Les modalités de l'authentification forte mise en œuvre, permettant de s'assurer du rôle effectif de l'utilisateur dans la validation de l'opération ;
- Les éléments de contexte dont le prestataire de services de paiement dispose.

La recommandation donne ensuite les consignes à adopter une fois cette analyse terminée. Si l'opération n'a pas été autorisée ou qu'un doute subsiste quant au consentement donné, le prestataire procède sans délai au remboursement. En cas de soupçon de fraude de la part de l'utilisateur, le

prestataire communique ses raisons à la Banque de France et est en droit de ne pas le rembourser. Et si l'opération est considérée comme autorisée, que l'utilisateur a fait preuve de négligence grave ou qu'il n'a pas satisfait intentionnellement à ses obligations, le prestataire peut également refuser le remboursement.

L'OSMP établit également des bonnes pratiques que les utilisateurs doivent respecter afin de conserver la sécurité de leurs moyens de paiement. Ainsi, le fait que ces pratiques aient ou non été respectées constitue un indice permettant aux prestataires de services de paiement de déterminer s'il y a eu une négligence grave ou pas de la part de leur client.

Est en outre rappelé qu'un dépôt de plainte préalable à l'instruction d'une réclamation n'est pas requis par la loi et qu'il ne peut donc pas être exigé de l'utilisateur.

Puis, l'Observatoire édicte des recommandations visant à prévenir la fraude. D'abord, il est demandé aux prestataires de services de paiement d'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.

Il leur est aussi demandé d'indiquer si un contrôle de concordance entre l'IBAN et le nom du bénéficiaire va avoir lieu ou non. Certains fraudeurs sont en effet capable de substituer leur IBAN à celui d'un bénéficiaire de l'utilisateur, tout en gardant le nom d'origine de ce bénéficiaire. Une telle indication de la part des prestataires de services de paiement permettrait alors aux utilisateurs d'être plus méfiants en cas de transfert d'argent et les inciterait à vérifier par eux-mêmes que l'IBAN enregistré est bien le bon.

Les professionnels doivent en outre explicitement informer leurs clients quant à la nature de l'opération au moment de la valider à l'aide de l'authentification forte. Souvent, les victimes de fraude pensent s'authentifier afin de bloquer des transactions frauduleuses imaginaires quand en réalité elles transfèrent leurs fonds aux fraudeurs. Leur fournir une information claire sur l'opération en cours a donc pour objectif de réduire ce risque.

Pour terminer, l'Observatoire recommande aux prestataires de services de paiement de mettre à la disposition de leurs utilisateurs des mécanismes de blocage des instruments de paiement accessibles à tout moment et gratuits.

Les recherches effectuées n'ont pas permis de déterminer quelles sont les conséquences de l'irrespect de cette recommandation de l'Observatoire. Toutefois, l'ACPR et l'OSMP étant tous deux rattachés à la Banque de France, nous pouvons supposer que les sanctions se rejoignent.

Nous pouvons en outre noter que l'article L133-18 du code monétaire et financier prévoit des pénalités en cas de retard dans le remboursement des opérations non autorisées. Dans cette hypothèse, les sommes dues produisent intérêt au taux légal dont la majoration augmente avec les jours de retard. Ainsi par exemple, au-delà de trente jours de retard, les sommes dues produisent intérêt au taux légal majoré de quinze points.

Enfin, relever un manquement à une recommandation au cours d'un procès renforce la défense du consommateur et démontre bien la mauvaise foi dont fait preuve la banque qui n'a que faire de ce que lui demande son autorité de tutelle.

Chapitre 2 : Les recours mis à la disposition d'une victime de fraude et la tendance jurisprudentielle à cet égard

Si les recommandations de l'ACPR et de l'OSMP visent à améliorer les réponses des prestataires de services de paiement aux réclamations de leurs clients, ces derniers ne sont jamais à l'abri de se voir refuser une demande de remboursement. Dès lors, d'autres recours s'offrent à eux.

En premier lieu, un consommateur mécontent du traitement de sa réclamation peut se tourner vers un médiateur bancaire, ce qui est d'ailleurs obligatoire en cas de fraude inférieure à 5 000 euros. Mais un tel recours peut s'avérer décevant, notamment du fait que les médiateurs se rangent souvent du côté des banques et refusent donc le remboursement des opérations non autorisées.

Dans ce cas, la victime peut décider de saisir le tribunal et de laisser les juges décider de l'issue du litige. La loi étant en faveur du consommateur et les juges appliquant la loi, les chances d'obtenir gain de cause pour les victimes sont réelles. Ce sont en effet sur les prestataires de services de paiement que repose la charge de la preuve et celle-ci peut s'avérer dure à rapporter. De plus, si une victime peut s'avérer fautive, c'est également une possibilité pour les banques et les juges statuent en fonction des éléments de contexte à leur disposition.

Après avoir étudié les saisines du médiateur et du tribunal, il conviendra de s'intéresser aux tendances jurisprudentielles en matière de fraude à la carte bancaire.

I. La saisine du médiateur ou du juge judiciaire en cas de réponse non satisfaisante du prestataire de services de paiement à une réclamation

La médiation est un recours amiable s'offrant à la victime de fraude dont le remboursement des opérations non autorisées a été refusé par sa banque. En cas d'échec de la médiation ou lorsqu'elle n'est pas obligatoire, le consommateur peut également décider de saisir le juge.

A. La médiation

La médiation bancaire est un dispositif légal gratuit prévu par les articles L611 et suivants et R612 et suivants du code la consommation. Son objectif est de permettre la résolution amiable du litige existant entre le professionnel et son client. Il s'agit d'une procédure reposant sur une démarche volontaire du consommateur et qui est arrêtable à tout moment. Elle est toutefois obligatoire lorsque les sommes en jeu sont inférieures à 5 000 euros.

Ainsi, lorsqu'une victime de fraude transmet une réclamation à son prestataire de services de paiement en vue d'obtenir le remboursement des opérations non autorisées mais que celui-ci lui est refusé, elle peut se tourner vers un médiateur bancaire. Une telle possibilité est d'ailleurs souvent rappelée par les professionnels en fin de réponse à une réclamation. Le médiateur bancaire doit être saisi par écrit dans l'année suivant la réclamation. Aucun recours judiciaire ne doit être en cours concernant le litige.

Une fois que le médiateur notifie la recevabilité de sa saisine, il dispose d'un délai de 90 jours pour proposer une solution au problème rencontré. Pour ce faire, il analyse le dossier et l'instruit par écrit. Il peut également décider d'entendre les parties. Le consommateur a la possibilité de se faire assister par un avocat ou par le tiers de son choix.

La proposition de solution apportée par le médiateur prend la forme d'un avis motivé en droit et/ou en équité. Elle peut donc être différente de celle qui serait rendue par un juge. Le rapport de médiation est envoyé par courrier aux parties. L'avis rendu n'est pas contraignant et le consommateur est libre

ou non de l'accepter. En cas d'acceptation, le médiateur veille alors à l'exécution de l'accord. En cas de refus à l'inverse, le consommateur a la possibilité d'agir en justice.

C'est l'article L613-1 du code de la consommation[22] qui pose les principes de la médiation. Ainsi, le médiateur doit accomplir sa mission « avec diligence et compétence, en toute indépendance et impartialité, dans le cadre d'une procédure transparente, efficace et équitable ». Toutefois, l'étude des avis de médiation rendus dans la pratique fait parfois s'interroger sur la réalité de l'indépendance et de l'impartialité des médiateurs.

Il arrive que les victimes de fraude bancaire faisant appel à l'ADC ait eu au préalable recours à un médiateur. Force est de constater que dans bien des cas, le médiateur se range du côté du prestataire de services de paiement et refuse lui aussi le remboursement des opérations frauduleuses. Souvent d'ailleurs, un rapport de médiation est similaire en de nombreux points aux réponses apportées par les banques aux réclamations. Ce qui l'en différencie légèrement est que le médiateur est dans l'obligation d'apporter une analyse un minimum poussée de la situation. Ainsi, il va par exemple détailler en quoi l'utilisateur a fait preuve de négligence grave ou pourquoi l'on peut dire que l'opération a fait l'objet d'une authentification forte. Mais l'issue reste la même puisqu'est refusé le remboursement pour les mêmes motifs peu convaincants que ceux avancés par le prestataire de services de paiement.

A ce constat s'ajoute le fait que les médiateurs sont sélectionnés, rémunérés et reconduits par les banques et établissements de paiement. Il faut simplement qu'ils soient choisis parmi les médiateurs référencés par la Commission d'évaluation et de contrôle de la médiation de la consommation.

L'article L613-2 du code de la consommation veille à l'indépendance et à l'impartialité du médiateur en prévoyant qu'« aucun lien hiérarchique ou fonctionnel entre le professionnel et le médiateur ne peut exister pendant l'exercice de sa mission de médiation ». Il poursuit en précisant que « le médiateur est clairement séparé des organes opérationnels du professionnel et dispose d'un budget distinct et suffisant pour l'exécution de ses missions ».

Mais c'est à se demander si ces dispositions suffisent à assurer des médiateurs totalement objectifs dans leurs analyses. Pourtant, c'est le fait de savoir que la proposition apportée a été élaborée en toute

[22] Les articles du code de la consommation cités sont reproduits au sein de l'annexe n°12.

indépendance et impartialité qui pousse le consommateur à se ranger du côté de l'avis du médiateur, qu'il lui soit favorable ou non.

B. Le recours judiciaire

En cas de refus du remboursement des opérations non autorisées suite à une réclamation ou à une tentative de médiation, la victime de fraude peut décider de se tourner vers la justice afin de faire valoir ses droits. Dans cette hypothèse, elle assigne son prestataire de services de paiement devant une juridiction afin de le faire condamner à lui verser les sommes prélevées frauduleusement.

Si la fraude porte sur un montant inférieur à 10 000 euros, le tribunal de proximité et le tribunal judiciaire sont compétents et l'avocat est facultatif, la procédure étant orale. A l'inverse, si la fraude porte sur un montant supérieur à 10 000, seul le tribunal judiciaire est compétent et l'avocat est obligatoire, la procédure étant cette fois écrite.

La durée d'une procédure est en moyenne de 15 mois. Une tentative de conciliation est toujours envisageable en cours de procès mais la pratique veut qu'elle n'est quasiment jamais mise en œuvre ; les banques ne prenant pas d'autres risques que celui d'être condamnées par le tribunal à rembourser leurs clients.

Un entretien avec Maître DELOMEL, avocat au barreau de Rennes, nous permet de recueillir son point de vue sur le sujet. Il traite en effet de nombreux dossiers de fraude à la carte bancaire. Cela ne le surprend pas : les techniques pratiquées par les escrocs tel que le spoofing et le phishing ne leur demandent pas beaucoup de matériel ni de compétences, ce qui rend les fraudes relativement simples à réaliser et donc fréquentes.

Toutefois, Maître DELOMEL estime que neuf personnes sur dix n'agissent pas, que ce soit par peur, manque de moyens ou découragement face à la longueur des procédures. En outre, il n'y a pas nécessairement de montant en dessous duquel les victimes se refusent à poursuivre leur banque : certaines vont vouloir agir pour récupérer 3 000 euros lorsque d'autres vont hésiter pour 8 000 euros.

Quant aux dossiers, Maître DELOMEL ne les trouve pas particulièrement durs à plaider. Si la victime n'a pas commis de fraude ni de négligence grave, le prestataire de services de paiement a une

obligation légale de remboursement. Dans le cas inverse, c'est à la banque ou à l'établissement de paiement de rapporter la preuve d'une fraude ou d'une négligence grave de son client. Ainsi, si Maître DELOMEL estime qu'au vu des éléments de l'affaire, une telle preuve est facilement rapportable, il ne va pas accepter le dossier car l'issue serait nécessairement défavorable au demandeur, ici le consommateur. Toutefois, si ce dernier a fauté mais qu'il y a de grandes chances pour que le professionnel ne soit pas capable d'en apporter la preuve, le défendre redevient tout à fait envisageable.

Maître DELOMEL observe que les décisions rendues sont en général profitables aux victimes. Mais cela ne l'étonne pas car la loi cherche à protéger les consommateurs et les juges appliquent la loi. Dès lors, il est logique que la majorité des jugements aillent dans un sens favorable aux victimes. Cependant, si Maître DELOMEL demande systématiquement des dommages et intérêts dans ses conclusions, ceux-ci ne sont que rarement accordés car les juges estiment que le remboursement du montant des opérations frauduleuses est suffisant pour réparer le préjudice subi.

Pour Maître DELOMEL, la DSP2 est efficace dans le sens où elle est bien appliquée par les banques. L'authentification forte ne présente que peu de faille et sécurise les transactions. Toutefois, il faut bien reconnaître qu'elle reste contournable par les escrocs et qu'elle ne permet donc pas d'abolir définitivement la fraude, ce qui rejoint nos observations jusqu'à présent.

Après avoir étudié les recours s'offrant à la victime en cas de fraude, il convient de s'intéresser à l'état de la jurisprudence en matière de fraude à la carte bancaire.

II. La tendance jurisprudentielle en matière de fraude à la carte bancaire

Lorsqu'une victime de fraude assigne sa banque devant le tribunal judiciaire, les juges vont pouvoir rechercher des fautes aussi bien de la part de l'utilisateur que de son prestataire. Tout dépendra des circonstances, étant précisé que la charge de la preuve repose souvent sur la banque.

S'il est possible de reprocher à la victime sa négligence grave qui s'appréciera au cas par cas, il faut aussi s'interroger sur la part de responsabilité qu'a eu le prestataire de services de paiement dans la survenance de la fraude.

A. Une appréciation de la négligence grave au cas par cas

Si l'argument régulièrement invoqué par les prestataires de services de paiement pour ne pas rembourser le montant des opérations non autorisées est la négligence grave de leurs clients, encore faut-il la prouver. La jurisprudence en la matière est en en effet constante : il incombe à la banque de prouver que l'utilisateur du service a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations[23].

La charge de la preuve repose donc sur le prestataire de services de paiement. Si une telle preuve peut s'avérer compliquée à rapporter, les juges refusent toute hypothèse de dérogation. Un arrêt de la Cour de cassation du 29 mai 2019[24] valide ainsi le raisonnement d'une cour d'appel qui excluait de mettre à la charge de l'utilisateur la preuve d'absence de négligence grave de sa part. Les juges du fond estiment en effet que cette règle ne place pas la banque dans une situation de net désavantage dans la présentation de sa cause et ne méconnaît pas le principe de l'égalité des armes.

En outre, la jurisprudence est unanime sur le fait que la négligence grave ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été utilisées[25].

En termes d'appréciation de la négligence grave, le constat est que les juges sont plus sévères avec une victime de phishing qu'avec une victime de spoofing, ces techniques de fraude étant les plus répandues.

En cas de phishing, il convient de se demander si la victime pouvait, au vu d'indices, se douter qu'il s'agissait d'une arnaque. Pour cela, les juges prévoient qu'il faut se mettre à la place d'un utilisateur normalement attentif, peu important qu'il soit ou non avisé des risques d'hameçonnage[26]. Ainsi, commet une négligence grave la personne qui répond à un courriel présentant de sérieuses anomalies tenant tant à la forme qu'au contenu du message qu'il comportait[27]. C'est donc au tribunal de rechercher, au regard des circonstances de l'espèce, si la victime avait pu ou non avoir conscience de la fraude[28].

[23] Voir par exemple Cass. com., 21 novembre 2018, n°17-18.888 et Cass. com., 26 juin 2019, n°18-12.581.
[24] Cass. com., 29 mai 2019, n°18-10.147.
[25] Voir par exemple Cass. com., 29 mai 2019, n°18-10.147 et Cass. com., 18 janvier 2017, n°15-18.102.
[26] Cass. com., 28 mars 2018, n°16-20.018.
[27] Cass. com., 1er juillet 2020, n°18-21.487.
[28] Cass. com., 24 novembre 2021, n°20-13.767.

En cas de spoofing, la négligence grave est plus difficile à caractériser. C'est en effet ce que prévoit un arrêt récent de la Cour d'appel de Versailles[29], qui explique que « face à un appel téléphonique évoquant de surcroît un piratage, la vigilance de la personne qui reçoit cet appel est moindre que celle d'une personne qui réceptionne un mail, laquelle dispose de davantage de temps pour en prendre connaissance et s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse ».

Et les juges ne s'arrêtent pas là puisqu'en plus de condamner la banque à rembourser la totalité des opérations non autorisées, ils estiment que la victime faussement accusée de négligence grave a subi un préjudice moral devant être réparé avec des dommages et intérêts à la charge de la banque. Cette décision est donc très favorable au consommateur et a de quoi gêner les prestataires de services de paiement, qui, en plus de devoir rembourser leurs clients, peuvent se voir contraints de les indemniser au titre d'une accusation de négligence grave que les juges ne considèrent pas caractérisée.

B. La possibilité de rechercher une faute du prestataire de services de paiement

Si la banque ou l'établissement de paiement doit démontrer une faute de l'utilisateur pour éviter de le rembourser, il n'est pas exclu que le prestataire ait lui aussi sa part de responsabilité dans la survenance de la fraude.

D'abord, les juges veillent à la bonne application de l'article L133-23 du code monétaire et financier en prévoyant que le prestataire de services de paiement doit prouver que l'opération en cause a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre[30]. Ainsi, apporter la preuve d'une faute de la part de l'utilisateur ne suffit pas, encore faut-il que la banque prouve qu'aucune défaillance n'a pu intervenir lors de la transaction. Cette obligation complique la défense des prestataires de services de paiement car une telle preuve peut être compliquée à rapporter et nécessiter des diagnostics assez poussés.

En outre, l'article L561-6 du code monétaire et financier prévoit que les professionnels du secteur bancaire « exercent, dans la limite de leurs droits et obligations, une vigilance constante et pratiquent un examen attentif des opérations effectuées en veillant à ce qu'elles soient cohérentes avec la

[29] CA de Versailles, 28 mars 2023, n°21/07299.
[30] Voir par exemple Cass. com., 12 novembre 2020, n°19-12.112.

connaissance actualisée qu'elles ont de leur relation d'affaires ». Les banquiers sont donc soumis à un devoir de vigilance qui les oblige à surveiller les transactions et à suspendre les opérations suspectes. Or, nous constatons en pratique que les cas dans lesquels des opérations totalement inhabituelles ont été autorisées par les banques sont loin d'être rares. En effet, bon nombre de transactions frauduleuses auraient dû alerter les professionnels, que ce soit par leur montant, leur fréquence ou leur destination. Dans ces hypothèses, le simple fait d'informer le payeur de l'opération en cours et de le questionner aurait souvent permis d'éviter l'aboutissement de la fraude.

Dès lors, il est cohérent que le banquier qui manque à son obligation de vigilance ait une part de responsabilité dans la survenance de la fraude et soit condamné. C'est en effet le raisonnement des juges du fond dans un arrêt du 17 mai 2017[31] qui prévoit que la négligence grave retenue contre la victime ne privait pas cette dernière d'invoquer le manquement du banquier à ses propres obligations. Ainsi, si le professionnel a laissé passer des débits inhabituels qui auraient dû l'alerter, il commet une faute et voit sa responsabilité engagée.

Pour finir, le prestataire de services de paiement peut commettre une faute en ne respectant pas les règles d'authentification forte. Un arrêt de la cour d'appel de Paris du 23 mars 2023[32] souligne par exemple la faute de la banque qui a laissé mettre en place un « Sécuripass » à partir d'un téléphone qui n'était pas le téléphone répertorié, ce qui ne répond pas à l'exigence d'authentification forte. Les juges font également remarquer que le signalement de cette activation a été envoyé au moyen d'un simple message sur la messagerie interne à la banque, dont l'existence a certes été signalée à l'utilisatrice par SMS mais sans qu'aucun caractère d'urgence n'apparaisse. Dans ces circonstances, la banque avait bien commis une faute et un partage de responsabilité entre elle et la victime négligente avait été décidé.

[31] Cass. com., 17 mai 2017, n°15.28.209.
[32] CA de Paris, 23 mars 2023, n°21/11361.

CONCLUSION

Bien que le taux de fraude ait diminué ces dernières années, les textes actuellement en vigueur ne sont pas parvenus à éradiquer ce risque qui continue de peser sur les consommateurs. Si la première directive sur les services de paiement a permis d'apporter à l'utilisateurs de services de paiement plus de sécurité, elle s'est vite montrée inadaptée aux techniques des fraudeurs qui se sont développées avec le progrès technologique et les nouvelles habitudes de consommation des individus.

C'est suite à ce constat que la seconde directive sur les moyens de paiement a vu le jour et a notamment apporté des règles d'authentification forte permettant de renforcer la sécurité des transactions en ligne grâce à une double authentification. Les prestataires de services de paiement se sont adaptés aux nouvelles exigences et la fraude a ainsi réduit. Toutefois, les escrocs, capables de récolter des informations confidentielles sur leurs victimes afin de leur faire valider par elles-mêmes des transactions frauduleuses, parviennent à contourner l'obstacle de l'authentification forte.

A cela s'ajoute la difficulté d'obtenir le remboursement du montant des opérations non autorisées, pourtant prévu par les textes. Les prestataires de services de paiement ont en effet tendance à accuser leurs clients de négligence grave pour les amener à penser qu'ils sont fautifs et qu'une indemnisation est donc impossible.

Face aux abus des banques et des établissements de paiement, l'Autorité de contrôle prudentiel et de résolution et l'Observatoire de la sécurité des moyens de paiement sont donc intervenus au travers de recommandations visant à améliorer le traitement des réclamations et l'application du droit au remboursement par les professionnels du secteur bancaire.

De plus, les victimes qui n'obtiennent pas satisfaction peuvent saisir le médiateur bancaire ou bien le tribunal afin de faire valoir leurs droits. Si la médiation s'avère souvent décevante, il est possible d'obtenir gain de cause devant un tribunal. En effet, la charge de la preuve repose sur la banque qui doit prouver la faute de l'utilisateur ainsi que son absence de responsabilité dans la survenance de la fraude. La négligence grave est appréciée au cas par cas et peut être difficile à caractériser, notamment lorsque la personne a été victime de spoofing où l'arnaque est plus compliquée à détecter.

Mais la règlementation en vigueur est insuffisante pour assurer une sécurité effective des utilisateurs de services de paiement. Les fraudeurs et les banques exploitent ses failles à l'insu des consommateurs, l'un pour prendre leur argent, l'autre pour ne pas les rembourser. De plus, l'authentification forte censée protéger les consommateurs a l'effet inverse lorsque les banques se retranchent derrière le respect de sa mise en place pour refuser d'indemniser les victimes.

En outre, la loi peut sembler injuste puisqu'elle oblige les prestataires de services de paiement sans évoquer les fraudeurs. Ainsi, les banques sont tenues de rembourser des sommes parfois très importantes alors qu'elles ne sont pas à l'origine de la fraude. A l'inverse, les escrocs qui ne sont en général pas identifiés gardent l'argent volé et ne paient pas pour leurs actes. Mais ces propos sont à nuancer, car il semble cohérent qu'une banque qui faillit à son devoir de vigilance soit condamnée puisque davantage d'attention de sa part aurait permis d'éviter la fraude.

Comme les textes ne parviennent pas à supprimer le risque de fraude, il faudrait dans un premier temps augmenter les campagnes de prévention afin de sensibiliser les utilisateurs de services de paiement aux techniques utilisées par les fraudeurs. Un consommateur averti serait en effet plus méfiant et le travail des fraudeurs deviendrait beaucoup plus compliqué. De plus, il semble nécessaire d'insister sur le rôle que peuvent jouer les banques dans la survenance de la fraude et durcir les sanctions lorsqu'elles ne détectent pas les opérations inhabituelles et donc frauduleuses. Pour terminer, l'idéal resterait de trouver des moyens permettant de parvenir à remonter jusqu'aux fraudeurs qui restent les principaux responsables. S'il est une bonne chose que les victimes soient rapidement indemnisées par les banques, ces dernières pourraient ensuite se retourner vers les escrocs afin d'obtenir le remboursement des sommes versées en indemnisation de la fraude.

BIBLIOGRAPHIE

Yves Picod, Nathalie Picod, Eric Chevrier. *Code de la consommation 2023*. Dalloz, 2022.

Jérôme Lasserre Capdeville, Michel Storck, Eric Chevrier, Pascal Pisoni. *Code monétaire et financier 2023*. Dalloz, 2023.

Journal officiel de l'Union européenne du 5 décembre 2007. *Directive 2007/64/CE du parlement européen et du conseil du 13 novembre 2007*. Obtenue sur le site https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32007L0064#d1e3293-1-1

Journal officiel de l'Union européenne du 23 décembre 2015. *Directive (UE) 2015/2366 du parlement européen et du conseil du 25 novembre 2015*. Obtenue sur le site https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32015L2366#d1e1158-35-1

OSMP. *Chiffres-clés de l'Observatoire au 1er semestre 2022*. 27 mars 2023. Obtenus sur le site https://www.banque-france.fr/donnees-clefs-sur-la-fraude-au-1er-semestre-2022

ACPR. *Recommandation 2022-R-01 du 9 mai 2022 sur le traitement des réclamations*. 17 mai 2022. Obtenue sur le site https://acpr.banque-france.fr/contenu-de-tableau/recommandation-2022-r-01-du-9-mai-2022-sur-le-traitement-des-reclamations

OSMP. *Recommandations de l'Observatoire : modalités de remboursement des opérations de paiement frauduleuses*. 16 mai 2023. Obtenues sur le site https://acpr.banque-france.fr/contenu-de-tableau/recommandation-2022-r-01-du-9-mai-2022-sur-le-traitement-des-reclamations

SITOGRAPHIE

Larcheron. *Larcheron Law*. 20 mars 2021. Opération de paiement non autorisée : la négligence grave du client ne dispense pas la banque de ses propres obligations. https://larcheron.law/operation-de-paiement-non-autorisee-la-negligence-grave-du-client-ne-dispense-pas-la-banque-de-ses-propres-obligations/

Certeurope. Comment évolue la sécurité de vos transactions ? https://www.certeurope.fr/blog/de-la-dsp-1-a-la-dsp2-comment-evolue-la-securite-de-vos-transactions/

iBanFirst. Que signifient DSP1 et DSP2 et pourquoi sont-ils importants ? https://blog.ibanfirst.com/fr/que-signifient-dsp1-et-dsp2-et-pourquoi-sont-ils-importants

La finance pour tous. 14 décembre 2021. Deuxième directive européenne sur les services de paiement – DSP2. https://www.lafinancepourtous.com/decryptages/finance-perso/banque-et-credit/directives-europeennes-sur-les-services-de-paiement/deuxieme-directive-europeenne-sur-les-services-de-paiement-dsp2/#:~:text=Transposition%20de%20la%20directive%20sur,depuis%20le%2013%20janvier%202018

Mooncard. 5 avril 2021. La DSP2 : objectifs et état des lieux. https://blog.mooncard.co/dsp2-objectifs-etat-des-lieux

La finance pour tous. 28 février 2020. Directive européenne sur les services de paiement – DSP1. https://www.lafinancepourtous.com/decryptages/finance-perso/banque-et-credit/directives-europeennes-sur-les-services-de-paiement/la-directive-europeenne-sur-les-services-de-paiement/

Certeurope. La directive européenne DSP2 et authentification forte : que prévoit la directive européenne ? https://www.certeurope.fr/blog/dsp2-et-authentification-forte-que-prevoit-la-directive-europeenne/

Meilleurtaux Banques. 10 novembre 2022. Votre banque a-t-elle le droit de vous accuser de négligence pour éviter de vous rembourser en cas de fraude ? https://banque.meilleurtaux.com/frais-bancaires/actualites/2022-novembre/votre-banque-telle-droit-vous-accuser-negligence-eviter-vous-rembourser-cas-fraude.html

INC. 27 décembre 2019. Point sur la directive services de paiement (DSP2). https://www.inc-conso.fr/content/point-sur-la-directive-services-de-paiement-dsp2

Boris Cassel. *Le Parisien*. 8 décembre 2016. Fraude à la carte bancaire : le casse du siècle ! https://www.leparisien.fr/economie/fraude-a-la-carte-bancaire-le-casse-du-siecle-08-12-2016-6427959.php

DGCCRF. 8 août 2022. La fraude aux paiements en ligne. https://www.economie.gouv.fr/dgccrf/la-fraude-aux-paiements-en-ligne

INC. 4 mai 2019. La carte bancaire. https://www.inc-conso.fr/content/banque/la-carte-bancaire

Sénat. Directive services de paiement dans le marché intérieur. https://www.senat.fr/dossier-legislatif/pjl17-292.html

Alexandre Loukil. *Capital*. 17 mai 2023. Carte bancaire : 5 conseils pour minimiser le risque de fraude. https://www.capital.fr/votre-argent/carte-bancaire-cb-5-conseils-pour-minimiser-le-risque-de-fraude-1468811#:~:text=Gare%20au%20

Microsoft. Types de fraude par carte de crédit. https://dynamics.microsoft.com/fr-fr/ai/fraud-protection/credit-card-fraud/

Stéphanie Alexandre. *Le Figaro*. 3 août 2017. Gare au skimming, une technique de fraude à la carte bancaire. https://leparticulier.lefigaro.fr/jcms/p1_1695730/gare-au-skimming-une-technique-de-fraude-a-la-carte-bancaire

Jechange. 24 mai 2023. Fraude, piratage, arnaque à la carte bancaire : déclaration, remboursement et prévention. https://www.jechange.fr/banques/carte-bancaire/fraude

La finance pour tous. 14 décembre 2021. Paiement par carte bancaire sur internet : 3D Secure et authentification forte. https://www.lafinancepourtous.com/pratique/banque/moyens-de-paiement/la-carte-bancaire/payer-par-carte-bancaire-sur-internet-3d-secure-authentification-forte/

E-Commerce Nation. 15 septembre 2022. Qu'est-ce que la 3D Secure ? Comment cela fonctionne ? https://www.ecommerce-nation.fr/quest-ce-que-la-3d-secure-et-comment-est-ce-que-ca-marche/

Orange Bank. 5 janvier 2023. Les types de fraudes bancaires en France en 2022. https://www.orangebank.fr/blog/les-types-de-fraudes-bancaires-en-France-en-2022/

Jocelyn Ziegler. *Village de la justice*. 18 juillet 2022. https://www.village-justice.com/articles/spoofing-nouvelle-escroquerie-bancaire,43219.html#:~:text=Le%20spoofing%20en%20anglais%20signifie,laquelle%20le%20client%20a%20confiance

Les clés de la banque. 8 mars 2021. Le phishing : comment le reconnaître et l'éviter ? https://www.lesclesdelabanque.com/particulier/le-phishing-comment-le-reconnaitre-et-leviter/

Service public. Médiateur bancaire : comment y recourir ? https://www.service-public.fr/particuliers/vosdroits/F20523

Trustpair. 17 février 2023. Les tendances de la fraude dans le secteur du e-commerce. https://trustpair.fr/blog/fraude-e-commerce/

ANNEXES

Annexe 1 : Articles de la DSP1

Annexe 2 : Articles de la DSP2

Annexe 3 : Considérant 95 de la DSP2

Annexe 4 : Considérant 6 et articles du règlement délégué (UE) 2018/389

Annexe 5 : Articles du code monétaire et financier

Annexe 6 : Projet de loi ratifiant l'ordonnance du 9 août 2017 de la Commission des finances du Sénat

Annexe 7 : Examen de l'amendement CF7 par la Commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale sur le projet de loi ratifiant l'ordonnance du 9 août 2017

Annexe 8 : Exemples de réponses des banques à des réclamations

Annexe 9 : Exemples de lettres envoyées par l'ADC France à l'intention des banques

Annexe 10 : Recommandation 2022-R-01 du 9 mai 2022 de l'ACPR

Annexe 11 : Extraits de la recommandation du 16 mai 2023 de l'OSMP

Annexe 12 : Articles du code de la consommation

Annexe 1 : Articles de la DSP1

Article 54

Consentement et retrait du consentement

1. Les États membres veillent à ce qu'une opération de paiement ne soit réputée autorisée que si le payeur a donné son consentement à l'exécution de l'opération de paiement. Une opération de paiement peut être autorisée par le payeur avant ou, si le payeur et son prestataire de services de paiement en ont convenu ainsi, après son exécution.

2. Le consentement à l'exécution d'une opération de paiement ou d'une série d'opérations de paiement est donné sous la forme convenue entre le payeur et son prestataire de services de paiement.

En l'absence d'un tel consentement, l'opération de paiement est réputée non autorisée.

3. Le consentement peut être retiré par le payeur à tout moment, mais pas après le moment d'irrévocabilité prévue à l'article 66. Le consentement à l'exécution d'une série d'opérations de paiement peut aussi être retiré avec pour effet que toute opération de paiement postérieure doit être réputée non autorisée.

4. La procédure pour donner le consentement fait l'objet d'un accord entre le payeur et le prestataire de services de paiement.

Article 55

Limitation de l'utilisation des instruments de paiement

1. Lorsqu'un instrument de paiement spécifique est utilisé aux fins de donner le consentement, le payeur et son prestataire de services de paiement peuvent convenir de limites de dépenses pour les opérations de paiement exécutées au travers dudit instrument de paiement.

2. Si le contrat-cadre le prévoit, le prestataire de services de paiement peut se réserver le droit de bloquer l'instrument de paiement, pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument de paiement, à la présomption d'une utilisation non autorisée ou frauduleuse de l'instrument de paiement ou, s'il s'agit d'un instrument de paiement doté d'une ligne de crédit, au risque sensiblement accru que le payeur soit dans l'incapacité de s'acquitter de son obligation de paiement.

3. Dans ces cas, le prestataire de services de paiement informe le payeur, de la manière convenue, du blocage de l'instrument de paiement et des raisons de ce blocage, si possible avant que l'instrument de paiement ne soit bloqué et au plus tard immédiatement après, à moins que le fait de donner cette information ne soit pas acceptable pour des raisons de sécurité objectivement motivées ou soit interdite en vertu d'une autre législation communautaire ou nationale pertinente.

4. Le prestataire de services de paiement débloque l'instrument de paiement ou remplace celui-ci par un nouvel instrument de paiement dès lors que les raisons justifiant le blocage n'existent plus.

Article 56

Obligations de l'utilisateur de services de paiement liées aux instruments de paiement

1. L'utilisateur de services de paiement habilité à utiliser un instrument de paiement a les obligations suivantes :

a) il utilise l'instrument de paiement conformément aux conditions régissant la délivrance et l'utilisation de cet instrument de paiement ; et

b) lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement, il en informe sans tarder son prestataire de services de paiement ou l'entité désignée par celui-ci.

2. Aux fins du paragraphe 1, point a), dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend notamment toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés.

Article 57

Obligations du prestataire de services de paiement liées aux instruments de paiement

1. Le prestataire de services de paiement délivrant un instrument de paiement a les obligations suivantes :

a) il s'assure que les dispositifs de sécurité personnalisés de tout instrument de paiement ne sont pas accessibles à d'autres parties que l'utilisateur de services de paiement autorisé à utiliser cet instrument, sans préjudice des obligations de l'utilisateur des services de paiement énoncées à l'article 56 ;

b) il s'abstient d'envoyer tout instrument de paiement non sollicité, sauf dans le cas où un instrument de paiement déjà donné à l'utilisateur de services de paiement doit être remplacé ;

c) il veille à la disponibilité, à tout moment, de moyens appropriés permettant à l'utilisateur de services de paiement de procéder à la notification prévue à l'article 56, paragraphe 1, point b), ou de demander le déblocage conformément à l'article 55, paragraphe 4; le prestataire de services de paiement fournit sur demande à l'utilisateur de services de paiement, pendant dix-huit mois à compter de la notification, les moyens de prouver qu'il a bien procédé à cette notification ; et

d) il empêche toute utilisation de l'instrument de paiement après une notification effectuée en application de l'article 56, paragraphe 1, point b).

2. Le prestataire de services de paiement supporte le risque lié à l'envoi au payeur d'un instrument de paiement ou de tout dispositif de sécurité personnalisé de celui-ci.

Article 58

Notification des opérations de paiement non autorisées ou mal exécutées

L'utilisateur de services de paiement n'obtient du prestataire de services de paiement la correction d'une opération que s'il signale sans tarder à son prestataire de services de paiement qu'il a constaté une opération de paiement non autorisée ou mal exécutée donnant lieu à une revendication, y compris au titre de l'article 75, et au plus tard dans les treize mois suivant la date de débit, à moins que, le cas échéant, le prestataire de services de paiement n'ait pas fourni ou mis à disposition les informations relatives à cette opération de paiement conformément au titre III.

Article 59

Preuve d'authentification et d'exécution des opérations de paiement

1. Les États membres exigent que, lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

2. Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a

agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 56.

Article 60

Responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées

1. Les États membres veillent, sans préjudice de l'article 58, à ce que, en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de cette opération de paiement non autorisée et, le cas échéant, rétablisse le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.

2. Une indemnisation financière complémentaire peut être déterminée conformément à la loi applicable au contrat conclu entre le payeur et son prestataire de services de paiement.

Article 61

Responsabilité du payeur en cas d'opérations de paiement non autorisées

1. Par dérogation à l'article 60, le payeur supporte, jusqu'à concurrence de 150 EUR, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou, si le payeur n'est pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, au détournement d'un instrument de paiement.

2. Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou du fait que le payeur n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 56. Dans ce cas, le montant maximal visé au paragraphe 1 du présent article ne s'applique pas.

3. Lorsque le payeur n'a pas agi de manière frauduleuse ni n'a manqué intentionnellement aux obligations qui lui incombent en vertu de l'article 56, les États membres peuvent limiter la responsabilité visée aux paragraphes 1 et 2 du présent article, en tenant compte notamment de la nature des dispositifs de sécurité personnalisés de l'instrument de paiement et des circonstances dans lesquelles celui-ci a été perdu, volé ou détourné.

4. Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière résultant de l'utilisation d'un instrument de paiement perdu, volé ou détourné, survenue après la notification prévue à l'article 56, paragraphe 1, point b).

5. Si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant, à tout moment, la notification de la perte, du vol ou du détournement d'un instrument de paiement, conformément à l'article 57, paragraphe 1, point c), le payeur n'est pas tenu, sauf agissement frauduleux de sa part, de supporter les conséquences financières résultant de l'utilisation de cet instrument de paiement.

Annexe 2 : Articles de la DSP2

Article 74

Responsabilité du payeur en cas d'opérations de paiement non autorisées

1. Par dérogation à l'article 73, le payeur peut être tenu de supporter, jusqu'à concurrence de 50 EUR, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou au détournement d'un instrument de paiement.

Le premier alinéa ne s'applique pas si :

a) la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur a agi frauduleusement ; ou

b) la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.

Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de la part du payeur ou du fait qu'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent en vertu de l'article 69. Dans ce cas, le montant maximal visé au premier alinéa ne s'applique pas.

Lorsque le payeur n'a pas agi de manière frauduleuse ni n'a manqué intentionnellement aux obligations qui lui incombent en vertu de l'article 69, les États membres peuvent limiter la responsabilité visée au présent paragraphe en tenant compte, notamment, de la nature des données de sécurité personnalisées et des circonstances particulières dans lesquelles l'instrument de paiement a été perdu, volé ou détourné.

2. Lorsque le prestataire de services de paiement du payeur n'exige pas une authentification forte du client, le payeur ne supporte aucune perte financière éventuelle à moins qu'il ait agi frauduleusement. Lorsque le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte du client, il rembourse le préjudice financier causé au prestataire de services de paiement du payeur.

3. Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière résultant de l'utilisation d'un instrument de paiement perdu, volé ou détourné, survenue après la notification prévue à l'article 69, paragraphe 1, point b).

Si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant, à tout moment, la notification de la perte, du vol ou du détournement d'un instrument de paiement, conformément à l'article 70, paragraphe 1, point c), le payeur n'est pas tenu, sauf agissement frauduleux de sa part, de supporter les conséquences financières résultant de l'utilisation de cet instrument de paiement.

Article 97

Authentification

1. Les États membres veillent à ce qu'un prestataire de services de paiement applique l'authentification forte du client lorsque le payeur :

a) accède à son compte de paiement en ligne ;

b) initie une opération de paiement électronique ;

c) exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

2. En ce qui concerne l'initiation des opérations de paiement électronique visée au paragraphe 1, point b), les États membres veillent à ce que, pour les opérations de paiement électronique à distance, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés.

3. Eu égard au paragraphe 1, les États membres veillent à ce que les prestataires de services de paiement aient mis en place des mesures de sécurité adéquates afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement.

4. Les paragraphes 2 et 3 s'appliquent également lorsque les paiements sont initiés par l'intermédiaire d'un prestataire de services d'initiation de paiement. Les paragraphes 1 et 3 s'appliquent également lorsque l'information est demandée par l'intermédiaire d'un prestataire de services d'information sur les comptes.

5. Les États membres veillent à ce que le prestataire de services de paiement gestionnaire du compte autorise le prestataire de services d'initiation de paiement et le prestataire de services d'information sur les comptes à se fonder sur les procédures d'authentification prévues par le prestataire de services de paiement gestionnaire du compte à l'intention de l'utilisateur de services de paiement conformément aux paragraphes 1 et 3 et, lorsque le prestataire de services d'initiation de paiement intervient, conformément aux paragraphes 1, 2 et 3.

Article 98

Normes techniques de réglementation concernant l'authentification et la communication

1. L'ABE, en étroite coopération avec la BCE et après avoir consulté toutes les parties concernées, y compris sur le marché des services de paiement, représentant tous les intérêts en présence, élabore des projets de normes techniques de réglementation à l'intention des prestataires de services de paiement visés à l'article 1er, paragraphe 1, de la présente directive, conformément à l'article 10 du règlement (UE) no 1093/2010, précisant :

a) les exigences relatives à l'authentification forte du client visée à l'article 97, paragraphes 1 et 2 ;

b) les dérogations à l'application de l'article 97, paragraphes 1, 2 et 3, sur la base des critères établis au paragraphe 3 du présent article ;

c) les exigences auxquelles doivent satisfaire les mesures de sécurité, conformément à l'article 97, paragraphe 3, afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement ; et

d) les exigences applicables aux normes ouvertes communes et sécurisées de communication aux fins de l'identification, de l'authentification, de la notification et de l'information, ainsi que pour la mise en œuvre des mesures de sécurité, entre les prestataires de services de paiement gestionnaires du compte, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement.

2. Les projets de normes techniques de réglementation visés au paragraphe 1 sont élaborés par l'ABE en vue de :

a) garantir un niveau de sécurité approprié pour les utilisateurs de services de paiement et les prestataires de services de paiement par l'adoption d'exigences efficaces et fondées sur les risques ;

b) garantir la sécurité des fonds et des données à caractère personnel des utilisateurs de services de paiement ;

c) garantir et maintenir une concurrence équitable entre l'ensemble des prestataires de services de paiement ;

d) garantir la neutralité du modèle commercial et des technologies ;

e) permettre le développement de moyens de paiement innovants, accessibles et faciles à utiliser.

3. Les dérogations visées au paragraphe 1, point b), reposent sur les critères suivants :

a) le niveau de risque lié au service fourni ;

b) le montant, le caractère récurrent de l'opération ou les deux ;

c) le moyen utilisé pour exécuter l'opération.

4. L'ABE soumet les projets de normes techniques de réglementation visés au paragraphe 1 à la Commission d'ici au 13 janvier 2017.

La Commission est habilitée à adopter lesdites normes techniques de réglementation, conformément aux articles 10 à 14 du règlement (UE) no 1093/2010.

5. Conformément à l'article 10 du règlement (UE) no 1093/2010, l'ABE réexamine et, le cas échéant, met à jour les normes techniques de réglementation à intervalles réguliers, afin notamment de tenir compte de l'innovation et des progrès technologiques.

Annexe 3 : Considérant 95 de la DSP2

Considérant 95 de la DSP2

La sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude. Il ne semble pas nécessaire de garantir le même niveau de protection aux opérations de paiement initiées et exécutées par des moyens autres que l'utilisation de plates-formes ou de dispositifs électroniques, telles que les opérations de paiement sur support papier, les ordres de paiement passés par courrier ou par téléphone. Une croissance solide des paiements par l'internet et par téléphone mobile devrait aller de pair avec un renforcement généralisé des mesures de sécurité. Les services de paiement proposés via l'internet ou d'autres moyens à distance, dont le fonctionnement ne dépend pas de l'endroit où sont physiquement situés le dispositif utilisé pour initier l'opération de paiement ni l'instrument de paiement utilisé, devraient, par conséquent, inclure l'authentification des opérations par des codes dynamiques, afin que l'utilisateur soit à tout moment conscient du montant et du bénéficiaire de l'opération qu'il autorise.

Annexe 4 : Considérant 6 et articles du règlement délégué (UE) 2018/389

Considérant 6 du règlement délégué (UE) 2018/389

(6) Pour garantir l'application de l'authentification forte du client, il est également nécessaire d'exiger des caractéristiques de sécurité adéquates pour les éléments d'authentification forte du client appartenant à la catégorie «connaissance» (quelque chose que seul l'utilisateur connaît), comme la longueur ou la complexité, pour les éléments appartenant à la catégorie «possession» (quelque chose que seul l'utilisateur possède), comme les spécifications de l'algorithme, la longueur de la clé et l'entropie de l'information, et pour les dispositifs et logiciels qui lisent les éléments appartenant à la catégorie «inhérence» (quelque chose que l'utilisateur est), comme les spécifications de l'algorithme, le capteur biométrique et les dispositifs de protection des formats d'écran, notamment pour atténuer le risque que ces éléments soient mis au jour, divulgués à des tiers non autorisés et exploités par ceux-ci. Il convient également de définir les exigences visant à assurer l'indépendance de ces éléments, afin que la compromission de l'un ne remette pas en question la fiabilité des autres, notamment lorsque l'un de ces éléments est utilisé au travers d'un dispositif multifonctionnel, à savoir un dispositif tel une tablette ou un téléphone mobile, qui peut servir tant pour donner l'instruction d'effectuer le paiement que pour le processus d'authentification.

CHAPITRE III

DÉROGATIONS À L'OBLIGATION D'AUTHENTIFICATION FORTE DU CLIENT

Article 10

Information sur le compte de paiement

1. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences définies à l'article 2 et au paragraphe 2 du présent article, lorsqu'un utilisateur de services de paiement est limité dans son accès à un ou à deux des éléments suivants en ligne sans que des données de paiement sensibles soient divulguées:

a) le solde d'un ou de plusieurs comptes de paiement désignés;

b) les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.

2. Aux fins du paragraphe 1, les prestataires de services de paiement ne sont pas exemptés de l'application de l'authentification forte du client lorsque l'une des conditions suivantes est remplie:

a) l'utilisateur du service de paiement accède pour la première fois en ligne aux informations visées au paragraphe 1;

b) plus de 90 jours se sont écoulés depuis la dernière fois que l'utilisateur de services de paiement a accédé en ligne aux informations visées au paragraphe 1, point b), et que la procédure d'authentification forte du client a été appliquée.

Article 11

Paiement sans contact au point de vente

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences définies à l'article 2, lorsque le payeur initie une opération de paiement électronique sans contact, pour autant que les conditions suivantes soient remplies:

a) le montant individuel de l'opération de paiement électronique sans contact ne dépasse pas 50 EUR; et

b) le montant cumulé des précédentes opérations de paiement électronique sans contact initiées par l'intermédiaire d'un instrument de paiement disposant d'une fonctionnalité sans contact, depuis la date de la dernière authentification forte du client, ne dépasse pas 150 EUR; ou

c) le nombre d'opérations de paiement électronique sans contact consécutives initiées par l'intermédiaire de l'instrument de paiement disposant d'une fonctionnalité sans contact, depuis la dernière authentification forte du client, ne dépasse pas cinq.

Article 12

Automates de paiement des frais de transport et de parking

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences définies à l'article 2, lorsque le payeur initie une opération de paiement électronique à partir d'un automate de paiement afin de régler des frais de transport ou de parking.

Article 13

Bénéficiaires de confiance

1. Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée ou modifie une liste de bénéficiaires de confiance par l'intermédiaire du prestataire de services de paiement gestionnaire de son compte.

2. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, lorsque le payeur initie une opération de paiement et que le bénéficiaire figure dans une liste de bénéficiaires de confiance préalablement créée par le payeur.

Article 14

Opérations récurrentes

1. Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée, modifie ou initie pour la première fois une série d'opérations récurrentes ayant le même montant et le même bénéficiaire.

2. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, pour l'initiation de l'ensemble des opérations de paiement ultérieures comprises dans la série d'opérations de paiement visées au paragraphe 1.

Article 15

Virements entre comptes détenus par la même personne physique ou morale

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences définies à l'article 2, lorsque le payeur initie un virement pour lequel le payeur et le bénéficiaire sont la même personne physique ou morale et les deux comptes de paiement sont détenus auprès du même prestataire de services de paiement gestionnaire du compte.

Article 16

Opérations de faible valeur

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance, pour autant que les conditions suivantes soient remplies:

a) le montant de l'opération de paiement électronique à distance ne dépasse pas 30 EUR; et

b) le montant cumulé des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas 100 EUR; ou

c) le nombre des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas cinq opérations de paiement électronique à distance individuelles consécutives.

Article 17

Procédures et protocoles de paiement sécurisés utilisés par les entreprises

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client à l'égard de personnes morales qui initient des opérations de paiement électronique 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 directive (UE) 2015/2366.

Annexe 5 : Articles du code monétaire et financier

Article L133-4
Pour l'application du présent chapitre :

a) Les données de sécurité personnalisées s'entendent des données personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification ;

b) Un identifiant unique s'entend d'une combinaison de lettres, de chiffres ou de symboles indiquée à l'utilisateur de services de paiement par le prestataire de services de paiement, que l'utilisateur de services de paiement doit fournir pour permettre alternativement ou cumulativement l'identification certaine de l'autre utilisateur de services de paiement et de son compte de paiement pour l'opération de paiement ;

c) Un instrument de paiement s'entend, alternativement ou cumulativement, de tout dispositif personnalisé et de l'ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement et utilisé pour donner un ordre de paiement ;

d) Un jour ouvrable est un jour au cours duquel le prestataire de services de paiement du payeur ou celui du bénéficiaire exerce une activité permettant d'exécuter des opérations de paiement ;

e) Une authentification s'entend d'une procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur ;

f) Une authentification forte du client s'entend d'une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories " connaissance " (quelque chose que seul l'utilisateur connaît), " possession " (quelque chose que seul l'utilisateur possède) et " inhérence " (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification ;

g) Les données de paiement sensibles s'entendent des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude. En ce qui concerne les activités des prestataires de services de paiement fournissant le service d'initiation de paiement et des prestataires de services de paiement fournissant le service d'information sur les comptes, le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles ;

h) Un groupe s'entend de l'ensemble formé par une société et celles qu'elle contrôle au sens de l'article L. 233-16 du code de commerce ou d'établissements au sens des articles 4,5,6 et 7 du règlement délégué (UE) n° 241/2014 de la Commission européenne qui sont liés entre eux par une relation au sens de l'article 10, paragraphe 1, ou de l'article 113, paragraphe 6 ou 7, du règlement (UE) n° 575/2013.

Article L133-17
I. – Lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, l'utilisateur de services de paiement en informe sans tarder, aux fins de blocage de l'instrument, son prestataire ou l'entité désignée par celui-ci.

II. – Lorsque le paiement est effectué par une carte de paiement émise par un établissement de crédit, une institution ou un service mentionné à l'article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds, il peut

être fait opposition au paiement en cas de procédure de redressement ou de liquidation judiciaires du bénéficiaire tant que le compte du prestataire de services de paiement du bénéficiaire n'a pas été crédité du montant de l'opération de paiement.

Article L133-18
En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse au payeur le montant de l'opération non autorisée 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, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et s'il communique ces raisons par écrit à la Banque de France. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.

Lorsque l'opération de paiement non autorisée est initiée par l'intermédiaire d'un prestataire de services de paiement fournissant un service d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte rembourse immédiatement, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. La date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il avait été débité.

En cas de manquement du prestataire de services de paiement aux obligations prévues aux deux premiers alinéas du présent article, les pénalités suivantes s'appliquent :

1° Les sommes dues produisent intérêt au taux légal majoré de cinq points ;

2° Au-delà de sept jours de retard, les sommes dues produisent intérêt au taux légal majoré de dix points ;

3° Au-delà de trente jours de retard, les sommes dues produisent intérêt au taux légal majoré de quinze points.

Si le prestataire de services de paiement qui a fourni le service d'initiation de paiement est responsable de l'opération de paiement non autorisée, il indemnise immédiatement le prestataire de services de paiement gestionnaire du compte, à sa demande, pour les pertes subies ou les sommes payées en raison du remboursement du payeur, y compris le montant de l'opération de paiement non autorisée.

Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire.

Article L133-19
I. – En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 50 €.

Toutefois, la responsabilité du payeur n'est pas engagée en cas :

– d'opération de paiement non autorisée effectuée sans utilisation des données de sécurité personnalisées ;

– de perte ou de vol d'un instrument de paiement ne pouvant être détecté par le payeur avant le paiement ;

– de perte due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.

II. – La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées.

Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument.

III. – Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement prévue à l'article L. 133-17.

IV. – Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17.

V. – Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L. 133-44.

VI. – Lorsque le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte du payeur prévue à l'article L. 133-44, il rembourse le préjudice financier causé au prestataire de services de paiement du payeur.

Article L133-23
Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

L'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services de paiement fournissant un service d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.

Article L133-44
I. – Le prestataire de services de paiement applique l'authentification forte du client définie au f de l'article L. 133-4 lorsque le payeur :

1° Accède à son compte de paiement en ligne ;

2° Initie une opération de paiement électronique ;

3° Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

II. – Pour les opérations de paiement électronique à distance, l'authentification forte du client définie au f de l'article L. 133-4 comporte des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés.

III. – En ce qui concerne l'obligation du I, les prestataires de services de paiement mettent en place des mesures de sécurité adéquates afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement.

IV. – Le prestataire de services de paiement gestionnaire du compte autorise le prestataire de services de paiement fournissant un service d'initiation de paiement et le prestataire de services de paiement fournissant le service d'information sur les comptes à se fonder sur ses procédures d'authentification lorsqu'ils agissent pour l'un de leurs utilisateurs conformément aux I et III et, lorsque le prestataire de services de paiement fournissant le service d'initiation de paiement intervient, conformément aux I, II et III.

V. – Le prestataire de services de paiement s'assure que les méthodes d'authentification qu'il fournit à ses clients respectent les exigences d'accessibilité fixées à l'article L. 412-13 du code de la consommation.

Article L561-6
Pendant toute la durée de la relation d'affaires et dans les conditions fixées par décret en Conseil d'Etat, ces personnes exercent, dans la limite de leurs droits et obligations, une vigilance constante et pratiquent un examen attentif des opérations effectuées en veillant à ce qu'elles soient cohérentes avec la connaissance actualisée qu'elles ont de leur relation d'affaires.

Annexe 6 : Projet de loi ratifiant l'ordonnance du 9 août 2017 de la Commission des finances du Sénat

L'apport principal de la commission des finances du Sénat : assurer une protection effective du consommateur sur l'ensemble des services proposés par les prestataires de services de paiement

- **Le périmètre couvert par la directive « DSP 2 » n'appréhende pas l'intégralité des nouveaux services de paiement, soulevant des risques pour l'utilisateur**

À l'instar de la directive « DSP 1 », **cette nouvelle directive ne couvre que le périmètre des comptes de paiement**, ce qui exclut les autres supports de bancarisation et d'épargne, tels les comptes d'épargne et les contrats d'assurance.

Les dispositions qu'elle prévoit, en particulier s'agissant de la protection du consommateur, ne valent donc pas au-delà de ce périmètre. **Il en résulte une difficulté majeure**, notamment dans la mesure où 80 % des comptes agrégés par les services d'information sur les comptes ne sont pas des comptes de paiement.

De fait, pour ces comptes hors périmètre de la directive « DSP 2 », la méthode du *web scraping* non authentifié demeurera applicable, y compris après septembre 2019, et **le cadre juridique ne garantit aucune protection effective de l'utilisateur en cas de fraude.**

Les dispositions contractuelles liant l'utilisateur de services de paiement à son établissement bancaire et au prestataire de services de paiement conduisent à **faire porter le risque par le consommateur : en cas de fraude ou de piratage, il se retrouverait seul responsable et ne pourrait pas être remboursé.**

- **Afin d'assurer une protection effective du consommateur pour l'ensemble des services proposés par les prestataires de services de paiement, la commission des finances a introduit une obligation d'assurance couvrant les comptes hors du périmètre de « DSP 2 »**

Il est nécessaire que le cadre juridique défini par la directive « DSP 2 » soit étendu aux comptes d'épargne. Cependant, **cette démarche doit intervenir au niveau européen**, afin de prolonger l'harmonisation déjà opérée pour les comptes de paiement.

Dans l'attente de cette initiative européenne, **la protection du consommateur doit être assurée** le plus rapidement possible **au plan national**.

C'est pourquoi la commission des finances a adopté **un amendement visant à garantir la possibilité pour l'utilisateur d'obtenir un remboursement auprès du prestataire en cas de fraude.**

Le nouvel article 1er *bis* A permet ainsi d'engager la responsabilité du prestataire tiers, dont la solvabilité est assurée par l'obligation d'assurance qu'il prévoit par ailleurs.

Conciliant la nécessaire protection de l'utilisateur et le développement de l'innovation, il rend obligatoire une pratique déjà appliquée selon une démarche volontaire par certains prestataires de services de paiement.

La commission des finances du Sénat a adopté le projet de loi ainsi modifié.

Annexe 7 : Examen de l'amendement CF7 par la Commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale sur le projet de loi ratifiant l'ordonnance du 9 août 2017

La commission examine l'amendement CF7 de M. Jean-Noël Barrot.

M. Jean-Noël Barrot. À mon tour, je félicite et remercie Mme la rapporteure pour son travail sur ce texte très technique. Pour répondre à Jean-Louis Bourlanges, je voudrais remettre le sujet en perspective. Cette transposition vise à trouver un équilibre entre deux impératifs : la sécurité et la libération de l'innovation. Au niveau européen, la directive a donc été négociée entre les banques – qui ont essayé de s'assurer de la sécurisation des transferts d'information – et les nouveaux entrants – notamment les start-up – qui essaient d'offrir de nouveaux services d'information aux usagers et aux épargnants et ont besoin d'avoir accès aux données de ces derniers, avec leur accord bien entendu.

Dans le cadre de cette directive, les banques se sont engagées à mettre en place des API. Avec l'accord des usagers, elles permettront aux nouveaux entrants de se connecter à leurs comptes et d'utiliser ou, *a minima*, de mobiliser les données de manière plus sécurisée, par le biais des API, plus sûres que les pratiques actuelles. Des applications téléchargeables sur les téléphones portables existent déjà. Elles vous demandent vos identifiants afin d'aspirer vos données bancaires – avec votre accord –, et vous livrent des informations sur vos comportements de paiement et d'épargne.

La directive a restreint l'utilisation des API au compte courant des utilisateurs. Mon amendement vise, par parallélisme, à étendre ces dispositions aux comptes d'épargne, dans un triple objectif : tout d'abord, assurer aux utilisateurs le même niveau de sécurité pour leurs comptes d'épargne que pour leur compte courant, puisque la directive vise à assurer la sécurité des comptes des épargnants.

Par ailleurs, si les applications de ces start-up et entreprises de services de paiement ont accès aux comptes d'épargne, cela offrira une meilleure lisibilité aux épargnants sur leurs frais bancaires. Ces applications pourront vous dire quel pourcentage de votre budget vous avez consommé en alimentation, en transports, *etc.* Avec mon amendement, elles mettront également en lumière les frais que vous payez. Cela améliorera la visibilité des usagers sur les frais d'agios, mais également sur ceux liés aux différents produits d'épargne.

Enfin, mon amendement améliorera l'allocation de notre épargne, grâce au soutien de ces nouveaux fournisseurs de services. Ils pourront accompagner les Françaises et les Français, dont l'épargne sera ainsi plus naturellement fléchée vers des produits plus dynamiques et vers les entreprises. C'est un des objectifs

poursuivis par le projet de loi relatif au plan d'action pour la croissance et la transformation des entreprises (PACTE).

Il me semble donc intéressant d'étendre le champ de la directive aux autres comptes d'épargne, quitte à faire éventuellement facturer ce service par les banques aux prestataires de services mobilisant ces données.

On pourra m'opposer le risque lié à l'extension du champ de la directive par la France seule. Mais il n'y a pas besoin d'attendre les autres pays européens pour améliorer la sécurité des épargnants français, la lisibilité des frais bancaires et l'allocation de l'épargne française. On peut simplement donner l'exemple en étendant le champ de la directive.

Mme la rapporteure. Je comprends parfaitement et partage la réflexion qui sous-tend cet amendement, mais je le prends comme un amendement d'appel. Sur la forme, il ne peut avoir les effets escomptés sans être précisé. Par ailleurs, sur le fond, la directive DSP2 ne concerne que les comptes de paiement, les comptes d'épargne ou d'assurance étant exclus de son champ. L'ordonnance qui nous est présentée transpose ces dispositions sans aller au-delà.

Vous avez tout à fait raison lorsque vous faites remarquer que les comptes agrégés, dans leur majorité, ne sont pas des comptes de paiement. Une partie du système sera donc régulée, avec des modalités d'accès encadrées, une autre partie ne l'étant pas. C'est pourquoi la question de l'extension du champ de la directive aux autres comptes se pose. Mais elle ne peut être réglée dans ce projet de loi : tout d'abord, il s'agirait d'une surtransposition
– l'ordonnance ne peut pas aller au-delà de ce que prévoit la directive, M. le président l'a souligné. Par ailleurs, le Gouvernement évalue actuellement les normes internes surtransposant le droit européen. Nous devons donc réaliser un travail d'analyse plus approfondi de votre proposition. Ensuite, des discussions doivent s'engager avec les gestionnaires des comptes en question : il est important de consulter ces professions avant d'envisager l'application d'un cadre juridique portant à conséquences pour eux. Enfin et surtout, cette question doit être traitée au niveau européen, notamment pour des raisons de concurrence.

Je vous propose donc de retirer votre amendement.

M. Jean-Louis Bourlanges. Vous avez raison, on ne peut intégrer la proposition de Jean-Noël Barrot dans une transposition de directive. Mais elle a le mérite de poser une question de fond, celle de la subsidiarité, question sur laquelle nous devrions être actifs. Si le texte reste en l'état – Jean-Noël Barrot l'a très bien expliqué – le système est déséquilibré. Mais, si nous prenons une mesure unilatérale, cela crée une distorsion de concurrence, qui entre dans le champ de la

subsidiarité.

Qu'est-ce que la subsidiarité ? Une décision doit être prise au niveau européen quand elle ne peut pas être traitée rationnellement au niveau national. En tant que Parlement, depuis le traité de Lisbonne, nous disposons d'un certain nombre de moyens d'action sur la Commission européenne. Nous devrions donc adresser à la Commission – qui a le pouvoir d'initiative – des messages d'appel solennels – je ne sais pas comment à ce stade, peut-être par le biais d'une résolution commune avec la commission des affaires européennes et un vote en séance publique de notre Assemblée. Si la Commission européenne a le monopole de l'initiative, rien ne nous empêche de transmettre une demande d'initiative.

Mme Véronique Louwagie. L'amendement proposé aboutirait à ce que s'applique en France, à des situations qui ne s'arrêtent pas à nos frontières, un dispositif unique en Europe. Par ailleurs, si, les uns et les autres, nous déplorons régulièrement des surtranspositions de directives, respectons donc en l'occurrence le principe, même s'il peut connaître des exceptions : ne surtransposons pas. Enfin, si un problème se pose, il faut l'aborder au niveau européen. Évaluons la mise en œuvre de cette directive et ses effets sur tous les acteurs, en termes tant d'offre de services que de sécurité globale du système, en prenant en compte l'évolution des menaces, probablement sans commune mesure aujourd'hui avec ce qu'elles étaient en 2015.

M. Jean-Noël Barrot. Je ne propose pas une surtransposition, je propose d'étendre le champ d'application des mesures transposées, ce qui est tout à fait possible.

Cela étant, ayant entendu les arguments de la rapporteure et d'autres collègues, je retire mon amendement. Il n'en serait pas moins intéressant que le débat lancé par Jean-Louis Bourlanges ait lieu en séance.

M. le président Éric Woerth. Effectivement, vous pouvez redéposer votre amendement en vue de la séance car le débat mérite d'avoir lieu.

L'amendement CF7 est ***retiré****.*

Annexe 8 : Exemples de réponses des banques à des réclamations

LA BANQUE POSTALE

Pour nous contacter :

Par messagerie 7J/7 24h/24
www.labanquepostale.fr(1)
ou application La Banque Postale(1)

Vous préférez téléphoner
0
(Service gratuit + prix appel)

Dans votre bureau de poste

LA POSTE

SD : 863006416868095X

654720 1193 593
V55 1/ 1 2

MR

Vos références clients :
Numéro de dossier : 00083325304710749520031

Le 29 mars 2023,

Monsieur,

Vous avez contesté une opération effectuée avec votre carte bancaire.

Les données dont nous disposons nous permettent d'affirmer que cette opération a été effectuée en vente à distance selon le protocole de sécurité 3DS Certicode Plus. Pour être débitée de votre compte, cette transaction a fait l'objet d'une authentification par la saisie de votre code personnel à cinq chiffres, que vous seul connaissez. Ce code a donc nécessairement été saisi par vos soins, ou bien divulgué.

Les conditions d'utilisation des Cartes émises par la Banque Postale stipulent que « le Titulaire de la carte « CB » doit prendre toutes les mesures propres à assurer la sécurité de sa carte « CB » et du code confidentiel et plus généralement de tout autre élément du dispositif de sécurité personnalisé. Il doit donc tenir absolument secret son code et ne pas le communiquer à qui que ce soit.
Elles prévoient également que « Toutes les opérations non autorisées sont à la charge du Titulaire de la carte, sans limitation de montant en cas de négligence grave ».

Dans ces conditions, la responsabilité de La Banque Postale ne saurait être engagée. La somme de 600,00 € ainsi que les éventuelles commissions afférentes restent donc débitées de votre compte.

Nous tenons à vous rappeler que La Banque Postale ne demande jamais à ses clients de lui fournir des informations bancaires ou confidentielles, comme les codes reçus par sms pour valider une opération, annuler ou activer une fonctionnalité. Ces codes ne permettent jamais l'annulation de l'opération décrite mais uniquement sa validation. Que ce soit par téléphone, par mail ou par n'importe quel autre moyen ne répondez pas à la sollicitation. Souvent un caractère d'urgence est invoqué. Ne cédez pas à la panique car une fois vos coordonnées dans les mains des fraudeurs, des transactions leur sont possibles. Alertez immédiatement votre conseiller en agence ou au 3639*.
*Service 0.15€/min + prix d'un appel

(1) Coût de connexion et/ou de communication selon le fournisseur d'accès ou l'opérateur de téléphonie mobile.
Pour nous écrire : La Banque Postale Centre Financier 87074 LIMOGES CEDEX 9

29193

Carrefour banque et assurance

Carrefour Banque - www.carrefour-banque.fr
Service Relations Clientèle - TSA 74116 - 77026 Melun-Cedex
S.A. au capital de 191 346 056,72 € - RCS Evry 313 811 515 - 1, place Copernic - 91051 Evry Cedex
SIRET 313 811 515 00078 - N° ORIAS : 07 027 515 (www.orias.fr) - N° TVA intracommunautaire FR 87 313 811 515

ADC DE FRANCE

3 RUE GUERRIER DE DUMAST

54000 NANCY

Evry, le 30 mai 2023

N/Réf : SQRC/VV/ 51276170739002

AFFAIRE:
29057_

Madame, Monsieur,

Nous faisons suite à votre courrier du 14 mai 2023 par lequel vous intervenez en soutien de

Nous confirmons que notre cliente a fait l'objet d'une escroquerie, et non d'une usurpation d'identité, lors du financement d'un prêt personnel de 10500,00€.

Pour information, le dossier a été étudié et validé après étude des documents fournis dans le respect de nos règles d'octroi.

Les fonds ont été versés sur le compte bancaire de en date du 15/12/22.

En conséquence, le remboursement des mensualités doit être effectué. Sans règlement de sa part, la procédure de recouvrement suivra son cours.

En cas de désaccord, vous pouvez saisir notre médiateur dont les coordonnées sont les suivantes: Monsieur le Médiateur : Médiateur de l'ASF (Association Française des Sociétés Financières), 24 Avenue de la Grande Armée 75854 PARIS CEDEX 17 ou http : //lemediateur.asf-France.com//

Nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées.

Valérie VANHOVE

Service Qualité Relation Client

pole juridique

De : <contact@adcfrance.fr>
Date : lundi 19 juin 2023 19:45
À : "pole juridique" <polejuridique@adcfrance.fr>
Joindre : 11062023 ADC FRANCE.PDF
Objet : Fwd: [SQRC/SE] - [PASS Réclamation] - Association de Défense des Consommateurs \ dossier

-------- Message transféré --------
Sujet :[SQRC/SE] - [PASS Réclamation] - Association de Défense des Consommateurs \ dossier

Date : Mon, 19 Jun 2023 16:45:49 +0200
De : Stéphanie EISENSCHMIDT <pass_clientele@carrefour.com>
Pour :contact@adcfrance.fr

Vos réf : dossier n° 29057 - 1 /GG
Nos réf : Prêt PASS n°51276170739002
Madame, Monsieur,

Nous faisons suite à votre courrier du 11/06/2023.

Nous regrettons de vous rappeler les termes de nos précédentes correspondances.

L'ensemble des éléments factuels nous conduisent à refuser votre demande de prise en charge.

Conformément aux dispositions contractuelles, nous vous invitons une nouvelle fois, à saisir le Médiateur de L'ASF.

Vous en souhaitant bonne réception,

Cordialement,

MME EISENSCHMIDT
Service Qualité Relation Clients

--

banque et assurance

Stéphanie EISENSCHMIDT
Service Qualité Relation Clients
TSA 56648 - 91 988 EVRY CEDEX
pass_clientele@carrefour.com

21/06/2023

Annexe 9 : Exemples de lettres envoyées par l'ADC à l'intention des banques

ASSOCIATION de DEFENSE des CONSOMMATEURS
de FRANCE

Nancy, le 28 juin 2023

La Banque Postale
Centre Financier
87 074 LIMOGES CEDEX 9

N/Réf. : dossier n°29076/TB **(à rappeler dans toutes vos correspondances)**

Madame, Monsieur,

Notre adhérent, Monsieur , domicilié , nous a fait part du litige qui l'oppose à votre société.

Monsieur a reçu un appel d'une personne prétendant être issue du service opposition carte bancaire et qui lui a expliqué qu'il avait été débité de 1000 euros. Cette personne lui a alors demandé de se connecter à son compte et de valider les paiements en attente grâce au code Certicode Plus, « pour qu'elle les annule ». Le fraudeur lui a ensuite fait télécharger une application « Révolut » pour que M. effectue des validations en communiquant les codes qu'il recevait.

Une fois l'appel terminé, M. a compris que quelque chose n'était pas normal et a immédiatement appelé son banquier qui a bloqué son compte et sa carte bancaire. Toutefois, cela n'a pas empêché les sommes de 1000 euros et 600 euros d'être prélevées du compte de notre adhérent. Ce dernier a ensuite porté plainte.

Par courrier du 29 mars 2023, vous refusez sa demande de remboursement de 600 euros au motif que la transaction a fait l'objet d'une authentification par la saisie du code personnel à cinq chiffres. Vous rappelez ensuite les conditions d'utilisation des cartes qui prévoient que « toutes les opérations non autorisées sont à la charge du titulaire de la carte, sans limitation de montant en cas de négligence grave ».

La jurisprudence en la matière est constante : il incombe à la banque de prouver que l'utilisateur du service a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations (Com., 21 novembre 2018, n°17-18.888 et Com., 26 juin 2019, n°18-12.581).

Toutefois, vous ne démontrez pas la négligence grave de votre client. En effet, le fait de valider une opération avec son code personnel ne constitue pas une preuve de négligence grave et les circonstances dans lesquelles la fraude a eu lieu sont à prendre en compte. C'est en effet le raisonnement de la Cour

ADC France
3-5, rue Guerrier de Dumast - 54000 NANCY
03 83 85 51 95 – contact@adcfrance.fr

www.adcfrance.fr

Siret : 33099551500047 - APE : 9499Z

d'appel de Versailles qui, dans un arrêt du 28 mars 2023 (n°21/07299), prévoit que face à un appel téléphonique évoquant de surcroît un piratage, la vigilance de la personne qui reçoit cet appel est moindre que celle d'une personne qui réceptionne un mail, laquelle dispose de davantage de temps pour en prendre connaissance et s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse. Dans ces conditions, la Cour ne retient pas la négligence grave du payeur et condamne la banque à lui rembourser les virements litigieux.

Dans notre cas, M. a été victime d'un appel frauduleux de la part d'une personne se faisant passer pour un employé du service d'opposition carte bancaire. Le fraudeur a notamment insisté sur la prétendue urgence de la situation en raison du prélèvement de 1000 euros. En ce cas, la réaction de M. ne peut être caractérisée comme de la négligence grave, puisqu'il croyait être en relation avec un professionnel et qu'il était évidemment perturbé par l'annonce du prélèvement.

De plus, il convient de souligner que M. n'a aucunement tardé dans la révélation des virements frauduleux à son banquier.

Dans ces circonstances, il n'est pas caractérisé à l'égard de votre client une négligence grave. Dès lors, s'applique l'article L133-18 du code monétaire et financier qui prévoit qu'« en cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L133-24, le prestataire de services de paiement du payeur rembourse au payeur le montant de l'opération non autorisée 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 ».

Nous vous demandons donc de rembourser M. des sommes de 1000 euros et 600 euros prélevées frauduleusement sur son compte, ainsi que des éventuelles commissions afférentes. Nous tenons en outre à vous faire remarquer qu'un règlement amiable serait préférable pour votre société, les juridictions ayant en effet tendance à accorder, en plus du remboursement total des opérations non autorisées, des dommages et intérêts aux victimes accusées à tort de négligence grave (CA de Versailles, 28 mars 2023, n°21/07299).

Dans cette attente, veuillez recevoir, Madame, Monsieur, nos sincères salutations.

Le service juridique

ADC France
3-5, rue Guerrier de Dumast - 54000 NANCY
03 83 85 51 95 – contact@adcfrance.fr

www.adcfrance.fr

Siret : 33099551500047 - APE : 9499Z

ASSOCIATION de DEFENSE des CONSOMMATEURS
de FRANCE

Nancy, le 28 juin 2023

Crédit Agricole
56-58 avenue André
Malraux
57 000 METZ

N/Réf. : dossier n°29043/TB
(à rappeler dans toutes vos correspondances)

Madame, Monsieur,

Notre adhérent, Monsieur , domicilié , nous a fait part du litige qui l'oppose à votre société.

Le 29 mars 2022, Monsieur a reçu un mail d'hameçonnage avec l'entête Canal+ lui proposant un chèque cadeau de 100 euros. Pensant que l'offre provenait réellement de Canal+ et souhaitant en profiter, Monsieur a alors réalisé un paiement de 1,99 euros.

Mais Monsieur a rapidement compris qu'il s'agissait d'une arnaque et a de suite contacté son banquier afin de faire opposition. Il a également porté plainte.

Malgré cela, Monsieur a été débité de la somme de 699 euros le 5 avril 2022 pour un achat chez Leroy Merlin, achat dont il n'est pas bien sûr pas à l'origine.

Par courrier recommandé du 5 mai 2022, Monsieur vous a demandé le remboursement de la somme prélevée frauduleusement mais vous le lui refusez sous prétexte que l'opération a été validée par le protocole d'authentification Sécuripass et que l'ensemble du système de sécurisation des paiements a fonctionné correctement.

Vous semblez oublier **l'article L133-19 du code monétaire et financier** qui prévoit que ce n'est qu'en cas d'agissement frauduleux de la part du payeur ou lorsqu'il n'a pas satisfait intentionnellement ou par négligence grave à ses obligations que la banque est en droit de lui faire supporter toutes les pertes occasionnées par des opérations de paiement non autorisées.

Et la jurisprudence en la matière est constante : il incombe à la banque de prouver que l'utilisateur du

service a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations (**Com., 21 novembre 2018, n°17-18.888** et **Com., 26 juin 2019, n°18-12.581**).

Or, si vous reconnaissez que Monsieur a répondu à un mail de phishing, vous ne démontrez aucunement sa négligence grave. De plus, notez que le phishing est une technique conçue pour tromper le destinataire et qu'y donner suite ne permet pas de prouver une quelconque négligence grave. Il convient également de souligner que M. n'a manqué à aucune de ses obligations puisqu'il vous a signalé sans tarder la situation afin de faire opposition.

Dès lors s'applique **l'article L133-18 du code monétaire et financier** qui prévoit qu'« en cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L133-24, le prestataire de services de paiement du payeur rembourse au payeur le montant de l'opération non autorisée 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 ».

En conséquence, nous vous demandons de rembourser à M. les 699 euros prélevés frauduleusement de son compte.

Dans cette attente, veuillez recevoir, Madame, Monsieur, nos sincères salutations.

Le service juridique

ADC France
3-5, rue Guerrier de Dumast - 54000 NANCY
03 83 85 51 95 – contact@adcfrance.fr

www.adcfrance.fr

Siret : 33099551500047 - APE : 9499Z

Annexe 10 : Recommandation 2022-R-01 du 9 mai 2022 de l'ACPR

Recommandation 2022-R-01 du 9 mai 2022
sur le traitement des réclamations

1. Contexte

Le traitement des réclamations est un enjeu de protection de la clientèle. Plusieurs textes, notamment de nature législative et réglementaire, imposent aux professionnels des secteurs de la banque et de l'assurance des obligations, en particulier, d'information concernant le processus de réclamation et de recours à la médiation de la consommation[1]. Certains professionnels proposent également un dispositif de médiation à leur clientèle agissant à des fins entrant dans le cadre de leur activité commerciale, industrielle, artisanale, libérale ou agricole.

Depuis 2011, l'Autorité de contrôle prudentiel et de résolution (ACPR) recommande à ces professionnels des bonnes pratiques dont l'objectif est de permettre :

- une information claire et transparente sur les modalités d'accès aux dispositifs de traitement des réclamations et de médiation ;
- un traitement des réclamations efficace, égal et harmonisé ;
- la mise en place d'actions correctives à partir des dysfonctionnements identifiés au travers des réclamations.

Certaines pratiques de marché, identifiées notamment à travers les informations reçues de la clientèle, conduisent l'ACPR à recommander aujourd'hui des bonnes pratiques qui, à l'instar des précédentes, visent à ce que l'ensemble des professionnels concernés se dotent d'une organisation simple et efficace permettant d'apporter aux réclamants, une réponse qualitative et motivée le plus rapidement possible, et en tout état de cause dans un délai n'excédant pas deux mois, sauf dispositions plus contraignantes.

2. Champ d'application de la recommandation

Une réclamation se définit comme l'expression d'un mécontentement envers un professionnel quel que soit l'interlocuteur ou le service[2] auprès duquel elle est formulée. Elle peut émaner de toute personne, y compris en l'absence de relation contractualisée avec le professionnel : clients (particuliers ou professionnels), anciens clients, bénéficiaires, personnes ayant sollicité du professionnel la fourniture d'un produit ou service ou qui ont été sollicitées par un professionnel, y compris leurs mandataires et leurs ayants droit.

Une demande de service ou de prestation, d'information ou d'avis n'est pas une réclamation[3].

[1] Le Comité consultatif du secteur financier a par ailleurs publié le 1er juillet 2021 un rapport sur la médiation bancaire et de l'assurance.
[2] Y compris auprès d'un délégataire ou d'un mandataire du professionnel (agent général d'assurance, agent de prestataire de services de paiement, distributeur de monnaie électronique…).
[3] Cf. Annexe : Illustrations de la notion de réclamation.

Mis en ligne le 17/05/2022

La présente recommandation s'adresse :

- aux entreprises d'assurance, aux mutuelles ou unions de mutuelles, aux institutions de prévoyance ou unions d'institutions de prévoyance, aux fonds de retraite professionnelle supplémentaire, aux mutuelles ou unions de retraite professionnelle supplémentaire et aux institutions de retraite professionnelle supplémentaire,

- aux établissements de crédit, aux sociétés de financement, aux établissements de paiement, aux prestataires de services d'information sur les comptes et aux établissements de monnaie électronique,

- aux intermédiaires d'assurance, aux intermédiaires en opérations de banque et en services de paiement et aux intermédiaires en financement participatif.

ci-après « le ou les (s) professionnel(s) », y compris lorsqu'ils exercent leur activité en France au titre du régime de libre prestation de services ou de libre établissement.
S'agissant des prestataires de services d'information sur les comptes, le périmètre de la présente recommandation porte sur le traitement des réclamations liées à la sécurité des données collectées.

3. Recommandation

Afin d'assurer l'efficacité du dispositif de traitement des réclamations et faciliter l'accès aux dispositifs de médiation proposés, l'ACPR recommande, conformément aux dispositions des articles L. 612-1 II 3° et L. 612-29-1 alinéa 2 du Code monétaire et financier, aux professionnels :

3.1. Sur l'organisation du traitement des réclamations et les moyens et procédures associés

3.1.1. De mettre en œuvre une organisation du traitement des réclamations permettant, quel que soit l'interlocuteur ou le service[4] auprès duquel la réclamation a été formulée :

- d'identifier les réclamations formulées par la clientèle quel que soit leur canal d'expression (écrit ou oral) ;

- pour les réclamations formulées à l'oral (numéro de téléphone non surtaxé, lieu d'accueil de la clientèle…) ou par messagerie instantanée ne permettant pas au réclamant de disposer d'une copie datée de sa réclamation, d'inviter ce dernier à formaliser son mécontentement au moyen d'un support écrit durable[5] s'il ne peut lui être donné immédiatement entière satisfaction ;

- lorsqu'un formulaire en ligne est proposé par le professionnel, de veiller à ce qu'il permette au réclamant de disposer d'une copie datée de sa réclamation ;

[4] Y compris auprès d'un délégataire ou d'un mandataire du professionnel (agent général d'assurance, agent de prestataire de services de paiement, distributeur de monnaie électronique...).
[5] Selon les modalités de traitement : courrier, courriel ou formulaire en ligne permettant au réclamant de disposer d'une copie datée de sa réclamation...

Mis en ligne le 17/05/2022

- de transmettre à l'interlocuteur ou au service compétent les réclamations écrites[6] que le destinataire n'est pas habilité à traiter ;

- de transmettre aux médiateurs toutes les correspondances qui leur sont destinées ;

- d'accuser réception, par écrit, d'une réclamation écrite dans un délai maximal de dix jours ouvrables à compter de son envoi. Cet accusé de réception mentionne comment accéder à la page dédiée visée au 3.2.2 ou, à défaut, les informations énumérées au 3.2.1[7]. Cet accusé de réception n'est toutefois pas nécessaire si le professionnel répond par écrit à la réclamation dans le délai susmentionné ;

- de répondre :

    - par écrit à toute réclamation écrite[8],

    - de façon claire, adaptée au cas d'espèce et argumentée,

    - dans le délai auquel le professionnel s'est engagé et, en tout état de cause, dans les deux mois à compter de l'envoi[9] de la première manifestation écrite d'un mécontentement, sauf dispositions législatives ou réglementaires plus contraignantes.

- d'enregistrer les réclamations écrites, les réponses apportées et de suivre leur traitement, y compris lorsque celui-ci a été en tout ou partie délégué.

3.1.2. De veiller à ce que l'organisation du traitement des réclamations ne repose pas sur une multitude de circuits de traitements ou d'intervenants distincts pour les réclamants.

3.1.3. De veiller à ce que les délais de réponse appliqués soient cohérents avec l'objet du mécontentement exprimé[10], en particulier lorsque celui-ci porte sur un délai d'exécution.

3.1.4. De veiller à ce que les collaborateurs habituellement en relation avec la clientèle ou susceptibles de recevoir des réclamations :

- soient formés à l'identification des réclamations et à leur dispositif de traitement ;

- puissent à tout moment se référer à un support d'aide à l'identification et à l'orientation des réclamations adapté aux activités du professionnel et à la typologie des mécontentements exprimés par les réclamants.

3.1.5. De veiller à ce que les collaborateurs habilités à traiter les réclamations disposent des compétences adaptées à cette mission et en particulier d'une bonne connaissance des produits, services et contrats, de la réglementation applicable ainsi que des outils et procédures internes.

---

[6] Dans l'ensemble de la recommandation, la notion de « réclamation écrite » s'entend comme une réclamation exprimée sur un support écrit durable, les réclamations formulées à l'oral ou par messagerie instantanée (sans remise une copie datée de la réclamation) faisant l'objet d'un traitement précisé supra.

[7] À l'exception de celles du 2ème tiret et de celles du 1er qui ne sont plus pertinentes eu égard à l'organisation retenue par le professionnel.

[8] Y compris lorsqu'il est donné satisfaction au réclamant, notamment par la réalisation d'un acte de gestion.

[9] Le cachet de la poste faisant foi pour les réclamations adressées par voie postale.

[10] Étant rappelé que ces délais de réponse ne peuvent excéder deux mois, sauf dispositions législatives ou réglementaires plus contraignantes (cf. point 3.1.1).

Mis en ligne le 17/05/2022

3.1.6. De prévoir les principes de responsabilités et délégations liées au traitement des réclamations.

3.1.7. De formaliser l'organisation du traitement des réclamations dans une (des) procédure(s) communiquée(s) à l'ensemble des collaborateurs concernés.

3.2. Sur l'information permettant d'accéder aux dispositifs de traitement des réclamations et de médiation

3.2.1. D'informer en langage clair et compréhensible :

- sur les modalités pratiques pour effectuer une réclamation (adresse postale, site internet, courriel…) ;

- que le réclamant est invité à formaliser son mécontentement au moyen d'une réclamation écrite s'il n'a pu lui être donné immédiatement entière satisfaction conformément au point 3.1.1[11] ;

- sur l'organisation retenue par le professionnel pour apporter une réponse à une réclamation et les délais de traitement auxquels il s'engage[12] ;

- sur le (ou les) médiateur(s) compétent(s) selon les produits ou la nature des litiges ainsi que sur les modalités pratiques pour le(s) saisir. Il est notamment précisé lorsqu'il s'agit d'un médiateur de la consommation que celui-ci peut en tout état de cause être saisi deux mois après l'envoi d'une première réclamation écrite, quel que soit l'interlocuteur ou le service auprès duquel elle a été formulée et qu'il y ait été ou non répondu.

3.2.2 De rendre l'information visée au 3.2.1 aisément accessible[13], notamment dans les lieux d'accueil de la clientèle et sur une page dédiée du site internet du professionnel n'impliquant pas une identification préalable du réclamant.

3.2.3 Dans toute réponse, de mentionner, le médiateur pouvant être sollicité au cas d'espèce ainsi que les modalités pratiques de sa saisine. Il est notamment précisé si ce médiateur peut être saisi sans délai ou, si tel n'est pas le cas et qu'il s'agit d'un médiateur de la consommation, que ce dernier peut en tout état de cause être saisi deux mois après l'envoi de la première réclamation écrite qui a été adressée au professionnel, quel que soit l'interlocuteur ou le service auprès duquel elle a été formulée.

3.2.4 S'il y a lieu, de faire figurer les informations visées au 3.2.3 pour chaque médiateur compétent au cas d'espèce, en précisant pour chacun d'eux ce qui relève de leur compétence.

3.2.5 D'éviter toute appellation ou diffusion d'informations susceptibles d'entraîner une confusion sur les rôles respectifs d'un service d'un professionnel et d'un dispositif de médiation.

[11] Pour les réclamations formulées à l'oral ou sur un support écrit non durable.
[12] Accusé de réception, réponse.
[13] Exemple : *via* un lien sur la page d'accueil ou la rubrique « contact » du site, une recherche à partir du mot « réclamation » dans le moteur de recherche du site.

Mis en ligne le 17/05/2022

3.3. Sur le suivi, le contrôle du traitement des réclamations et la prise en compte des dysfonctionnements, manquements ou mauvaises pratiques identifiés à travers les réclamations

3.3.1. De mettre en place les moyens et procédures permettant :

- d'identifier, à travers les réclamations écrites[14] et les demandes transmises par un médiateur, les dysfonctionnements, manquements à la réglementation ou mauvaises pratiques commerciales et de prendre, dans des délais raisonnables, les mesures correctives pour y remédier, notamment à l'égard des clients concernés par une application erronée d'une disposition légale, réglementaire ou contractuelle ;

- d'analyser la qualité du dispositif de traitement des réclamations mis en place en procédant notamment à l'examen de la volumétrie, de la nature, des délais de traitement des réclamations et de la qualité[15] des réponses apportées ;

- de soumettre, au moins annuellement, aux instances de gouvernance appropriées du professionnel et de son groupe, une synthèse comportant une analyse de la qualité du dispositif mis en place, une description des éventuels dysfonctionnements, manquements à la réglementation ou mauvaises pratiques commerciales identifiés à travers les réclamations et des mesures correctives envisagées ou mises en œuvre.

3.3.2. De fixer les modalités de mise en œuvre, par les mandataires[16] et délégataires habituellement en relation avec la clientèle ou susceptibles de recevoir des réclamations, des bonnes pratiques visées aux points 3.2.1 et 3.2.2 et de s'assurer de l'effectivité de celles-ci.

3.3.3. Pour les entités tenues de se doter d'un contrôle interne, d'intégrer également dans les dispositifs mis en œuvre les bonnes pratiques issues de la présente recommandation ainsi que les risques liés à la protection de la clientèle identifiés à travers les réclamations[17].

La présente recommandation remplace la recommandation 2016-R-02 du 14 novembre 2016 modifiée le 6 décembre 2019 à compter du 31 décembre 2022.

Annexe Illustrations de la notion de réclamation.

[14] Y compris les réclamations adressées au professionnel portant sur la commercialisation d'un de ses produits ou services par un autre professionnel.
[15] Présence des informations visées au 3.1.1 (pour les accusés de réception), 3.2.3 et 3.2.4, clarté, caractère adapté au cas d'espèce, présence d'une argumentation pertinente et conforme aux dispositions applicables (légales, réglementaires, contractuelles)…
[16] Agent général, agent de prestataire de services de paiement, distributeur de monnaie électronique…
[17] Y compris si les dysfonctionnements, manquements à la réglementation ou mauvaises pratiques commerciales sont imputables, en tout ou partie, à l'action d'un tiers (exemple : intermédiaire, délégataire de gestion).

Mis en ligne le 17/05/2022

Annexe

Illustrations de la notion de réclamation

Les réclamations, qui se caractérisent par l'expression d'un mécontentement, peuvent porter sur des sujets très divers. Cette annexe a pour ambition d'aider les professionnels à mieux les identifier en donnant quelques exemples concrets[18] pour lesquels des difficultés d'identification ont pu être constatées. La liste des situations visées n'est donc pas exhaustive.

Est par exemple une réclamation, tout mécontentement[19] portant sur :

- Les communications publicitaires, notamment leur réception ;
- Une technique de vente (acte de démarchage) ;
- La qualité du consentement donné ou son absence ;
- La teneur d'un discours commercial ;
- La qualité d'accueil ;
- L'information précontractuelle ou le conseil, y compris si le produit ou service n'a pas été souscrit (absence, qualité) ;
- L'absence ou le délai de traitement[20] d'une demande d'informations ou de communication de documents ;
- La qualité d'une réponse apportée ;
- L'absence ou le délai d'exécution d'une opération ou de versement de prestations[21] ;
- Le refus d'octroi ou de souscription d'un produit ou service, y compris par une personne n'étant par ailleurs pas cliente du professionnel ;
- La tarification d'un produit ou service (niveau, information…), y compris lorsque le professionnel dispose d'une liberté tarifaire ;
- L'indemnisation (refus de garantie, montant des prestations annoncé ou versé…) ;
- Une expertise (choix de l'expert, délai de réalisation, conclusions…) ;
- L'absence de remise d'une attestation de refus d'ouverture de compte ;
- L'absence ou le délai de traitement d'une demande de résiliation/clôture.

En l'absence de tout mécontentement exprimé, les demandes suivantes ne sont pas des réclamations :

- Demande de geste ou remise commercial(e) ;
- Demande de communication de documents ;
- Demande d'exécution du contrat (demande d'opération, de prestation…) ;
- Demande d'information ou d'explications (clauses du contrat, fonctionnement du produit ou service, procédure pour souscrire ou mettre fin à un produit ou service, application de mesures gouvernementales…) ;
- Demande d'avis ou de conseil : de type juridique, sur ses droits, sur le choix d'un contrat en fonction d'une situation de famille.

[18] À cette même fin, les professionnels peuvent également se référer au questionnaire sur la protection de la clientèle et les pratiques commerciales ainsi qu'aux guides d'aide de remplissage associés.
[19] Même si le mécontentement est exprimé afin de signaler une pratique et que le réclamant ne sollicite pas une mesure en sa faveur.
[20] Une réclamation peut prendre la forme d'un courrier de relance.
[21] Une réclamation peut prendre la forme d'un courrier de relance.

Mis en ligne le 17/05/2022

Annexe 11 : Extraits de la recommandation du 16 mai 2023 de l'OSMP

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*.

Articles 12 : Articles du code de la consommation

Article L613-1
Le médiateur de la consommation accomplit sa mission avec diligence et compétence, en toute indépendance et impartialité, dans le cadre d'une procédure transparente, efficace et équitable.
Il établit chaque année un rapport sur son activité.
Il satisfait aux conditions suivantes :
1° Posséder des aptitudes dans le domaine de la médiation ainsi que de bonnes connaissances juridiques, notamment dans le domaine de la consommation ;
2° Etre nommé pour une durée minimale de trois années ;
3° Etre rémunéré sans considération du résultat de la médiation ;
4° Ne pas être en situation de conflit d'intérêts et le cas échéant le signaler.
Il est inscrit sur la liste des médiateurs notifiée à la Commission européenne.
Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat.

Article L613-2
Lorsqu'il est employé ou rémunéré exclusivement par le professionnel, le médiateur de la consommation satisfait aux conditions supplémentaires suivantes :
1° Il est désigné, selon une procédure transparente, par un organe collégial mis en place par l'entreprise, comprenant des représentants d'associations de défense des consommateurs agréées et des représentants du professionnel, ou relevant d'une instance nationale consultative dans le domaine de la consommation ou propre à un secteur d'activité dans des conditions fixées par décret ;
2° A l'issue de son mandat, le médiateur a l'interdiction de travailler pendant au moins trois ans pour le professionnel qui l'a employé ou pour la fédération à laquelle ce professionnel est affilié ;
3° Aucun lien hiérarchique ou fonctionnel entre le professionnel et le médiateur ne peut exister pendant l'exercice de sa mission de médiation. Le médiateur est clairement séparé des organes opérationnels du professionnel et dispose d'un budget distinct et suffisant pour l'exécution de ses missions.