RAPPORT d'ACTIVITÉ

du médiateur de la Consommation

du

CRÉDIT AGRICOLE CHARENTE PÉRIGORD

EXERCICE 2022

Rapport d'activité 2022
du médiateur de la consommation
du Crédit Agricole Charente Périgord

1/ Nom de l'établissement (et code interbancaire CIB) et période concernée

Caisse Régionale de Crédit Agricole de CHARENTE-PERIGORD
Code interbancaire : 12406
Période : **dossiers reçus et traités** par le médiateur entre le **1er janvier 2022 et le 31 décembre 2022**.

2/ Coordonnées du médiateur

- Adresse postale à laquelle les clients peuvent faire parvenir leurs réclamations

Monsieur le Médiateur du Crédit Agricole Charente Périgord
CS 72424 Soyaux
16024 ANGOULÊME CEDEX

- Site Web : https://www.lemediateur-ca-charente-perigord.fr/
- Adresse électronique : **mediateur.ca.charente.perigord@gmail.com**

3/ Évolution de l'activité

- Nombre de dossiers reçus en 2018 : 78
- Nombre de dossiers reçus en 2019 : 97
- Nombre de dossiers reçus en 2020 : 114
- Nombre de dossiers reçus en 2021 : 200
- **Nombre de dossiers reçus en 2022 : 161 (-20 %)**

4/ Activité du médiateur

Durée du mandat : 3 ans à compter avril 2016 - mandat renouvelé pour 3 ans en avril 2019 et renouvellement 2022.

Champ de compétence :
- Légal ☑
Force contraignante des avis
☑ Non

Procédure de traitement des réclamations (réception des demandes, processus de traitement des réclamations) :

- Réception directe des courriers ? Oui ☑

- Envoi d'un accusé de réception ? oui ☑

Délai moyen d'envoi de l'accusé de réception : 1,66 jour (fériés non neutralisés)

- Si le dossier est hors champ de compétence, transmission au service Réclamation : oui (si accord du client) ☑

En cas de réponse affirmative : - indiquer le nombre de dossiers concernés : 11

- Êtes-vous informé des suites données par ces derniers ? non ☑

Origine de la saisine (sur l'ensemble des demandes reçues) :

Origine de la saisine	Nombre de dossiers reçus concernés
Par le client	156
Par l'intermédiaire d'associations	3
Par l'intermédiaire d'un avocat ou d'un conseil	3
À l'initiative de l'établissement de crédit	0
Total	**162**

À noter que sur 156 demandes reçues des clients, 59 sont parvenues via le site Internet et 26 via un mail soit une courte majorité de saisines par voie électronique.

Nombre de réclamations reçues :

Réclamations	Nombre
Réclamations recevables traitées par le médiateur (entrant dans le champ de compétence et ayant suivi la procédure instaurée par l'établissement).	**111**
Réclamations dans le champ de compétence mais jugées irrecevables parce que les recours internes n'avaient pas été épuisés.	31
Réclamations que le médiateur a estimées hors du champ de sa compétence voir détail des motifs ci-après).	20
Total des réclamations reçues	**162**

Motifs invoqués pour les réclamations estimées hors du champ de compétence	Nombre de dossiers concernés
Absence de litige	**1**
Litige ne concernant pas la banque	**1**
Faits légalement prescrits	**4**
Action contentieuse en cours	**1**
Opération de crédit / Négo directe	**4**
Épargne	**1**
Assurances	**4**
Placements boursiers et financiers	
Politique tarifaire	
Surendettement	
Comptes professionnels	
Autres (Abandon) :	**4**

5/ Analyse par thèmes des réclamations

Thèmes	Nombre de dossiers reçus	Nombre de dossiers jugés recevables et traités par le médiateur
Fonctionnement du compte :	**9**	**3**
Ouverture, clôture, transfert de compte	2	1
Découvert autorisé/non autorisé	1	0
Interdiction bancaire		
Contestations d'écritures,…	6	2
Moyens de paiement :	**127**	**103**
Cartes bancaires (suppression des moyens de paiement, refus de délivrance, perte, vol, utilisation frauduleuse,…)	108	86
Chèques (suppression des moyens de paiement, refus de délivrance, utilisation frauduleuse, perte, vol, falsification,…)		
Autres moyens de paiement (virement, prélèvement,…)	19	17
Ventes avec primes		
Ventes groupées		
Tarification :	**2**	**0**
Tarification/fonctionnement de compte de dépôt	1	
Tarification/fonctionnement de compte titres		
Tarification/autres	1	
Opérations de crédit (refus d'octroi, rupture de crédit, échéances impayées, demande de renégociation,…)	7	**0**
Épargne (CEL, PEL, PEA, PEP, produits d'épargne réglementée…)	**3**	**2**
Placements financiers/boursiers (opérations sur titres, mauvaise exécution d'un ordre,…)	0	**0**
Assurances	**2**	**2**
Autres (investissement immobilier, successions)	**6**	**1**
Infondés, absence de litige ou litige commercial	**5**	**0**

Il y a une légère baisse des litiges liés à la fraude aux moyens de paiement : 127 contre 152 en 2021 mais seulement 65 en 2020 et 28 en 2019.

La mise en place de l'authentification forte en renforçant la matérialisation de l'autorisation a contraint les fraudeurs, en réalité les escrocs, à utiliser des méthodes de fraude sociale particulièrement traumatisantes pour des victimes souvent privées du remboursement en raison de leur imprudence avouée ou manifeste. Au cours de l'exercice, on a vu disparaître quasiment les fraudes par obtention frauduleuse du code 3DSécure et depuis mi-2021 la prédominance de fraudes par tromperie de la victime qui pense annuler une opération et la valide ou communique toutes les informations permettant un

enrôlement frauduleux avec l'apparition significative d'enrôlements frauduleux et de paiements Apple Pay ou Samsung Pay. Malgré le développement d'une communication grand public présentant régulièrement les méthodes de fraude, une partie de la clientèle se laisse encore piéger par des modes opératoires bien connus : Carte Vitale, Colis, écran bleu, acheteur le Bon coin ou autre, prélèvement rejeté.

6/ Analyse des réclamations traitées par le médiateur

*Cette partie du rapport concerne les réclamations traitées soit **109 dossiers** dont 4 dossiers 2021 en stock au 31 décembre 2021. Sur les 111 dossiers recevables 2022, 5 dossiers sont en attente au 31 décembre 2022.*

Délais de réponse :

	En jours	Nombre de dossiers concernés
Délai moyen de réponse	**19 jours**	109
Dossiers traités dans un délai de moins de 1 mois	**17 jours**	**95 soit 87 % des dossiers**
Dossiers traités dans un délai entre 1 et 2 mois	37 jours	12 soit 13 % des dossiers
Dossiers traités dans un délai de plus de 2 mois	0	0

NB : le délai est calculé à partir de la date de prise en charge et non de dossier complet. Le délai de réponse du médiateur est souvent impacté par le délai de réponse des clients à qui il faut demander de décrire **précisément** les circonstances de la fraude mais dans tous les cas le délai maximum de 90 jours n'a jamais été dépassé.

Nature des propositions de solution

Proposition de solution		Nombre de dossiers concernés
Propositions favorables au client	**Totalement favorable**	**2**
	Partiellement favorables	**40**
Propositions de solutions défavorables au client		**62**
Dossiers sans suite (abandon ou accord en cours de médiation)		**5**

Le taux de propositions partiellement ou totalement favorables aux clients n'est que de 38 % du fait de la prédominance des demandes liées aux fraudes aux moyens de paiement et comportant des indices manifestes d'une imprudence grave (phishing, etc..). De plus, la plupart des fraudes concernent des opérations parfaitement authentifiées (Sécuripass, Sécuricode).
Cependant, on est en présence de procédures d'enrôlement (Apple Pay, Samsung Pay) qui mériteraient d'être renforcées ou d'algorithmes du système de prévention qui pourraient quelquefois être plus pertinents. Par ailleurs, il est parfois difficile d'identifier la négligence grave du consommateur, ce qui, au cas par cas, conduit à des propositions partiellement ou totalement favorables aux clients.

Il ne serait pas pertinent d'établir une analyse des réclamations autres que fraudes au vu de leur faible nombre. Signalons, cependant l'utilité des bilans patrimoniaux lors de litiges portant sur la

commercialisation d'un produit d'épargne, support qui est privilégié pour apprécier la pertinence de la prescription.

Nombre de cas où l'avis du médiateur a été suivi par la banque.

Suivi des propositions de solution		Nombre de dossiers concernés
Avis du médiateur suivi par la banque	Totalement	72
	Partiellement	9
Avis du médiateur non suivi*		28

*Le tableau ci-dessus comptabilise la position de la banque. **Le cas le plus fréquent de désaccord avec la banque est lié à l'appréciation de la validité de l'authentification forte et de la gravité de négligence commise ou non par le client.**

La position des clients suite aux propositions du médiateur est difficile à évaluer. En effet, dans le cas où les propositions ne leur sont pas favorables, plus de la moitié des requérants ne fait pas connaître sa position. **Il y a cependant 15 cas de propositions totalement ou partiellement favorables aux clients qui ont été acceptées par les deux parties soit un taux d'accord de 40,5 %.**

Aspects financiers

	Montant du préjudice invoqué	Montant des rétrocessions et indemnisations
Minimum par dossier	100 €	61 €
Maximum par dossier	11 760 €	5 500 €
Moyenne	**1 471 €**	**1. 010€**

Quelques exemples de médiation

- Ventes sur Le bon Coin ou via les réseaux sociaux : Le vendeur propose un paiement par PayPal et via un faux site PayPal et un faux conseiller PayPal collecte les données bancaires et fait valider des paiements. La victime a malheureusement communiqué toutes les données personnelles et validé les paiements (croyant les annuler). Sauf circonstances particulières ou défaillances du système de surveillance de la banque, le remboursement ne pourra être proposé.
- Fraudes « à l'écran bleu », à la carte Vitale notoirement gratuite, aux droits de douane : le client communique toutes ses données bancaires et un faux conseiller obtient les codes manquants et l'authentification forte. S'il n'y a pas de dysfonctionnement dans les systèmes de prévention de la banque, le remboursement ne peut être défendu.
- Cas d'enrôlements Samsung Pay et Apple Pay reposant sur un simple SMS : l'authentification par simple SMS est jugée insuffisante bien qu'apparemment admise par les autorités monétaires. S'il n'y a pas négligence grave du client, il est proposé une prise en charge partielle.
- Fraudes au virement à partir de l'espace privé : s'il n'y a pas de preuves d'une négligence grave du client dans la protection de l'accès à son espace privé, en l'absence d'authentification forte du virement lui-même, il sera aussi proposé une prise en charge partielle ou totale.
- Sortie en capital d'un PER : la banque et le client ont sous-évalué des informations qui pouvaient

justifier la sortie en capital : un remboursement partiel des incidences fiscales indues a été obtenu.

7/ Appréciation d'ordre général sur l'évolution des litiges

- **Prédominance écrasante des litiges liés aux fraudes aux moyens de paiement (127/161 = 78 %)**
  - Augmentation inquiétante des accès frauduleux à l'espace privé et virements suite à réponse à des mails de phishing probables ou avoués sur la base de thèmes récurrents (Carte Vitale, Colis taxe, vente entre particuliers, prélèvement impayé).
  - Apparition d'enrôlement frauduleux à des moyens de paiement à distance s'appuyant sur les cartes bancaires (Apple Pay, Samsung Pay, Paylib, Lydia) avec de forts soupçons de présence de logiciels espions sur les smartphones (Androïd et IOS).
  - Paiements non initiés mais validés par la victime elle-même par Sécuripass et Sécuricode suite à fraudes « sociales » : faux policier, faux conseiller bancaire proposant l'annulation d'une ou plusieurs opérations frauduleuses.
  - Messages d'alerte fraude émis par la banque rendus inopérants par la manipulation des victimes.
  - Peu de litiges liés à des paiements non authentifiés.
  - Outre les sites opérant sur les crypto monnaies, apparition de sites de jeux ou paris en ligne destinataires des fonds détournés.

- **Ressenti des clients :**

  En cas « d'arnaque » les clients voient dans les banques une sorte d'assurance « tous risques » et attendent un remboursement automatique y compris pour des arnaques sur des sites de vente entre particuliers ou commerçants fantômes.

  Les conséquences d'une imprudence grave (communication involontaire de données de sécurité, mauvaise utilisation du moyen de paiement ou de validation), parfois difficile à matérialiser, mais prévues au Code Monétaire et financier, sont mal acceptées par les clients au demeurant de bonne foi. À noter aussi, une large surestimation des capacités assurantielles des cartes bancaires et déception supplémentaire des victimes.

  Le dépôt de plainte n'est pas toujours accepté et les suites données par la justice rarement perçues par les victimes.

- **Qualité de l'information sur l'existence du médiateur**

  - Communication au verso du relevé de compte adressé aux clients et dans les conditions générales.
  - Page Internet accessible aux clients sur le site de la Banque.
  - Site internet du médiateur.
  - Affichage dans tous les lieux d'accueil des clients.
  - Information sur les réponses aux réclamations.

8/ Propositions et suggestions

Sur le fonctionnement de la médiation :

20 % des saisines sont encore irrecevables (% en baisse) en l'absence de saisine préalable du service réclamations de la banque ou hors champ. **La situation s'améliore nettement**.

L'envoi simultané des propositions de solution aux deux parties et le recueil de chaque avis sont en pratique peu pertinents quand l'avis du médiateur est défavorable au consommateur. Il serait plus

simple de ne demander l'accord du client que lorsque la proposition de solution lui est favorable et la banque d'accord.

Sur les dossiers traités :
La sécurisation des moyens de paiements électroniques profite essentiellement aux commerçants en ligne (et aux fraudeurs) sûrs d'être payés en cas d'authentification forte.
Par contre, l'authentification forte a contraint les fraudeurs à trouver des moyens pour obtenir l'accès aux outils de validation d'où le fort développement de la fraude « sociale » et un ressenti des fraudes plus violent pour les consommateurs qui portent dorénavant un peu plus la responsabilité de l'authentification forte.
La réaction première de nombreux clients est de mettre en doute la sécurité du système informatique bancaire alors que le point faible est souvent, hélas, l'utilisateur qui malgré les campagnes d'information (encore insuffisantes) maîtrise imparfaitement le système de paiement à distance et les règles élémentaires de prudence sur internet.

Sur la prévention de fraudes
Il faut poursuivre l'information des usagers par tous moyens et rappeler leurs responsabilités dans l'usage des systèmes d'authentification. La typologie des victimes montre une majorité de personnes utilisant peu les paiements à distance et donc moins au fait des risques mais il y a aussi des utilisateurs assidus d'internet.
Deux catégories de clients me paraissent oubliées de la communication relative à la sécurité des moyens de paiement : ceux qui sont restés fidèles au relevé de compte papier et reçoivent peu d'informations et ceux qui n'utilisent que leur smartphone. Les smartphones se prêtent mal à une information complexe mais des développements récents vont dans le bon sens.
Cependant, la facilité d'utilisation du smartphone et en particulier des validations par empreinte digitale ou reconnaissance faciale a un effet pervers car elle réduit le temps de réflexion et c'est justement ce que cherche le faux conseiller qui manipule la victime.

On pourrait aussi insister sur la protection des outils informatiques et de la téléphonie (y compris du compte chez l'opérateur téléphonique) qui interviennent dans l'installation des systèmes d'authentification forte, protection totalement absente ou insuffisante dans l'immense majorité des dossiers de fraude d'où les interceptions de codes SMS d'activation inexpliquée. Certes, ces sécurités sont inopérantes face à la fraude « sociale ».
Par ailleurs, les fraudeurs opérant à toute heure, les banques devraient développer un service permanent permettant de bloquer les opérations de virement faites à partir de l'espace privé à l'instar de ce qui existe pour les cartes bancaires (SOS Cartes).
Il serait aussi urgent que les autorités monétaires prennent en compte la multiplication des initiateurs de paiement (fabricants de téléphones, néo banques, etc..) et durcissent les conditions d'enrôlement de cartes bancaires et d'ouverture des comptes à distance. En effet, les enrôlements via l'application de la banque sont plus robustes que ceux acceptés par certains opérateurs non-banquiers. De plus, l'installation des cartes bancaires sur smartphone permet la multiplication de cartes virtuelles ce qui semble contraire à la notion de carte personnelle et unique.

Sur la réponse sociétale.

Enfin, je regrette une nouvelle fois, une absence de réponse pénale visible pour les victimes, absence de réponse alimentée par le refus fréquent de la police et de la gendarmerie de recueillir des dépôts de plainte.

D'une part, cela entretient le public dans l'idée que les fraudes aux moyens de paiement sont d'abord des dysfonctionnements du système bancaire, et, que les banques doivent en assumer toutes les conséquences, ce qui revient à nier la réalité criminelle de ces activités alors qu'il s'agit bien d'escroqueries caractérisées.

D'autre part, le questionnement détaillé des victimes permettrait d'identifier au moins en France des sites commerciaux voire des banques qui hébergent des comptes clients douteux, de repérer des sites qui fournissent des services de mailing frauduleux, de découvrir les filières de revente des biens acquis frauduleusement et de mieux connaître les modes opératoires pour mieux informer le public.

Face à la demande clairement exprimée d'un remboursement automatique des fraudes, on peut se demander si cela ne conduirait pas les banques à financer à l'infini la cybercriminalité ?

On peut aussi s'interroger sur la responsabilité de sites commerciaux qui profitent des achats frauduleux et ne sont pas organisés pour bloquer les opérations de livraison ou annuler les commandes quand les fraudes sont rapidement détectées. Cependant, très rares sont les victimes qui pensent à contacter les sites bénéficiaires et il semble que la transformation des produits des fraudes en bien matériels régresse au profit d'opérations purement financières. Un point particulier d'étonnement : la possibilité de paris en ligne à haute fréquence (toutes les minutes) sans authentification quelconque !

Enfin s'agissant de virements frauduleux, la demande de retour des fonds devrait être rapide et systématisée bien qu'il ne faille pas en espérer grand-chose d'autant plus que le développement du virement instantané va encore réduire les possibilités.

Enfin on pourrait s'interroger sur la nécessité de mettre en place une réponse assurantielle. Le risque vol est en général assurable. Par contre, le vol de la monnaie scripturale ou électronique ne l'est pas. D'un côté, les pouvoirs publics estiment que le risque de cybermalveillance est assurable pour les entreprises, d'un autre des assureurs de renom estiment le contraire. Un positionnement clair du législateur serait le bienvenu ce qui ne résoudrait pas pour autant les difficultés de gestion d'une telle assurance (maîtrise du risque, preuves, etc..).

Soyaux le 6 février 2023.

André LANDEZ
Médiateur de la consommation
du Crédit Agricole Charente Périgord