



Grenoble/Voiron

24 bis rue Mallifaud, 38100, Grenoble

Le 22/10/2020

## **COMMUNIQUÉ DE PRESSE Fraude à la carte bancaire et crise sanitaire**

### **Les consommateurs font toujours plus les frais de fraudes**

**Alors que les paiements par carte bancaire « sans contact » et par Internet se sont imposés avec la crise sanitaire comme des mesures barrières pour freiner la progression de la Covid-19, l'UFC-Que Choisir rend publique une enquête exclusive<sup>1</sup> qui montre que 30 % des fraudes ne sont pas remboursées par les banques. En conséquence, et devant le risque accru d'escroqueries, l'association saisit les pouvoirs publics pour obtenir enfin le plein respect des droits des consommateurs. Parallèlement, elle met à leur disposition des outils pour les accompagner dans leurs démarches pour se faire rembourser.**

#### **Fraude à la carte bancaire : une explosion à venir avec la crise sanitaire**

La fraude bancaire, qui consiste à débiter les comptes des consommateurs en détournant leurs moyens de paiement, a de beaux jours devant elle avec la crise. Inquiets quant aux risques sanitaires, les Français se sont reportés vers des moyens de paiement dématérialisés pour régler leurs dépenses, comme le montre la progression du paiement « sans contact » (+ 67 %) ou à distance (+ 13 %) depuis le déconfinement<sup>2</sup>.

Ces nouvelles habitudes ne sont pas sans danger. En effet, elles sont respectivement deux et dix-sept fois plus fraudées que les transactions avec composition du code secret<sup>3</sup>. En conséquence, ces escroqueries pourraient bondir de l'ordre de 20 % pour atteindre plus de 660 millions d'euros en 2020 selon l'estimation de l'UFC-Que Choisir<sup>4</sup>.

#### **Enquête UFC-Que Choisir : 30 % des fraudes non remboursées**

Alors que les banques sont en retard pour la sécurisation des transactions à distance<sup>5</sup>, notre nouvelle enquête<sup>6</sup> pointe des manœuvres pour échapper à leur obligation de rembourser les sommes dues aux victimes. Il en ressort ainsi que près d'une personne fraudée sur trois n'a pas été remboursée cette année (30 %, + 4 points). Avec comme premier motif opposé aux consommateurs, les accusations de négligence.

Dans la grande majorité des cas<sup>7</sup>, cet alibi ne tient pourtant pas la route. En raison des risques de détournements du seul code SMS (3D-Secure) pour authentifier les paiements à distance, ce dispositif n'est plus considéré comme étant suffisamment sécurisé. Par conséquent, comme l'a confirmé le Gouverneur de la Banque de France<sup>8</sup> à la demande de l'UFC-Que Choisir, les banques qui continuent de n'utiliser que cette seule technique obsolète ne peuvent plus invoquer la négligence de leurs clients pour refuser de les rembourser. Les consommateurs n'ont pas à payer au nom du retard technologique de leur banque !

L'étude montre également la persistance de pratiques qui visent à décourager les consommateurs dans leurs démarches. A cet égard, plus d'un sondé sur quatre (26 %) a dû se plier à une kyrielle de formalités pour démontrer sa bonne foi (dépôt de plainte, rédaction d'une lettre de contestation, envoi d'une copie du relevé de compte, etc.). En conséquence, au sein de notre échantillon, le délai moyen de remboursement s'allonge de quatre jours pour atteindre 25 jours, un comble alors qu'il devrait intervenir, selon la loi, au plus tard le premier jour ouvré suivant le signalement de la fraude !

<sup>1</sup> Résultats détaillés dans le numéro *Que Choisir* 596 en kiosque le 22 octobre 2020.

<sup>2</sup> Présentation du 4<sup>ème</sup> rapport annuel de l'Observatoire de la sécurité des moyens de paiement (OSMP), Banque de France.

<sup>3</sup> Le taux de fraude des paiements par carte bancaire avec composition du code serait est de 0,01 %. Il atteint 0,019 % pour le paiement sans contact et 0,17 % pour les paiements à distance. Rapport annuel 2019 de l'OSMP, 2020.

<sup>4</sup> Estimation à taux de fraude et volume de paiement global constants à partir des statistiques du Rapport annuel 2019 de l'OSMP.

<sup>5</sup> Depuis le 14 septembre 2019, les consommateurs devraient, en principe, pouvoir utiliser un dispositif d'authentification renforcée pour utiliser leurs moyens de paiements à distance. C'est-à-dire valider leurs transactions à l'aide d'au moins deux des trois facteurs suivants, à savoir : quelque chose qu'ils connaissent (un mot de passe, par exemple), quelque chose qu'ils possèdent (une carte bancaire) et / ou une caractéristique personnelle (une empreinte digitale).

<sup>6</sup> Enquête réalisée entre le 2 et le 9 septembre 2020 auprès de 1535 consommateurs victimes de fraude au cours des douze derniers mois abonnés à la newsletter de l'UFC-Que Choisir.

<sup>7</sup> D'une part, moins d'un consommateur sur deux (46 %) est équipé d'un dispositif d'authentification forte à juillet 2020. D'autre part, le taux de fraude des transactions authentifiées est bien moins élevé. Il était quatre fois plus faible que pour les transactions non authentifiées en 2018.

<sup>8</sup> Réponse à sa saisine suite au communiqué de presse de l'UFC-Que Choisir, « *Fraude bancaire : Pas de report pour rembourser les consommateurs* » de septembre 2019.



Grenoble/Voirion

24 bis rue Mallifaud, 38100, Grenoble

Le 22/10/2020

### **Paiement par carte bancaire « sans contact » : un risque à maîtriser d'urgence**

L'analyse des statistiques de la Banque de France permet enfin de mettre en évidence les fraudes liées au « sans contact ». A l'occasion du déconfinement, les consommateurs se sont vu imposer une augmentation systématique du plafond du paiement « sans contact » à 50 euros, sans pouvoir s'y opposer. Pourtant, la sécurité de cette technologie est préoccupante puisqu'elle expose à des fraudes plus nombreuses et de montants plus élevés. Pire, faire opposition à sa carte bancaire en cas de vol ne permet pas d'y échapper. En effet, tant que le plafond de paiements sans contact successifs n'est pas atteint (jusqu'à cinq opérations ou un montant cumulé de 150 euros), cette fonction demeure utilisable, puisque le code secret n'est pas demandé et que la carte n'a pas à se connecter au réseau de la banque émettrice. Il est dès lors indispensable de rendre aux consommateurs le contrôle sur ce mode de paiement.

**Mobilisée au côté des consommateurs durant la crise sanitaire, notamment pour leur permettre de régler leurs dépenses en toute sécurité, l'UFC-Que Choisir :**

- Rappelle qu'elle met à leur disposition, en libre-accès, un [arbre décisionnel](#) quant à la conduite à tenir en cas de fraude, deux lettres types de réclamation « [Fraude à la carte bancaire - Contestation de l'utilisation d'un code 3d Secure](#) » ainsi que « [Fraude à la carte bancaire - Demande de remboursement](#) » et que son [réseau d'associations locales](#) peut les accompagner ;
- Encourage les victimes à lui signaler toutes fraudes non-indemnisées à l'adresse [fraudebancaire@quechoisir.org](mailto:fraudebancaire@quechoisir.org) ;
- Saisit l'Autorité de contrôle prudentiel et de résolution (ACPR) sur l'explosion des non-remboursements injustifiés pour qu'elle s'assure du strict respect de la réglementation anti-fraude ;
- Exhorte les pouvoirs publics à adopter un cadre juridique garant des droits des consommateurs qui impose de sanctionner les manœuvres dilatoires des banques.