OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2020

BANQUE DE FRANCE
EUROSYSTÈME

www.observatoire-paiements.fr

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2020

Adressé à
Monsieur le ministre de l'Économie, des Finances
et de la Relance
Monsieur le président du Sénat,
Monsieur le président de l'Assemblée nationale

par François Villeroy de Galhau,
gouverneur de la Banque de France,
président de l'Observatoire de la sécurité
des moyens de paiement

JUILLET 2021

SOMMAIRE

SYNTHÈSE

Dans un contexte de crise sanitaire qui a profondément marqué l'année 2020, l'Observatoire de la sécurité des moyens de paiement a été le témoin privilégié de son impact tant sur les habitudes de paiement des ménages et des professionnels français que sur l'évolution des modes opératoires des fraudeurs. Ce rapport annuel 2020 rend compte des tendances observées du fait de la crise, ainsi que des actions engagées par l'Observatoire pour préserver un haut niveau de sécurité et de confiance dans les moyens de paiement scripturaux.

Le ***chapitre 2*** *du rapport présente* ***les évolutions des flux de paiement et de la fraude aux moyens de paiement en 2020****. Il souligne notamment l'accélération du mouvement de digitalisation des paiements du fait de la crise, qui s'illustre :*

- *d'une part, par un recul très net, à compter du confinement de mars 2020, des opérations impliquant un contact physique : chèques (– 25 % en valeur), retraits d'espèces (– 15 % en valeur), paiements par carte avec saisie du code confidentiel ont ainsi enregistré une baisse de leurs flux inédite par rapport à leurs tendances historiques ;*

- *d'autre part, une croissance sans précédent de deux usages : le paiement sans contact (+ 86 % en valeur) qui s'est imposé comme le moyen de paiement privilégié au point de vente et a pleinement profité de l'élévation du plafond de paiement de 30 à 50 euros le 11 mai 2020 ; et le paiement sur Internet (+ 8 % en valeur) porté notamment par l'évolution du commerce de proximité traditionnel vers de nouveaux modes de consommation (livraison à domicile,* click and collect, *etc.).*

Ce chapitre montre également qu'en dépit de l'incidence de la crise sanitaire sur les pratiques de paiement, le niveau de la fraude observé sur les paiements émis en France reste maîtrisé, à l'exception notoire du chèque dont le taux de fraude progresse sensiblement.

- *Pour la troisième année consécutive, le chèque reste le moyen de paiement le plus fraudé tant en montant qu'en proportion. En effet, malgré la baisse de son usage en 2020, sa part dans les montants fraudés de l'ensemble des moyens de paiement reste la plus élevée à 42 %, pour 538 millions d'euros, et son taux de fraude progresse à 0,088 %, représentant l'équivalent d'un euro de fraude pour 1 100 euros de paiement. Le vol de chèques et de chéquiers demeure toujours le principal mode opératoire avec une part prépondérante des montants fraudés à 68 %, en nette progression sur un an (55 % en 2019).*

- *Le taux de fraude sur les cartes de paiement françaises se maintient à un niveau globalement maîtrisé à 0,068 %, soit l'équivalent d'un euro de fraude pour 1 500 euros d'opérations, en dépit du report massif des flux vers des types de transactions plus sensibles au risque de fraude, comme le paiement sans contact (dont le taux de fraude baisse à 0,013 % malgré l'augmentation du plafond de paiement et se rapproche du taux de fraude sur les paiements avec saisie du code confidentiel) et le paiement à distance (taux de fraude quasi stable à 0,174 %).*

- *Si le taux de fraude sur les virements reste particulièrement faible à 0,0008 % (soit un euro de fraude pour 120 000 euros de paiement), l'Observatoire souligne toutefois la recrudescence des fraudes par ingénierie sociale ciblant principalement les entreprises. En effet, le renforcement des échanges digitaux et la pratique généralisée du télétravail, occasionnant une perte des repères habituels pour les services comptables et financiers, ont été propices à la mise en œuvre de ce type de fraude. Par ailleurs, les administrations publiques ont également été confrontées au développement d'une fraude visant le dispositif d'activité partielle des entreprises, basée sur*

l'usurpation de l'identité d'entreprises bénéficiaires pour détourner les aides financières mises en place dans le cadre de la crise de la Covid-19.

- *La fraude sur les prélèvements se réduit fortement, à 1,9 million d'euros en 2020 (– 83 % sur un an). Son taux de fraude s'établit ainsi au niveau le plus faible de l'ensemble des moyens de paiement, à 0,0001 %, soit l'équivalent d'un euro de fraude pour un million d'euros de paiement.*

*Le **chapitre 1** dresse le **premier bilan de la migration de la Place française vers l'authentification forte du porteur pour les paiements par carte sur Internet**. Cette évolution apparaît d'autant plus nécessaire qu'elle intervient dans un contexte de renforcement d'accroissement de ce mode de paiement, lequel concentre plus des deux tiers de la fraude alors qu'il ne représente que 22 % des transactions.*

Si la mise en œuvre du plan de migration établi par l'Observatoire a dû être aménagée pour tenir compte des contraintes sanitaires, avec notamment l'octroi d'une période de flexibilité de trois mois accordée mi-2020, la situation à fin juin 2021 met en évidence un haut niveau de conformité de la Place française :

- *Plus de 80 % des porteurs de cartes réalisant des achats sur Internet ont été enrôlés dans un dispositif d'authentification forte qu'ils utilisent pour valider leurs transactions. Les actions entreprises par la Banque de France et l'Autorité de contrôle prudentiel et de résolution auprès des établissements les moins avancés devraient permettre d'atteindre une pleine conformité à l'automne 2021.*

- *Environ 95 % des flux des e-commerçants français sont conformes à la réglementation, c'est-à-dire qu'ils font appel à une demande d'authentification de leur client ou bénéficient d'une exemption reconnue valide par l'émetteur de la carte.*

Ces résultats sont le fruit du travail de coordination conduit dans le cadre de l'Observatoire, qui s'est attaché à assurer une migration ambitieuse tout en préservant l'activité du e-commerce, dans un environnement fortement contraint par la crise sanitaire. Ils permettent de valider la fin du plan de migration de Place, étant entendu que l'Observatoire continuera à piloter attentivement les suites de celui-ci en vue d'assurer à court terme la pleine conformité du marché français tout en renforçant le bon fonctionnement des paiements sur Internet.

*Le **chapitre 4** rend compte des travaux conduits par l'Observatoire afin de **renforcer la sécurité des paiements par chèque**. Ils ont permis de mieux identifier les principales vulnérabilités de ce moyen de paiement exploitées par les fraudeurs, et de définir un ensemble d'objectifs de sécurité à même de les prévenir. Ces objectifs s'articulent notamment autour du renforcement par les établissements bancaires de la capacité d'analyse et des dispositifs de prévention de la fraude, du développement de la coopération entre les acteurs de la filière et, enfin, de la sensibilisation des utilisateurs.*

L'Observatoire s'attachera à suivre la mise en œuvre de ces objectifs par les acteurs de marché et à évaluer sur la durée leur efficacité au regard des évolutions de la fraude annuelle sur ce moyen de paiement.

*Enfin, le **chapitre 3** rend compte des **travaux de veille sur la sécurité des paiements en temps réel**, dans un contexte où l'usage du virement instantané, bien qu'encore limité (1 % des virements émis en nombre en 2020), tend à se développer avec des flux multipliés par trois en un an. Si ces paiements offrent un plus grand confort aux utilisateurs par la mise à disposition immédiate des fonds, ils nécessitent une gestion de la sécurité adaptée aux enjeux du temps réel.*

L'Observatoire recommande ainsi la mise en place d'un ensemble de mesures de prévention de la fraude au moment de l'initiation du paiement, associant à l'exigence d'authentification forte du payeur prévue par la règlementation, la mise en place de plafonds de paiement adaptés à l'usage du client, ainsi que d'outils d'identification en temps réel des transactions présentant un niveau de risque élevé. L'Observatoire rappelle également le rôle important joué par le comportement des utilisateurs pour assurer la sécurité de leurs moyens de paiement, et invite les acteurs du marché à conduire des actions de sensibilisation appropriées lors de la mise à disposition de solutions de paiement instantané.

1

PREMIER BILAN DU DÉPLOIEMENT DE L'AUTHENTIFICATION FORTE DU PAYEUR POUR LES PAIEMENTS PAR CARTE SUR INTERNET

1.1 Le plan de déploiement de l'authentification forte des paiements sur Internet

Le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique est une disposition clé en matière de sécurité des paiements introduite par la deuxième directive européenne sur les services de paiement (DSP 2). Si cette directive est en vigueur depuis le 13 janvier 2018, différents textes de second niveau émis par l'Autorité bancaire européenne (ABE, *European Banking Authority* – EBA) ont clarifié les règles applicables aux transactions par carte sur Internet :

- les normes techniques de réglementation relatives à l'authentification forte (RTS SCA [1]), qui ont précisé les conditions de mise en œuvre de cette dernière, devaient entrer en application le 14 septembre 2019 ;
- l'avis du 16 octobre 2019 (EBA-OP-2019-11) actait la nécessité de laisser aux acteurs de marché, sous la responsabilité des autorités nationales, un délai additionnel courant jusqu'au 31 décembre 2020 pour se conformer aux dispositions régies par les normes précitées ; ce délai était complété par une phase de bilan à conduire au premier trimestre 2021.

Dans ce contexte, l'Observatoire a élaboré un plan de migration pour la Place française, document dont la version finale a été publiée le 30 octobre 2019 sur son site Internet [2]. Toutefois, la survenance au printemps 2020 de la crise sanitaire liée à la pandémie de Covid-19 a conduit l'Observatoire à y intégrer des mesures d'assouplissement et en particulier à prévoir une marge de flexibilité de trois mois supplémentaires.

1.1.1 Le plan de migration de la Place française

Le plan de migration vers l'authentification forte des paiements validé par l'Observatoire comporte deux volets :

- un volet à l'attention des consommateurs : l'enrôlement des porteurs de carte dans des dispositifs d'authentification conformes à la définition de l'authentification forte de la DSP 2, en remplacement de l'usage du code SMS à usage unique (ou SMS OTP – *one time password*) comme facteur unique d'authentification ;
- un volet à l'attention des acteurs professionnels de la chaîne des paiements, y compris les e-commerçants : la mise à niveau des infrastructures d'authentification afin d'assurer la gestion des règles de responsabilité et des cas d'exemption d'authentification forte prévus par la directive.

Ces deux volets ont fait l'objet d'indicateurs de suivi assortis de cibles et d'échéances, ainsi que de plans d'actions visant à accompagner la mise en conformité de la Place française.

1 *Regulatory technical standard on strong customer authentication and common and secure communication.*

2 Cf. *https://www.banque-france.fr/sites/default/files/medias/documents/2019-10-30_-_osmp_-_plan_de_migration_dsp2.pdf*

1.1.2 Les solutions d'authentification forte du porteur

L'authentification forte repose sur l'utilisation de deux éléments ou plus appartenant aux moins à deux catégories différentes de facteur d'authentification, parmi les trois catégories suivantes :

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

La DSP 2 prévoit que ces éléments doivent être indépendants : la compromission de l'un ne doit pas remettre en question la fiabilité des autres, de manière à préserver la confidentialité des données d'authentification. En outre, concernant les paiements à distance, la DSP 2 ajoute un requis supplémentaire : les données d'authentification doivent être liées à l'opération de paiement, de sorte qu'elles ne peuvent être réutilisées pour une opération de paiement ultérieure :

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

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

T1 Les principales solutions d'authentification forte pour les paiements par carte sur Internet

Combinaison de facteur(s) d'authentification	Connaissance	Inhérence
Possession	Saisie d'un code confidentiel dans l'application bancaire sécurisée du porteur ou Saisie d'un code à usage unique transmis par SMS ou par serveur vocal + saisie d'un code confidentiel ou Saisie d'un code confidentiel sur un boîtier fourni par la banque	Lecture d'une empreinte biométrique dans l'application bancaire sécurisée du porteur

Source : Observatoire de la sécurité des moyens de paiement.

1.1.3 Le rôle des commerçants dans la migration

Dans le contexte antérieur à la DSP 2, les commerçants qui acceptaient des paiements par carte en ligne avaient la faculté de recourir à un paiement sécurisé en choisissant d'activer le protocole 3D-Secure Ils n'étaient toutefois pas tenus de justifier leur choix quand ils ne demandaient pas l'authentification de leur client. Ce mode d'activation « à la main du commerçant » n'est plus autorisé ; en effet, la nouvelle réglementation change les règles de décision en matière d'authentification :

- les commerçants doivent désormais recourir à une authentification forte, et ce à chaque paiement accepté sur Internet, sauf en cas d'exemption applicable ;
- l'activation d'un des cinq motifs d'exemption prévus par les textes pour fluidifier le parcours de paiement et tenir compte de niveaux de risques différenciés peut être sollicitée par le commerçant, mais reste soumise à l'accord de la banque émettrice de la carte.

Les commerçants qui acceptent des paiements par carte sur Internet ont ainsi été invités à se rapprocher de leur banque et, le cas échéant, de leur prestataire technique d'acceptation, afin de préparer ces évolutions, en particulier :

- vérifier que leur contrat d'acceptation des paiements en ligne prévoit bien la possibilité de recourir au protocole 3D-Secure ;
- s'assurer de leur capacité technique à émettre des paiements via 3D-Secure ;
- veiller à une utilisation croissante de ce protocole qui permette d'assurer la continuité de leur activité, en particulier dans la perspective de l'abaissement programmé des seuils de rejet des transactions non conformes (ou *soft declines*), et de faciliter, avec la version 2 du protocole 3D-Secure, la capacité à recourir aux exemptions pour les commerçants qui le souhaiteraient.

De façon symétrique, les professionnels du marché des paiements ont été invités par l'Observatoire à se rapprocher de leur clientèle de commerçants afin de les sensibiliser à ces nouvelles exigences et de les accompagner dans ces évolutions.

1.2 Les actions d'accompagnement de la migration

Afin de stimuler et de guider la migration de l'ensemble des acteurs de la Place française, l'Observatoire avait prévu dans sa feuille de route plusieurs actions d'accompagnement, prévues dans le plan initial ou dans les compléments apportés en septembre 2020.

1.2.1 La clarification des règles applicables aux différentes catégories de transactions

En matière de paiements par carte à distance, la réglementation prévoit différentes qualifications, qui déterminent l'obligation d'application ou non de l'authentification forte :

- Les **transactions initiées électroniquement par le client** (*customer initiated transaction* – CIT) correspondent aux paiements effectués par le porteur de la carte sur Internet, que ce soit au travers d'un navigateur ou d'une application. Ces transactions sont visées par l'obligation d'authentification forte du porteur, mais peuvent toutefois faire l'objet d'une exemption prévue par les RTS dès lors que les conditions d'application de celle-ci sont réunies *(cf. ci-après)*.
- Les **transactions initiées électroniquement par le commerçant** (*merchant initiated transaction* – MIT) correspondent aux opérations initiées par le commerçant sans présence active du porteur de la carte, dans des situations où l'émission du paiement est dissociée de l'engagement à payer, par exemple : dans le cas d'un abonnement, d'un paiement en plusieurs fois, d'un service payé en fonction de la consommation (abonnement modulable, réservation d'un moyen de transport, etc.), de paiements exécutés en plusieurs fois au moment de la livraison des différents éléments d'un panier d'achat, ou encore de frais de garantie de réservation payables en cas de non présentation du client. Ces transactions, généralement émises en-dehors de la présence active du client sur le site du commerçant, ne sont pas soumises à l'obligation d'authentification forte du porteur, mais doivent comporter la trace d'une authentification forte réalisée au moment de l'engagement à payer du client (selon un processus dit de « chaînage » des transactions). Cet engagement, correspondant à un « mandat MIT », doit préciser les conditions de règlement auxquelles s'engage le client (montant, nombre d'opérations, périodicité, durée de validité).
- Les **transactions à distance émises par un canal non électronique** (*mail order/telephone order* – **MOTO**), qui correspondent aux transactions pour lesquelles les données de carte ont été transmises par le porteur via un canal ne permettant pas leur traitement automatique (par exemple par courrier, fax, courriel, appel téléphonique ou serveur vocal), et dont la saisie à des fins de paiement est assurée par le commerçant. Ces transactions sont exclues du périmètre de la DSP 2 et ne sont pas soumises à l'exigence d'authentification forte du porteur.
- Les **transactions effectuées avec des instruments de paiement anonymes**, notamment des cartes prépayées anonymes, ne sont pas soumises à l'obligation d'authentification forte du porteur.
- Les **transactions dites « *one-leg* » pour lesquelles l'émetteur de la carte ou l'acquéreur de la transaction n'est pas localisé dans l'Espace économique européen**, qui ne peuvent pas toujours être authentifiées et pour lesquelles l'authentification forte est seulement requise sur une base du meilleur effort (« *best effort* »).

Dans le cas des transactions de type CIT initiées par carte sur Internet, **cinq motifs d'exemption d'authentification** forte sont prévus par les RTS :

- **Les paiements de faible valeur** (article 16) : cette exemption porte sur les paiements d'un montant unitaire d'au plus trente euros, et est applicable dès lors que le montant cumulé des dernières opérations consécutives exemptées à ce titre au moyen d'une carte donnée ne dépasse pas cent euros ou que leur nombre n'excède pas cinq opérations. Le fonctionnement de cette exemption est similaire avec celui du paiement sans contact pour les règlements au point de vente (prévu à l'article 11, avec des plafonds plus élevés).
- **Les paiements présentant un faible niveau de risque** (article 18) : cette exemption porte sur les opérations reconnues par le commerçant et/ou par la banque du porteur et/ou par la banque du commerçant comme présentant un niveau de risque réduit, au motif que les paramètres de la transaction correspondent aux habitudes de paiement du porteur (achat depuis son terminal habituel, adresse de livraison connue, nature de l'achat, montant, etc.).
- **Les paiements récurrents** (article 14) : cette exemption porte sur les paiements d'un montant et d'une périodicité fixes, à compter de la deuxième transaction. Cette exemption présente toutefois un intérêt limité pour les paiements par carte, dont les opérations au-delà de la souscription sont initiées par le commerçant (de type MIT).
- **Les paiements vers un bénéficiaire de confiance** (article 13) : cette exemption porte sur les paiements à destination d'un bénéficiaire qui aurait été désigné comme de confiance par le porteur de la carte. Dans ce cas, l'opération d'enregistrement du bénéficiaire de confiance doit elle-même faire l'objet d'une authentification forte du porteur de la carte.
- **Les paiements initiés électroniquement via des processus ou protocoles de paiement sécurisés réservés à un usage entre professionnels** (article 17) : le recours à cette exemption nécessite une évaluation préalable des processus et des protocoles par l'autorité nationale compétente (en France, par la Banque de France) visant à assurer que le niveau de sécurité offert est au moins équivalent à celui d'une authentification forte.

La DSP 2 prévoit qu'il appartient à l'établissement teneur de compte du porteur de protéger ce dernier contre la fraude. Cette disposition implique que l'application d'une exemption ne peut être tenue de façon certaine pour acquise : même si une transaction répond aux critères d'éligibilité du point de vue du bénéficiaire, la banque du porteur peut rejeter son application dès lors qu'elle identifie un risque aggravé pour son client, et alors demander une authentification forte pour sécuriser l'opération.

L'Observatoire s'est attaché à s'appuyer sur ces règles de qualification pour déterminer les conditions de mise en place de l'authentification forte pour certains cas d'usage particuliers, récapitulées dans le tableau 2.

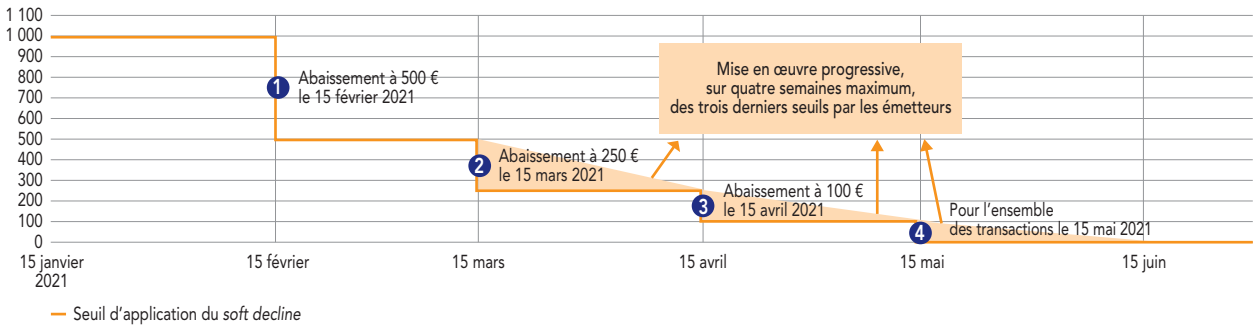
T2 Conditions de mise en place de l'authentification forte pour les cas particuliers

Cas d'usage	Description	Qualification et exigences associées
Paiement « *one-click* »	Paiement initié en ligne par le porteur, à l'achat d'un service ou d'un bien physique ou numérique, à l'aide d'une carte enregistrée dans l'espace client (« *card on file* »).	Transaction initiée par le client (CIT) qui nécessite une authentification forte sauf en cas d'applicabilité d'une des cinq exemptions prévues par les RTS. L'enregistrement de la carte dans l'espace client doit faire l'objet d'une authentification forte systématique au titre des actions susceptibles de comporter un risque de fraude.
Paiement(s) à l'expédition ou différé(s)	Paiement(s) lié(s) à une commande en ligne et faisant l'objet d'un différé (précommande, paiement à l'expédition, etc.).	Au moment de l'achat, obligation d'authentification forte (CIT) sauf en cas d'applicabilité d'une des cinq exemptions prévues par les RTS. L'authentification au moment de l'achat doit correspondre à la totalité du panier. Au moment de l'expédition, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chaînage).
Transactions récurrentes ou échelonnées	Série de paiements liée à un abonnement souscrit en ligne ou un paiement en plusieurs fois (facilité de paiement accordée au client, etc.).	Au moment de l'achat ou de la souscription de l'abonnement, obligation d'authentification forte (CIT) : • sur un montant correspondant à la totalité du panier s'il est connu à l'avance ; • sur un montant à zéro euro (ou « demande d'information ») si le montant total n'est pas connu ou estimable. Pour les échéances ultérieures, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chaînage).
Paiement associé à une réservation	Paiement d'un bien ou d'un service dont le déclenchement et le montant sont conditionnés par la consommation effective. Ce cas d'usage couvre également la non-consommation, lorsque le porteur ne se présente pas pour consommer le service réservé (« *no show* »).	Au moment de la réservation, obligation d'authentification forte (CIT) : • sur la valeur maximale si elle est connue ; • sur un montant à zéro euro (ou « demande d'information ») si le montant n'est pas connu. Quand le montant définitif est connu, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chaînage).
Paiement au travers d'une solution de portefeuille électronique	Paiement au travers d'un compte de paiement ou de monnaie électronique fourni par un prestataire de services de paiement (PSP) agréé, alimenté au moyen d'une carte de paiement préenregistrée par l'utilisateur.	Au moment du paiement par portefeuille électronique auprès du commerçant : • Mise en œuvre par le PSP de sa solution d'authentification forte dans le respect des règles DSP 2 ; • Dans l'hypothèse où le solde du payeur auprès du PSP n'est pas suffisant, l'opération d'alimentation de compte par carte est soumise aux règles DSP 2 (application d'une authentification forte sauf en cas d'exemption). Toutefois, si l'enregistrement de la carte par le PSP a fait l'objet d'une authentification forte, l'opération d'alimentation de compte peut être qualifiée en tant que MIT par le PSP, qui doit fournir à l'émetteur la preuve d'authentification (chaînage).

Note : CIT (*customer initiated transaction*) : transaction initiée par le client, RTS (*regulatory technical standard*) : norme technique de réglementation, MIT (*merchant initiated transaction*) : transaction initiée électroniquement par le commerçant.

Source : Observatoire de la sécurité des moyens de paiement.

G1 Trajectoire de mise en place du *soft decline* au 1er semestre 2021 (axe des ordonnées : montant en euros)



Source : Observatoire de la sécurité des moyens de paiement.

1.2.2 Le plan de montée en charge des émissions de *soft decline*

Le *soft decline* est un mécanisme standardisé par lequel l'émetteur de la carte rejette une transaction identifiée comme non conforme à la réglementation (c'est-à-dire dépourvue de demande d'authentification ou d'élément susceptible de justifier le recours à une exemption), en offrant la possibilité au commerçant de soumettre une nouvelle fois la transaction via 3D-Secure. Comme prévu dans le plan de migration initial, ce mécanisme a été introduit début avril 2020, sur une base réduite visant à éviter tout impact négatif pour les e-commerçants (émission en réponse à des transactions jusqu'alors rejetées ou *hard decline*).

Le dispositif a ensuite été utilisé comme un levier de mise en conformité progressive du marché français, avec une approche par seuils décroissants *(cf. graphique 1)* :

- 1er octobre 2020 : rejet des transactions non conformes de plus de 2 000 euros,
- 15 janvier 2021 : rejet des transactions non conformes de plus de 1 000 euros,
- 15 février 2021 : rejet des transactions non conformes de plus de 500 euros,
- 15 mars 2021 : rejet progressif des transactions non conformes de plus de 250 euros,
- 15 avril 2021 : rejet progressif des transactions non conformes de plus de 100 euros,
- 15 mai 2021 : rejet progressif de toutes les transactions non conformes.

Pour les trois derniers seuils, qui portaient sur des volumes de transactions et de commerçants plus importants, la mise en place du *soft decline* a été étalée sur quatre semaines par les émetteurs.

1.2.3 Le renforcement de la continuité des infrastructures d'authentification

Le plan de migration de Place validé par l'Observatoire prévoit en cible l'utilisation généralisée du protocole 3D-Secure, notamment sous sa version 2 qui permet au commerçant de bénéficier des exemptions prévues par la DSP 2 à sa demande ou à l'initiative de l'émetteur.

Cette utilisation plus systématique du protocole 3D-Secure rend le secteur du e-commerce dépendant du bon fonctionnement des infrastructures d'authentification, notamment les serveurs d'authentification des banques (*authentication control servers* – ACS) et les serveurs de routage des flux 3D-Secure mis en place par les systèmes de paiement par carte (*directory servers* – DS). Ces infrastructures ayant ainsi pris une dimension systémique pour le e-commerce, l'Observatoire s'est attaché à définir des mécanismes de continuité visant à assurer la capacité pour les marchands à poursuivre leurs opérations en cas de défaillance d'un des maillons de la chaîne d'authentification [3], et s'est assuré de leur bonne appropriation par l'ensemble des acteurs du marché.

1.3 Le bilan de la migration

L'Observatoire souligne la forte mobilisation de l'ensemble des acteurs de l'écosystème des paiements pour conduire à son terme le plan de migration, en dépit du contexte de crise sanitaire. À fin juin 2021, les indicateurs d'avancement attestent d'un haut niveau de conformité atteint sur les deux volets du plan de migration.

3 Cf. encadré n° 1.

Cet acquis confirme la pertinence du dispositif adopté qui a permis d'associer, de façon quasi continue, l'ensemble des parties prenantes au pilotage opérationnel du plan de migration, et conforte l'Observatoire dans ses différentes attributions.

Il met également en valeur l'intérêt des échanges réguliers ou consacrés à des sujets spécifiques au bénéfice d'une réduction du niveau de fraude tout en prenant en compte les impératifs économiques des acteurs du e-commerce dans une période de crise sanitaire particulièrement critique.

1.3.1 L'équipement des porteurs

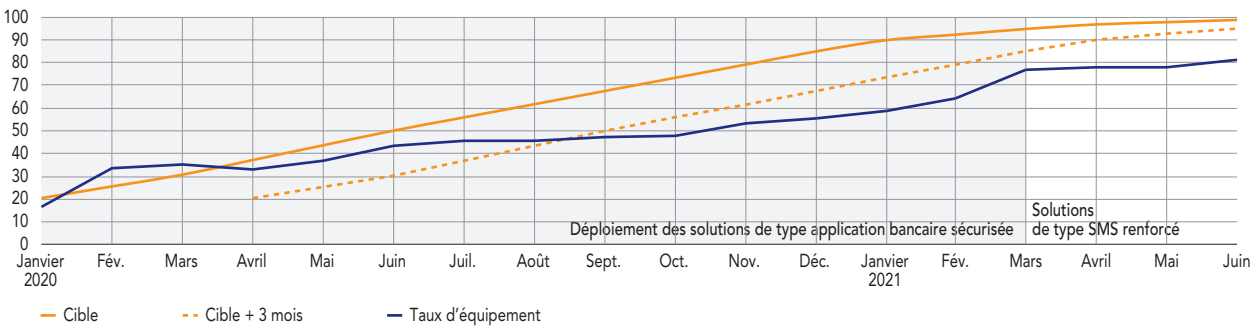
La part des porteurs de carte enrôlés dans un dispositif d'authentification forte a progressé tout au long du plan de migration. À fin juin 2021, l'Observatoire estime que plus de 80 % des porteurs de carte actifs sur Internet (c'est-à-dire ayant réalisé au moins un paiement en ligne au cours des trois derniers mois) sont équipés et utilisent désormais ce mode d'authentification en remplacement du SMS OTP.

L'Observatoire note que, si le déploiement du plan d'équipement des porteurs a été ralenti par la crise sanitaire, les actions de surveillance conduites au niveau individuel par la Banque de France ont permis de rattraper au premier trimestre 2021 une partie du retard accumulé par certaines banques sur le déploiement de leur solution d'authentification par application mobile sécurisée. Au cours du deuxième trimestre 2021, les banques ont commencé à procéder à l'enrôlement des porteurs non éligibles à la solution mobile vers des solutions alternatives, en particulier de SMS renforcé. Il apparaît urgent pour les établissements qui n'auraient pas finalisé cette deuxième vague de le faire avant la fin du troisième trimestre 2021.

Durant cette phase d'équipement des porteurs, l'Observatoire s'est attaché à suivre l'évolution des taux d'échecs sur les différentes solutions d'authentification, qui reflète à la fois le niveau d'appropriation des porteurs et la sensibilité des solutions au contexte d'utilisation. Il ressort de ces évolutions deux enseignements :

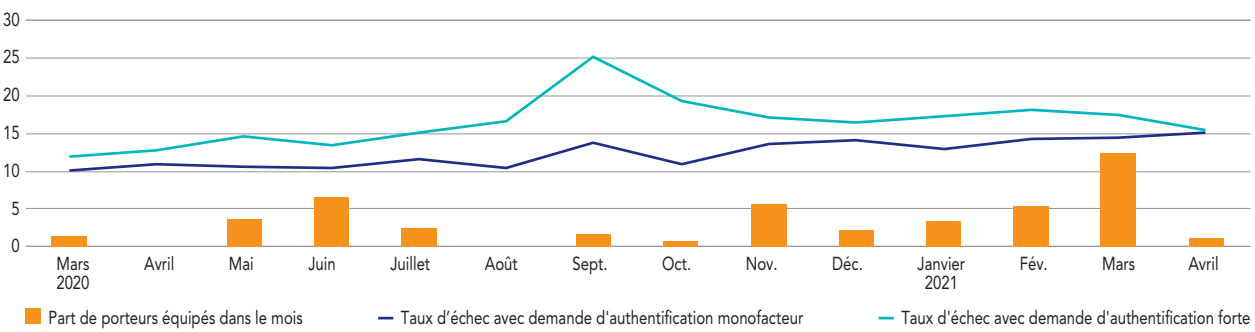
- D'une part, le taux d'échec des solutions d'authentification forte apparaît comme structurellement plus élevé que

G2 Suivi de la trajectoire d'équipement des porteurs (% de porteurs actifs enrôlés)



Source : Observatoire de la sécurité des moyens de paiement.

G3 Suivi des taux d'échec par mode d'authentification (en %)



Source : Observatoire de la sécurité des moyens de paiement.

celui de l'authentification simple par SMS-OTP, ce qui s'explique par l'usage majoritaire de dispositifs de type application bancaire sécurisée, soit une technologie plus exigeante en matière de conditions d'utilisation (qualité et stabilité de la connexion Internet, état de mise à jour de l'application et du système d'exploitation, etc.) que le recours aux technologies de type SMS ;

- D'autre part, l'écart entre les taux d'échec des deux solutions, qui avait atteint plus de dix points en septembre 2020, s'est ensuite résorbé de façon quasi continue, et semble désormais stabilisé à un niveau de l'ordre de trois points, ce qui traduit la bonne appropriation des nouvelles solutions d'authentification par les utilisateurs.

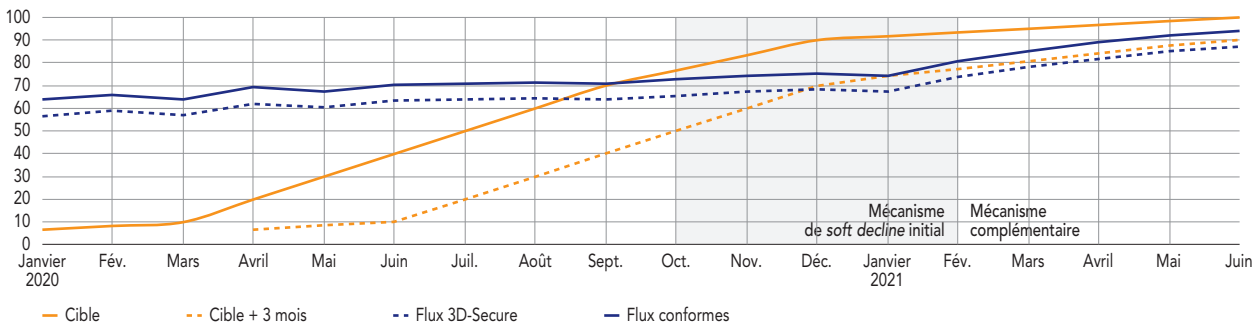
1.3.2 L'équipement des commerçants

La montée en charge du recours au protocole 3D-Secure par les commerçants a été très progressive, en raison du besoin de fiabiliser les nouvelles infrastructures d'authentification fondées sur le protocole 3D-Secure v2. Elle s'est toutefois accélérée sous l'effet du plan de montée en régime du mécanisme de *soft decline*. Ainsi, à fin juin 2021, 87 % des flux de paiement éligibles à la DSP 2 transitent par les protocoles 3D-Secure, ce qui assure leur conformité ; en complément, les flux non 3D-Secure de moins de trente euros, qui bénéficient d'une exemption a priori, représentent environ 7 % des flux. Le taux de conformité à fin juin atteint ainsi près de 95 % des flux CIT en valeur.

En complément, l'Observatoire souligne que la version 2 du protocole 3D-Secure est devenue prépondérante (plus des trois quarts des flux 3D-Secure en juin), et a permis de faciliter le recours aux exemptions par les commerçants : en mai, environ 60 % des transactions ont ainsi bénéficié d'un mode sans authentification validé par l'émetteur de la carte.

L'Observatoire note par ailleurs qu'une phase de rodage et de montée en charge progressive de la version 2 du protocole 3D-Secure s'est avérée nécessaire pour fiabiliser son fonctionnement et assurer ainsi une maîtrise du taux d'échec des transactions. Depuis février 2021, la progression

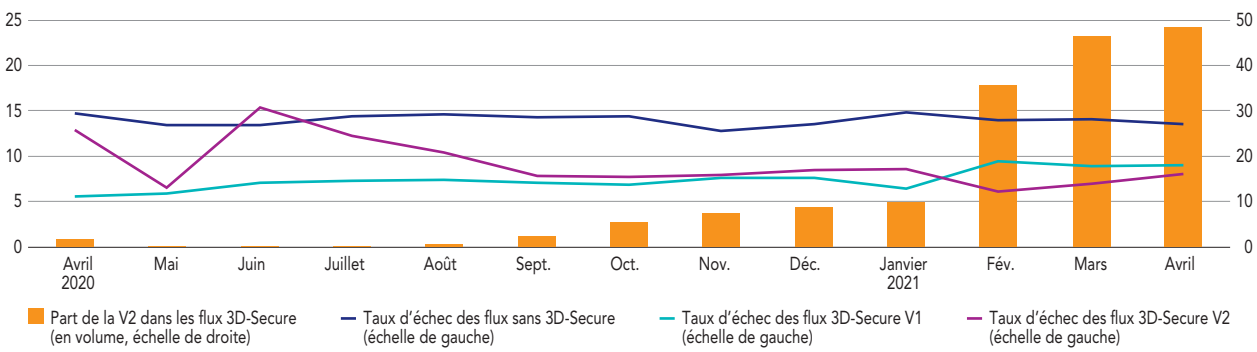
G4 Suivi de la trajectoire de mise en conformité des flux par les commerçants (% des flux CIT conformes en valeur)



Notes : Les flux conformes comprennent les flux 3D-Secure et les flux de faibles montants non 3D-Secure.
CIT – *customer initiated transaction*.

Source : Observatoire de la sécurité des moyens de paiement.

G5 Suivi des taux d'échec par version de protocole (en %)



Source : Observatoire de la sécurité des moyens de paiement.

des flux sur cette version s'est accompagnée d'une baisse sensible du taux d'échec, devenu structurellement inférieur à celui de la version 1, ce qui est logique étant entendu que la version 2 permet aux commerçants de bénéficier de transactions exemptées d'authentification forte, dont le taux de succès est proche de 100 %.

1.3.3 Perspectives

L'Observatoire se félicite de l'engagement de l'ensemble des acteurs dans la réussite du plan de migration, qui a permis d'atteindre un haut niveau de conformité sur les deux volets tout en préservant le bon fonctionnement du secteur du e-commerce pendant toute la durée de la migration. Compte tenu de ces résultats, l'Observatoire acte la fin du plan de migration collectif de la Place française tel que validé en octobre 2019. En tant qu'autorités compétentes, la Banque de France et l'Autorité de contrôle prudentiel et de résolution s'assureront de la mise en conformité résiduelle, en agissant directement auprès des établissements concernés sur une base individuelle.

Au-delà de la mise en conformité du marché français, l'Observatoire souligne toutefois la nécessité de veiller à la bonne application de l'ensemble des règles prévues par la DSP 2, et continuera ainsi à porter une attention particulière à plusieurs points :

- La poursuite des actions de pédagogie à l'attention des consommateurs, afin de veiller à la bonne appropriation des nouvelles solutions d'authentification, mais aussi à l'adoption de bons réflexes en matière de sécurité lors de leurs opérations sur Internet ;
- Le respect des règles de qualification des transactions, afin d'assurer que certains acteurs du e-commerce n'abusent pas des qualifications de type MOTO ou MIT, qui échappent à l'obligation d'authentification forte prévue par la DSP 2 ;
- Le suivi du niveau de performance des nouvelles solutions et infrastructures d'authentification, ainsi que des mécanismes de continuité associés, afin d'assurer un haut niveau de fluidité et de résilience du e-commerce ;
- L'extension progressive des requis de la DSP2 aux secteurs de l'hôtellerie, des transports et de l'événementiel. En effet, les professionnels de ces secteurs, particulièrement affectés par la crise sanitaire, ont bénéficié d'un régime d'exclusion à l'émission de *soft declines* par les émetteurs. L'Observatoire veillera à ce que les pratiques de recours à l'authentification forte par les commerçants de ces secteurs soient mises en conformité de façon progressive et pragmatique, en fonction de la capacité individuelle des acteurs à conduire les évolutions nécessaires.

Ces différents sujets continueront à faire l'objet de travaux de consolidation au second semestre 2021, sous le pilotage du groupe de travail multipartite qui a assuré le pilotage de la migration.

ENCADRÉS

❶

Mécanismes de traitement des flux de paiement du e-commerce en cas de défaut des infrastructures ou des dispositifs d'authentification

A – Principes communs applicables en cas d'incident

La survenance d'un incident affectant les infrastructures et dispositifs d'authentification, quelle qu'en soit l'origine, doit entraîner sans délai la mise en œuvre des diligences suivantes (et ce même dans l'hypothèse où les mécanismes présentés ci-après ne pourraient pas être activés) :

- **la suspension du mécanisme d'émission de message de *soft decline* par les établissements émetteurs** : si le niveau de risque d'une transaction donnée est jugé trop élevé, la banque doit alors privilégier l'émission d'un message de *hard decline* ;
- **l'évaluation du degré de criticité de l'incident, afin d'assurer le cas échéant la notification d'incident majeur à l'autorité compétente en la matière** (au titre de la DSP 2 pour les prestataires de services de paiement – PSP et/ou au titre du cadre de surveillance de l'Eurosystème pour les *schemes*).

B – Mécanismes de traitement en cas d'incident affectant le domaine « émetteur »

Du côté des émetteurs des cartes, les serveurs d'authentification des banques (*authentication control servers* – ACS) sont chargés de traiter les flux d'authentification 3D-Secure en provenance des e-commerçants, et donc soit de procéder à l'authentification forte du payeur, soit de valider le recours à une exemption. En cas d'incident affectant les ACS ou un autre composant du domaine 3D-Secure émetteur, les demandes d'authentification restent sans réponse au niveau des émetteurs, et sont ainsi mises en échec ; par ailleurs, en cas d'indisponibilité de la solution d'authentification forte, le porteur ne peut pas finaliser sa transaction.

1. Incident affectant les infrastructures du domaine émetteur

Afin d'assurer la capacité des commerçants à émettre des transactions en cas de défaillance d'un ACS ou d'un autre composant du domaine émetteur, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau du *scheme* :

- en cas d'absence de réponse de l'ACS après un délai prédéfini (*timeout* strictement encadré par les règles du *scheme*), le *scheme* qui traite la transaction est invité à se substituer à l'ACS par l'émission d'un cryptogramme d'authentification, quel que soit le contexte de la transaction (montant, score de risque, transfert de responsabilité) ;
- cette émission doit être assortie d'un indicateur permettant à l'émetteur d'identifier qu'il s'agit d'une transaction bénéficiant du mécanisme de *fallback* émetteur ;
- de façon optionnelle et comme pour toute autre transaction, le *scheme* peut accompagner cette réémission d'informations à valeur ajoutée : niveau de risque, éligibilité de la transaction à une exemption d'authentification forte, etc.

Au niveau des serveurs d'autorisation (SAE) des banques émettrices :

- évaluation du niveau de risque de la transaction en *fallback* émetteur et validation le cas échéant de la transaction même si elle n'est pas éligible à une exemption ; cette évaluation devra prendre en compte le cas échéant les implications futures de l'opération (en cas d'initiation de série d'opérations récurrentes ou de mandat de MIT – *merchant initiated transaction* [1] par exemple) ;
- les transactions issues du mécanisme de *fallback* émetteur ne doivent donner lieu à aucune émission de *soft decline* : si le niveau de risque est jugé trop élevé, la banque doit émettre un message de *hard decline* ;
- les transactions autorisées non exemptées d'authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement ;
- les conditions du transfert de responsabilité restent inchangées selon les règles du *scheme*.

1 Transactions initiées électroniquement par le commerçant.

Les établissements émetteurs sont tenus :

(i) de veiller à la bonne utilisation de ce mécanisme par les *schemes* afin d'assurer qu'il ne soit pas mis en œuvre en dehors des plages d'indisponibilité de leur ACS,

(ii) d'accepter de manière proportionnée aux risques les demandes d'autorisation,

(iii) d'évaluer la criticité de l'incident au regard des critères établis par l'Autorité bancaire européenne (EBA/GL/2017/10) et le cas échéant le notifier comme incident opérationnel ou de sécurité majeur à la Banque de France et à l'Autorité de contrôle prudentiel et de résolution (ACPR) [2].

De leur côté, les *schemes* mettent en place une surveillance des taux de réponse des émetteurs sur les transactions bénéficiant du mécanisme de *fallback* émetteur.

2. Incident affectant les solutions d'authentification forte de l'émetteur

Afin d'assurer la capacité des commerçants à émettre des transactions en cas de défaillance d'un ACS ou d'un autre composant du domaine émetteur, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau des serveurs d'authentification (ACS) des banques émettrices :

- activation d'un dispositif d'authentification de secours, relevant potentiellement de l'authentification simple (de type SMS-OTP) en cas d'indisponibilité d'une solution d'authentification forte alternative ;
- les transactions n'ayant pas fait l'objet d'une authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement ;
- du point de vue des règles de responsabilité applicables, la transaction doit être considérée comme fortement authentifiée du point de vue des *schemes*.

Les établissements émetteurs sont tenus de veiller à la bonne utilisation de ce mécanisme, afin d'assurer i) qu'il est mis en œuvre de façon diligente en cas d'incident identifié et ii) qu'il ne soit pas utilisé en dehors des plages d'indisponibilité des solutions d'authentification forte.

La nature de l'incident sur les solutions d'authentification forte de l'émetteur est également susceptible de faire l'objet d'une notification à la Banque de France et à l'ACPR au titre des incidents majeurs.

C – Mécanismes de traitement en cas d'incident affectant le domaine « accepteur »

Du côté des *schemes*, les *directory servers* (DS) sont chargés de router les flux de paiement 3D-Secure en provenance des e-commerçants vers les ACS des banques émettrices. En cas d'incident affectant les DS ou la *gateway* d'accès, les paiements 3D-Secure ne peuvent être réalisés.

Afin d'assurer la capacité des commerçants à émettre des transactions en cas de défaillance d'un *directory server* ou de leur *gateway* d'accès, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau du *scheme* :

- mise en place d'un indicateur permettant d'identifier les demandes d'autorisation bénéficiant du mécanisme de *fallback* accepteur.

Au niveau des commerçants :

- sous réserve de faisabilité au regard du règlement IFR – *interchange fee regulation* (notamment en cas d'absence de sélection active de la marque par le consommateur), bascule sur le deuxième *scheme* si la carte est cobadgée ;
- en cas d'incapacité à émettre une transaction via 3D-Secure, émission de la transaction directement en autorisation en l'identifiant comme relevant du mécanisme de *fallback* accepteur.

Au niveau des serveurs d'autorisation (SAE) des banques émettrices :

- évaluation du niveau de risque de la transaction en *fallback* accepteur et validation le cas échéant de la transaction même si elle n'est pas éligible à une exemption ; cette évaluation devra prendre en

2 Les incidents opérationnels et de sécurité majeurs des prestataires de services de paiement doivent être notifiés au titre de l'article L. 521-10 du Code monétaire et financier, mettant en application les critères des orientations de l'Autorité bancaire européenne (EBA/GL/2017/10). Les notifications sont à transmettre par le biais d'une interface sécurisée dédiée, conformément aux orientations de l'Autorité bancaire européenne en la matière. Les PSP sont invités à transmettre toute demande de documentation par courriel à l'adresse suivante : *2323-NOTIFICATIONS-UT@banque-france.fr*

compte le cas échéant les implications futures de l'opération (en cas d'initiation de série d'opérations récurrentes ou de mandat de MIT par exemple) ;
- les transactions issues du mécanisme de *fallback* accepteur ne doivent donner lieu à aucune émission de *soft decline* : si le niveau de risque est jugé trop élevé, la banque doit émettre un message de *hard decline* ;
- Les transactions autorisées non exemptées d'authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement.

Les établissements acquéreurs sont tenus de veiller à la bonne utilisation de ce mécanisme par leurs commerçants, afin d'assurer qu'il ne soit pas mis en œuvre en dehors des plages d'indisponibilité des *directory servers* ou de leurs *gateways* d'accès.

De leur côté, les établissements émetteurs sont tenus d'accepter de manière proportionnée aux risques les demandes d'autorisation.

Enfin, les *schemes* mettent en place une surveillance du taux d'utilisation de ce dispositif côté acquéreur et des taux de réponse des émetteurs. Ils sont également tenus de notifier à l'Eurosystème, le cas échéant via la Banque de France comme surveillant principal, les incidents majeurs affectant leurs infrastructures dans le cadre du « *Major incident reporting framework for payment schemes and retail payment systems* » (2018).

2

ÉTAT DE LA FRAUDE EN 2020

2.1 Vue d'ensemble

2.1.1 Cartographie des moyens de paiement

Dans le contexte de la crise de la Covid-19, l'activité des paiements a globalement bien résisté en raison des flux financiers exceptionnels qu'elle a occasionnés. Ainsi, les opérations de paiement scripturales réalisées par les particuliers, les entreprises et les administrations représentent en 2020 un volume de 25,3 milliards de transactions (contre 26 milliards en 2019, soit – 4 %) pour un montant total de 35 902 milliards d'euros (contre 28 658 milliards d'euros en 2019, soit + 25 %).

Au niveau de la structure des paiements, la dématérialisation des paiements observée depuis plusieurs années s'est encore accentuée en 2020 sous les effets de la crise sanitaire. En effet, les paiements électroniques ont davantage été plébiscités par les agents économiques : d'une part, une partie des paiements de proximité s'est reportée vers les paiements à distance du fait du confinement et des restrictions de circulation ; d'autre part, les agents ont privilégié les modes de paiement dématérialisés ou sans contact dans les paiements de proximité résiduels pour des raisons sanitaires. C'est ainsi que :

- La **carte** reste toujours le moyen de paiement le plus utilisé par les Français puisqu'elle représente plus de la moitié des transactions scripturales en volume (55 % en 2020 comme en 2019) pour un montant total de 578 milliards d'euros en 2020. Toutefois, son usage a légèrement baissé en 2020 (– 4,3 % en volume par rapport à 2019) en raison du recul des paiements de proximité (– 8,7 % du nombre de transactions sur ce canal par rapport à 2019), en liaison avec la fermeture des magasins et les restrictions de déplacement. Les paiements de proximité représentent encore une part importante des règlements par carte, près des deux tiers. Parmi ces paiements de proximité, on observe une progression marquée de la part des montants réglés en mode sans contact qui passe de 9 % en 2019 à 19 % en 2020. Les paiements sans contact ont ainsi représenté en 2020, 5,1 milliards d'opérations (soit + 37 % par rapport à 2019) pour un montant total de 79,7 milliards d'euros (soit + 86 % par rapport à 2019). Les paiements par carte en ligne ont, quant à eux, profité des effets de la crise, avec une progression de 13,2 % en nombre de transactions et de 8,3 % en valeur. En revanche, les retraits par carte ont pâti de la crise sanitaire avec près de 1,1 milliard d'opérations en 2020 (soit – 4,3 % par rapport à 2019), pour un montant de près de 116 milliards d'euros (soit – 3,4 % par rapport à 2019). Cela s'explique pour partie par la préférence à utiliser des moyens de paiement électroniques au détriment des espèces pour les paiements en magasin.
- Le **virement** n'a pas été affecté par la crise sanitaire, au contraire, puisque le nombre de transactions a progressé de 5 % sur un an avec près de 4,5 milliards de transactions en 2020, pour un montant total, en hausse significative, à 32 712 milliards d'euros (soit + 30 % par rapport à 2019). Cette forte hausse s'explique, pour l'essentiel, par des opérations financières atypiques qui ont notamment été réalisées par les administrations publiques pour faire face à la dynamique des dépenses engagées par l'État dans le contexte de la crise sanitaire. En effet, ce sont les virements de gros montant (VGM), échangés au travers d'infrastructures de paiement dédiées, qui expliquent cette tendance. Sur un an, ils progressent ainsi de 64,8 % en valeur, alors que les virements SEPA [1] classiques, davantage utilisés par les entreprises et les particuliers, diminuent de 15,4 % en valeur. En ce qui concerne le virement instantané, il est loin de rivaliser avec les autres types de virement puisqu'il représente encore une minorité des flux (1 % en volume et 0,08 % en valeur). Toutefois, son déploiement s'est accéléré en 2020 avec des volumes qui ont été multipliés par plus de trois à 45,5 millions de transactions pour un montant total qui a été multiplié par près de 4, à 26,6 milliards d'euros. Le montant moyen d'un virement instantané s'élève à 585 euros en 2020. Le virement reste l'instrument de paiement privilégié pour les règlements de montant élevé (paiements des salaires et pensions, paiements interentreprises, etc.). Il représente 91 % du montant total des paiements scripturaux et se positionne comme le troisième moyen de paiement le

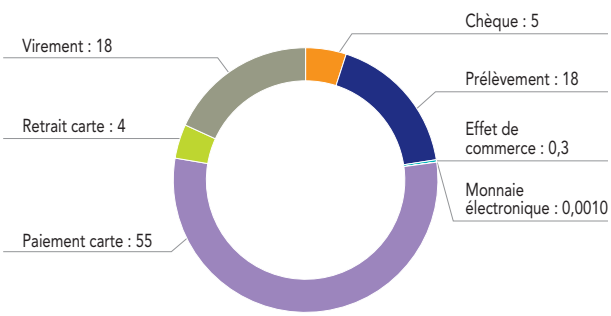
1 *Single Euro Payments Area*. La zone SEPA comprend les vingt-sept pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande, le Royaume-Uni et Saint-Martin.

plus utilisé en France (17,7 %) en nombre de transactions, juste après la carte et le prélèvement.

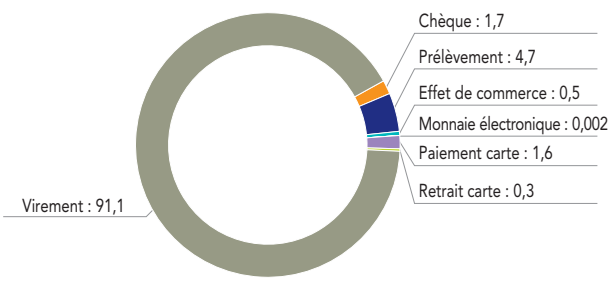
- **Le prélèvement** conserve le deuxième rang des instruments de paiement scripturaux les plus utilisés en nombre d'opérations. Il représente ainsi 18,3 % des transactions en nombre et atteint 5 % du montant total des transactions scripturales en 2020, soit sur un an une progression de l'ordre de 6 % en volume et une légère baisse de 1,6 % en valeur. Le prélèvement, essentiellement utilisé pour des encaissements récurrents, s'est montré très souple durant la crise, intégrant pour les échéances de règlement, des reports, des allégements, voire des suspensions.
- Le déclin continu du **chèque**, observé depuis les années 2000, s'est amplifié en 2020, tant en nombre qu'en valeur d'opérations (– 25,9 % en volume et – 24,6 % en valeur), avec une émission de près de 1,2 milliard de chèques, pour un montant global de 614 milliards d'euros. Si le chèque conserve encore son rang de troisième moyen de paiement le plus utilisé en valeur de transactions (avec une part à 1,7 % en 2020), il est presque détrôné par la carte dont la part est de 1,6 % en 2020.
- **Les effets de commerce** (lettres de change relevé et billets à ordre relevé), qui constituent moins de 1 % des transactions scripturales tant en nombre d'opérations (0,3 %) qu'en valeur (0,6 %), poursuivent leur déclin (– 8 % en volume et – 15 % en valeur par rapport à 2019).

G1 Usage des moyens de paiement scripturaux en France en 2020 (en %)

a) En volume



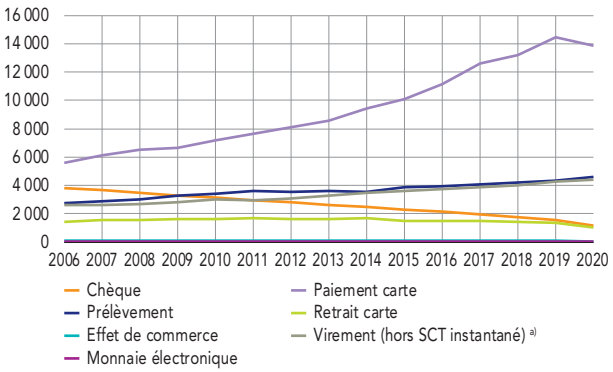
b) En montant



Source : Observatoire de la sécurité des moyens de paiement.

- Enfin, **la monnaie électronique** représente toujours une part marginale des transactions scripturales (moins de 1 % tant en volume qu'en valeur) mais enregistre une hausse de son encours total qui s'établit à 688 millions d'euros (soit + 22,6 % par rapport à 2019).

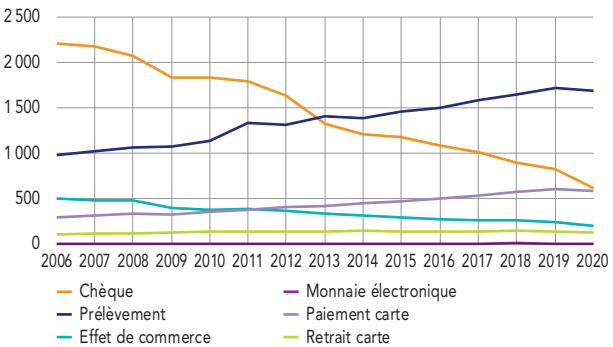
G2 Usage des moyens de paiement en France depuis 2006
(en millions d'opérations)



a) SCT instantané (*SEPA instant credit transfer*) : virement instantané.

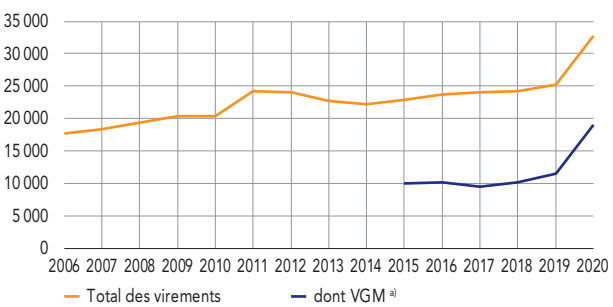
Source : Observatoire de la sécurité des moyens de paiement.

G3 Montant des transactions hors virements en France depuis 2006
(en milliards d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G4 Montant des virements en France depuis 2006 (en milliards d'euros)



a) VGM : virements de gros montant, émis au travers de systèmes de paiement de montant élevé (Target 2, Euro1), correspondant exclusivement à des paiements professionnels.

Source : Observatoire de la sécurité des moyens de paiement.

2.1.2 Impacts de la crise de la Covid-19 sur les moyens de paiement

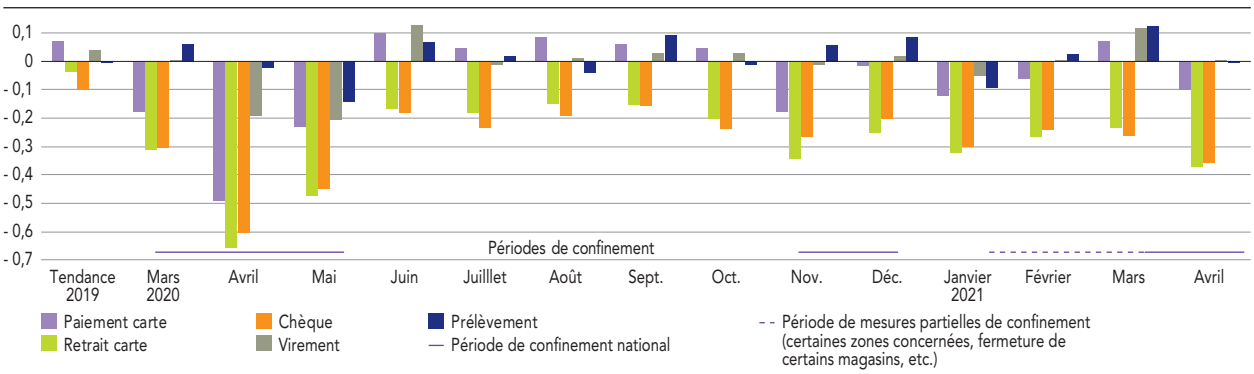
Au-delà de ces évolutions globales, l'Observatoire note que les mesures adoptées par le Gouvernement en réponse à la crise sanitaire ont eu des effets différents selon les instruments de paiement et les périodes :

- Le confinement de mi-mars à mi-mai 2020 a très fortement influé sur les flux de l'ensemble des moyens de paiement, avec un repli qui a atteint plus de 50 % pour la carte et le chèque, dans un contexte de forte réduction de l'activité de commerce de détail. Les flux de paiement SEPA (virement et prélèvement), représentatifs de l'activité des entreprises et des administrations, ont accusé un recul sensiblement plus faible, de moins de 20 %.
- La période estivale qui a suivi le déconfinement a été marquée par le retour au rythme de progression historique pour les flux de paiement, à l'exception toutefois des chèques et des retraits, qui ont connu par la suite un repli beaucoup plus important que par le passé.
- Les deux autres périodes de confinement (de mi-novembre à mi-décembre 2020, puis en avril 2021) ont eu un impact beaucoup plus limité sur les flux de paiement.

L'évolution des flux de paiement par carte au cours de ces périodes met en évidence une modification des habitudes d'achat et de paiement des consommateurs :

- Les paiements sur Internet ont été beaucoup moins affectés par les périodes de confinement, et se sont développés de façon quasi continue tout au long de la crise sanitaire, notamment à la suite de la mise en place de services en ligne par les commerçants de proximité, tels que les services de livraison ou le « *click and collect* ». Les paiements sur Internet ont ainsi progressé de plus de 20 % en nombre, par rapport à leur niveau d'avant-crise.
- Le paiement sans contact a bénéficié à la fois de l'élévation de plafond de paiement, passé de 30 à 50 euros le 11 mai 2021, et de la plus forte aversion des consommateurs pour les paiements avec contact physique (espèces, chèque, carte avec saisie du code), pour s'imposer comme le mode de paiement privilégié en proximité. Ainsi, dès le déconfinement de mai 2020, le paiement sans contact a connu une croissance spectaculaire, avec des progressions de plus de 50 % en nombre et un doublement en valeur pendant l'été 2020. Ce mode de paiement a toutefois été également affecté par les mesures sanitaires visant le commerce de proximité (notamment les

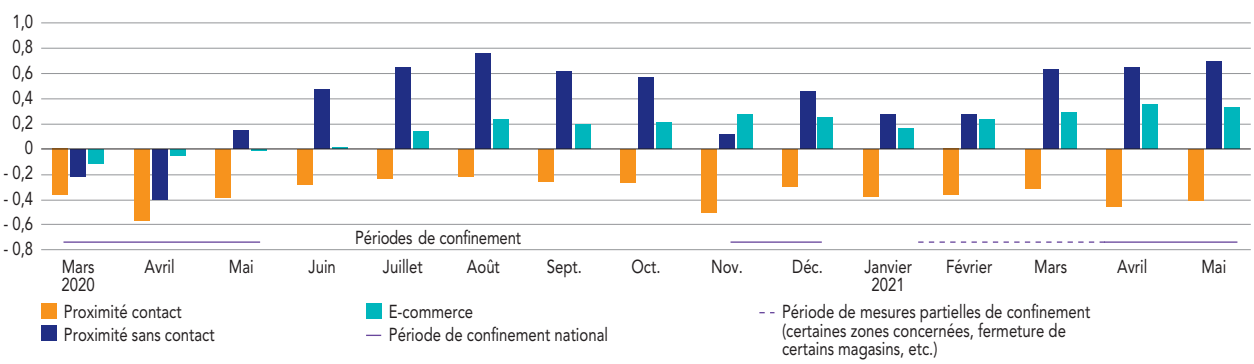
G5 Évolution des flux de paiement en volume par rapport à la période de référence pré-crise (mars 2019 – février 2020) (en %)



Note : La « tendance 2019 » correspond à la progression annuelle des flux entre 2018 et 2019.

Source : Observatoire de la sécurité des moyens de paiement.

G6 Évolution des flux de paiement par carte en volume par rapport à la période de référence pré-crise (mars 2019 – février 2020) (en %)



Source : Observatoire de la sécurité des moyens de paiement.

deux confinements suivants, ainsi que la fermeture des centres commerciaux de février à mai 2021).
- En contrepartie de ces progressions, le paiement par carte avec saisie du code a très fortement diminué depuis le début de la crise, restant en retrait de plus de 20 % en volume y compris hors périodes de confinement.

2.1.3 Fraude aux moyens de paiement

En 2020, la fraude aux transactions scripturales atteint un montant global de 1,28 milliard d'euros pour près de 7,8 millions de transactions frauduleuses, ce qui représente une hausse sur un an de 8,4 % en valeur et de 4,2 % en volume. Cette progression des montants fraudés est portée principalement par le virement et dans une moindre mesure par les paiements par carte. Toutefois, les taux de fraude de la plupart des moyens de paiement sont restés globalement maîtrisés à l'exception du chèque qui progresse sensiblement. Ainsi :

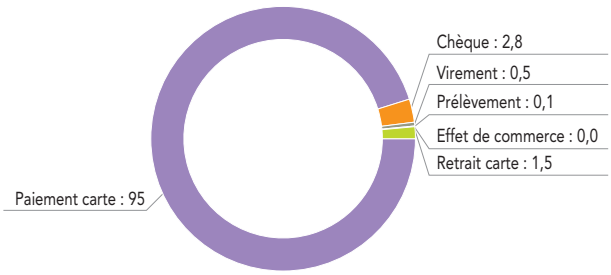
- Le **chèque** reste le moyen de paiement le plus fraudé en France, tant en montant qu'en taux de fraude et ce pour la troisième année consécutive. En effet, si les montants fraudés sont restés quasi inchangés à 538 millions d'euros, contre 539 millions en 2019, leur part dans la fraude totale aux moyens de paiement scripturaux reste la plus élevée à 42 % (contre 46 % en 2019), en raison notamment de la moyenne élevée de la transaction frauduleuse par chèque qui s'établit à 2 438 euros. Avec la poursuite de la baisse de son usage en 2020 (– 24,6 % en valeur) et la progression de l'usage de chèques perdus ou volés (+ 23,4 % en montant pour représenter 68 % des montants fraudés sur le chèque), ainsi que celle des chèques régulièrement émis (+ 81 % des montants fraudés, à 37 millions d'euros), le taux de fraude progresse sensiblement à 0,088 % (contre 0,066 % en 2019), et reste donc supérieur à celui de la carte (0,068 %).
- En cumulant les transactions de paiement et de retrait, les montants fraudés sur la **carte** sont quasi stables d'une année à l'autre (473 millions, contre 470 millions d'euros en 2019, soit + 0,6 % sur an), mais représentent toujours une écrasante majorité (97 %) du nombre de transactions frauduleuses. Avec un montant moyen des transactions frauduleuses de 63 euros, la carte ne concentre toutefois que 37 % de la fraude globale en montant (à hauteur de 34 % pour les paiements et de 3 % pour les retraits). Le taux de fraude sur les opérations par carte reste maîtrisé à 0,068 % (contre 0,064 % en 2019), soit un euro de fraude pour 1 470 euros de paiement, malgré l'orientation massive des flux vers des pratiques plus sensibles à la fraude comme les paiements sans contact (+ 86 % des flux en valeur par rapport à 2019) et les paiements à distance (+ 8,3 % des flux en valeur par rapport à 2019), en comparaison des paiements de proximité avec saisie du code confidentiel (– 17 % des flux en valeur par rapport à 2019). Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,009 %, soit un euro de fraude pour 11 100 euros de paiement) mais plus significative, bien que quasi stable, sur les paiements à distance (à 0,174 %, soit un euro de fraude pour 575 euros de paiement, contre 0,170 % en 2019). La fraude sur la carte reste largement concentrée sur les paiements sur Internet, plus des deux tiers, alors qu'ils ne comptent que pour 22 % transactions. Avec la croissance du e-commerce, ce constat rend indispensable la généralisation des mesures d'authentification forte prévues par la DSP 2.
- La fraude au **virement** progresse à nouveau en 2020 de manière importante (+ 65 % en valeur par rapport à 2019) avec un montant annuel passant de 162 millions à 267 millions d'euros, s'élevant désormais à 21 % des montants de fraude aux moyens de paiement scripturaux. Cette progression résulte, pour l'essentiel, des fraudes par ingénierie sociale qui ont crû significativement en 2020 (+ 101 millions d'euros sur un an). Les confinements successifs et la pratique généralisée du télétravail ont mis à mal les organisations et les repères des directions financières et comptables des entreprises. Les fraudeurs ont profité du contexte pour solliciter des virements en urgence ou user des circonstances exceptionnelles de la crise pour justifier d'un changement de coordonnées bancaires de la part d'un fournisseur. Cela a également touché les virements des administrations publiques, où des fraudeurs ont pu usurper l'identité d'entreprises pour obtenir des aides exceptionnelles auprès des pouvoirs publics comme celle liée à l'activité partielle. Toutefois, malgré cette hausse des montants fraudés, le taux de fraude sur le virement, bien qu'en progression sensible, reste à un niveau bas à 0,0008 % (contre 0,0006 % en 2019). Cela représente un euro de fraude pour 125 000 euros de paiement, en raison de la forte dynamique des flux de virement (+ 30 % en montant par rapport à 2019 et une part à 91 % des transactions scripturales en valeur). Selon les différents types de virement, on continue à observer un taux de fraude sensiblement plus élevé sur le virement instantané, à 0,0397 %, en légère progression sur un an. Toutefois, si la poursuite de l'usage du virement instantané se fait dans des conditions de sécurité globalement maîtrisées, sa généralisation appelle une attention renforcée des utilisateurs et des professionnels (*cf. chapitre 3, l'étude de veille sur la sécurité des paiements en temps réel*), en particulier lorsque le bénéficiaire des fonds sollicite l'envoi des fonds sur un compte tenu à l'étranger.
- La fraude au **prélèvement** poursuit sa baisse avec des montants fraudés ramenés de 11 millions à 2 millions d'euros en 2020 (– 82 % en valeur par rapport à 2019),

de sorte que ce moyen de paiement affiche le montant de fraude annuel le plus limité parmi les moyens de paiement scripturaux accessibles aux particuliers. Son taux de fraude s'établit à un niveau extrêmement bas, à 0,0001 %.

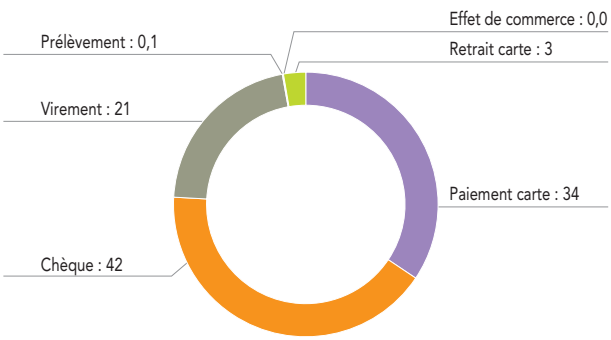
- Enfin, les **effets de commerce** restent relativement épargnés par la fraude, avec un montant de l'ordre de 539 000 euros en 2020, et un taux de fraude de 0,0003 % équivalent à un euro de fraude pour 365 500 euros de paiement.

G7 Répartition de la fraude sur les moyens de paiement scripturaux en 2020 (en %)

a) En volume

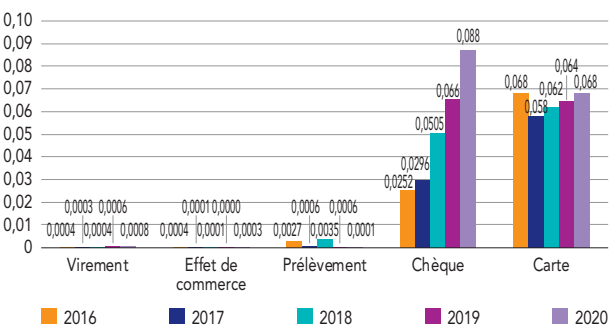


b) En montant



Source : Observatoire de la sécurité des moyens de paiement.

G8 Évolution du taux de fraude par moyen de paiement, de 2016 à 2020 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.2 État de la fraude sur le paiement et le retrait par carte

2.2.1 Vue d'ensemble

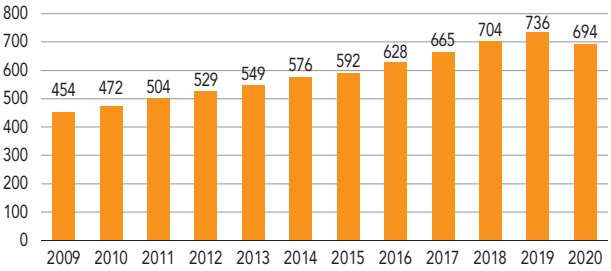
De nombreux contributeurs alimentent les statistiques sur les paiements par carte et apportent ainsi un éclairage utile sur la fraude qui en découle (*cf. encadré 2* infra).

La fraude sur les transactions de paiement et de retrait effectuées en France et à l'étranger avec des cartes françaises a très légèrement augmenté en 2020 (+ 0,6 % en valeur par rapport à 2019). Elle représente 473 millions d'euros pour un montant total de transactions de 694 milliards d'euros, soit une baisse de 5,7 % par rapport à 2019. Le taux de fraude sur les cartes de paiement françaises se dégrade très légèrement et s'établit à 0,068 %, contre 0,064 % en 2019, ce qui constitue l'équivalent d'un euro de fraude pour 1 470 d'euros de transactions.

Le montant de la fraude sur la carte, cumulant la fraude sur les cartes françaises et la fraude enregistrée sur les transactions réalisées en France avec des cartes étrangères, atteint 525 millions d'euros en 2020. Il baisse ainsi de 5,6 % par rapport à 2019, pour un montant total de transactions, également en baisse de 8,1 %, et d'une valeur totale de 725 milliards d'euros. Sur la base de ces éléments, le taux de fraude global sur les transactions par carte traitées dans les systèmes monétiques français est stable à 0,072 %. Ce taux équivaut à un euro de fraude pour 1 390 euros de transactions.

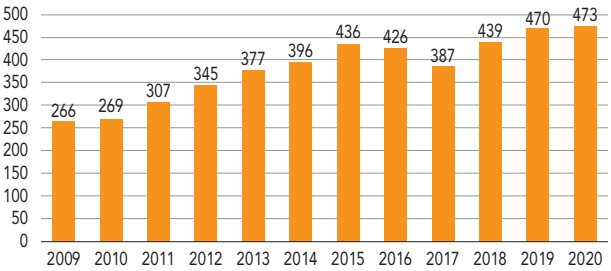
Le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2020 s'élève à 1,4 million, en hausse de 2,2 % par rapport à 2019. Toutefois, cette progression ne s'est pas accompagnée d'une augmentation du montant unitaire des transactions frauduleuses puisque celui-ci diminue au contraire à 63 euros, contre 65 euros en 2019. Cette situation s'explique par le renforcement des mesures pour sécuriser les paiements par carte (authentification renforcée des paiements en ligne, systèmes d'analyse du risque et de *scoring* des transactions, alertes SMS aux porteurs, etc.). Ces dispositions permettent de détecter et de désactiver plus rapidement des cartes compromises. Les fraudeurs sont donc contraints de multiplier les tentatives de fraude, tout en réduisant leur montant unitaire pour échapper aux mécanismes de détection des opérations frauduleuses.

G9 Montant total des transactions par cartes françaises
(en milliards d'euros)



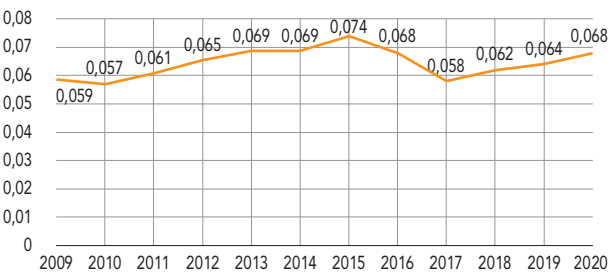
Source : Observatoire de la sécurité des moyens de paiement.

G10 Montant total de la fraude des cartes françaises
(en millions d'euros)



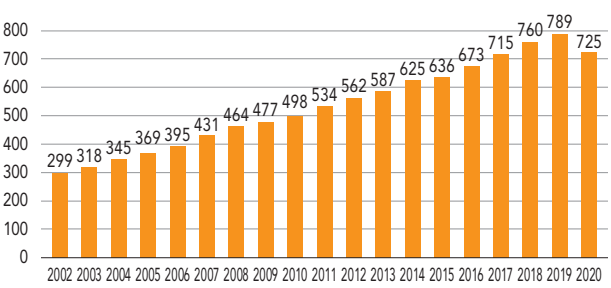
Source : Observatoire de la sécurité des moyens de paiement.

G11 Taux de fraude des cartes françaises (en %)



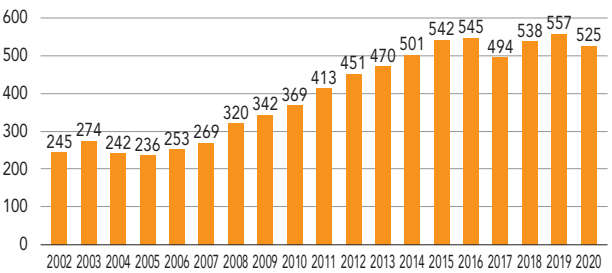
Source : Observatoire de la sécurité des moyens de paiement.

G12 Montant des transactions traitées dans les systèmes français, cartes françaises et étrangères (en milliards d'euros)



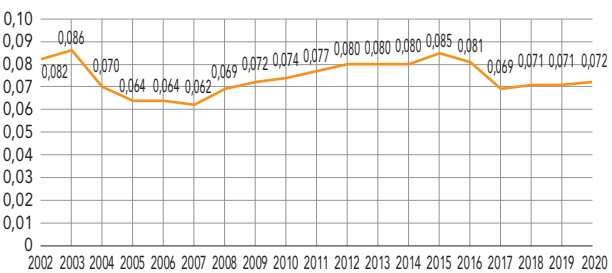
Source : Observatoire de la sécurité des moyens de paiement.

G13 Montant de la fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères (en millions d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G14 Taux de fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.2.2 Répartition de la fraude par zone géographique

Le montant de la fraude sur les transactions de paiement et de retrait effectuées en France avec des cartes françaises, c'est à dire sur les transactions nationales, progresse de 7,4 % en 2020, s'établissant à 290,7 millions d'euros, contre 270,7 millions d'euros en 2019. Dans un contexte de baisse des flux des transactions nationales (– 3,8 % en valeur par rapport à 2019), le taux de fraude sur les transactions nationales se dégrade très légèrement, tout en se maintenant à un niveau relativement bas, à 0,044 % (contre 0,040 % en 2019), ce qui représente l'équivalent d'un euro de fraude pour environ 2 270 euros de transactions.

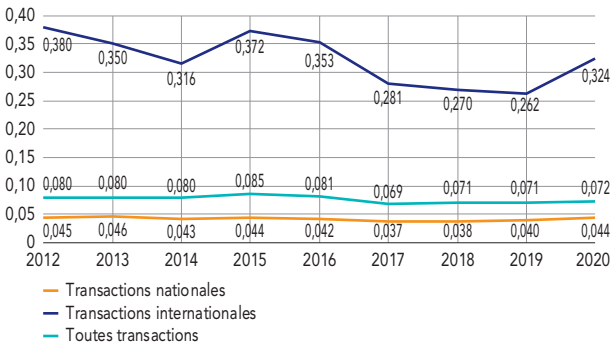
Avec le fort recul des flux internationaux liés à l'ajournement des séjours à l'étranger (– 34 % en valeur par rapport à 2019), les montants fraudés sur les transactions internationales [2] sont logiquement en baisse mais dans de moindres proportions (– 18,2 % en valeur par rapport à 2019). Ainsi, le taux de fraude sur les transactions internationales ressort en hausse à 0,327 % (contre 0,262 % en 2019), soit à un niveau sept fois plus élevé que celui des transactions nationales. Les transactions internationales restent plus vulnérables à la fraude. Elles se chiffrent à

seulement 10 % de la valeur totale des transactions par carte, mais comptent pour 45 % du montant total de la fraude.

Selon les différentes zones géographiques, on observe :

- pour les porteurs français, une progression significative des taux de fraude tant sur les opérations qu'ils réalisent au sein de la zone SEPA [3] (0,429 % en 2020, contre 0,333 % en 2019) que sur celles qu'ils effectuent hors de l'espace européen SEPA (0,533 % en 2020, contre 0,441 % en 2019) ;

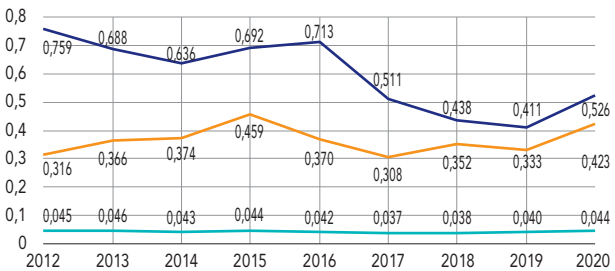
G15 Taux de fraude par zone géographique (en %)



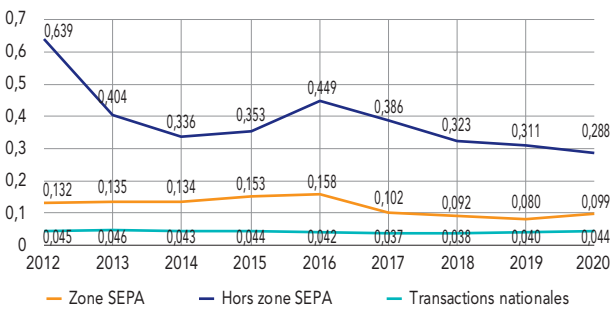
Source : Observatoire de la sécurité des moyens de paiement.

G16 Taux de fraude par zone géographique (en %)

a) Porteurs français



b) Commerçants français



Note : SEPA – *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

- pour les commerçants français, une hausse du taux de fraude sur les transactions qu'ils acceptent et qui sont réalisées avec des cartes émises dans l'espace européen SEPA (0,099 % en 2020, contre 0,080 % en 2019). À l'inverse, le taux de fraude sur les transactions par cartes émises en-dehors de la zone SEPA baisse à 0,290 %, contre 0,311 % un an plus tôt, mais il reste à un niveau particulièrement élevé.

2.2.3 Répartition de la fraude par type de transaction

Fraude sur les transactions nationales

Bien que le montant total de la fraude sur les transactions nationales ait progressé en 2020 (+ 7,4 % en valeur par rapport à 2019), les taux de fraude sur l'ensemble des canaux d'initiation sont globalement restés stables.

En effet, selon les différents types de transaction, on observe :

- Pour les paiements de proximité et sur automate, une baisse significative des montants fraudés (– 17,8 % par rapport à 2019) liée au recul des flux de transaction (– 5,4 % en valeur par rapport à 2019), mais aussi en raison de la très nette diminution de l'utilisation de cartes perdues ou volées (– 19,5 % de la fraude en valeur pour cette typologie par rapport à 2019) résultant des restrictions sur l'ouverture des points de vente durant les périodes de confinement. Dans le même temps, les paiements sans contact ont sensiblement progressé en 2020 (+ 37,7 % en volume et + 88,6 % en valeur) et le taux de fraude est plus élevé que celui des transactions impliquant la saisie du code personnel. Au final, le taux de fraude sur les paiements de proximité est en très légère baisse à 0,009 % (contre 0,010 % en 2019), soit des niveaux très bas de fraude.
- Pour les paiements à distance, une hausse de la fraude (+ 16,4 % en valeur par rapport à 2019). Cela s'explique d'une part, par la dynamique des flux en faveur du e-commerce (+ 13,5 % en valeur par rapport à 2019) engendrée par la situation sanitaire qui a modifié les habitudes d'achat des consommateurs et incité les commerçants à développer des espaces de vente en ligne ; et d'autre part, par le report des agissements

2 Les transactions internationales comprennent les transactions de paiement et de retrait effectuées à l'étranger avec des cartes françaises ainsi que les transactions de paiement et de retrait effectuées en France avec des cartes étrangères.

3 *Single Euro Payments Area*. La zone SEPA comprend les vingt-sept pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande, le Royaume-Uni et Saint-Martin.

des fraudeurs vers ce canal davantage plébiscité par les consommateurs avec une multiplication des attaques par *phishing*[4]. Toutefois, le taux de fraude sur les paiements à distance est resté maîtrisé à 0,174 %, contre 0,170 % en 2019 grâce aux efforts de sécurisation des émetteurs de moyens de paiement, des commerçants et des entreprises, qui ont déployé des dispositifs d'authentification du porteur, ainsi que des outils d'analyse de risque et de *scoring* des transactions. Ce taux reste cependant élevé, puisqu'il est dix-neuf fois supérieur à celui des paiements de proximité et sur automate. Il devrait s'améliorer grâce à la généralisation des mesures d'authentification forte pour les paiements en ligne prévues par la deuxième directive européenne sur les services de paiement (DSP 2), dont la mise en œuvre complète a été ralentie en 2020 en raison de la crise de la Covid-19 (*cf. chapitre 1*). La fraude sur les paiements à distance reste toujours largement concentrée sur les secteurs du « Commerce généraliste et semi-généraliste » et des « Services aux particuliers et professionnels (*cf. encadré 3*).

- Pour les retraits aux distributeurs, une baisse des montants fraudés (– 9,4 % en valeur par rapport à 2019) en lien avec le recul de l'activité (– 13,7 % en valeur par rapport à 2019) dans la mesure où les consommateurs comme les commerçants ont eu tendance à privilégier les paiements électroniques au détriment des moyens de paiement physiques au cours de la crise sanitaire. Le taux de fraude est resté quasi stable à 0,029 %, contre 0,028 % un an plus tôt.

Fraude sur les transactions internationales

Si la fraude sur les transactions internationales a globalement baissé en 2020, les évolutions sont contrastées selon les canaux d'initiation et les zones géographiques. D'une manière générale, on observe toujours une meilleure maîtrise de la fraude sur les transactions réalisées au sein de la zone SEPA que sur celles effectuées avec des pays situés en-dehors de cette zone. Cela résulte des efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et des terminaux de paiement vers le standard de sécurité EMV (Europay Mastercard VISA)[5] et des effets de la réglementation européenne en matière de sécurisation des paiements et de généralisation des dispositifs d'authentification forte[6].

- Pour les cartes françaises, la fraude reste largement concentrée sur les paiements à distance dont la part dans les montants fraudés représente 94 % du total de la fraude au sein de l'espace européen SEPA (à 129,1 millions d'euros avec un taux de fraude à 0,582 % en 2020) et 90 % du total de la fraude en dehors de la zone SEPA (à 40,5 millions d'euros avec un taux de fraude à 0,921 % en 2020). Dans le même temps, les paiements de proximité restent très sensibles à la fraude dans certains pays, où les automates de paiement et de retrait continuent de recourir à la lecture de la piste magnétique de la carte, ce qui la rend vulnérable à la contrefaçon.
- Pour les cartes étrangères, les niveaux de fraude restent beaucoup plus élevés pour les transactions à distance, avec des taux se situant à 0,207 % pour les cartes émises au sein de l'espace européen SEPA et à 0,711 % pour celles émises en-dehors de la zone SEPA. Pour ces dernières, les acquéreurs français ne peuvent pas toujours exiger une authentification forte du porteur, la DSP 2 n'étant pas applicable sur les cartes émises en dehors de l'Union européenne.

Fraude sur les paiements sans contact

Dans le contexte de la crise de la Covid-19, les règlements par carte sans contact ont été largement plébiscités par les consommateurs et les commerçants comme « geste barrière » puisqu'ils sont à nouveau en forte progression de 38 % en volume et de 89 % en valeur par rapport à 2019 au plan national. Ce renforcement de l'usage du sans contact a été également favorisé par le relèvement du plafond de 30 à 50 euros, le 11 mai 2020 à la sortie du premier confinement.

Sur l'année 2020, près de 5,1 milliards de paiement sans contact ont été réalisés (contre 3,7 milliards en 2019) pour un montant total de 78,4 milliards d'euros (contre 41,6 milliards d'euros en 2019). C'est ainsi qu'en 2020, près d'un paiement par carte sur deux (46 % précisément) en situation de proximité a été réalisé en mode sans contact, ce qui représente 19 % en valeur de ces paiements en valeur. Reflet de l'augmentation du plafond à 50 euros, le montant moyen d'un paiement sans contact s'établit à 15,4 euros, contre 11,3 euros en 2019.

Si on ajoute aux paiements nationaux sans contact ceux réalisés en France au moyen de cartes étrangères et ceux effectués avec des cartes françaises à l'étranger (c'est-à-dire les paiements internationaux), 5,3 milliards d'opérations ont été réalisées pour un montant total de 81,1 milliards d'euros, soit une progression sur un an de 35 % en volume et de 83 % en valeur.

En dépit de la croissance des règlements en mode sans contact et du relèvement du plafond, le taux de fraude sur les transactions nationales sans contact ne s'est pas dégradé, au contraire, puisqu'il baisse très légèrement à 0,013 % (contre 0,019 % en 2019), avec un montant total de fraude de près de 10,5 millions d'euros. Le taux de fraude sur les paiements sans contact se situe toujours

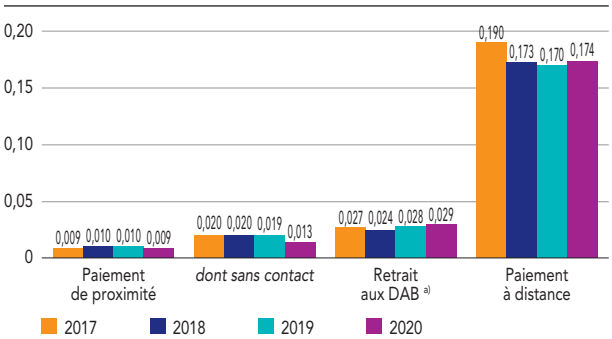
à un niveau intermédiaire entre celui des paiements de proximité (0,009 %) et celui des retraits (0,029 %), et bien en deçà de celui des paiements à distance (0,174 %). Si l'on ajoute à cette fraude nationale celle sur les transactions internationales, le taux de fraude s'améliore également à 0,016 % (contre 0,020 % en 2019), avec un montant total de fraude de 13 millions d'euros. Cette baisse en 2020 cache cependant des hausses de taux pour les paiements sans contact effectués avec des pays en-dehors de la zone SEPA, que ce soit pour les porteurs ou les commerçants français. À cet égard, l'Observatoire recommande aux porteurs français, pour une sécurité optimale, **de désactiver la fonctionnalité sans contact de leurs cartes lors de leurs déplacements en dehors de la zone SEPA**, dans la mesure où les plafonds habituels de paiement ne sont pas toujours effectifs.

En 2019 et comme les années précédentes, la fraude sur les paiements sans contact résulte essentiellement du vol ou de la perte de la carte, sans utilisation donc de technologies avancées de captation des données de la carte. Dans la mesure où les émetteurs de carte fixent des plafonds sur le montant unitaire d'une transaction (montant fixé à 50 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (cumul fixé au plus à 250 euros), le préjudice subi par le consommateur, en cas de perte ou de vol d'une carte, est limité. Il est d'ailleurs rappelé que le porteur est protégé par la loi en cas de fraude et doit être remboursé des fraudes subies ayant eu recours au mode sans contact (*cf. annexe 2*). En ce qui concerne, les transactions internationales en mode sans contact, l'origine de la fraude est différente puisqu'elle résulte principalement de l'usage de cartes contrefaites (40 % des montants fraudés), puis du vol ou perte de carte (29 % des montants fraudés).

En ce qui concerne le paiement par mobile, dont les données sont intégrées à celles du paiement sans contact, son usage semble avoir été nourri par la pandémie de la Covid-19, avec une progression des transactions nationales de 135 % en volume avec 126,9 millions de transactions et de 179 % en valeur pour un montant total de transactions d'un peu plus de 2,7 milliards d'euros. Toutefois, ce mode de paiement continue de représenter une part très marginale à l'échelle de l'ensemble des flux de paiement par carte sans contact (2,5 % en volume et 3,4 % en valeur). Le montant moyen d'un règlement national par mobile s'établit à 21,2 euros en 2020, contre 17,8 euros en 2019. Avec les paiements effectués en France par des équipements étrangers et ceux réalisés à l'étranger par des équipements français, le montant total des transactions atteint un peu plus de 3 milliards d'euros pour 147,7 millions d'opérations, soit une progression sur un an de 118 % en volume et de 144 % en valeur.

Alors qu'en 2019 la fraude sur le paiement par mobile était anecdotique, en 2020 elle s'accroît fortement en lien avec le développement de son usage. Ainsi, la fraude sur les transactions nationales par mobile a été multipliée par sept tant en nombre (29 807 en 2020, contre 4 159 en 2019) qu'en montant (2,4 millions d'euros en 2020, contre un peu plus de 330 000 euros en 2019). En conséquence, le taux de fraude sur les transactions nationales par mobile progresse en 2020 pour s'établir à 0,091 % (contre 0,03 % en 2019). La fraude sur le paiement par mobile, toutes zones géographiques confondues, progresse significativement avec un taux de fraude qui s'établit à 0,13 % (contre 0,04 % en 2019). Comme pour le paiement sans contact, ce sont les transactions effectuées avec les pays hors SEPA qui sont particulièrement vulnérables à la fraude.

G17 Comparaison des taux de fraude sur les transactions nationales, par type de transaction (en %)



a) DAB : distributeurs automatiques de billets.

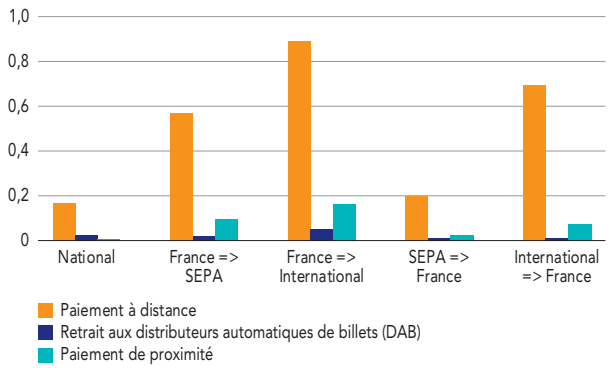
Source : Observatoire de la sécurité des moyens de paiement.

4 Le *phishing* ou l'hameçonnage repose généralement sur l'envoi de courriels usurpant des chartes visuelles et logos connus de leurs destinataires (par exemple un établissement de crédit) et invitant les victimes à se connecter à un site qui s'avère frauduleux. L'objectif est de collecter des données de la carte.

5 EMV est un standard international de sécurité des cartes de paiement à puce, dont les spécifications ont été développées par le consortium EMVCo regroupant American Express, JCB Cards, MasterCard et Visa. Le standard EMV pour les paiements de proximité et les retraits prévoit notamment le recours à la combinaison d'une puce sécurisée sur la carte, associée à la saisie d'un code confidentiel, communément dénommée « *chip and PIN* » (puce et code PIN).

6 Les dispositifs d'authentification forte reposent sur la vérification de l'identité du client par le biais de deux des trois éléments suivants : i) un élément que seul le client connaît (mot de passe, code) ; ii) un élément que seul le client possède (téléphone, carte) ou iii) une caractéristique personnelle du client (empreinte digitale, iris ou reconnaissance vocale).

G18 Taux de fraude par type de transaction et origine géographique (en %)

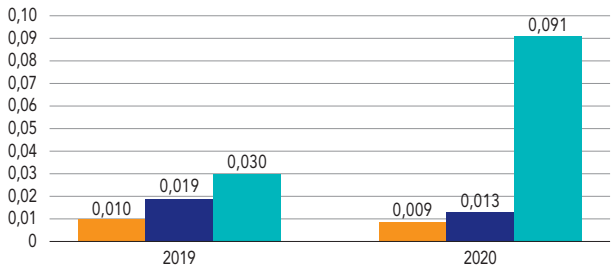


Note : SEPA – *Single Euro Payments Area*.

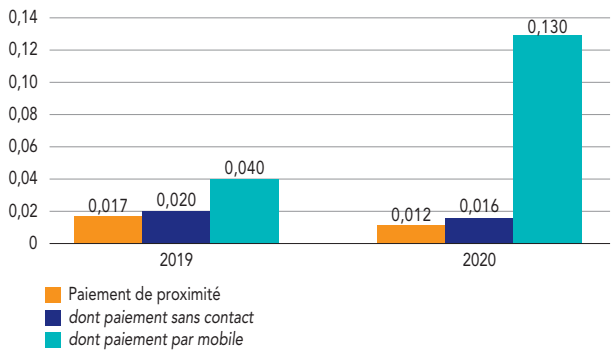
Source : Observatoire de la sécurité des moyens de paiement.

G19 Taux de fraude sur les paiements de proximité (en %)

a) Transactions nationales



b) Transactions nationales et internationales



Source : Observatoire de la sécurité des moyens de paiement.

Il est rappelé que contrairement au paiement par carte sans contact, le paiement par mobile n'est pas plafonné, la seule limite étant le plafond de la carte de paiement, le préjudice subi peut donc s'avérer plus élevé. La fraude sur le paiement par mobile résulte principalement de cartes perdues ou volées qui sont enrôlées dans une application de paiement par mobile. L'Observatoire réitère donc ses recommandations adressées aux acteurs – banques, systèmes de paiement par carte et fournisseurs de solutions technologiques – pour mettre en œuvre des mesures d'authentification forte, tant pour sécuriser l'enrôlement des utilisateurs au sein des applications de paiement par mobiles que pour authentifier le porteur pour les transactions ultérieures.

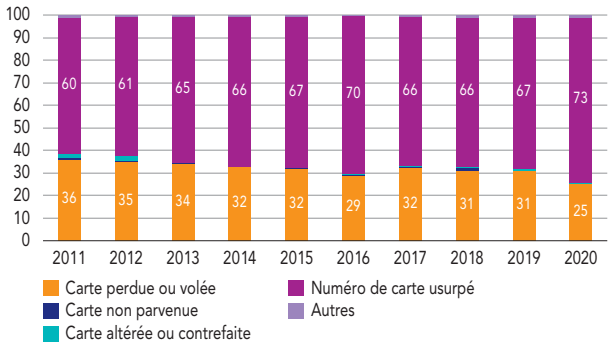
2.2.4 Répartition de la fraude par typologie

L'origine de la fraude sur les transactions nationales par carte, de loin la plus importante, reste liée à l'usurpation des numéros de carte qui permet la réalisation de paiements frauduleux à distance (73,1 % des montants fraudés en 2020, contre 66,9 % en 2019). Il en est de même pour les transactions internationales, puisque cette typologie de fraude représente, à elle seule, 90 % des montants fraudés pour les opérations réalisées au sein de l'espace SEPA et 81 % en-dehors de cette zone. En 2020, cette typologie de fraude repose sur les attaques par hameçonnage (*phishing*) et logiciels malveillants (*malwares*) qui se sont fortement intensifiées durant la crise en utilisant notamment le thème de la pandémie de la Covid-19, pour capitaliser sur la peur et la confusion qu'elle propageait auprès des consommateurs. Pour contourner les dispositifs d'authentification du payeur, certaines formes d'hameçonnage par courriel ou SMS parviennent à leurrer le porteur de carte pour qu'il fournisse à la fois les données de sa carte et ses codes d'authentification reçus par SMS. Dans certains cas, le fraudeur réussit même à joindre par téléphone le porteur de la carte et l'amène à authentifier la transaction frauduleuse via son application bancaire (hameçonnage par téléphone ou *vishing*).

La seconde typologie de fraude reste l'usage de cartes perdues ou volées qui touche principalement les opérations de proximité. Toutefois, la part de cette typologie dans la fraude sur les transactions nationales a baissé, passant de 30,6 % en 2019 à 24,7 % en 2020 sous l'effet des restrictions de déplacement et d'ouverture des commerces durant les périodes de confinement.

La contrefaçon de cartes demeure marginale puisqu'elle n'est à l'origine que de 1 % des paiements nationaux frauduleux. La part de cette typologie de fraude dans les montants fraudés sur les transactions internationales est un peu plus élevée (5 % pour les transactions au sein de la zone SEPA et 11 % en-dehors de cette zone). Ces niveaux très bas s'expliquent principalement par l'adoption de technologies de cartes à puce par le plus grand nombre de systèmes de cartes privatives et par le

G20 Répartition de la fraude aux paiements par carte selon la typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

renforcement continu de la sécurité des cartes à puce EMV existantes.

Enfin, le suivi des points physiques de compromission montre que le nombre d'attaques par *jackpotting* ou *skimming* de distributeurs automatiques de billets, d'automates de carburant et de terminaux de paiement continue à diminuer en 2020 (*cf. encadré 4* infra).

2.3 État de la fraude sur le chèque

2.3.1 Vue d'ensemble

En 2020, si la fraude sur le chèque a baissé pendant la première période de confinement en raison de la fermeture des commerces physiques et des agences bancaires, elle est repartie à la hausse post-confinement avec la reprise de son usage. Ainsi, les montants fraudés sur le chèque sont restés quasi inchangés à 538 millions d'euros, contre 539 millions d'euros en 2019, avec, en revanche, une progression significative du nombre de chèques fraudés de 20 % (à 220 730, contre 183 488 en 2019). La fraude sur le chèque baisse selon un rythme inférieur à celui de la diminution des flux de paiement par chèque (– 24,6 % en valeur par rapport à 2019), de sorte que le taux de fraude progresse à nouveau sensiblement en 2020 à 0,088 % (contre 0,066 % en 2019), soit un niveau supérieur à celui de la carte de paiement (0,068 % en 2020). Cela représente l'équivalent d'un euro de fraude pour 1 140 euros de paiement par chèque. La part du chèque dans le total de la fraude aux moyens de paiement scripturaux atteint 42 %, contre 37 % pour la carte, alors même que le chèque est utilisé douze fois moins que celle-ci. Avec ces chiffres, **le chèque reste le premier moyen de paiement le plus fraudé en France à la fois en taux et en montant**.

2.3.2 Répartition de la fraude par typologie

L'utilisation de chèques perdus ou volés reste le principal mode opératoire de fraude avec une part dans les montants fraudés qui progresse sensiblement à 68 %, contre 55 % en 2019. Les chèques perdus ou volés représentent aussi 89 % des cas de fraude au chèque. Ce type de fraude consiste à utiliser des chèques perdus ou volés pour régler l'achat de biens ou de services ou pour les remettre directement à l'encaissement. Dans ce dernier cas, le fraudeur utilise un compte qu'il a ouvert frauduleusement sur la base de fausses pièces d'identité ou par usurpation d'identité, ou a recours à une tierce personne, parfois appelée « mule », qui va accepter d'encaisser le chèque pour son compte. Le recrutement de cet intermédiaire se fait le plus souvent via les réseaux sociaux, que le fraudeur charge, en contrepartie d'une promesse de rémunération ou par tromperie, d'encaisser les chèques perdus ou volés pour lui reverser ensuite les fonds. Ce phénomène est en fort développement ces dernières années, l'Observatoire rappelle donc que les personnes qui participent à ce type de fraude encourent le risque d'être reconnues complices de fraude, un délit passible de poursuites judiciaires. Il appelle par ailleurs les utilisateurs à être particulièrement attentifs à la bonne réception de leur commande de chéquiers et aux modalités de conservation de ceux-ci (comme rappelé parmi les bonnes pratiques en matière de vigilance présentées en annexe 1 de ce rapport).

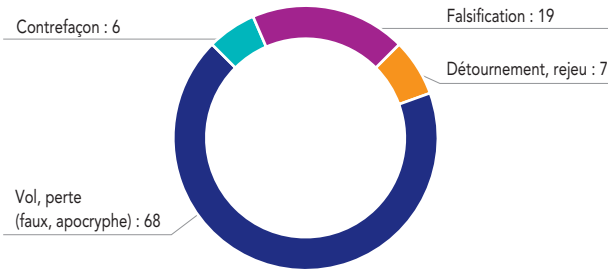
Le second type de fraude rencontrée en 2020 demeure la falsification de chèques régulièrement émis. Ce procédé consiste à modifier frauduleusement le montant ou le bénéficiaire d'un chèque valide – subtilisé par exemple dans la boîte aux lettres du bénéficiaire du chèque –, puis à le remettre à l'encaissement. Ce type de fraude est en baisse en 2020 en raison du recul des paiements par chèque. En 2020, la falsification représente 19 % des montants fraudés par chèque (contre 27 % en 2019) et 6 % des cas de fraude.

Le détournement de chèque régulièrement émis progresse fortement en 2020 pour atteindre 37 millions d'euros, contre 20 millions d'euros en 2019, soit une hausse de 81 % sur un an. Ce type de fraude recouvre principalement des chèques émis régulièrement et interceptés par le fraudeur dans les circuits d'acheminement vers le bénéficiaire et qu'il encaisse sur son propre compte sans aucune altération. Ce type de fraude constitue la troisième typologie de fraude en 2020 avec 7 % des montants fraudés sur le chèque.

La contrefaçon de chèque, c'est-à-dire l'utilisation de chèques fabriqués de toutes pièces par des faussaires et ensuite revendus sur le *darkweb* à des tiers qui les utilisent

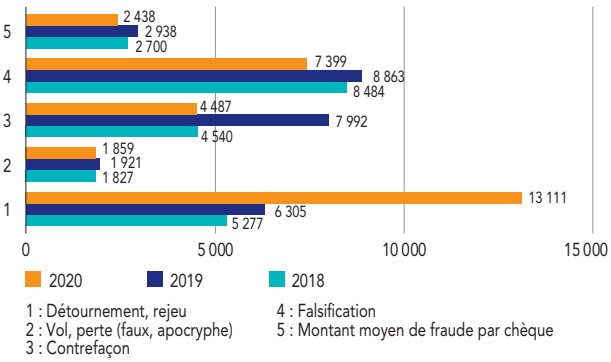
auprès de commerçants ou de vendeurs particuliers, représente 6 % des montants fraudés (contre 14 % en 2019) et 3 % des cas de fraude. Ce type de fraude recule par rapport à 2019, probablement sous l'effet de la fermeture des commerces et de l'action répressive des forces de l'ordre contre les faussaires.

G21 Répartition de la fraude par chèque en montant par typologie de fraude (en %)



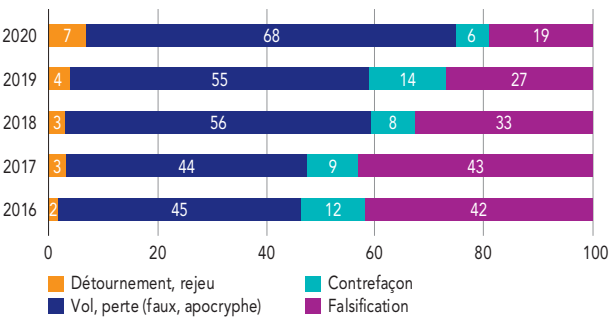
Source : Observatoire de la sécurité des moyens de paiement.

G22 Montant unitaire de fraude par chèque par typologie de fraude, 2018–2020 (en euros)



Source : Observatoire de la sécurité des moyens de paiement.

G23 Répartition de la fraude par chèque en montant, par typologie de fraude, 2016–2020 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

Le montant moyen d'un chèque frauduleux baisse à 2 438 euros, contre 2 938 en 2019 en lien avec la progression des chèques perdus ou volés qui portent en général sur des montants plus faibles par rapport aux autres types de fraude. Les montants unitaires restent particulièrement élevés pour la falsification de chèque (7 399 euros, contre 8 863 euros en 2019) et le détournement (13 111 euros, contre 6 305 euros en 2019).

Face à la hausse continue de la fraude au chèque constatée au cours des cinq dernières années, l'Observatoire a mené une étude sur les pistes de renforcement de la sécurité du chèque en y associant l'ensemble des parties prenantes concernées (banques, autorités publiques, associations de consommateurs, d'entreprises et de commerçants, et prestataires techniques intervenant dans le cycle de traitement de ce moyen de paiement). Le résultat de cette étude, qui comprend des recommandations à l'attention des différentes catégories d'acteurs impliqués, est présenté au chapitre 4 du présent rapport.

2.4 État de la fraude sur le virement

2.4.1 Vue d'ensemble

En 2020, la fraude sur les virements émis depuis un compte tenu en France progresse à nouveau pour s'établir à un peu plus de 267 millions d'euros. Il s'agit d'une hausse significative de 65 % par rapport à 2019 avec un nombre de cas de fraude qui a plus que doublé, avec près de 36 000 opérations frauduleuses en 2020. Le montant moyen d'un virement frauduleux diminue par conséquent, à 7 436 euros, contre 10 144 euros en 2019.

Pour autant, le taux de fraude sur le virement reste à un niveau très bas, à 0,0008 % (contre 0,0006 % en 2019), soit un euro de fraude pour 125 000 euros de paiement, qui s'explique par la forte croissance des flux de ce moyen de paiement (+ 30 % en valeur par rapport à 2019) et leur importance dans les opérations scripturales (91 % du montant total des paiements scripturaux émis en 2020). **Le virement reste le moyen de paiement le moins fraudé en proportion, alors qu'il est celui qui véhicule les montants globaux les plus importants.** Toutefois, ce taux de fraude masque certaines disparités selon le canal d'initiation de l'ordre de virement, le type de virement émis ou encore la destination géographique des fonds.

2.4.2 Répartition de la fraude par canal d'initiation

L'initiation de virement depuis les espaces de banque en ligne (sur Internet ou via application mobile) reste particulièrement vulnérable à la fraude puisque ce canal concentre toujours une part prépondérante des montants fraudés sur ce moyen de paiement (54 % en 2020, contre 55 % en 2019). Cette part reste proportionnellement élevée dans la mesure où les virements émis depuis ce canal ne représentent que 37 % de l'ensemble des flux de virement en valeur et 26 % en volume. Toutefois, le taux de fraude sur ce canal d'initiation est en baisse à 0,0012 % (contre 0,0023 % en 2019), sous les effets probables de la généralisation progressive de l'authentification forte du client pour l'accès aux services de banque en ligne et pour les opérations sensibles qui y sont réalisées. Cela correspond à un euro de fraude pour 83 300 euros de paiement. La fraude sur ce canal résulte de faux ordres de virement initiés par des fraudeurs à partir de l'usurpation des données personnelles de connexion aux espaces de banque en ligne ou mobile du client légitime, mais aussi d'ordres de virement initiés par le client lui-même à la suite d'une manipulation par le fraudeur.

Le canal télématique (principalement utilisé par la clientèle professionnelle) représente 35 % des montants fraudés sur ce moyen de paiement, soit une part en progression d'une année à l'autre (24 % en 2019), avec néanmoins un taux de fraude en sensible hausse sur un an à 0,0008 % (contre 0,0002 % en 2019), quoique toujours extrêmement bas. Si ce mode d'initiation des virements demeure le plus sécurisé, la hausse de la fraude en 2020 s'explique par la recrudescence des fraudes au moyen de techniques d'ingénierie sociale [7], qui exploitent le facteur humain plutôt que la technologie.

Enfin, la fraude sur les virements émis sur support papier (courrier, appel téléphonique, etc.) est en baisse, avec une part qui ne représente plus que 12 % des montants fraudés sur ce moyen de paiement (contre 21 % en 2019). Cette diminution est corrélée à celle des flux initiés depuis ce canal (– 12 % en valeur par rapport à 2019). Le taux de fraude sur les ordres de virement papier reste quasi stable sur un an à 0,0018 % (contre 0,0017 % en 2019), mais à un niveau plus élevé que celui des autres canaux d'initiation. La fraude aux virements émis sur support papier résulte soit de l'émission de faux ordres par le fraudeur, qui usurpe alors l'identité du titulaire du compte débité, soit de techniques de manipulation par ingénierie sociale visant à conduire le titulaire du compte à émettre un ordre de virement illégitime. Ce canal est particulièrement exposé à la fraude compte tenu de ses caractéristiques propres qui ne permettent pas la mise en place des dispositifs avancés de sécurisation, notamment l'authentification forte.

2.4.3 Répartition de la fraude par type de virement

Dans la mesure où la quasi-totalité des virements (98 % des volumes) sont émis sous la forme du virement SEPA classique, ceux-ci concentrent logiquement une part très importante des montants fraudés, soit 79 % des cas de fraude en 2020. Toutefois, le virement SEPA classique ne véhiculant que 31 % des flux en valeur, son taux de fraude s'établit à un niveau relativement faible de 0,0019 % (contre 0,0011 % en 2019), soit l'équivalent d'un euro de fraude pour environ 51 630 euros de paiement.

En ce qui concerne le virement SEPA instantané, sa part dans les montants fraudés reste faible à 4 % compte tenu de son usage encore très modeste (1 % en volume et 0,08 % en valeur des virements émis). En revanche son taux de fraude s'établit à 0,0397 %, soit à un niveau supérieur de près de cinquante fois au taux global sur le virement (à savoir tous types de virement confondus), en légère progression sur un an (0,0311 % en 2019). En effet, le nombre de transactions frauduleuses par virement instantané a été multiplié par près de dix sur un an et représente 20 % des cas de fraude, tandis que le montant moyen a diminué de moitié de 3 022 euros à 1 481 euros. Si l'accélération du déploiement du virement instantané se fait dans des conditions de sécurité globalement maîtrisées, sa généralisation appelle toutefois une attention renforcée des utilisateurs et des professionnels (*cf. chapitre 3, l'étude de veille sur la sécurité des paiements en temps réel*), en particulier lorsque le bénéficiaire des fonds sollicite l'envoi des fonds sur un compte tenu à l'étranger.

Enfin, les virements de gros montants (VGM), échangés au travers d'infrastructures de paiement dédiées et correspondant exclusivement à des paiements de montants unitaires élevés ou urgents par une clientèle d'entreprises et d'administrations, sont relativement épargnés par la fraude avec un taux de fraude extrêmement bas à 0,00001 %, ce qui équivaut à un euro de fraude pour dix millions d'euros de paiement.

2.4.4 Répartition de la fraude par zone géographique

Si toutes les zones géographiques enregistrent une progression des montants fraudés sur le virement, cette augmentation est toutefois particulièrement marquée pour les virements émis en dehors de la zone SEPA, dont le montant fraudé a été multiplié par plus de trois, mais aussi pour ceux

7 L'ingénierie sociale se définit comme « l'art de manipuler son interlocuteur » pour qu'il réalise une action ou divulgue une information confidentielle.

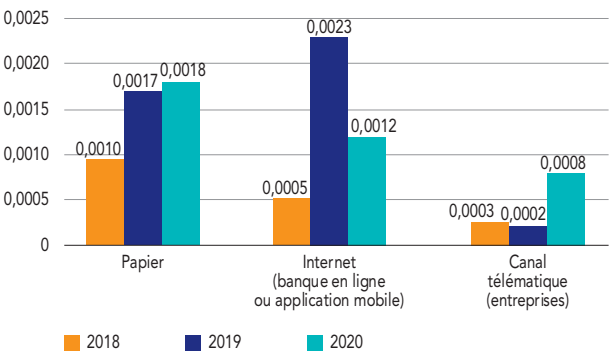
émis vers la zone SEPA (hausse de68 % du montant fraudé par rapport à 2019). Ainsi, les virements transfrontaliers subissent en proportion une fraude plus importante que les virements nationaux, puisqu'ils concentrent 55 % des montants fraudés alors qu'ils ne comptent que pour 12 % des virements émis en montant. La fraude sur les virements nationaux est également en progression mais en comparaison plus mesurée (+ 44 % par rapport à 2019). Pour autant, le taux de fraude sur les virements nationaux reste stable, à un niveau très bas à 0,0004 %, compte tenu de l'importance des flux qui représentent 88 % de l'ensemble des virements émis. Les transfrontaliers conservent, quant à eux, des taux structurellement plus élevés et qui se dégradent d'une année à l'autre à 0,0033 % pour ceux émis vers un pays de la zone SEPA (contre 0,0016 % en 2019) et à 0,0046 % pour ceux émis en dehors (contre 0,0011 %). Cela montre que les fraudeurs ont régulièrement recours à des comptes ouverts à l'étranger pour recueillir les fonds frauduleusement acquis. **L'Observatoire appelle les utilisateurs à une vigilance accrue à l'égard de l'identité de leur interlocuteur et la légitimité de la demande lorsque la destination des fonds semble être un compte étranger (numéro d'IBAN ne commençant pas par FR).**

2.4.5 Répartition de la fraude par typologie de fraude

Le détournement est le type de fraude prépondérante avec une part dans les montants fraudés à 58 %, contre 35 % en 2019, mais qui se concentre sur un nombre plus réduit de cas de fraude, avec une part de seulement 16 % du nombre de virements frauduleux. Cette situation s'explique par le fait que ce type de fraude cible principalement les entreprises et les administrations, et que, par conséquent, il touche moins de victimes mais pour des préjudices financiers plus élevés. La crise sanitaire, avec le renforcement des échanges digitaux et la perte des repères habituels pour les équipes financières et comptables, a été propice à la recrudescence des fraudes au moyen de techniques d'ingénierie sociale. Les procédés de tromperie les plus répandus en 2020 sont ceux relatifs à la fraude au président, à la fraude au changement de coordonnées bancaires ou encore à la fraude au faux conseiller bancaire. Des administrations publiques ont également pu être victimes de telles fraudes, comme la fraude à l'activité partielle, où des fraudeurs ont réussi à usurper l'identité d'entreprises (raison sociale et numéro d'identification) pour détourner les aides financières mises en place dans le cadre de la crise de la Covid-19.

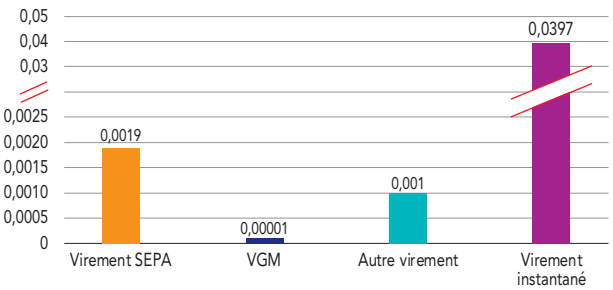
Le faux virement, c'est-à-dire l'émission d'un ordre de virement par le fraudeur, qui en 2019 représentait 61 % des montants fraudés, est en net recul avec une part qui passe à 34 %. Toutefois, ce type de fraude constitue toujours la majeure partie des cas de fraude (79 % en 2020) dans la mesure où il vise davantage les particuliers qui sont soumis à des plafonds sur le montant des virements initiés à distance, obligeant ainsi les fraudeurs à multiplier leurs méfaits pour des montants plus faibles. Pour l'essentiel, l'initiation de faux virement se fait depuis les espaces de banque en ligne (sur Internet ou par application mobile) et à partir des données personnelles de connexion obtenues par les fraudeurs le plus souvent par hameçonnage (*phishing*) ou par des logiciels malveillants (*malwares*). Comme en 2019, les fraudeurs ont profité de la mise en place de solutions d'authentification forte par les banques pour exploiter les actions de communication associées, en envoyant de faux messages visant à collecter les données personnelles de connexion aux espaces de banque en ligne ou mobile, pour ensuite initier des virements frauduleux. Par ailleurs, d'importantes attaques par *phishing* ont été observées durant les périodes de confinement avec notamment des procédés de faux sites de banque en ligne créés à partir de reproductions de tout ou partie du contenu des portails d'établissements existants. À propos de ce phénomène, l'Observatoire invite le public à appliquer les mesures de précaution lors de la connexion aux espaces de banque en ligne qui sont rappelées en annexe 1 de ce rapport.

G24 Taux de fraude sur les virements par canal d'initiation (en %)



Source : Observatoire de la sécurité des moyens de paiement.

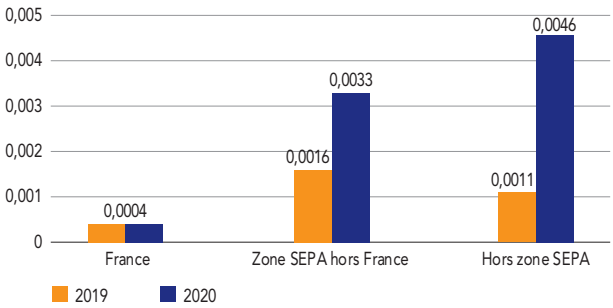
G25 Taux de fraude sur les virements par type de virement (en %)



a) Note : SEPA – *Single Euro Payments Area*, VGM – virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

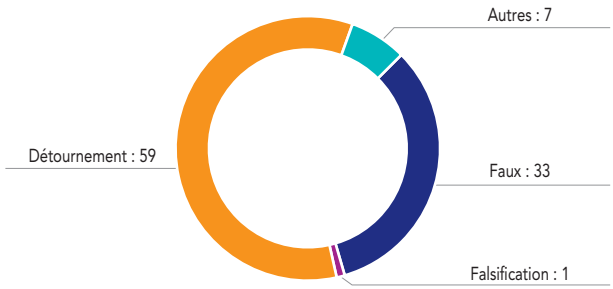
G26 Taux de fraude sur les virements par zone géographique (en %)



Note : SEPA – *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

G27 Répartition de la fraude au virement en montant, par typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.5 État de la fraude sur le prélèvement

2.5.1 Vue d'ensemble

En 2020, les prélèvements frauduleux émis au débit d'un compte tenu en France ont fortement chuté à 1,9 million d'euros, contre 11 millions d'euros en 2019, soit une baisse de 83 %, alors même que les flux émis n'ont que légèrement baissé à 1,6 % en valeur. **Le prélèvement est le moyen de paiement qui présente le montant annuel de fraude le plus limité parmi les instruments de paiement accessibles aux particuliers, ainsi que le taux de fraude le plus bas** à 0,0001 %, contre 0,0006 % en 2019, ce qui équivaut à un euro de fraude pour 1 millions d'euros de transaction. Le montant moyen d'un prélèvement frauduleux s'établit à 292 euros, contre 253 euros en 2019.

2.5.2 Répartition de la fraude par typologie

En 2020, la fraude au prélèvement a pour principale origine le faux prélèvement, c'est-à-dire l'émission d'ordres de prélèvement par un créancier fraudeur sans aucune autorisation ou réalité économique, puisque ce type de fraude représente, à lui seul, 95 % des montants fraudés et 94 % des cas de fraude. Le détournement, c'est-à-dire l'usurpation par un fraudeur de l'IBAN[8] aux fins de souscrire des services (de téléphonie par exemple), n'a quasiment pas été rencontré en 2020 avec une part qui s'établit à moins de 1 % des montants fraudés, alors que celle-ci était de 61 % en 2019.

2.5.3 Répartition de la fraude par zone géographique

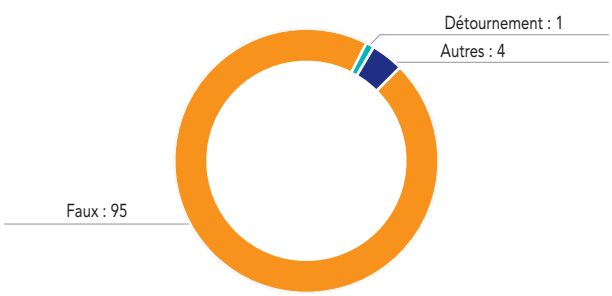
La fraude au prélèvement s'est développée sur les transactions émises vers des comptes de débiteurs tenus par des établissements de la zone SEPA alors qu'elles étaient peu touchées en 2019 : elles représentent 25 % des montants fraudés, alors qu'elles ne comptent que pour 2 % de la valeur totale des flux de prélèvement. En conséquence, le taux de fraude ressort à 0,00164 %, contre 0,0001 % pour le taux global de ce moyen de paiement. Le taux de fraude sur les prélèvements nationaux est, quant à lui, extrêmement bas, à 0,00009 %.

G28 Répartition de la fraude au prélèvement en montant, par zone géographique (en %)

Note : SEPA – *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

G29 Répartition de la fraude au prélèvement en montant, par typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

8 *International bank account number.*

Typologie de la fraude au chèque en 2020

Principaux cas de fraude	Mesures de prévention
Techniques de fraude dérivées du processus dit de « **cavalerie** » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement d'un décaissement des fonds par virements, retraits ou paiements par carte. Ces remises de chèque peuvent se faire : • soit directement par le biais de comptes frauduleusement ouverts sous une fausse identité ou une identité usurpée (par exemple, les comptes de professionnels et d'entrepreneurs bénéficiant de mécanismes de crédit en compte immédiat des chèques remis à l'encaissement), • soit indirectement par le biais d'une tierce personne, souvent des particuliers, qui accepte, contre promesse de rémunération ou dans un contexte de chantage affectif, d'encaisser les chèques frauduleux (fraude à la « mule »)	**Identification des flux d'encaissement atypiques** au regard du profil du client et de ses habitudes afin de : • temporiser l'encaissement des fonds, le temps de vérifier la légitimité de la remise auprès du remettant et la régularité du chèque auprès de la banque tirée, • renforcer la vigilance sur les opérations ultérieures de retrait ou de transfert des fonds vers un autre établissement, immédiatement consécutives à une remise de chèques.
Vol de chéquiers dans les circuits de distribution : les circuits de distribution font intervenir de nombreux prestataires extérieurs aux banques, notamment pendant le transport ou lors de la remise au client. Le vol de chéquiers ou de formules de chèques vierges peut se produire à deux niveaux : • en amont de la délivrance au client : chez les prestataires fabricants et/ou expéditeurs, chez les prestataires transporteurs ou distributeurs vers les agences bancaires, dans les boîtes à lettres des clients bénéficiaires, • lors de la remise en agences bancaires, les fraudeurs utilisent des pièces d'identité volées ou falsifiées pour se faire remettre un chéquier. **Vol de chéquiers lors de la détention par le client lui-même** faisant suite à un cambriolage, un vol ou la perte de son chéquier.	**Mise en opposition systématique et rapide des chèques volés ou perdus**, même en cas de souscription d'une assurance couvrant ces événements. La déclaration se fait auprès de l'établissement bancaire. Rappel régulier par les banques des obligations de vigilance des détenteurs de chéquiers et lettres-chèques et des modalités de mise en opposition des chèques. **Traçabilité des envois** de chéquiers et lettres-chèques durant les phases de transport. **Information par la banque de la mise à disposition d'un chéquier**, soit en agence bancaire, soit par pli postal selon l'option définie par le client lors de la souscription au moyen de paiement, et indication d'un délai attendu de mise à disposition, permettant au client d'informer sa banque en cas de retard constaté. **Les commerçants peuvent se prémunir des chèques volés ou perdus en accédant au Fichier national des chèques irréguliers (FNCI)** de la Banque de France, service officiel de prévention des impayés chèques [1].
Falsification d'un chèque régulier intercepté par les fraudeurs, consistant à altérer le chèque subtilisé par grattage, gommage ou effacement, se manifeste par le fait que, concrètement, les fraudeurs tirent profit des vulnérabilités présentes sur le chèque subtilisé pour le modifier, par exemple : • en substituant, par grattage ou gommage, le nom du bénéficiaire légitime inscrit avec une encre faible, • en réécrivant un nom de bénéficiaire sur celui du bénéficiaire légitime, • en ajoutant une mention (par exemple nom ou sigle, tampon de société, etc.) après celui du bénéficiaire légitime sur l'espace libre de la ligne non remplie, • en ajoutant un montant en lettres et/ou en chiffres sur l'espace libre laissé avant ou après la mention manuscrite.	**Remplir les chèques de préférence avec un stylo à bille à encre noire**, sans laisser d'espace avant, ni après les mentions obligatoires, par exemple en tirant un trait horizontal. **Vigilance particulière sur les chèques envoyés par voie postale**, en vérifiant la bonne réception du chèque par le bénéficiaire légitime et en consultant régulièrement ses comptes. **Pour les accepteurs de chèque, examen systématique du chèque et des mentions portées, ainsi que de leur cohérence avec l'identité du payeur.** Il s'agit de réaliser un examen physique du chèque afin d'identifier les éventuelles altérations avant son acceptation, ainsi que de contrôler l'identité du payeur, via la demande par exemple d'une pièce d'identité.
Contrefaçon de chèque, en créant un faux chèque de toutes pièces, émis sur une fausse banque, mais le plus souvent sur une banque existante.	**Pour les accepteurs de chèque, examen physique approfondi du chèque et des documents d'identité du payeur** (*cf. ci-dessus*). Il s'agit de vérifier la cohérence des données du chèque et la présence des éléments de sécurité habituellement choisis par la banque émettrice (par exemple, microlettres visibles à la loupe sur les lignes du chèque, encres fluorescentes visibles sous une lampe à ultraviolets, qualité des motifs imprimés, etc.). **Les commerçants peuvent se prémunir des faux chèques en accédant au Fichier national des chèques irréguliers (FNCI)** de la Banque de France, service officiel de prévention des impayés chèques [1]. Cela permet de vérifier la cohérence entre la ligne magnétique et le visuel du chèque et de consulter le fichier recensant les faux chèques connus des établissements bancaires.

1 Cf. *https://www.verifiance-fnci.fr*

Source : Observatoire de la sécurité des moyens de paiement.

Typologie de la fraude au virement en 2020

Cas de fraude rencontrés	Mesures de prévention
En 2020, la fraude de type **détournement au moyen de techniques d'ingénierie sociale** a revêtu essentiellement les formes exposées ci-après : • **La fraude au président :** le fraudeur usurpe l'identité d'un haut responsable de l'entreprise pour obtenir d'un collaborateur la réalisation d'un virement urgent et confidentiel à destination de l'étranger. Pour ce faire, le fraudeur utilise des informations recueillies sur l'entreprise et ses dirigeants sur Internet ou directement auprès des services de l'entreprise. • **La fraude aux coordonnées bancaires :** le fraudeur usurpe l'identité d'un fournisseur, bailleur ou autre créancier, et prétexte auprès du client, locataire ou débiteur, un changement de coordonnées bancaires aux fins de détourner le paiement des factures ou loyers. Le fraudeur envoie les nouvelles coordonnées bancaires par courrier électronique ou avec un courrier en bonne et due forme du créancier. • **La fraude au faux technicien :** le fraudeur usurpe l'identité d'un technicien informatique (de la banque, par exemple) pour effectuer des faux tests dans le but de récupérer des identifiants de connexion, provoquer des virements frauduleux ou encore procéder à l'installation de logiciels malveillants. • **La fraude au faux conseiller bancaire :** le fraudeur usurpe le numéro de téléphone du conseiller bancaire, généralement en période d'absence de ce dernier, et contacte le client pour obtenir des informations et données sensibles.	**Outils de surveillance et de détection des transactions à caractère inhabituel** qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison par exemple de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Un contre-appel auprès du client peut alors être fait afin de vérifier le bien-fondé de l'ordre de virement. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des entreprises et des particuliers.
Les **attaques informatiques** ont principalement visé en 2020 les sites de banque en ligne et ont été réalisées essentiellement par deux moyens. • ***Malwares* :** des logiciels malveillants (tels que les troyens, les *spammeurs*, les virus, etc.) qui s'installent sur l'ordinateur d'une entreprise ou d'un particulier à son insu lors de l'ouverture d'un courriel frauduleux, de la navigation sur des sites infectés ou encore lors de la connexion de périphériques infectés (clé USB par exemple). Ces *malwares* permettent à des fraudeurs d'analyser et de collecter les données transitant par l'ordinateur ou le système d'information du client. Ainsi, lors de la connexion au site de banque en ligne d'un client, le *malware* récupère les identifiant et mot de passe que le client a saisis puis les réutilise pour s'y connecter lui-même, faire une demande d'ajout de bénéficiaire et initier un ordre de virement frauduleux. • ***Phishing* ou hameçonnage :** technique permettant de collecter des données personnelles et bancaires à partir de courriels non sollicités invitant leurs destinataires à cliquer sur un lien renvoyant vers un faux site (celui d'une banque en ligne ou d'un marchand en ligne) lequel le plus souvent demande à l'internaute de communiquer ses coordonnées bancaires. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide (facture à régler sous peine de la suspension d'un service, régularisation d'une interdiction bancaire ou encore une mise à jour sécuritaire). Des variantes du *phishing* sur d'autres canaux sont également mises en œuvre, comme le *smishing* par SMS.	**Déploiement d'un dispositif d'authentification forte pour la validation des ordres de virement** saisis en ligne. **Mise en place d'une temporisation ou d'une authentification forte du client pour l'ajout de nouveaux bénéficiaires** de virement depuis le site de banque en ligne. **Fixation de plafonds maximaux de virements** sur le site de banque en ligne. **Mise à disposition aux clients de solutions informatiques de sécurisation** permettant la recherche d'infections de type *malware* sur les postes de la clientèle. **Outils de surveillance et de détection** des transactions à caractère inhabituel qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison, par exemple, de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Une alerte peut être adressée au client pour lui permettre de faire opposition à la transaction, le cas échéant, pendant la durée de temporisation. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des particuliers, notamment pour réaliser régulièrement les mises à jours sur les systèmes d'exploitation.

Source : Observatoire de la sécurité des moyens de paiement.

Typologie de la fraude au prélèvement en 2020

Cas de fraude rencontrés	Mesures de prévention
Émission illégitime d'ordres de prélèvement (faux prélèvement) : le créancier fraudeur s'enregistre en tant qu'émetteur de prélèvement auprès d'un prestataire de services de paiement et émet massivement des prélèvements vers des IBAN (*international bank account numbers*) qu'il a obtenus illégalement et sans aucune autorisation.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire. **Envoi d'une alerte aux clients débiteurs** lors de la première occurrence d'un ordre de prélèvement émis par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »). **Vigilance sur la communication de son IBAN** dans ses interactions commerciales et ses actions en ligne.
Entente frauduleuse entre créancier et débiteur : un créancier fraudeur émet des prélèvements sur un compte détenu par un débiteur complice de façon régulière et en augmentant progressivement les montants. Un peu avant la fin de la période de rétraction légale (de treize mois après le paiement du prélèvement), le débiteur conteste les prélèvements qui ont été débités sur son compte, au motif qu'il n'a pas signé de mandats de prélèvement correspondants. Au moment des rejets des prélèvements, le solde du compte du créancier fraudeur ne permet plus le remboursement des opérations contestées car les fonds ont été transférés vers un compte tenu à l'étranger.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire.
Usurpation d'IBAN pour la souscription de service (détournement) : le débiteur fraudeur communique à son créancier les coordonnées bancaires d'un tiers lors de la signature du mandat de prélèvement et bénéficie ainsi du service, sans avoir à en honorer les règlements prévus.	**Envoi d'une alerte aux clients débiteur** lors de la première occurrence d'un ordre de prélèvement émis par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays, ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »).

Source : Observatoire de la sécurité des moyens de paiement.

ENCADRÉS

❷ Statistiques de fraude sur les cartes : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire recueille les données de l'ensemble des émetteurs de cartes de type « interbancaire » ou « privatif » [1].

Les statistiques calculées par l'Observatoire pour l'année 2020 portent ainsi sur :

- 682,3 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 89 millions de cartes de type « interbancaire » émises en France (dont 81 millions de cartes avec la fonction sans contact) ;
- 11,9 milliards d'euros de transactions réalisées (principalement en France) avec 5,6 millions de cartes de type « privatif » émises en France ;
- 31,2 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».

Les données recueillies proviennent :

- des cent vingt membres du Groupement des cartes bancaires CB. Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard Europe et de Visa Europe France ;
- de sept émetteurs de cartes privatives : American Express, Oney Bank, Crédit Agricole Consumer Finance, Cofidis, Franfinance, JCB et UnionPay International.

1 Les systèmes de paiement par carte dits « interbancaires » correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. À l'inverse, les systèmes privatifs sont ceux pour lesquels un seul prestataire de services de paiement assure de façon exclusive les fonctions d'émetteur et d'acquéreur.

❸

Fraude nationale sur les paiements à distance selon le secteur d'activité

L'Observatoire a collecté des données permettant de fournir des indications sur la répartition de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions nationales.

La fraude sur la vente à distance se concentrent principalement sur le « Commerce généraliste et semi généraliste », les « Services aux particuliers et aux professionnels » et la « Téléphonie et communication » puisque ces trois secteurs d'activité représentent à eux seuls 65 % des montants fraudés en 2020. Le secteur du « Voyage, transport » qui figure traditionnellement parmi les secteurs les plus touchés par la fraude voit sa part diminuer de moitié dans la fraude totale (de 12,9 % en 2019 à 6,7 % en 2020) sous l'effet de la très nette réduction des paiements par carte à destination de ce secteur (– 81 % en 2020 par rapport à 2019) en lien avec la crise de la Covid-19.

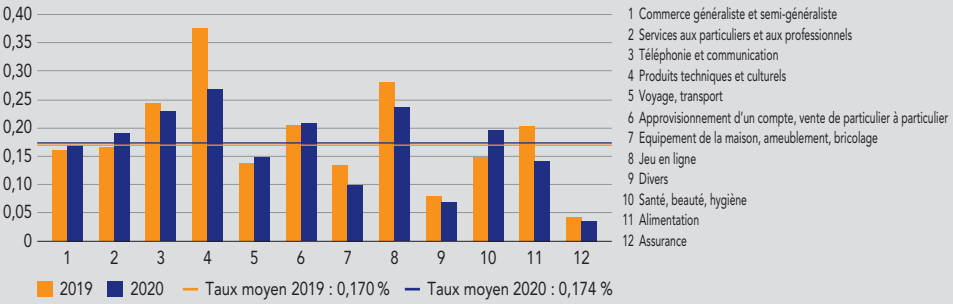
D'une année à l'autre, les taux de fraude par secteur d'activité n'enregistrent pas de dégradation significative avec même une nette amélioration pour le taux de fraude du secteur des « Produits techniques et culturels » qui passe de 0,376 % en 2019 à 0,270 % en 2020. Toutefois, ce secteur avec celui de la « Téléphonie et communication » et du « Jeu en ligne » ont les taux de fraude les plus élevés de l'ensemble des secteurs d'activité, supérieurs à la moyenne (*cf. graphique*).

Répartition de la fraude par secteur d'activité (montant en millions d'euros, part en pourcentage)

		Montant	Part
1	Commerce généraliste et semi-généraliste	60,6	27,3
2	Services aux particuliers et aux professionnels	55,1	24,9
3	Téléphonie et communication	29,1	13,1
4	Produits techniques et culturels	18,7	8,4
5	Voyage, transport	14,9	6,7
6	Approvisionnement d'un compte, vente de particulier à particulier	14,2	6,5
7	Équipement de la maison, ameublement, bricolage	10,9	4,9
8	Jeu en ligne	6,3	2,8
9	Divers	5,3	2,3
10	Santé, beauté, hygiène	4,0	1,8
11	Alimentation	1,9	0,9
12	Assurance	0,9	0,4
Total		**221,9**	**100,0**

Source : Systèmes de paiement par carte internationaux.

Taux de fraude en vente à distance par secteur d'activité, transactions nationales (en %)



Source : Observatoire de la sécurité des moyens de paiement.

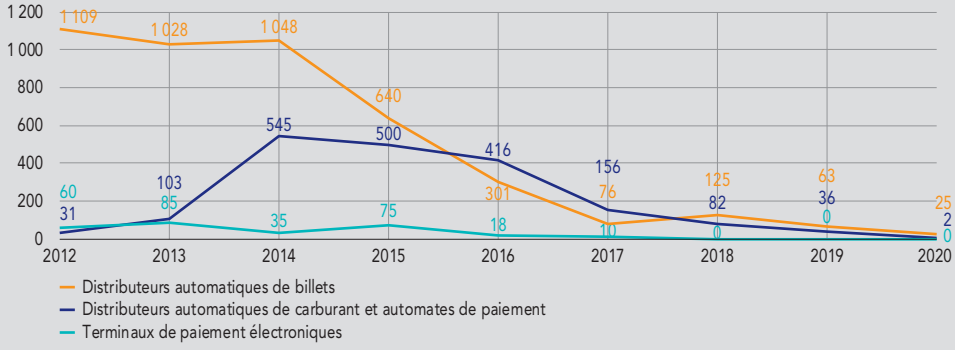
❹ Indicateurs des services de police et de gendarmerie sur le piratage des terminaux

Le nombre de piratages de distributeurs automatiques de billets (DAB) a continué de baisser en 2020 avec 25 cas recensés, contre 63 un an plus tôt. Les attaques de distributeurs automatiques de carburant (DAC) ont quasiment disparu avec seulement 2 cas enregistrés (contre 26 cas en 2019). Enfin, aucun piratage d'automates de paiement, comme les bornes de parking, ni aucune compromission de terminaux de paiement chez les commerçants n'ont été constatés.

En ce qui concerne les modes opératoires, une recrudescence de faits de « *jackpotting* », est apparue au cours de l'été 2020. Cette technique de fraude consiste à attaquer physiquement ou logiquement un DAB par le piratage de l'ordinateur intégré afin d'en prendre le contrôle et ainsi actionner les mécanismes de délivrance des billets. Il s'agit de techniques de fraude très sophistiquées qui ne peuvent être mis en œuvre que par des réseaux organisés ou des délinquants spécialisés. Au-delà des mesures de protection physique et logique des DAB déployées par les professionnels des paiements, l'action répressive des forces de l'ordre (infiltration, exploitation des images de vidéosurveillance, mises sur écoute, etc.) permet de démanteler ces réseaux et de contenir cette typologie de fraude.

En revanche, la fraude par « *skimming* » qui consiste à récupérer, par le biais de terminaux de paiement trafiqués ou usurpés, les données bancaires stockées sur la bande magnétique de la carte, semble maîtrisée. Les commerçants doivent toutefois rester vigilants pour prévenir les tentatives de substitution d'un terminal de paiement légitime par un terminal trafiqué ou toute installation par un tiers d'un dispositif externe frauduleux (lecteur, caméra, clavier, etc.). Les données de la carte ainsi obtenues par les réseaux criminels sont ensuite revendues sur des sites dédiés du *darkweb* ou au travers d'applications téléphoniques. Elles sont ensuite réencodées sur des cartes à piste magnétique qui sont alors utilisées pour des paiements en proximité et des retraits à l'étranger, principalement dans les pays où la technologie de carte à puce EMV (Europay Mastercard VISA) est peu déployée (pays d'Amérique ou d'Asie du Sud-Est notamment), ou soit pour effectuer des paiements à distance, principalement sur les sites de e-commerce qui n'ont pas mis en œuvre l'authentification du porteur de la carte.

Nombre d'infractions constatées sur les distributeurs et terminaux (en unités)



Source : Observatoire de la sécurité des moyens de paiement.

3

ÉTUDE DE VEILLE TECHNOLOGIQUE SUR LA SÉCURITÉ DES PAIEMENTS EN TEMPS RÉEL

3.1 Introduction

Dans le domaine des paiements, l'instantanéité est longtemps restée l'apanage des paiements en espèces. En effet, il suffit d'un simple échange de main à main pour qu'une somme d'argent change de propriétaire et que le bénéficiaire puisse immédiatement utiliser l'argent reçu. Par définition, l'instantanéité protège aussi le bénéficiaire des risques d'absence de provision.

Au cours de ces cinq dernières années, les innovations technologiques ont permis le développement de solutions électroniques de paiement en temps réel. La validation du paiement permet ainsi une extinction immédiate des dettes et des créances. Ces solutions en temps réel participent à la confiance des utilisateurs dans les nouveaux usages numériques (vente à distance, règlement de prestations à domicile, remboursement entre amis, etc.). Les projets de solutions européennes de paiement comme l'initiative européenne pour les paiements « EPI » (*European Payments Initiative*) ou l'initiation de paiement via les interfaces réglementaires qui ont été mises en place à la suite de la deuxième directive européenne sur les services de paiement (DSP 2) s'inscrivent résolument dans une démarche de développement des paiements en temps réel.

3.1.1 Définition du temps réel dans les paiements électroniques

Du point de vue d'un consommateur, le règlement par carte bancaire à un point de vente pourrait être ressenti comme un paiement instantané : une autorisation est donnée au bout de quelques secondes et le consommateur peut repartir aussitôt après avec la marchandise. Cependant, à cet instant précis, le marchand n'a pas reçu le montant de la transaction sur son compte mais seulement une confirmation de l'autorisation du paiement. Le règlement se fera ultérieurement après avoir passé plusieurs étapes de télécollecte, de contrôle, de traitement et de compensation.

Cet exemple illustre la difficulté à définir la notion de « temps réel » pour les paiements électroniques. L'Observatoire de la sécurité des moyens de paiement (OSMP) propose de définir le paiement en temps réel en s'inspirant des caractéristiques essentielles du paiement en espèces. Ainsi, un paiement électronique peut être considéré comme étant en « temps réel », si les trois conditions suivantes sont remplies : i) le donneur d'ordre est immédiatement débité de son compte en banque, ii) le bénéficiaire est immédiatement crédité et peut immédiatement disposer des fonds reçus, et iii) la solution de paiement est accessible en continu (24 h/24, 7 j/7). Il est précisé que le concept d'immédiateté tolère un délai de quelques secondes après l'initiation du paiement.

3.1.2 Périmètre de l'étude

La précédente définition élimine de fait la plupart des paiements scripturaux du périmètre de cette étude. Par conséquent, celle-ci se concentre principalement sur le virement instantané et dans une moindre mesure sur la monnaie électronique, sous réserve qu'elle ne circule qu'entre comptes de monnaie électronique d'un même établissement. Le paiement instantané conjugue ainsi la rapidité des autorisations en temps réel des cartes et la disponibilité immédiate des fonds des paiements en espèces.

Les paiements en temps réel posent de nouveaux défis en matière de lutte contre la fraude. De fait, les paiements instantanés ouvrent une voie nouvelle pour les fraudeurs en facilitant et accélérant les opérations de rebond vers d'autres comptes jouant ainsi sur le facteur temps pour rapidement faire disparaître les fonds détournés. Dans ce contexte,

les stratégies de lutte contre la fraude, déployées par les établissements bancaires [1], se focalisent actuellement sur : i) le renforcement du contrôle du consentement du payeur, notamment à travers les dispositifs d'authentification forte, et ii) le déploiement d'outils d'analyse en temps réel (*scoring* des transactions, analyses comportementales, etc.). L'efficacité de ces outils, parfois basée sur des moteurs d'intelligence artificielle, constitue une des principales promesses pour assurer la sécurité des paiements en temps réel.

La sécurité des paiements en temps réel est toutefois mise à l'épreuve par le développement des fraudes par détournement. Selon la terminologie de l'Observatoire, il s'agit des cas où le fraudeur amène par la tromperie, notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur de confiance, le titulaire légitime du compte à émettre régulièrement un paiement à destination d'un numéro de compte qui n'est pas celui du bénéficiaire légitime ou qui ne correspond à aucune réalité économique. Les techniques d'authentification forte comme les analyses de risques en temps réel sont alors inefficaces, puisque c'est le titulaire du compte qui est à l'origine de la transaction. En 2020, ce type de fraude aurait représenté une grande partie des virements instantanés frauduleux. Au-delà des outils de prévention des établissements bancaires, la vigilance des utilisateurs reste donc indispensable.

3.2 Le développement du temps réel dans les paiements

3.2.1 Les différentes opérations en temps réel

L'ajout de bénéficiaire en temps réel ou « à la volée »

Souvent, la procédure d'ajout d'un bénéficiaire dans l'espace de banque en ligne nécessite un délai de 24 h à 72 h avant de pouvoir effectuer un virement vers ce nouveau bénéficiaire. Ce délai est mis à profit par les établissements bancaires pour informer le client de l'ajout du nouveau bénéficiaire et de cette manière lui donner le temps de réagir en cas de fraude. Ce délai permet aussi aux établissements bancaires de contraindre l'automatisation de la fraude, dans le cas où les identifiants bancaires ont été obtenus via des procédés de piratage informatique de type *malware* ou *phishing*.

Toutefois, ces mesures de temporisation sont susceptibles d'entraver le développement des paiements en temps réel. Dans le même temps, les utilisateurs apprécient la fluidité des cinématiques où le bénéficiaire du paiement est identifié par un attribut différent de son IBAN [2], comme un numéro de téléphone ou une adresse électronique. C'est pourquoi les établissements offrent de plus en plus la possibilité d'ajouter des bénéficiaires en temps réel ou « à la volée ». Ce changement de paradigme doit naturellement s'accompagner d'outils de contrôle tels que l'authentification forte ou le *scoring* afin de minimiser les déviations frauduleuses liées à cette opération *(cf. encadré 5)*.

Les transactions intragroupes et les paiements en monnaie électronique

Un circuit d'échange intrabancaire ou intragroupe (parfois qualifié de « quasi-système ») désigne la situation dans laquelle le transfert de fonds s'effectue entre deux comptes domiciliés dans les livres d'un même établissement ou d'un même groupe. On parle de paiements « *on-us* », c'est-à-dire sans recours à un système interbancaire de paiement. Selon les configurations des systèmes informatiques, les paiements « *on-us* » peuvent aussi être réalisés en temps réel.

La monnaie électronique rentre dans ce schéma-là, si le payeur et le bénéficiaire ont ouvert un compte dans les livres de l'émetteur de monnaie électronique et si la transaction se fait en unités de monnaie électronique préfinancées. Par conséquent, une transaction en ligne avec un portefeuille électronique (par exemple : Paypal, Paylib, etc.) n'est pas en temps réel si la transaction est finalement réglée au moyen d'un compte bancaire tiers rattaché au portefeuille électronique.

Le virement instantané

Le temps réel s'est longtemps heurté aux contraintes des circuits interbancaires de compensation et de règlement. En Europe, les travaux conduits sous l'égide du Conseil des paiements de détail en euros (*Euro Retail Payments Board* – ERPB) à partir de 2015 ont favorisé la définition d'un nouvel instrument de paiement en euro : le virement instantané SEPA [3] (en anglais SEPA *credit transfer* Inst, ou SCT Inst). Celui-ci constitue une variante du virement SEPA classique (SEPA *credit transfer*, ou SCT), qui est soumise à des contraintes supplémentaires en matière de délai d'exécution des opérations (moins de dix secondes), de crédit immédiat au compte du bénéficiaire et de disponibilité 24 h/24 et 7 j/7 (*cf. encadré 6 sur les cas d'usage du virement instantané*).

Ce nouveau moyen de paiement est défini par le Conseil européen des paiements (*European Payments Council* – EPC) et encadré par un ensemble de règles, de procédures et de messages. L'EPC a publié en novembre 2016 un recueil de règles [4] (communément appelé *rulebook*) et des guides de

Caractéristiques du virement classique et du virement instantané

	Virement classique (SCT)	Virement instantané (SCT Inst)
Disponibilité de l'initiation	En fonction de l'offre de services de la banque	24/7/365 y compris week-end et jours fériés
Exécution du règlement	Traitement par lot conduisant à un règlement différé de la transaction	Règlement quasi immédiat : crédit du bénéficiaire dans un délai cible de dix secondes après que la banque du bénéficiaire a apposé son horodatage sur la transaction
Information du donneur d'ordre et du bénéficiaire	En fonction de l'offre de services de la banque du donneur d'ordre et du bénéficiaire	Information immédiatement accessible par le donneur d'ordre de l'exécution de la transaction et par le bénéficiaire de la disponibilité des fonds
Montant maximal de la transaction	Aucun plafond	100 000 euros
Délai de rappel des fonds pour émission frauduleuse (*recall*)	Capacité de *recall* pour émission frauduleuse dans un délai de dix jours ouvrables maximum après règlement de l'ordre initial et obligation pour la banque du bénéficiaire d'y répondre dans les quinze jours ouvrables suivants. Les consentements du bénéficiaire et de sa banque sont un prérequis.	À date, même chose que pour virement classique, mais le délai de dix jours pourrait passer à treize mois en novembre 2021
Délai de demande de retours des fonds à l'initiative du client (*request for recall by the originator*)	Le délai de demande de retours des fonds à l'initiative du client s'élève à treize mois à compter de la date de débit en compte du virement SEPA instantané initial. Celle-ci peut être liée à une erreur (IBAN incorrect, montant incorrect, ou à une demande du client sans motif particulier).	
Adhésion au *scheme*	Obligatoire	Optionnelle

Note : SEPA, *Single Euro Payments Area* ; IBAN, *international bank account number*.

Source : Observatoire de la sécurité des moyens de paiement.

mise en œuvre (*implementation guidelines*), que doivent appliquer les établissements adhérant à ce moyen de paiement. Ce nouveau *scheme*, pour lequel l'adhésion par les établissements reste optionnelle, est opérationnel depuis le mois de novembre 2017. En juin 2021, 127 établissements français ont adhéré à ce *scheme*.

Dans le même temps, plusieurs systèmes de paiement ont été établis pour assurer le règlement des virements instantanés en Europe, comme RT1 opéré par ABE Clearing, SEPA (EU) opéré par la STET ou encore TIPS (TARGET *Instant Payment Settlement*) opéré par l'Eurosystème. Les virements instantanés (SCT Inst) sont opérés depuis novembre 2018 et le rapport annuel de l'Observatoire 2020 fait état de quarante-cinq millions de transactions réalisées par virement instantané représentant 1 % des virements émis et 0,08 % des montants. Le taux de fraude associé s'élève à 0,040 %. L'usage du virement instantané est en progression constante, le nombre de transactions en virement instantané ayant été multiplié par plus de trois en 2020 par rapport à 2019. Le pourcentage de rappel (« *recall* ») sur les virements instantanés est dix fois plus important que sur le virement classique (0,01 % pour les SCT Inst, contre 0,001 % pour les SCT) et la très grande majorité des « *recall* » sur le SCT Inst le sont pour motifs de fraude.

3.2.2 Le temps réel : de nouveaux risques, mais aussi de nouvelles opportunités pour la sécurité des paiements

La disponibilité immédiate des fonds

La capacité d'utilisation immédiate des fonds est à double tranchant. Elle est à la fois un argument majeur en faveur du paiement en temps réel et un nouveau vecteur de fraude. Le temps réel permet en effet aux fraudeurs de faire disparaître encore plus rapidement les fonds frauduleusement obtenus. Le retour des fonds demandé par le *recall* de virement SEPA (classique ou instantané) est très incertain car il dépend de la réponse favorable du bénéficiaire et de sa banque. On note ainsi que le taux de réponse est généralement plus faible pour les banques étrangères que pour les banques françaises. En cas de fraude, le *recall* est donc très rarement positif.

1 Nous utiliserons par commodité dans cette étude les termes « banque » et « bancaire » pour désigner l'ensemble des prestataires de services de paiement, c'est-à-dire les établissements de crédit, les établissements de paiement et les établissements de monnaie électronique.

2 *International bank account number.*

3 *Single Euro Payments Area.*

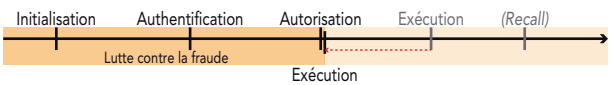
4 La dernière version de ce *rulebook* est la version 1.1, elle a été publiée en mars 2020 et sa période d'application est fixée du 1er avril 2020 au 21 novembre 2021 (cf. *www.europeanpaymentscouncil.eu/document-library/rulebooks/2019-sepa-instant-credit-transfer-rulebook-version-11*).

Le rajout de bénéficiaires à la volée

Cette fonctionnalité est nécessaire au développement des paiements en temps réel. Elle réduit néanmoins la capacité des contrôles de fiabilité du compte rajouté et de cohérence du destinataire avec le profil du client.

Le temps disponible entre l'autorisation du paiement et son exécution est réduit à quelques secondes

Les systèmes d'analyse des risques des banques des donneurs d'ordre peuvent fonctionner en amont de l'autorisation (c'est le cas pour les transactions par carte bancaire) et en aval de l'autorisation avant son exécution (c'est le cas habituellement des virements). S'agissant des paiements en temps réel, le fait que l'exécution intervienne immédiatement après l'autorisation contraint énormément les systèmes d'analyse des risques. Ceux-là peuvent continuer à surveiller les transactions en aval de leur exécution, mais les chances de succès d'un *recall* sont par définition plus limitées. Pour lutter contre la fraude des paiements en temps réel, les établissements bancaires doivent ainsi trouver un équilibre entre l'analyse des nouvelles méthodes de fraude pour bloquer les transactions dans un laps de temps très court et la réduction au strict nécessaire des alertes pour pouvoir les traiter et ne pas occasionner de gêne excessive vis-à-vis de l'utilisateur.



Information de l'utilisateur en cas de fraude

Le développement de la lutte contre la fraude s'articule également autour de la capacité des systèmes à alerter rapidement l'utilisateur dès qu'une opération de paiement est exécutée, voire suspectée comme frauduleuse. La deuxième directive européenne sur les services de paiement (DSP 2) prévoit déjà que l'information sur l'ordre de paiement transmis soit immédiatement accessible au payeur (article 48). Les systèmes d'alerte en mode « *push* » vont plus loin et cherchent à appeler l'attention de l'utilisateur pour le faire réagir rapidement en cas de fraude. Leur efficacité dépend de leur capacité à capter l'attention de l'utilisateur dans un flot de courriels et de notifications.

3.3 La lutte contre la fraude

3.3.1 L'authentification forte

L'authentification forte permet à l'établissement bancaire de vérifier que le donneur d'ordre est bien le titulaire légitime du compte. En se fondant sur des attributs d'identification vérifiés, elle apporte un niveau de garantie élevé quant au consentement de la personne, physique ou morale, sur l'ordre de paiement. L'authentification forte doit être demandée en même temps que l'établissement bancaire présente un récapitulatif de l'ordre de paiement au payeur afin qu'il s'assure de son exactitude et de sa cohérence.

L'authentification repose sur l'établissement de ce lien dynamique et la mise en œuvre d'au moins deux éléments parmi les trois catégories suivantes : i) un élément de connaissance (mot de passe, code secret, etc.) ; ii) un élément de possession (téléphone portable, carte à puce, etc.) ; et iii) une caractéristique personnelle (empreinte digitale, reconnaissance faciale, etc.).

C'est le sens des exigences d'authentification forte portées par la DSP 2 qui s'appliquent à la fois :

- lorsque le client exécute à distance une action susceptible de comporter un risque de fraude, ce qui est le cas lorsque le client souhaite enregistrer un nouveau bénéficiaire de confiance dans son espace de banque en ligne pour réaliser un virement (*cf. encadré 7*) ;
- lorsque le client initie une opération de paiement électronique, ce qui est le cas des paiements en temps réel en virement instantané ou en monnaie électronique.

3.3.2 Le paramétrage des droits en matière de paiement instantané

Les établissements bancaires ont également la possibilité d'encadrer les paiements en temps réel par différents paramètres bloquants, qui peuvent parfois être modifiables pour tout ou partie par le client. Il peut s'agir de plafonds par opération, de plafonds par période de temps (par jour, sur sept jours glissants, etc.), de limitations géographiques des bénéficiaires, etc. Ces outils, principalement conçus pour protéger les établissements bancaires des risques de crédit, sont assez rudimentaires en matière de lutte contre la fraude. Ils peuvent toutefois se révéler utiles en cas de phénomènes de fraude incontrôlés, notamment pour limiter les préjudices financiers.

3.3.3 Les outils de détection automatique des transactions suspectes

Face au développement des opérations de paiement en temps réel, les banques se dotent d'outils d'analyse en temps réel fondés sur des algorithmes complexes et des techniques d'intelligence artificielle.

La méthode mathématique principalement utilisée pour exploiter des volumes importants de données est la classification binaire supervisée, le but étant d'identifier un évènement probable de fraude. Cette approche nécessite la récupération d'un historique de données labellisées par des experts (marquage des transactions comme autorisées ou frauduleuses, par exemple) et repose généralement sur des modèles constitués d'ensembles d'arbres de décision. Ces modèles peuvent aussi détecter et exploiter des signaux faibles en repérant des corrélations complexes entre un grand nombre de variables. Ces méthodes supervisées sont performantes mais ne sont applicables que si les comportements frauduleux sont bien définis et que le nombre de cas enregistrés est suffisant.

Or les fraudeurs cherchent sans cesse à contourner les processus de contrôle. Il peut alors être pertinent d'adopter, en complément, des approches dites non supervisées, qui consistent à assimiler la fraude à une anomalie et donc à détecter les pratiques qui dévient du comportement « normal ». Plusieurs établissements bancaires explorent ainsi des outils d'intelligence artificielle, comme le *machine learning* ou apprentissage automatique, pour améliorer ces outils de filtrage en temps réel (*cf. encadré 8 cas d'usage*). Ces approches peuvent également se révéler intéressantes lorsque des évènements causent des changements rapides et brutaux dans les comportements des utilisateurs, à l'instar des périodes de confinement liées à l'épidémie de la Covid-19.

Quelle que soit la méthode utilisée, les établissements bancaires sont souvent confrontés à la complexité du filtrage et d'autorisation des flux. Si l'outil de filtrage identifie un ordre de virement instantané atypique nécessitant une investigation, il devient impossible de contrôler l'opération dans le délai attendu. Les règles du virement instantané appellent en effet une autorisation ou un refus du paiement dans un délai très court, et ne permettent pas à l'établissement bancaire d'exécuter le paiement tout en communiquant à la banque du bénéficiaire une suspicion de fraude [5]. Le principal défi de ces outils d'analyse en temps réel est donc de réduire les « faux positifs », c'est-à-dire des opérations signalées à tort comme potentiellement frauduleuses, tout en récupérant les « faux négatifs », c'est-à-dire les opérations signalées comme valides et qui sont en réalité frauduleuses.

Aujourd'hui, le manque de recul sur l'utilisation du paiement instantané et la nécessité d'avoir accès à de grands ensembles de données ne permettent pas encore d'obtenir des systèmes de lutte contre la fraude d'un niveau équivalent à celui de la carte. Les paiements électroniques en temps réel sont encore récents, et par conséquent les outils automatiques de détection des transactions suspectes doivent rester agiles pour apprendre au contact des nouveaux cas de fraude.

3.3.4 L'information du payeur en temps réel

Enfin, les établissements bancaires peuvent proposer des service d'alertes « *push* ». L'utilisateur a la possibilité de suivre en temps réel les opérations réalisées sur son compte à l'aide de notifications paramétrables sur l'application de banque en ligne ou via les interfaces logicielles. Ces outils facilitent la gestion des comptes au quotidien, et permettent aussi au client de détecter plus rapidement une opération frauduleuse et de réagir le cas échéant auprès de sa banque. Dans le cadre du virement instantané, l'émetteur doit ainsi être immédiatement informé de la réussite ou de l'échec du virement instantané.

3.3.5 La vigilance de la banque du bénéficiaire et de ses prestataires

En complément des outils de détection automatique des transactions frauduleuses par la banque du payeur, la sécurité des paiements en temps réel peut aussi bénéficier des outils de vigilance déployés par la banque du bénéficiaire. Ceux-là peuvent permettre d'identifier des opérations atypiques en réception qui ne correspondent pas au profil attendu du client. Les alertes peuvent ainsi conduire à renforcer le niveau de vigilance sur les opérations ultérieures initiées à partir du compte du bénéficiaire. En effet, dans le cas des fraudes sur des paiements en temps réel, les fonds détournés à l'aide de paiements instantanés sont rapidement retirés, utilisés ou transférés vers un autre compte.

3.4 Conclusion et recommandations

Un paiement électronique est qualifié de « temps réel » lorsqu'il remplit ces trois conditions : 1) le donneur d'ordre est immédiatement débité de son compte en banque, 2) le bénéficiaire est immédiatement crédité et peut immédiatement disposer des fonds reçus, et 3) la solution

5 Lors de la revue des règles du SCT Inst en 2020, certains participants avaient exprimé auprès du Conseil européen des paiements (*European Payments Council* – EPC) le souhait d'intégrer un indicateur de fraude, qui aurait pu conduire la banque du payeur à autoriser le paiement tout en communiquant une suspicion de fraude à la banque du bénéficiaire. Cette évolution a toutefois été écartée en raison du manque de recul sur l'utilité d'un tel marqueur en matière de lutte contre la fraude et sur les conséquences que cela pourrait impliquer sur la responsabilité de la banque du bénéficiaire qui recevrait une telle transaction.

de paiement est accessible en continu (24 h/24, 7 j/7). À ce titre, le virement instantané est le principal instrument de paiement en temps réel et plusieurs projets misent sur son développement, comme les solutions d'initiation de paiement introduites par la DSP 2 ou le projet d'une solution européenne de paiement portée par plusieurs banques européennes (*European Payments Initiative* – EPI).

Les paiements en temps réel apportent des bénéfices certains aux utilisateurs, payeurs comme bénéficiaires. Mais ils peuvent aussi faciliter la réalisation de la fraude en accélérant le détournement des fonds. Les établissements bancaires sont contraints de déterminer, en quelques secondes, le niveau de sécurité de l'opération, car une fois l'opération exécutée, les demandes de retour des fonds ont très peu de chances d'aboutir.

Dans ce contexte, la lutte contre la fraude repose en majorité sur des actions en amont de l'exécution de l'opération de paiement. Pour créer la confiance dans les paiements en temps réel, l'Observatoire invite les prestataires de services de paiement ainsi que leurs agents à :

- mettre en œuvre, dans les conditions fixées par la DSP 2, l'authentification forte de leurs utilisateurs pour l'autorisation des paiements en temps réel et pour toute opération sensible périphérique (ajout d'un bénéficiaire, changement de coordonnées, etc.) ;
- améliorer en continu les outils de prévention de la fraude en temps réel ; à ce titre, l'Observatoire encourage les établissements à explorer les technologies basées sur l'apprentissage automatique qui pourraient à terme améliorer la performance des systèmes d'analyse de risques actuellement déployés ;
- faire usage si nécessaire des mesures de paramétrage des droits, de type plafonds et limitations, pour limiter les préjudices d'un développement incontrôlé de la fraude.

La sécurité des paiements en temps réel suppose aussi des mesures de vigilance en aval de l'exécution. L'Observatoire appelle ainsi les prestataires de services de paiement des bénéficiaires des fonds à identifier les opérations atypiques en réception, notamment quand celles-ci précèdent d'autres opérations en sortie.

Enfin, l'Observatoire rappelle le rôle essentiel joué par les utilisateurs dans la sécurité des paiements en temps réel, en particulier dans un contexte de développement des fraudes usant de techniques de manipulation ou de tromperie. Par conséquent, l'Observatoire invite les utilisateurs à :

- prêter une attention particulière, avant de valider l'ordre de paiement, à l'origine de la demande et l'identité de l'interlocuteur, et vérifier les coordonnées bancaires du bénéficiaire ;
- saisir des données bancaires exclusivement sur des sites Internet ou des applications mobiles réputés fiables et de confiance ; à cet égard, les utilisateurs sont invités à privilégier les sites et applications référencés et à s'y connecter directement, en considérant avec la plus grande prudence les liens reçus par des moyens de communication peu sécurisés tels que les SMS et courriels ;
- avertir, aussi rapidement que possible après l'exécution du paiement, son établissement bancaire de toute opération suspecte non autorisée ou frauduleuse.

Au-delà des actions de sensibilisation aux risques de fraude, l'Observatoire appelle les prestataires de services de paiement à soutenir la vigilance des utilisateurs par la mise à disposition d'outils de confirmation du bénéficiaire et d'information active et en temps réel des opérations réalisées sur leur compte.

ENCADRÉS

❺ Bénéficiaire occasionnel et bénéficiaire de confiance pour les virements

Au titre de l'article 13 du règlement délégué (UE) 2018/389 sur les normes techniques de règlementation relatives à l'authentification forte du client, les paiements électroniques peuvent bénéficier de l'exemption de l'authentification forte, sous réserve que le bénéficiaire soit enregistré par le payeur comme bénéficiaire de confiance auprès de son prestataire de services de paiement (PSP) gestionnaire de compte.

Ainsi chaque utilisateur a la possibilité de créer une « liste blanche », tenue par sa banque, de commerçants qui ne sont pas concernés par l'authentification forte. Par exemple, après un premier achat authentifié avec succès sur un site de e-commerce, il peut être proposé à l'utilisateur d'ajouter ce site dans cette liste blanche afin que les achats futurs sur ce même site ne requièrent pas d'authentification forte supplémentaire.

À cet effet, les PSP gestionnaires de comptes devront être en mesure de différencier les bénéficiaires de confiance désignés par le titulaire du compte des autres bénéficiaires enregistrés.

❻ Les cas d'usage du virement instantané

Le virement instantané peut être utilisé dans de nombreuses situations :

- Le paiement de personne à personne (P2P) : partage d'addition, achats en ligne entre particuliers ou paiements sur une brocante, etc.
- Le paiement des entreprises aux consommateurs : restitution directe des fonds après le retour des marchandises, paiement direct des réclamations d'assurance, règlement des gains de jeux, etc.
- Paiements des consommateurs aux marchands : commerce électronique ou en magasin, en alternative aux cartes ;
- Le paiement entre entreprises, notamment grâce au rehaussement du plafond à 100 000 euros au 1er juillet 2020 : paiements en temps réel dans le cadre de livraisons de marchandises, règlement des factures aux fournisseurs.

❼ Les outils de confirmation du bénéficiaire ou « *Confirmation of Payee* » (CoP)

La confirmation du bénéficiaire est un outil qui permet aux utilisateurs réalisant un virement, de s'assurer qu'ils envoient leurs paiements au destinataire prévu avant l'exécution. Il s'agit d'un service de vérification de correspondance entre l'IBAN [1] et le nom du compte qui permet d'éviter que les virements ne soient accidentellement acheminés vers de mauvais bénéficiaires.

Ces outils permettent d'introduire un obstacle pour les fraudeurs en avertissant les utilisateurs des risques liés à l'envoi de paiements vers un compte dont le nom ne correspond pas à l'IBAN du bénéficiaire. L'Observatoire encourage l'utilisation de tels outils qui permettent d'abord de réduire les erreurs mais qui peuvent aussi susciter la vigilance des utilisateurs en cas de fraude par manipulation du titulaire légitime du compte (ingénierie sociale de type fraude au faux fournisseur, fraude au président, etc.).

1 *International bank account number.*

❽ Cas d'usage du *machine learning* pour la sécurité des paiements en temps réel

À la suite de la croissance rapide des volumes de paiement, un établissement a constaté une augmentation du nombre d'alertes de fraude sur le paiement en monnaie électronique. Or 90 % de ces alertes étaient des faux négatifs et ne correspondaient donc pas à un cas réel de fraude. Afin d'optimiser son système d'alerte, l'établissement utilise depuis 2019, un prototype d'algorithme de détection de la fraude assistée par ordinateur et développé en interne. Cet algorithme est basé sur le principe du « *machine learning* ».

Il se compose d'une combinaison de modules « supervisés » et de modules « non supervisés ».

- Les modules supervisés sont fondés sur une base de données reprenant l'ensemble des comportements de fraudeurs identifiés depuis le 1er janvier 2018. L'algorithme est nourri par cet historique de cas de fraudes avérées et cherche à retrouver ces comportements parmi les utilisateurs.
- Les modules non supervisés se fondent sur l'idée que certains comportements non encore identifiés peuvent néanmoins relever de la fraude. Le module analyse l'ensemble des comportements utilisateurs, et signale ceux qui lui paraissent « inhabituels ».

Grâce à ce développement, les tests réalisés ont permis de détecter 97 cas de fraudes avérées sur un total de 100 alertes.

4

ÉTUDE SUR LA FRAUDE AU CHÈQUE : ENSEIGNEMENTS ET RECOMMANDATIONS

La fraude au chèque a sensiblement augmenté au cours des cinq dernières années, au point de devenir, depuis 2019, l'instrument de paiement le plus fraudé à la fois en taux et en montant devant la carte (538 millions d'euros de fraude en 2020, soit 42 % du total de la fraude aux moyens de paiement scripturaux). L'analyse conduite en 2018 sur les moyens de paiement non connectés avait déjà montré que le chèque était difficilement compatible avec des dispositifs avancés de sécurisation, tels que le recours à l'authentification forte. Face à cette hausse des risques, l'Observatoire a mené une étude spécifique pour mieux connaître les phénomènes de fraude au chèque, identifier ses principales vulnérabilités et émettre des recommandations pour lutter contre son développement.

4.1 Un moyen de paiement en rapide décroissance, mais encore utilisé chez certains particuliers et personnes morales

Les statistiques de la Banque de France montrent que l'usage du chèque a atteint un sommet à la fin des années 1990. En 2000, il était l'instrument de paiement scriptural le plus utilisé (34 % des transactions) devant la carte (25 %). En vingt ans, le volume de chèques émis a été divisé par trois pour atteindre 1,2 milliard de transactions en 2020, soit 5 % des transactions scripturales. Cela correspond à environ 1,8 chèque par mois et par Français. Malgré la baisse observée, l'usage du moyen de paiement par chèque reste une spécificité française à l'échelle de l'Europe.

Cette baisse des transactions par chèque, d'environ 4 % par an entre 2000 et 2010, s'est accélérée tout au long de la décennie 2010-2020 pour atteindre 9 % en 2019. Il est attendu que les conséquences de la crise sanitaire de la Covid-19 détournent encore plus durablement les utilisateurs de ce moyen de paiement. En 2020, les transactions par chèque ont chuté de 26 % en nombre et de 25 % en valeur. Il n'est pas possible de faire précisément la part entre la baisse conjoncturelle liée à la crise économique et la baisse structurelle liée aux changements d'habitude de paiement des particuliers et des entreprises. Toutefois, les premières statistiques disponibles sur 2021 ne témoignent d'aucun retour des flux sur les tendances antérieures à la pandémie.

Cela étant, le chèque reste un moyen de paiement important. Avec 614 milliards d'euros échangés en 2020, il reste le troisième moyen de paiement scriptural en montant, derrière le virement et le prélèvement, toujours devant les paiements par carte (hors retraits). En effet, s'il est de plus en plus rarement utilisé, le chèque reste associé à des transactions d'un montant plus important puisque le montant moyen du chèque était de 522 euros en 2020.

Cette moyenne cache la grande diversité des utilisateurs de chèques tant à l'émission qu'à l'acceptation. Cet instrument de paiement est en effet utilisé par les particuliers – plus de huit français sur dix possèdent un chéquier –, mais aussi les associations, les professionnels et les entreprises de toute taille. Chez les particuliers, beaucoup disent encore être confrontés à des transactions qui ne peuvent se faire que par chèque. Son utilisation serait également plus importante chez les ménages en situation de fragilité financière. Chez les entreprises, une enquête de l'Association française des trésoriers d'entreprises (AFTE) menée auprès de ses adhérents a montré que peu d'entreprises, à l'exception des commerçants, n'acceptaient pas de chèques. Si 14 % des entreprises interrogées déclaraient ne pas en émettre, 46 % disaient avoir des projets pour arrêter d'en émettre.

Le chèque reste en effet considéré comme un moyen de paiement simple, accessible et universel. Il est autant utilisé en proximité qu'à distance via les courriers postaux. Dans le monde des professionnels, certains préfèrent encore émettre des chèques qu'utiliser des cartes commerciales. Certains professionnels l'apprécient aussi pour effectuer leur comptabilité. Les délais et les oublis d'encaissement par les bénéficiaires peuvent également apporter un gain de trésorerie aux entreprises qui en émettent. Pour les particuliers, le chèque reste une facilité de crédit à court terme (paiements en plusieurs fois en remettant plusieurs chèques au créancier, accord avec ce dernier sur la date de remise à l'encaissement, etc.). Le chèque peut encore être utilisé pour le loyer, les soins médicaux, les dépenses de loisirs, les frais d'école et de cantine, les factures liées à l'habitation, ou encore les travaux. En revanche, le chèque est beaucoup moins utilisé par les administrations et de moins en moins accepté par les commerçants en raison des impayés liés au motif « sans provision ». Les grands réseaux de distribution continuent toutefois d'accepter ce moyen de paiement (alimentation, ameublement, mode, etc.).

En l'état actuel des choses et à défaut de nouvelles mesures, il est donc attendu que le chèque reste présent dans le paysage des moyens de paiement d'ici 2030. En lien avec le Comité national des paiements scripturaux (CNPS), l'Observatoire pourrait étudier l'intérêt de mesures plus contraignantes pour les utilisateurs et ainsi accélérer le déport des usages vers des moyens de paiement plus sécurisés.

4.2 Un moyen de paiement vulnérable compte tenu de la baisse et des évolutions de son usage

La baisse de l'usage du chèque nourrit ses vulnérabilités :

- D'une part, au cours des vingt dernières années, les évolutions normatives ont essentiellement porté sur les instruments de paiement électroniques comme la carte et les instruments SEPA (*Single Euro Payments Area*), comme le virement et le prélèvement. La deuxième directive européenne sur les services de paiement (DSP 2), qui exclut le chèque de son champ d'application, renforce ainsi la sécurité des moyens de paiement électroniques, notamment via l'authentification forte. Par conséquent, par un effet de « vase communicant », les fraudeurs déportent leurs attaques vers les instruments de paiement les moins sécurisés tel que le chèque, qui comporte certaines caractéristiques propices à la fraude comme son support papier ou l'absence de plafond dans son usage.
- D'autre part, la baisse de l'usage du chèque peut expliquer une moindre vigilance des utilisateurs, voire une méconnaissance du moyen de paiement. Le chèque n'est pas un instrument de paiement garanti : son encaissement est sous réserve de bonne fin et peut être refusé en cas de manque de provision du tireur, d'irrégularités, d'utilisation frauduleuse, etc. Les transactions se faisant moins nombreuses, les utilisateurs ne connaissent plus aussi bien les précautions à prendre avant d'émettre ou d'accepter un chèque, ni les conditions de conservation. À titre d'exemple, les particuliers laissent plus souvent leurs chéquiers à domicile, dans des endroits peu protégés en cas de cambriolage.
- Enfin, en réponse à la baisse de la demande, les établissements bancaires n'investissent plus dans la promotion de ce moyen de paiement. Si les banques maintiennent leurs investissements dans la lutte contre les remises frauduleuses, le système de paiement par chèque est resté stable au cours des vingt dernières années, depuis sa mise en place au tournant des années 2000.

Au-delà de la baisse des volumes, les risques associés au recours à la voie postale dans les nouveaux usages des clients, émetteurs comme bénéficiaires de chèques, accentuent sa vulnérabilité :

- Si le chèque est un instrument de paiement matériel, l'évolution rapide de la consommation des moyens de paiement depuis dix ans a également eu une incidence sur l'usage du chèque. Avec l'émergence de la banque à distance, de plus en plus de clients préfèrent recevoir leur chéquier par pli postal, et parfois même faire leurs remises à l'encaissement par courrier.
- L'envoi par courrier de chèques comme moyen de règlement est encore une pratique fréquente. Le chèque reste en effet un instrument de paiement souvent utilisé pour les paiements à distance (loyers, factures, règlement des fournisseurs, transactions entre particuliers, etc.).

Dans ces conditions, malgré la baisse de son usage, l'existence de ces vulnérabilités laisse peu espérer une baisse équivalente de la fraude au chèque. Celle-ci est susceptible de rester à un niveau élevé, exposant les utilisateurs – émetteurs comme bénéficiaires – à des risques de préjudices importants. En effet, contrairement aux autres instruments de monnaie scripturale, le cadre législatif ne comporte aucune disposition spécifique destinée à protéger le bénéficiaire en cas de fraude au chèque, le crédit à l'encaissement se faisant sous réserve de paiement effectif par la banque tirée [1]. En effet, la banque du tireur du chèque peut refuser le paiement du chèque pour différents motifs (insuffisance de

provision, opposition au paiement du tireur, irrégularité du chèque, etc.). Faute d'opposition préalable de la part du tireur, les parties prenantes s'exposent à un préjudice financier [2].

4.3 Les premiers enseignements sur la fraude à partir des statistiques de l'Observatoire

4.3.1 Le vol de chèque reste la première source de fraude devant la falsification et la contrefaçon

Depuis le début des statistiques de fraude établies par l'Observatoire sur l'ensemble des moyens de paiement en 2016, l'ampleur de la fraude au chèque a presque doublé en passant de 272 millions d'euros en 2016 à 538 millions d'euros en 2020. Il est ainsi devenu l'instrument de paiement le plus fraudé tant en montant (42 % du total de la fraude) qu'en taux (0,088 %) sous l'effet de la multiplication des attaques. Ces évolutions appellent d'autant plus l'attention de l'Observatoire que le chèque est un instrument de paiement national, qui n'est pas utilisé pour des transactions européennes ou internationales. Celles-ci sont, dans le cas des autres instruments de paiement, plus fraudées que les transactions nationales.

En revanche, la fraude se concentre sur un nombre limité de chèques. S'il représente 42 % de la fraude en montant, le chèque ne représente que 3 % des cas de fraude. Ainsi, 1,9 chèque sont frauduleux sur dix mille chèques émis, contre plus de cinq transactions par carte sur dix mille qui sont frauduleuses. L'Observatoire recense ainsi un cas de fraude au chèque pour trente-trois cas de fraude à la carte. Il en résulte une fraude relativement « discrète » mais efficace, avec un montant moyen de fraude de 2 438 euros, soit un montant quatre fois plus important que le montant moyen du chèque émis. Par rapport à la carte, les victimes sont ainsi beaucoup moins nombreuses, mais leur préjudice est beaucoup plus important.

Les statistiques de l'Observatoire détaillent les trois grandes typologies de fraude au chèque :

- Le vol de formules vierges est la première typologie de fraude avec 89 % des cas de fraude et 68 % des montants. C'est la typologie qui a le plus augmenté depuis 2016. Le montant moyen d'un chèque volé était de 1 860 euros en 2020.
- La falsification et le détournement de chèques régulièrement émis mais interceptés par le fraudeur est la deuxième typologie de fraude avec 8 % des cas de fraude, mais 26 % des montants. Dans le cas d'une falsification, le chèque est frauduleusement modifié, après son émission, dans son montant ou dans son ordre. Le montant moyen d'un chèque falsifié était de 7 399 euros en 2020. Dans le cas d'un détournement, le chèque est laissé en état mais remis à l'encaissement sur un compte qui n'est pas celui du destinataire. Le montant moyen d'un chèque détourné était de 13 111 euros en 2020. Alors que la falsification était en légère hausse depuis 2016, elle a baissé de 30 % en 2020, dans des proportions légèrement supérieures à l'usage du chèque. En revanche, le détournement a progressé pour la quatrième année consécutive pour atteindre 37 millions d'euros en 2020.
- La contrefaçon de chèques, c'est-à-dire des chèques créés de toutes pièces par des faussaires, est la troisième typologie de fraude avec 3 % des cas de fraude et 6 % des montants. Pour les fraudeurs, il reste plus facile de voler des chèques que d'en fabriquer. Après avoir fortement augmenté en 2019, cette typologie de fraude a reculé en 2020 pour revenir à 32 millions d'euros, soit des niveaux comparables à ceux observés entre 2016 et 2018. Le montant moyen des chèques contrefaits était de 4 487 euros en 2020, contre 7 991 euros en 2019.

4.3.2 Les limites des statistiques de l'Observatoire

Les statistiques de l'Observatoire sont fondées sur les déclarations des établissements bancaires en tant que remettants. Cette méthodologie permet d'exclure les tentatives de fraudes qui sont déjouées avant la présentation du chèque à l'encaissement (par exemple, chèque contrefait identifié au moment de sa remise en agence). À l'instar des autres moyens de paiement, l'approche retenue par l'Observatoire est celle de la « fraude brute » qui consiste à retenir le montant initial des opérations de paiement non autorisées par le payeur sans prendre en compte les mesures qui peuvent être prises par les contreparties pour réduire le préjudice. Or, dans le cas spécifique du chèque, cette approche ne permet pas de tenir compte des mesures de temporisation des encaissements mises en place par certains établissements bancaires, qui permettent de déjouer certaines remises frauduleuses de chèques après que le chèque a été présenté au système d'échange.

1 C'est la raison pour laquelle certains utilisateurs souscrivent à des solutions d'assurance. Des assurances aux moyens de paiement sont parfois comprises dans les formules de compte offertes par les établissements bancaires. Les commerçants peuvent aussi souscrire aux services de garantisseurs, qui les protègent contre les risques d'impayés et de fraude.

2 Le chèque est exclu du champ d'application de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (dite DSP 2) et n'est donc pas concerné par les dispositions de cette dernière en matière de remboursement des opérations non autorisées.

Par ailleurs, la méthodologie de l'Observatoire identifie la méthode d'émission d'un chèque frauduleux, mais elle n'identifie pas la méthode d'utilisation des chèques frauduleux. Il est ainsi impossible de faire la part entre, d'une part, les chèques frauduleux qui sont utilisés auprès de bénéficiaires de bonne foi, et d'autre part, les chèques frauduleux qui sont remis à l'encaissement par le fraudeur, directement sur son propre compte ou indirectement par le biais d'une tierce personne. Cette dernière, parfois qualifiée de « mule », peut consciemment participer à une escroquerie en espérant en retirer un bénéfice. Elle peut aussi être trompée par son interlocuteur, qui tire profit de sa fragilité ou de sa naïveté. La qualification du rôle du remettant dépend des enquêtes de police et des décisions de justice. Pour les établissements bancaires, au-delà des soupçons qu'ils peuvent avoir, il est impossible de savoir avec certitude si le client est complice ou victime d'une escroquerie.

Enfin, comme pour les autres moyens de paiement, les statistiques de l'Observatoire ne permettent pas de caractériser le profil des fraudeurs (faussaire isolé, bandes organisées, réseaux mafieux, etc.), ni des victimes (particuliers, professionnels, commerçants, entreprises, etc.). Seules les enquêtes de police peuvent permettre d'obtenir des informations fiables sur le profil des fraudeurs et leurs méthodes.

4.4 Parmi les différents phénomènes de fraude, les remises frauduleuses de chèque sont en forte croissance

Compte tenu des limites de ses statistiques régulières sur la fraude au chèque, l'Observatoire a recueilli de façon exceptionnelle des éléments qualitatifs et statistiques supplémentaires auprès des établissements bancaires pour mieux apprécier l'évolution des phénomènes de fraude depuis 2016. Ces travaux ont permis de confirmer les trois principaux phénomènes de fraude suivants.

4.4.1 Phénomène de fraude n° 1 : les remises frauduleuses de chèque reposant sur différents mécanismes d'escroquerie

Les remises frauduleuses concernent les chèques frauduleux qui sont remis à l'encaissement par le fraudeur. Celui-ci cherche alors à tromper la banque en encaissant les chèques et en récupérant les fonds par différents moyens avant que le chèque ne soit finalement rejeté pour fraude. La source de la fraude est variable, mais il s'agit principalement de chèques volés (environ pour les deux tiers), ensuite de chèques falsifiés ou détournés (environ pour un tiers), plus rarement de chèques contrefaits. Quel que soit le mode opératoire retenu, les montants moyens de ces remises frauduleuses sont élevés.

Deux principaux modes opératoires sont utilisés par les fraudeurs :

- **Majoritairement l'encaissement de chèques par le biais d'une tierce personne :** le développement des escroqueries sur Internet a nourri la hausse des remises frauduleuses via des intermédiaires, parfois appelés « mules », que ceux-ci soient volontaires ou trompés, qui accepteront d'encaisser les chèques frauduleux sur leur compte avant de restituer au donneur d'ordre une partie des fonds.
- **Parfois, le compte ouvert sous une fausse identité :** le fraudeur remet lui-même les chèques à l'encaissement sur un compte ouvert sous une fausse identité. Les remises frauduleuses peuvent être liées à des entrées en relation récentes, parfois réalisées à distance. De fait, le nombre d'entrées en relation à distance a sensiblement augmenté ces dernières années, y compris dans les réseaux bancaires historiques. Si les contrôles se sont perfectionnés, notamment par l'apport des nouvelles technologies de vérification d'identité, la fraude à l'entrée en relation peut parfois être corrélée avec des remises frauduleuses de chèque.

Selon les situations, les personnes servant d'intermédiaires sont plus ou moins actives dans la réalisation d'opérations frauduleuses, certaines pouvant ne pas avoir conscience de l'illégalité de leurs actes. Les méthodes de recrutement de ces personnes intermédiaires font également appel à différentes stratégies d'escroquerie, parmi lesquelles l'Observatoire retient principalement :

- **Les personnes attirées par des promesses d'argent simple et rapide :** ces personnes peuvent être recrutées sur les réseaux sociaux ou avoir répondu à une sollicitation d'un site Internet promettant des solutions de financement rapide. Ces personnes, souvent jeunes et vulnérables, espèrent ainsi gagner de l'argent facilement et rapidement. Il s'agit principalement de jeunes personnes, d'étudiants, de personnes isolées mais aussi de personnes d'âge moyen, parfois en difficulté financière.
- **Les personnes victimes de chantage affectif ou amoureux :** les remises frauduleuses de chèque peuvent aussi être commises par des personnes qui pensent venir en aide à un proche, une entreprise ou une association. Les fraudeurs prennent alors prétexte d'une situation d'urgence pour convaincre le remettant d'encaisser

rapidement le chèque ou exploitent les sentiments de leur victime, comme par exemple dans le cas de fraude à la romance.

- **Les arnaques à l'embauche :** le recrutement se fait à distance au détour d'une offre d'emploi. L'employeur fictif envoie alors un chèque frauduleux à la personne, qui se croit embauchée, sous de faux prétextes (premier salaire, avances pour achat de matériel, etc.), lui demandant par la suite de retourner une partie des fonds reçus en excès.
- **Les arnaques lors de ventes entre particuliers :** le fraudeur achète un bien grâce à un chèque frauduleux en indiquant sur le chèque une somme plus importante que le prix convenu. Le fraudeur demande ensuite au vendeur de lui restituer les fonds reçus en excès, principalement par virement.

L'Observatoire estime que les remises frauduleuses auraient représenté 60 % du total de la fraude en 2020, soit environ 323 millions d'euros de fraude. Toutefois, les établissements bancaires ont déployé différents outils d'identification des remises frauduleuses potentielles, qui permettent de déjouer certaines de ces tentatives par la temporisation de l'encaissement du chèque. Le chèque est alors rejeté avant que le compte du remettant ne soit crédité et avant que le fraudeur n'ait réussi à récupérer les fonds correspondants aux chèques remis. Si cette statistique pourra être affinée dans les prochains rapports de l'Observatoire, une première estimation montre que ces outils de temporisation auraient permis d'arrêter 136 millions d'euros de fraude en 2020, soit une efficacité de 42 % sur le total des remises frauduleuses.

4.4.2 Phénomène de fraude n° 2 : les chèques volés utilisés auprès des personnes qui acceptent le chèque comme moyen de règlement

Depuis l'établissement des premières statistiques consolidées de l'Observatoire en 2016, le vol est toujours ressorti comme le premier risque d'insécurité pour le chèque. C'était encore vrai en 2020, année durant laquelle les pertes et les vols de chèque ont représenté 89 % des cas de fraude et 68 % du montant total de la fraude. Cela correspond à presque 200 000 chèques volés en 2020, soit 1,7 chèque volé sur 10 000 chèques émis.

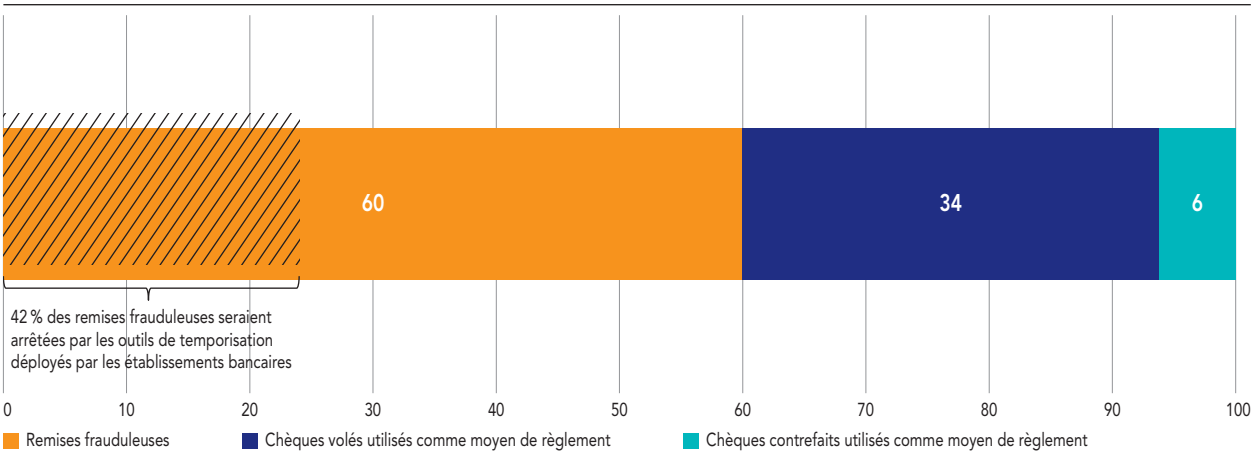
Une partie importante des chèques volés est utilisée dans le cadre de remises frauduleuses. Le reste des chèques volés est utilisé auprès de bénéficiaires de bonne foi, comme les commerçants, les professionnels de santé et les administrations mais aussi les particuliers, etc.

L'Observatoire estime que l'utilisation de chèques volés auprès de bénéficiaires de bonne foi, professionnels comme particuliers, aurait représenté environ 34 % de la fraude en 2020, soit environ 183 millions d'euros de fraude en 2020.

4.4.3 Phénomène de fraude n° 3 : les chèques contrefaits utilisés auprès de personnes qui acceptent le chèque comme moyen de règlement

La contrefaçon de chèque avait doublé entre 2018 et 2019 pour atteindre 77 millions d'euros. La contrefaçon de chèque est une typologie de fraude, dont l'évolution semble dépendre de l'activisme de quelques faussaires agissant sur le *darknet* [3]. Ceux-là agiraient souvent seuls

Profil de la fraude au chèque en 2020 : les trois principaux phénomènes de fraude identifiés par l'Observatoire (en %)



Source : Observatoire de la sécurité des moyens de paiement.

en revendant en bitcoins des services de fabrication de faux chèques et des conseils pour les écouler sans difficulté. Le préjudice avait doublé en 2019 pour atteindre 77 millions d'euros (+ 108 %). **En 2020, cette typologie de fraude est revenue dans des moyennes similaires à la période 2016-2018 pour atteindre 32 millions d'euros, soit 6 % du total de la fraude au chèque.**

Au final, l'Observatoire recense, en 2020, 7 207 chèques contrefaits pour un montant moyen de 4 487 euros. Même si certains faux chèques seraient remis à l'encaissement dans le cadre de remises frauduleuses, l'essentiel des chèques contrefaits seraient utilisés par des filières organisées ou des délinquants isolés auprès de commerçants pour acheter des biens à forte valeur ajoutée dans l'objectif de les revendre par la suite (téléphones mobiles, téléviseurs, équipements de la maison, etc.).

4.5 Les recommandations de l'Observatoire

Pour lutter contre le développement de la fraude au chèque, l'Observatoire exprime dix recommandations correspondant à cinq objectifs. Ces recommandations s'adressent à l'ensemble des acteurs de la chaîne, des utilisateurs aux professionnels du chèque, en premier lieu les établissements bancaires et leurs prestataires spécialisés. La mise en œuvre de ces recommandations n'appelle, sauf exception, aucune modification législative ou réglementaire. **L'Observatoire souligne également qu'il appartiendra à chaque acteur de mobiliser les leviers les plus adaptés à due proportion de leur efficacité attendue et de leur profil de risque.**

4.5.1 Objectif n° 1 : mieux appréhender les développements de la fraude au chèque pour mieux orienter les investissements

Davantage que pour les moyens de paiement électroniques, la compréhension des phénomènes de fraude au chèque suppose la collecte d'éléments subjectifs éparses (analyse des experts dans les centres de traitement, appréciation des conseillers bancaires, résultats des enquêtes de police, etc.). Cette difficulté est liée à la nature même de ce moyen de paiement, qui est un support papier non traçable. En dépit de ces contraintes, l'Observatoire souhaite convenir de certains indicateurs statistiques supplémentaires qui doivent permettre à la Banque de France de mieux exercer sa surveillance sur la sécurité de ce moyen de paiement, et aux établissements bancaires d'orienter leurs investissements en fonction des risques.

Recommandation n° 1

Réviser la collecte statistique de la Banque de France pour améliorer la connaissance des phénomènes de fraude au chèque

L'Observatoire appelle la Banque de France à réviser sa collecte statistique « Recensement de la fraude au moyen de paiement » pour renforcer le suivi et la connaissance collective de la fraude au chèque. Les établissements bancaires seront associés à ces travaux de refonte. Les pistes d'une collecte auprès des établissements en tant que tirés et remettants et d'une meilleure prise en compte de la fraude déjouée devront être étudiées. Les évolutions méthodologiques pourront idéalement être prises en compte à partir des statistiques de l'Observatoire sur les données de 2022.

4.5.2 Objectif n° 2 : lutter contre les remises frauduleuses

Selon les organisations des banques, les contrôles sur la régularité des chèques remis à l'encaissement sont faits parfois en agence, par des unités spécialisées ou par les centres de traitement. Dans les centres de traitement, les machines réalisent un contrôle de la régularité formelle du chèque, notamment par le contrôle de présence des mentions obligatoires. Toutefois, ces machines ne permettent pas de mener un contrôle approfondi sur l'ensemble des chèques. Seuls les contrôles réalisés par les experts permettent d'identifier d'éventuelles anomalies sur le chèque de type contrefaçon ou falsification.

Les procédures de remise à l'encaissement des chèques peuvent limiter les risques de remises frauduleuses, par exemple avec l'authentification du remettant via sa carte bancaire ou encore par la collecte de données contextuelles. Face au développement de la fraude à l'encaissement de chèques par le biais d'une tierce personne, les banques ont aussi construit des outils de détection des remises frauduleuses ou atypiques. En cas de soupçon ou de remise atypique, la banque peut retarder le crédit du chèque ou, si le chèque est crédité, renforcer les contrôles sur les opérations ultérieures (virements, retraits d'espèces, transactions par carte, etc.).

Le titulaire du compte peut aussi participer à la lutte contre les remises frauduleuses. En effet, les chances de succès d'une remise frauduleuse diminuent d'autant que la réclamation du client tiré est adressée rapidement à sa banque avant que le remettant ait eu le temps d'utiliser ou de transférer les fonds frauduleusement acquis. La vigilance du titulaire du compte peut être soutenue par les outils et les

procédures de surveillance des opérations par chèque mis en place par sa banque. Ces outils peuvent ainsi générer des alertes sur des opérations atypiques par chèque qui seraient suspectées de fraude. Pour les chèques dits « circulants », d'un montant supérieur à 10 000 euros, la banque du tireur reçoit physiquement le chèque et peut donc en contrôler sa régularité. Pour les chèques dits « non circulants », d'un montant inférieur à 10 000 euros, la banque du tireur reçoit les données du chèque, mais elle peut demander une copie du chèque et/ou l'original. Pour aider l'établissement du tireur à prioriser ses contrôles, l'établissement présentateur de chèques peut lui transmettre un indicateur de soupçon de fraude.

Recommandation n° 2

Améliorer les contrôles de la banque du remettant contre les remises frauduleuses

L'Observatoire encourage le développement d'outils de prévention des remises frauduleuses fondés sur l'analyse comportementale, la connaissance de la clientèle et les mesures de temporisation des encaissements.

Pour soutenir le développement de ces outils, l'Observatoire appelle les pouvoirs publics à permettre aux banques en tant que présentateurs de chèques de consulter le Fichier national des chèques irréguliers (FNCI) tenu par la Banque de France aujourd'hui ouvert aux seuls bénéficiaires de chèques, à condition que la consultation ne soit pas obligatoire et qu'elle n'engage pas leur responsabilité. Cela pourrait permettre aux banques en tant que banquier remettant de connaître les chèques mis en opposition au moment de la remise ou lors des traitements.

L'Observatoire recommande aussi de renforcer les contrôles sur les chèques de montant élevé, notamment lorsque les remises ne correspondent pas au profil habituel du client remettant. Il invite également les prestataires et les banques à explorer les nouvelles technologies qui pourraient permettre de renforcer les contrôles automatisés en matière d'identification des falsifications, des endossements irréguliers et des détournements.

Recommandation n° 3

Soutenir le développement des contrôles du côté de l'établissement tiré

L'Observatoire appelle les établissements bancaires à proposer des solutions de sécurisation des chèques émis à leurs clients, qui utilisent ce moyen de paiement. Ces services, souvent existants du côté de la clientèle entreprise, permettent à l'établissement bancaire de réaliser des contrôles de cohérence entre les informations transmises par le client sur les chèques émis et les demandes de règlement reçues.

4.5.3 Objectif n° 3 : lutter contre les chèques volés qui sont utilisés auprès de bénéficiaires de bonne foi

La lutte contre la fraude au chèque repose en premier lieu sur la personne acceptant le chèque comme moyen de paiement. Outre les actions de prévention contre les vols de chèque, l'Observatoire estime que le meilleur outil de lutte contre les chèques volés reste le Fichier national des chèques irréguliers (FNCI) tenu par la Banque de France et consultable via le service Vérifiance-FNCI-Banque de France. En utilisant ce service, le créancier peut identifier un chèque volé avant de l'accepter comme moyen de règlement, à condition que le chèque ait préalablement été mis en opposition par son titulaire légitime.

Or, la contribution de ce service à la lutte contre l'utilisation des chèques volés s'est amoindrie au fil des années : les consultations du FNCI ont déjoué 32 % des cas de fraude au chèque volé en 2016, mais seulement 11 % en 2020. Pour préserver l'efficacité de ce fichier, l'Observatoire souhaite que :

1) D'une part, tout chèque volé fasse l'objet d'une mise en opposition et que celle-ci intervienne le plus rapidement possible après le vol. Or, l'Observatoire constate que depuis 2016 le volume de mises en opposition baisse, tandis que les risques liés aux chèques volés augmentent.

2) D'autre part, que les personnes acceptant le chèque comme moyen de règlement consultent largement le FNCI. Or, l'Observatoire note que le nombre de consultations du FNCI baisse plus rapidement que l'usage du chèque. Ainsi, en 2020, 4 % des chèques émis ont été soumis à une consultation préalable du FNCI avant d'être acceptés.

3 Un *darknet* est un réseau Internet qui utilise des protocoles spécifiques pour accueillir des activités illégales, dissidentes et anonymes.

Recommandation n° 4

Protéger les chèques du vol dans leur acheminement et chez le client

Dans leur acheminement

Chaque année, entre quarante et cinquante millions de chéquiers sont remis aux clients en France. L'Observatoire appelle les établissements bancaires à sécuriser par tout moyen l'acheminement des chéquiers par pli postal et d'adopter en ce domaine un dispositif de vigilance permanente assurant une réaction rapide. L'Observatoire soutient également les travaux de coopération de la profession bancaire avec le groupe La Poste pour répondre aux vulnérabilités éventuelles dans les circuits postaux.

L'Observatoire appelle dans le même temps les utilisateurs à être particulièrement vigilants sur les risques liés à l'envoi des chèques par voie postale et à préférer dans la mesure du possible le retrait sécurisé en agence. En cas d'envoi par pli postal, les dispositifs soutenant la vigilance et la réactivité des clients, comme les SMS, notifications et appel téléphoniques, sont bienvenus.

Dans l'environnement du client

L'Observatoire appelle les établissements bancaires à mieux sensibiliser leurs clients sur les risques liés aux formules de chèques en leur possession. Les établissements peuvent pour cela informer leurs clients du stock de formules en leur possession, via l'espace de banque en ligne ou par courrier. Ils peuvent aussi proposer aux clients qui n'utilisent plus leurs chéquiers de détruire les formules anciennes et non utilisées ou de les remettre à leur agence bancaire pour destruction.

L'Observatoire encourage les établissements à construire une politique de dotation des clients en chéquiers visant à limiter les risques de perte et de vol chez le client. Les établissements bancaires peuvent adapter les renouvellements de chéquiers en fonction de l'usage réel du chèque par le client, afin d'éviter les remises qui ne sont pas nécessaires ou qui ne sont pas demandées, ou limiter le nombre de formules par chéquier pour certains clients.

Recommandation n° 5

Simplifier les procédures de mise en opposition pour perte ou vol

En cas de perte ou de vol au cours de l'acheminement

L'Observatoire appelle les établissements bancaires à poursuivre le suivi rapproché des envois de chéquiers par pli postal pour déclarer sans tarder au Fichier national des chèques irréguliers (FNCI) les chèques perdus ou volés chez le façonnier ou lors de leur acheminement. Cette procédure de mise en opposition doit être prise en charge par l'établissement bancaire, dans la mesure où le client vigilant n'aurait jamais reçu les formules et ne pourrait être tenu responsable de l'incident.

En cas de perte ou de vol dans l'environnement du client

Les procédures de mise en opposition des chèques pour perte ou vol, qui sont encadrées par des dispositions législatives, supposent parfois un formalisme contraignant (par exemple, confirmation par courrier avec accusé de réception) qui est peu compatible avec l'objectif d'une mise en opposition réactive et exhaustive. Elles sont également associées à des pratiques tarifaires, dont certains estiment qu'elles pourraient conduire certains clients à renoncer à l'opposition.

L'Observatoire appelle les établissements bancaires, comme interlocuteurs privilégiés de leurs clients, à simplifier les procédures d'opposition dans le respect des dispositions législatives (article L. 131-35 du Code monétaire et financier). Celles-ci devraient être possibles via les espaces de banque en ligne et être adaptées à tous les profils. Afin que les frais de mise en opposition ne conduisent pas insidieusement les titulaires à renoncer à la mise en opposition ou bien à en demander la levée, l'Observatoire demande aux établissements bancaires d'être attentifs sur les potentielles conséquences de ces pratiques tarifaires sur les mises en opposition.

Recommandations n° 6

Offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du Fichier national des chèques irréguliers (FNCI)

L'Observatoire considère que le service Vérifiance-FNCI-Banque de France reste aujourd'hui le meilleur outil de lutte contre l'usage des chèques perdus et volés. L'Observatoire appelle par conséquent les bénéficiaires à utiliser davantage ce service pour se prémunir contre l'usage de chèques perdus ou volés. La consultation du FNCI comporte des effets vertueux, puisque l'augmentation de sa consultation rend encore plus efficace l'indicateur multichèques (IMC) qui permet d'identifier l'utilisation anormale de chèques rattachés à un même compte.

L'Observatoire note néanmoins que son usage reste limité à un nombre très restreint de bénéficiaires. Pour y répondre, compte tenu de la diversité des besoins résultants de la population hétérogène des bénéficiaires de chèques, l'Observatoire privilégie la diversité de modes de consultation, que la consultation soit directe ou bien intégrée à une offre de services plus large.

Promotion du service Vérifiance-FNCI-Banque de France en consultation directe

L'Observatoire soutient les travaux du service Vérifiance-FNCI-Banque de France pour diversifier ses consultations et offrir ses services à une palette plus diversifiée d'accepteurs de chèques (commerçants, entreprises, professionnels). L'Observatoire note avec intérêt la nouvelle offre « Agile » de Vérifiance-FNCI-Banque de France destinée aux professionnels, artisans et petits commerçants. L'Observatoire accueille également favorablement la mise à disposition de nouveaux outils de consultation reposant sur les téléphones mobiles.

Promotion du service Vérifiance-FNCI-Banque de France en consultation indirecte

L'Observatoire appelle les acteurs privés, les banques et les sociétés spécialisées dans la sécurité du chèque, à développer et à offrir à leurs différents clients des outils de vérification des chèques avant acceptation (entreprises, personnes publiques, associations, particuliers). Ces outils embarqueraient la consultation du service Vérifiance-FNCI-Banque de France, mais peuvent aussi contenir des services additionnels (contrôle des mentions obligatoires, moteur de ***scoring*** contre les impayés, etc.).

4.5.4 Objectif n° 4 : lutter contre la falsification et la contrefaçon du chèque

Les experts consultés par l'Observatoire ont exprimé la sophistication croissante des techniques de fraude s'attaquant au support physique du chèque. Cela concerne :

- Tout d'abord la falsification, où le chèque est régulièrement émis par le titulaire du compte, puis frauduleusement modifié dans son montant ou son ordre. La falsification peut être commise par le bénéficiaire même du chèque, ou bien par un tiers étranger à la transaction ayant réussi à voler le chèque émis.
- Ensuite la contrefaçon, lorsqu'un faux chèque est fabriqué de toutes pièces. Les enquêtes de l'Office central de lutte contre les technologies de l'information et de la communication (OCLCTIC) montrent que la contrefaçon de chèques s'est considérablement « professionnalisée ». Plutôt que de fabriquer des faux chèques établis sur une banque inexistante ou sur des identités fictives, les principaux faussaires actifs sur le *darknet* privilégieraient les faux chèques établis sur des identités réelles après avoir volé ou détourné des relevés d'identité bancaire (RIB). Le faussaire peut également fournir une fausse pièce d'identité permettant à l'utilisateur de répondre à la vérification d'identité demandée par le créancier. La contrefaçon de chèque est ainsi étroitement liée à la fraude documentaire et à l'usurpation d'identité. Si les méthodes des faussaires se sont perfectionnées, la contrefaçon de chèque est devenue en parallèle accessible avec peu de moyens.

Les normes actuelles NF K11-111 sur les formules de chèque payable en France de mai 1998, dont l'application est obligatoire pour les chèques libellés en euros, indiquent que « *les mesures destinées à éviter les risques de falsification des chèques, notamment de leur montant, de leur bénéficiaire et de leur date, sont laissées à l'initiative de l'établissement tiré de chèques, auquel il appartient de choisir les dispositions à prendre, en déconseillant notamment l'altération des vignettes qui peut nuire à leur traitement par certaines machines* ». Chaque banque peut à ce titre intégrer d'autres éléments sécuritaires reposant sur le papier, les encres ou le tramage. Il peut s'agir de filigranes, de tramage au trait ou à la guilloche, de motifs fluorescents visibles sous lampe à ultraviolets, d'intégration dans le papier d'agents réactifs aux agents chimiques utilisés par les fraudeurs, etc.

Recommandation n° 7

Renforcer la surveillance de la Banque de France sur la résistance physique des formules contre la falsification et la contrefaçon

L'Observatoire appelle la Banque de France à réviser son référentiel de sécurité du chèque dont la version actuelle date de 2016. Via cette révision, la Banque de France pourra appeler les établissements bancaires à intégrer dans leurs formules des éléments de sécurité contre la falsification et la contrefaçon qui puissent être vérifiés par les bénéficiaires de chèques avant leur acceptation comme moyen de règlement.

Recommandation n° 8

Assurer l'efficacité du service Vérifiance-FNCI-Banque de France contre la contrefaçon de chèque

Au-delà des chèques mis en opposition, rattachés à des comptes clos, en interdit bancaire ou judiciaire, le Fichier national des chèques irréguliers (FNCI), tenu par la Banque de France, recense les faux chèques que lui déclarent les établissements bancaires. Cet indicateur aurait empêché 8 % des tentatives d'utilisation des chèques contrefaits en 2020. Par conséquent, l'Observatoire demande aux établissements bancaires de continuer à veiller à l'exhaustivité de leurs déclarations des faux chèques au FNCI. L'Observatoire appelle également l'Association du paiement à réviser le protocole CHPN (Chèque – Protocole normalisé) pour véhiculer sur les terminaux de caisse des commerçants l'information sur le nom de la banque, qui peut être déduite à la lecture de la ligne magnétique du chèque.

4.5.5 Objectif n°5 : prolonger l'impact de ces actions par une plus forte coopération entre les acteurs de la filière et une meilleure vigilance des utilisateurs du chèque

Recommandation n° 9

Structurer durablement la coopération entre les acteurs dans la lutte contre la fraude et soutenir l'action des forces de l'ordre

L'Observatoire décide de pérenniser le groupe de travail sur la fraude au chèque. Celui-ci devient un groupe de travail permanent, aux côtés du groupe de travail sur les statistiques de fraude et du groupe de travail sur la veille technologique. Il aura pour objectif de suivre la mise en œuvre des recommandations de l'Observatoire sur la lutte contre la fraude au chèque et de structurer la coopération en ce domaine. Ce groupe de travail pourra notamment solliciter la coopération des plateformes de réseaux sociaux qui servent régulièrement au recrutement de personnes utilisées par les fraudeurs pour encaisser des chèques à leur place.

L'Observatoire appelle par ailleurs les établissements bancaires, les acteurs spécialisés du traitement du chèque et les forces de l'ordre à construire un partenariat structuré, via l'identification de points de contact principaux, permettant aux professionnels du traitement de chèque qui sont témoins récurrents de fraude au chèque de remonter une information structurée, choisie et qualitative aux forces de l'ordre et ainsi soutenir leurs actions répressives.

Recommandation n° 10

Soutenir par un plan de communication la vigilance des utilisateurs dans l'usage du chèque

En parallèle de la publication de cette étude, l'Observatoire publie des supports de communications destinés à sensibiliser les utilisateurs sur les risques de fraude au chèque et renforcer leur vigilance. Ce plan de communication doit notamment alerter le grand public sur les risques d'escroquerie, comme l'encaissement de chèques pour le compte d'un fraudeur. Ces supports de communication pourront être relayés par la Banque de France, en tant qu'opérateur de la stratégie nationale d'éducation financière. Ces supports pourront également être partagées avec la *Task-force* nationale de lutte contre les arnaques mise en place à l'été 2020 pour lutter contre les escroqueries financières en ligne et pilotée par la Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF). Ce plan de communication souhaite aussi valoriser la plateforme Pharos (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements)sur le signalement des escroqueries financières et la mise à disposition prochaine de la plateforme Thésée (Traitement harmonisé des enquêtes et des signalements pour les e-escroqueries) portée par le ministère de l'Intérieur qui devrait faciliter le dépôt de plainte contre les escroqueries en ligne.

4.6 Conseils de prudence pour l'utilisation du chèque

Conseil n° 1 :
N'acceptez jamais d'encaisser un chèque qui ne vous est pas destiné ou qui ne correspond pas à ce qui a été convenu

Il ne faut sous aucun prétexte accepter d'encaisser un chèque qui ne vous est pas destiné ou qui ne correspond pas à un bien ou un service que vous avez vendu. Si vous découvrez des contenus illicites sur Internet qui seraient liés à la fraude au chèque, vous pouvez les signaler sur la plateforme Pharos (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) du ministère de l'Intérieur *internet-signalement.gouv.fr*. Soyez de surcroît très vigilants quand vous concluez des transactions, réglées par chèque, qui auraient été conclues dans l'urgence ou dans des conditions qui vous seraient trop favorables. Le chèque n'est pas un moyen de paiement garanti et il peut toujours vous revenir impayé. Une vigilance s'impose également pour les chèques de banque, qui peuvent également être fraudés. Si la situation vous le permet, demandez à votre interlocuteur de régler par un autre moyen de paiement. N'acceptez jamais de rembourser un trop perçu issu d'un règlement par chèque, il y a de fortes chances que cela relève d'une arnaque.

Conseil n° 2 :
Soyez très vigilants dans la réception et la conservation de vos chéquiers, en mettant les formules en opposition dès que vous constatez leur perte ou leur vol

Dans la mesure du possible, choisissez un envoi sécurisé à votre domicile ou le retrait à votre agence de votre chéquier. En cas de retard de réception, contactez votre banque au plus vite. Conservez vos chéquiers une fois reçus en lieu sûr, dans des endroits cachés, en évitant de les rassembler au même endroit que vos pièces d'identité. En cas de perte, vol ou utilisation frauduleuse des chèques, mettez en opposition au plus vite les formules concernées selon la procédure définie par votre établissement bancaire.

Conseil n° 3 :
Remplissez vos chèques de préférence avec un stylo à bille à l'encre noire, sans laisser d'espace avant ni après les mentions obligatoires, par exemple en tirant un trait horizontal

Pour vous protéger des risques d'utilisation frauduleuse des chèques que vous émettez, veillez à écrire au moyen d'un stylo non effaçable à bille noire et à renseigner, sans rature ni surcharge, l'ensemble des mentions obligatoires (montant en chiffres et en lettres, date et lieu d'émission, signature). Dans la mesure du possible, dans le cadre de transactions à distance, privilégiez d'autres moyens de paiement – carte, virement, prélèvement – à l'envoi d'un chèque par voie postale.

Conseil n° 4 :
Professionnels et commerçants : en tant qu'émetteurs ou bénéficiaires réguliers de chèques, renseignez-vous sur le service Vérifiance-FNCI-Banque de France ou les solutions de sécurisation proposées par votre établissement bancaire et les acteurs spécialisés dans la fraude au chèque

En tant qu'émetteur, des solutions de sécurisation existent pour vous protéger des utilisations frauduleuses des chèques que vous émettez. En tant que bénéficiaire de chèques, le service Vérifiance-FNCI-Banque de France vous permet de consulter le Fichier national des chèques irréguliers (FNCI) dans lequel sont recensés les formules mises en opposition et de vérifier certaines informations du chèque. D'autres services proposés par les banques ou des acteurs spécialisés dans ce moyen de paiement vous permettent de consulter indirectement le service Vérifiance-FNCI-Banque de France et de bénéficier d'outils supplémentaires pour identifier les chèques frauduleux.

Conseil n° 5 :
Professionnels et commerçants : restez vigilants en toutes circonstances sur la crédibilité du débiteur et la qualité de la formule qui vous est présentée

L'absence du chèque dans le FNCI (réponse « verte ») ne vous protège pas entièrement des risques de fraude et d'impayés. Pour vous protéger des chèques volés qui n'auraient pas encore été mis en opposition, demandez au débiteur un document officiel d'identité avec photographie, comme le droit vous y autorise. Examinez avec la plus grande attention les documents présentés. Compte tenu des usurpations d'identité et des risques de contrefaçon sur le chèque, soyez toujours attentifs à la qualité et à la propreté des chèques qui vous sont présentés en vérifiant au minimum l'absence d'altération sur la formule et la présence des microlettres, visibles à la loupe, sur les lignes du chèque. En cas de doute, demandez un autre moyen de paiement.

ANNEXES

A1 CONSEILS DE PRUDENCE POUR L'UTILISATION DES MOYENS DE PAIEMENT

Face à l'ingéniosité des fraudeurs qui cherchent des moyens de contournement au fur et à mesure du durcissement des dispositifs de sécurité, les utilisateurs des instruments de paiement scripturaux (carte, chèque, virement et prélèvement) doivent renforcer leur vigilance et s'informer régulièrement sur les dispositifs de protection en vigueur et les comportements à adopter en matière de sécurité.

On recense à ce jour plusieurs typologies de fraude visant les moyens de paiement scripturaux :

- **la fraude par établissement de faux ordres de paiement**, soit après le vol ou la contrefaçon d'un instrument physique, soit par détournement de données ou d'identifiants bancaires par un tiers ;
- **la fraude par détournement ou falsification d'un ordre de paiement régulier**, en dupliquant un ordre de paiement émis par son porteur légitime ou en modifiant ses attributs (montant, nom du bénéficiaire ou du donneur d'ordre, etc.) ;
- **la fraude par utilisation ou répudiation abusive** par le titulaire légitime d'un moyen de paiement, caractérisée par la contestation infondée d'un ordre de paiement valablement émis, aboutissant ainsi à l'annulation de l'encaissement des fonds.

Les types de fraudes ne s'appliquent pas de la même façon aux différents instruments de paiement et varient selon les canaux d'initiation de paiement utilisés (paiement de proximité, paiement à distance sur Internet, banque en ligne, etc.).

Votre comportement concourt directement à la sécurité de leur utilisation. Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

SOYEZ RESPONSABLES

- Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, pas même à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.
- Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile, etc.), gardez-le secret, ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui.

En particulier, ne communiquez vos mots de passe, codes confidentiels et identifiants personnels ni à des autorités administratives ou judiciaires, ni à votre banque, surtout par téléphone ou par courriel. Ils ne sont jamais susceptibles de vous demander cette information.

- Lorsque vous composez un code ou un mot de passe confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal, du distributeur ou du téléphone avec votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.
- Pensez à consulter régulièrement les consignes de sécurité publiées sur le site de votre banque et assurez-vous qu'elle dispose de vos coordonnées afin de vous contacter rapidement en cas d'opérations douteuses sur votre compte. En cas de contact de votre banque, par téléphone ou par courriel pour de telles opérations, rappelez-vous que vous n'avez pas à lui communiquer vos mots de passe et identifiants personnels.
- N'acceptez jamais de payer un vendeur ou loueur de biens que vous ne connaissez pas par transfert d'argent préalable à la mise à disposition ou la livraison du bien. Il peut s'agir de fraudeurs qui, après avoir récupéré les fonds transférés, font disparaître tout lien de communication (adresse e-mail, compte de réseau social, etc.).

SOYEZ ATTENTIFS

Lors de votre enrôlement pour bénéficier de l'authentification forte (conformément à la DSP 2)

Pour les actions relatives à la mise en place du nouveau dispositif d'authentification forte, le porteur doit suivre strictement les consignes reçues de sa banque au travers des canaux de communication habituels.

En cas de doute sur l'origine des consignes reçues, il est préférable de se référer aux informations accessibles via son espace client ou de contacter directement son conseiller bancaire.

Lors de la connexion à votre espace client de banque en ligne

- Choisissez un fournisseur d'accès Internet reconnu et suivez ses conseils de sécurité.
- Vérifiez la présence de https (« s » pour *secure*) devant l'adresse du site et l'icône d'une clé ou d'un cadenas dans la barre d'état du navigateur Internet.
- Contrôlez qu'aucune autre fenêtre Internet n'est ouverte, saisissez vous-même l'adresse exacte fournie par votre banque.

- N'accédez pas à votre banque en ligne depuis un ordinateur public ou connecté à un réseau Wi-Fi public.
- N'accédez jamais à votre banque en ligne depuis un courrier électronique ou un SMS.
- Si vous pensez avoir fourni vos codes d'accès de banque en ligne à un tiers via un site Internet, un lien SMS ou directement par téléphone, contactez immédiatement votre banque, aux coordonnées habituelles, pour lui signaler (n'utilisez pas celles des messages que vous venez de recevoir).

Lors des paiements à un professionnel ou à un particulier

- Vérifiez l'utilisation qui est faite de votre carte bancaire par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider une transaction.
- Lorsqu'un chèque est automatiquement rempli par le commerçant, soyez attentif aux mentions indiquées avant de le signer et vérifiez plus particulièrement le montant.
- Quelques précautions lors du remplissage d'un chèque permettent de réduire les risques de fraude : évitez les ratures ou surcharges, inscrivez le nom du bénéficiaire du chèque et les montants en chiffres et en lettres sans laisser d'espace libre, puis tirez un trait sur l'espace restant non utilisé. Le lieu de paiement et la date doivent être renseignés en même temps que les autres mentions. La signature du chèque ne doit pas déborder sur la ligne de chiffres en bas du chèque. En aucun cas, la signature ne doit être apposée seule sur un chèque, c'est-à-dire sans les mentions relatives au montant et au bénéficiaire préalablement renseignées.

Lors des retraits aux distributeurs de billets

- Vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.
- Suivez exclusivement les consignes indiquées à l'écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.
- Mettez immédiatement en opposition votre carte si elle a été avalée par l'automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l'agence.

Lors des paiements sur Internet

- Ne stockez pas de coordonnées bancaires sur votre ordinateur (numéro de carte, numéro de compte, relevé d'identité bancaire, etc.), évitez de les transmettre par simple courriel et vérifiez la sécurisation du site du commerçant en cas de saisie en ligne (cadenas en bas de la fenêtre, adresse commençant par « https», etc.).
- Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les mentions légales du commerçant ainsi que ses conditions générales de vente.
- Ne répondez pas à un courriel, SMS, appel téléphonique ou autre invitation qui vous paraissent douteux. En particulier, ne cliquez jamais sur un lien inclus dans un message référençant un site bancaire.
- Protégez votre ordinateur, en activant les mises à jour de sécurité proposées par les éditeurs de logiciel (en règle générale gratuites) et en l'équipant d'un antivirus et d'un pare-feu.
- Changez régulièrement vos mots de passe, et évitez d'utiliser la fonction d'enregistrement pour des utilisations ultérieures (une usurpation de vos identifiants et de vos coordonnées bancaires vous expose à des fraudes sur tous vos moyens de paiement).
- N'utilisez pas un mot de passe commun pour l'utilisation de vos moyens de paiement, l'accès à votre banque en ligne et l'accès aux autres sites Internet sur lesquels vous avez un compte client.

Lors de la réception d'un ordre de paiement ou d'un moyen de paiement

- Lors de la réception d'un mandat de prélèvement, vérifiez que les informations relatives au créancier (nom/raison sociale et adresse) sont en cohérence avec vos engagements contractuels. Si votre banque a mis en place une liste des créanciers autorisés à effectuer des prélèvements sur votre compte (appelée aussi « liste blanche »), pensez à la mettre à jour.
- Si vous êtes bénéficiaire d'un paiement à distance et que vous ne connaissez pas personnellement le payeur (par exemple, en situation de vente sur Internet), vérifiez la cohérence des informations fournies (nom, adresse, identifiant du payeur, etc.) avant de donner votre accord à la transaction. En cas de doute, vérifiez auprès de la banque du payeur la régularité du moyen de paiement proposé et la qualité du payeur.
- Si vous êtes bénéficiaire d'un chèque de banque (par exemple, en cas de vente d'un véhicule), contactez la banque émettrice en recherchant par vous-même ses coordonnées (sans vous fier aux mentions présentes sur le chèque) pour en confirmer la validité avant de finaliser la transaction.
- Vérifiez la présence effective des mentions obligatoires d'un chèque, notamment la signature de l'émetteur du chèque, le nom de la banque qui doit payer, une indication de la date et du lieu où le chèque est établi, ainsi que la cohérence des informations (bénéficiaire, montant,

zone numéro de chèque de la ligne magnétique) et l'absence de ratures ou surcharges pouvant indiquer une origine frauduleuse.

Lors de vos déplacements à l'étranger

- Renseignez-vous sur les précautions à prendre et contactez avant votre départ l'établissement émetteur de votre carte, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.
- Pensez à vous munir des numéros internationaux de mise en opposition de vos moyens de paiement.

SACHEZ RÉAGIR

Vous avez perdu ou on vous a volé un instrument de paiement ou vos identifiants bancaires

- Faites immédiatement opposition en appelant le numéro que vous a communiqué votre banque ou l'émetteur de votre moyen de paiement. Pensez à le faire pour toutes vos cartes, chéquiers ou appareils mobiles comportant une application de paiement et qui ont été perdus ou volés. De même, contactez votre banque si vous avez communiqué vos coordonnées bancaires (numéro de compte, relevé d'identité bancaire, etc.) à un tiers qui vous paraît douteux.
- En cas de vol, déposez également au plus vite une plainte auprès de la police ou de la gendarmerie.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 50 euros. Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

Vous constatez des activités suspectes sur un de vos moyens de paiement

N'hésitez pas à contacter votre banque afin d'évaluer la régularité des opérations de paiement non identifiées ou pour lesquelles vous avez un doute. Contactez plus particulièrement votre banque lorsque vous recevez des informations par téléphone, courriel ou SMS confirmant ou demandant la validation d'opérations de paiement en cours, que vous n'auriez pas initiées.

Vous constatez des anomalies sur votre relevé de compte, alors que vos instruments de paiement sont toujours en votre possession

N'hésitez pas également à faire opposition afin de vous prémunir contre toute nouvelle tentative de fraude qui utiliserait les données usurpées de votre instrument de paiement.

Si, dans un délai de treize mois à compter de la date de débit de l'opération contestée (délai fixé par la loi), vous déposez une réclamation auprès de votre prestataire de services de paiement (PSP) gestionnaire de compte, les sommes contestées doivent vous être remboursées dans le délai d'un jour ouvré sans frais. Dans ces conditions, votre responsabilité ne peut être engagée. Néanmoins ceci ne vaut pas en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir).

Bien entendu, en cas d'agissement frauduleux de votre part, les dispositions protectrices de la loi ne trouveront pas à s'appliquer et vous resterez tenu des sommes débitées, avant comme après l'opposition, ainsi que des éventuels autres frais engendrés par ces opérations (par exemple, en cas d'insuffisance de provision).

A2 PROTECTION DU PAYEUR EN CAS DE PAIEMENT NON AUTORISÉ

L'ordonnance de transposition de la deuxième directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 13 janvier 2018, a modifié le cadre législatif concernant la responsabilité du payeur en cas d'opération de paiement non autorisée. Les grands principes issus de la première directive concernant les services de paiement restent toutefois inchangés.

La charge de la preuve incombe au prestataire de services de paiement (PSP). Ainsi, lorsqu'un payeur nie avoir autorisé une opération de paiement, il incombe à son PSP de prouver que l'opération de paiement en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre. La loi encadre désormais strictement les conventions de preuve puisqu'elle prévoit que l'utilisation de l'instrument de paiement, telle qu'enregistrée par le PSP, 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, par négligence grave, aux obligations lui incombant en la matière.

La transposition de la deuxième directive concernant les services de paiement (DSP 2) prévoit que si l'opération de paiement contestée a impliqué un prestataire de service d'initiation de paiement, le payeur doit contester l'opération de paiement auprès de son PSP gestionnaire de comptes, qui aura la charge de le rembourser. Ce dernier se retourne ensuite vers le prestataire de service d'initiation de paiement qui doit prouver que l'opération de paiement en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

Il convient toutefois de distinguer si l'opération de paiement contestée est effectuée ou non sur le territoire de la République française ou au sein de l'Espace économique européen [1] (EEE) afin de déterminer l'étendue de la responsabilité du payeur.

OPÉRATIONS NATIONALES OU INTRACOMMUNAUTAIRES

Ces dispositions de protection du payeur couvrent :

- les opérations de paiement effectuées en euros ou en francs CFP [2] sur le territoire de la République française [3] ;
- les opérations intracommunautaires dans lesquelles le PSP du bénéficiaire et celui du payeur sont situés :
  - l'un sur le territoire de la France métropolitaine, dans les départements d'outre-mer ou à Saint-Martin,
  - l'autre dans un autre État partie à l'accord sur l'EEE, et réalisées en euros ou dans la devise nationale de l'un de ces États.

Concernant les opérations de paiement non autorisées, c'est-à-dire en pratique dans les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, l'utilisateur de services de paiement doit contester, auprès de son PSP et dans un délai de treize mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son PSP doit alors rembourser l'opération de paiement non autorisée au payeur dans le délai d'un jour ouvré et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. La transposition de la DSP 2 prévoit que le PSP du payeur peut retarder le remboursement lorsqu'il a de bonnes raisons de soupçonner une fraude du payeur. Dans ce cas, une notification doit être adressée à la Banque de France. Une indemnisation complémentaire peut aussi éventuellement être versée. Nonobstant le délai maximal de contestation de treize mois, le payeur doit, lorsqu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer sans tarder son PSP.

AVANT INFORMATION AUX FINS DE BLOCAGE DE L'INSTRUMENT DE PAIEMENT

Avant l'information aux fins de blocage de l'instrument de paiement, le payeur peut supporter, à concurrence de cinquante euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de l'instrument de paiement. Toutefois, si l'opération de paiement est effectuée sans utilisation des données de sécurité personnalisées, ou que le payeur ne pouvait pas détecter la perte ou le vol de son instrument de paiement, ou que la perte résulte d'une action d'une personne placée sous la responsabilité du PSP, alors le payeur ne voit pas sa responsabilité engagée et il ne supporte aucune perte financière (même en-deçà de cinquante euros).

1 L'Espace économique européen est constitué de l'Union européenne, du Liechtenstein, de la Norvège et de l'Islande.

2 Franc CFP (colonies françaises du Pacifique) ou franc Pacifique.

3 L'ordonnance du 9 août 2017 transposant la DSP 2 prévoit qu'une large part de ses dispositions s'applique à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna.

La responsabilité du payeur n'est pas non plus engagée si l'opération de paiement non autorisée a été effectuée en détournant à son insu l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas plus engagée en cas de contrefaçon de l'instrument de paiement si ce dernier était en possession de son titulaire au moment où l'opération non autorisée a été réalisée.

En revanche, 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, à ses obligations de sécurité, d'utilisation ou de blocage de l'instrument de paiement, telles que convenues avec son PSP.

Enfin, si le PSP ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement, le payeur ne supporte aucune conséquence financière, sauf à avoir agi de manière frauduleuse.

APRÈS INFORMATION AUX FINS DE BLOCAGE DE L'INSTRUMENT DE PAIEMENT

Après avoir informé son PSP, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de l'instrument de paiement ou de l'utilisation détournée des données qui lui sont liées.

Là encore, les agissements frauduleux du payeur le privent de toute protection et il demeure responsable des pertes liées à l'utilisation de l'instrument de paiement.

L'information aux fins de blocage peut être effectuée auprès du PSP ou auprès d'une entité que ce dernier aura indiquée à son client, suivant les cas, dans le contrat de services de paiement ou dans la convention de compte de dépôt.

Lorsque l'utilisateur a informé son PSP de la perte, du vol, du détournement ou de la contrefaçon de l'instrument de paiement, ce dernier lui fournit sur demande et pendant dix-huit mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

OPÉRATIONS EXTRAEUROPÉENNES

La DSP 2 élargit partiellement son application aux opérations de paiement qui impliquent un PSP établi dans l'EEE et un autre établi en dehors de l'EEE. Pour ce type d'opération de paiement, souvent appelé « *one leg* », les dispositions protectrices de la directive s'appliquent assez largement à la partie de l'opération de paiement qui s'effectue dans l'EEE. Par exemple, un payeur qui dispose d'un instrument de paiement émis par un PSP établi en France peut bénéficier d'un régime protecteur même si cet instrument de paiement est utilisé aux États-Unis. Ainsi, en cas d'opération de paiement non autorisée effectuée au profit d'un bénéficiaire dont le PSP est établi aux États-Unis (ou ailleurs hors de l'EEE), le payeur peut demander à son PSP établi en France d'être remboursé dans les mêmes conditions que celles applicables aux opérations de paiement nationales ou intracommunautaires.

Des dispositions spécifiques sont prévues pour les opérations de paiement par carte lorsque :

- l'émetteur est situé à Saint-Pierre-et-Miquelon ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le PSP est situé dans un État non européen [4], quelle que soit la devise dans laquelle l'opération de paiement est réalisée ;
- l'émetteur est situé en Nouvelle-Calédonie, en Polynésie française ou à Wallis-et-Futuna, au profit d'un bénéficiaire dont le PSP est situé dans un État autre que la République française, quelle que soit la devise utilisée.

Dans ces cas, le plafond de cinquante euros s'applique pour les opérations de paiement non autorisées effectuées en cas de perte ou de vol de la carte, même si l'opération de paiement a été réalisée sans utilisation des données de sécurité personnalisées.

Par ailleurs, le délai maximal de contestation de l'opération de paiement est ramené à soixante-dix jours et peut être conventionnellement étendu à cent vingt jours. Le remboursement d'une opération de paiement non autorisée doit toujours être effectué dans un délai d'un jour ouvré.

4 Un État non européen est un État qui n'est pas partie à l'accord sur l'Espace économique européen.

A3 MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

Les missions, la composition et les modalités de fonctionnement de l'Observatoire de la sécurité des moyens de paiement sont précisées par les articles R. 141-1, R. 141-2 et R. 142-22 à R. 142-27 du Code monétaire et financier.

PÉRIMÈTRE CONCERNÉ

En application de l'article 65 de la loi n° 2016-1691 du 9 décembre 2016 et conformément à la stratégie nationale des moyens de paiement, l'article L. 141-4 du Code monétaire et financier a été modifié en élargissant la mission de l'Observatoire de la sécurité des cartes de paiement à l'ensemble des moyens de paiement scripturaux. La compétence de l'Observatoire de la sécurité des moyens de paiement couvre donc désormais, en plus des cartes émises par les prestataires de services de paiement ou par les institutions assimilées, tous les autres moyens de paiement scripturaux.

Selon l'article L. 311-3 du Code monétaire et financier, un moyen de paiement s'entend comme tout instrument qui permet à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé. Les moyens de paiement couverts par l'Observatoire sont les suivants :

Le virement est fourni par le prestataire de services de paiement qui détient le compte de paiement du payeur et qui consiste à créditer, sur la base d'une instruction du payeur, le compte de paiement d'un bénéficiaire par une opération ou une série d'opérations de paiement réalisées à partir du compte de paiement du payeur.

Le prélèvement vise à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur.

La carte de paiement est une catégorie d'instrument de paiement offrant à son titulaire les fonctions de retrait ou de transfert de fonds. On distingue différentes typologies de cartes :

- les cartes de débit sont des cartes associées à un compte de paiement permettant à son titulaire d'effectuer des paiements ou retraits qui seront débités selon un délai fixé par le contrat de délivrance de la carte ;
- les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai. L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;
- les cartes commerciales, délivrées à des entreprises, à des organismes publics ou à des personnes physiques exerçant une activité indépendante, ont une utilisation limitée aux frais professionnels, les paiements effectués au moyen de ce type de cartes étant directement facturés au compte de l'entreprise, de l'organisme public ou de la personne physique exerçant une activité indépendante ;
- les cartes prépayées permettent de stocker de la monnaie électronique.

La monnaie électronique constitue une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise (par les établissements de crédit ou les établissements de monnaie électronique) contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

Le chèque consiste en un écrit par lequel une personne, appelée tireur, donne l'ordre à un établissement de crédit, appelé tiré, de payer à vue une certaine somme à son ordre ou à une tierce personne, appelée bénéficiaire.

Les effets de commerce sont des titres négociables qui constatent au profit du porteur une créance de somme d'argent et servent à son paiement. Parmi ces titres on distingue la lettre de change et le billet à ordre.

ATTRIBUTIONS

Conformément aux articles L. 141-4 et R. 141-1 du Code monétaire et financier, les attributions de l'Observatoire de la sécurité des moyens de paiement sont de trois ordres :

- il assure le suivi de la mise en œuvre des mesures adoptées par les émetteurs, les commerçants et les entreprises pour renforcer la sécurité des moyens de paiement ;
- il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de moyens de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents moyens de paiement scripturaux ;

- il assure une veille technologique en matière de moyens de paiement scripturaux, avec pour objet de proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des moyens de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

En outre, le ministre chargé de l'Économie et des Finances peut, aux termes de l'article R. 141-2 du Code monétaire et financier, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

COMPOSITION

L'article R. 142-22 du Code monétaire et financier détermine la composition de l'Observatoire. Conformément à ce texte, l'Observatoire comprend :

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel et de résolution ou son représentant ;
- un représentant de la Commission nationale de l'informatique et des libertés ;
- quatorze représentants des émetteurs de moyens de paiement et des opérateurs de systèmes de paiement ;
- cinq représentants du collège consommateurs du Conseil national de la consommation ;
- huit représentants des organisations professionnelles de commerçants et des entreprises dans les domaines, notamment, du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;
- deux personnalités qualifiées en raison de leur compétence.

La liste nominative des membres de l'Observatoire figure en annexe 4.

Les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans. Leur mandat est renouvelable.

Le président est désigné parmi ces membres par le ministre chargé de l'Économie et des Finances. Son mandat est de trois ans, renouvelable. Monsieur François Villeroy de Galhau, gouverneur de la Banque de France, en est l'actuel président.

MODALITÉS DE FONCTIONNEMENT

Conformément à l'article R. 142-23 et suivants du Code monétaire et financier, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté un règlement intérieur qui précise les conditions de son fonctionnement.

Le secrétariat de l'Observatoire, assuré par la Banque de France, est chargé de l'organisation et du suivi des séances, de la centralisation des informations nécessaires à l'établissement des statistiques de la fraude sur les moyens de paiement, de la collecte et de la mise à disposition des membres des informations nécessaires au suivi des mesures de sécurité adoptées et à la veille technologique en matière de moyens de paiement. Le secrétariat prépare également le rapport annuel de l'Observatoire, remis chaque année au ministre chargé de l'Économie et des Finances et transmis au Parlement.

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'Économie et des Finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail permanents chargés, l'un d'harmoniser et d'établir des statistiques en matière de fraude, l'autre d'assurer une veille technologique relative aux moyens de paiement.

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat sont tenus au secret professionnel par l'article R. 142-25 du Code monétaire et financier, et doivent donc conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. À cette fin, l'Observatoire a inscrit dans son règlement intérieur l'obligation incombant aux membres de s'engager auprès du président à veiller strictement au caractère confidentiel des documents de travail.

A4 LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

En application de l'article R. 142-22 du Code monétaire et financier, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel sont nommés pour trois ans par arrêté du ministre de l'Économie. Le dernier arrêté de nomination date du 20 juin 2021.

PRÉSIDENT

François VILLEROY DE GALHAU
Gouverneur de la Banque de France

REPRÉSENTANTS DES ASSEMBLÉES

Éric BOCQUET
Sénateur

Rémi REBEYROTTE
Député

REPRÉSENTANT DU SECRÉTARIAT GÉNÉRAL DE L'AUTORITÉ DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION

- Le Secrétaire général ou son représentant :
  Dominique LABOUREIX
  Geoffroy GOFFINET

REPRÉSENTANTS DES ADMINISTRATIONS

Sur proposition du secrétariat général de la Défense et de la Sécurité nationale :
- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  Emmanuel PROUFF

Sur proposition du ministre de l'Économie, de l'Industrie et du Numérique :
- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Pierre-Jean CANAULT
- Le directeur général du Trésor ou son représentant :
  Clément ROBERT
- La Présidente de l'Institut d'émission des départements d'outre-mer (IEDOM) et directrice générale de l'Institut d'émission d'outre-mer (IEOM) :
  Marie-Anne POUSSIN-DELMAS
- Le directeur général de la Concurrence, de la Consommation et de la Répression des fraudes ou son représentant :
  Aurélien HAUSER

Sur proposition du garde des Sceaux, ministre de la Justice :
- Le directeur des Affaires criminelles et des Grâces ou son représentant :
  Sophie LACOTE

Sur proposition du ministre de l'Intérieur :
- Le chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ou son représentant :
  Omar MERCHI

Sur proposition du ministre de la Défense :
- Le directeur général de la Gendarmerie nationale ou son représentant :
  Étienne LESTRELIN

Sur proposition de la Commission nationale de l'informatique et des libertés :
- Le chef du service des Affaires économiques ou son représentant :
  Clémence SCOTTEZ

REPRÉSENTANTS DES ÉMETTEURS DE MOYENS DE PAIEMENT ET DES OPÉRATEURS DE SYSTÈMES DE PAIEMENT

Thomas GOUSSEAU
Membre du conseil d'administration
Association française des établissements de paiement et de monnaie électronique (Afepame)

Amelia NEWSOM-DAVIS
Directrice *Pay Services* d'Orange
Association française du Multimédia Mobile (AF2M)

Corinne DENAEYER
Chargée d'études
Association française des sociétés financières (ASF)

Jean-Marie DRAGON
Responsable monétique et paiements innovants
BNP Paribas (BNPP)

Carole DELORME D'ARMAILLE
Directrice générale
Office de coordination bancaire et financière (OCBF)

Caroline GAYE
Directrice générale
American Express France (Amex)

Violette BOUVERET
Vice-présidente *Cyber & Intelligence*
MasterCard France

Philippe LAULANIE
Administrateur
Groupement des cartes bancaires (GCB)

Philippe MARQUETTY
Directeur – Produits, Paiements et *Cash management*
Société Générale

Évelyne BOTTOLLIER-CURTET
Card scheme relationships manager
Groupe BPCE

Romain BOISSON
Directeur régional
Visa Europe France

Jérôme RAGUÉNÈS
Directeur – Systèmes et Moyens de paiement
Fédération bancaire française (FBF)

Jean-Marie VALLÉE
Directeur général
STET

Marie-Anne LIVI
Directrice – Stratégie et relations de place
Crédit Agricole

REPRÉSENTANTS DES ENTREPRISES

Bernard COHEN-HADAD
Président de la Commission financement des entreprises
Confédération des petites et moyennes entreprises (CPME)

Émilie TISON
Confédération du commerce de gros et international
Mouvement des entreprises de France (MEDEF)

Isabelle CHARLIER
Head of treasury Banking management and Digitalization
Association française des trésoriers d'entreprise (AFTE)

REPRÉSENTANTS DU COLLÈGE « CONSOMMATEURS » DU CONSEIL NATIONAL DE LA CONSOMMATION

Mélissa HOWARD
Juriste
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN
Juriste
Union nationale des associations familiales (Unaf)

Mathieu ROBIN
Chargé de mission Banque Assurance
UFC – Que choisir

Hervé MONDANGE
Juriste
Association Force ouvrière consommateurs (Afoc)

Bernard FILLIAT
Association pour l'information et la défense des consommateurs salariés CGT (INDECOSA-CGT)

REPRÉSENTANTS DES ORGANISATIONS PROFESSIONNELLES DE COMMERÇANTS

Jean-Michel CHANAVAS
Délégué général
Mercatel

Isabelle CLAIRAC
Directrice générale de Market Pay
Fédération du commerce et de la distribution (FCD)

Philippe JOGUET
Correspondant sur les questions financières
Conseil du commerce de France (CdCF)

Marc LOLIVIER
Délégué général
Fédération du e-commerce et de la vente à distance (Fevad)

Magalie CARRÉ
Chambre de commerce et d'industrie de région Paris – Île-de-France (CCIP)

PERSONNALITÉS QUALIFIÉES EN RAISON DE LEURS COMPÉTENCES

Claude FRANCE
Directeur général des opérations France
Worldline

David NACCACHE
Professeur
École normale supérieure (ENS)

A5 MÉTHODOLOGIE DE MESURE DE LA FRAUDE AUX MOYENS DE PAIEMENT SCRIPTURAUX

CADRE GÉNÉRAL

Définition de la fraude aux moyens de paiement

La fraude est définie dans le présent rapport comme **l'utilisation illégitime d'un moyen de paiement ou des données qui lui sont attachées ainsi que tout acte concourant à la préparation ou la réalisation d'une telle utilisation** :

- **ayant pour conséquence un préjudice financier** : pour l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire du moyen de paiement, le bénéficiaire légitime des fonds (l'accepteur et/ou le créancier), un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ;
- **quel que soit le mode opératoire retenu** :
  - les moyens employés pour récupérer, sans motif légitime, les données ou le support du moyen de paiement (vol, détournement du support ou des données, piratage d'un équipement d'acceptation, etc.),
  - les modalités d'utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait, en situation de proximité ou à distance, par utilisation physique de l'instrument de paiement ou des données qui lui sont attachées, etc.),
  - la zone géographique d'émission ou d'utilisation du moyen de paiement ou des données qui lui sont attachées ;
- **et quelle que soit l'identité du fraudeur** : un tiers, l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

La fraude, ainsi définie, est mesurée par l'Observatoire en comptabilisant l'ensemble des opérations de paiement qui ont donné lieu à une écriture au compte d'au moins une des contreparties de la transaction et qui ont fait l'objet d'un rejet *a posteriori* pour motif de fraude. Ainsi, sont exclues de la fraude :

- les tentatives de fraude (auquel cas la fraude est stoppée avant exécution de l'opération) ;
- les utilisations irrégulières d'un moyen de paiement du seul fait d'un défaut de provision suffisante et se traduisant notamment par un impayé ;
- l'utilisation d'une fausse identité ou d'une identité usurpée pour ouvrir un compte et/ou pour obtenir un moyen de paiement en vue de réaliser des paiements.

Par ailleurs, l'approche retenue pour évaluer la fraude est celle dite de la « fraude brute » qui consiste à retenir le montant initial des opérations de paiement sans prendre en compte les mesures qui peuvent être prises ultérieurement par les contreparties en vue de réduire le préjudice (par exemple, interruption de la livraison des produits ou de la fourniture de services, accord amiable pour le rééchelonnement du paiement en cas de répudiation abusive du paiement, dommages et intérêts suite à un recours en justice, etc.). L'Observatoire de la sécurité des cartes de paiement avait estimé dans son rapport annuel 2015 [1] que l'impact des mesures de cette nature réduisait de 5 % l'estimation brute de la fraude pour les paiements par carte.

Les données de fraude sont collectées par le secrétariat de l'Observatoire auprès de l'ensemble des établissements concernés, selon une approche différenciée par moyen de paiement (voir ci-après). Compte tenu du caractère confidentiel des données individuelles collectées, seules les statistiques consolidées à l'échelle nationale sont mises à disposition des membres de l'Observatoire et présentées dans son rapport annuel.

Typologie de la fraude aux moyens de paiement

Afin d'analyser la fraude aux moyens de paiement, l'Observatoire a retenu quatre types de fraude, étant précisé que ceux-ci ne s'appliquent pas de la même manière aux différents instruments de paiement :

- **faux** (vol, perte, contrefaçon) : fraude par l'établissement d'un faux ordre de paiement soit au moyen d'un instrument de paiement physique (carte, chéquier, etc.) volé, perdu ou contrefait, soit via le détournement de données ou d'identifiants bancaires ;
- **falsification** : fraude par l'utilisation d'un instrument de paiement falsifié (instrument de paiement authentique dont les caractéristiques physiques ou les données attachées ont été modifiées par le fraudeur ou par un complice) ou par altération d'un ordre de paiement régulièrement émis en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.) ;
- **détournement** : fraude visant à utiliser l'instrument de paiement ou l'ordre de paiement sans altération ou modification d'attribut (à titre d'exemple, un fraudeur encaisse un chèque non altéré sur un compte qui n'est pas détenu par le bénéficiaire légitime du chèque) ;
- **rejeu** : fraude par l'utilisation abusive d'un instrument de paiement par son titulaire légitime après la déclaration de sa perte ou de son

vol ou par la contestation de mauvaise foi d'un ordre de paiement valablement émis par le titulaire légitime de l'instrument de paiement, ou par la réutilisation d'un ordre de paiement déjà traité.

MESURE DE LA FRAUDE À LA CARTE DE PAIEMENT

Transactions couvertes

La fraude à la carte de paiement, telle que mesurée dans le présent rapport, porte sur les transactions de paiement (de proximité et à distance) et de retrait effectuées par carte de paiement et réalisées en France et à l'étranger dès lors que l'une des contreparties de la transaction est considérée comme française : carte émise par un établissement français ou accepteur de la transaction (commerçant ou distributeur automatique de billets – DAB/guichet automatique bancaire – GAB) situé en France. Aucune distinction n'est faite quant à la nature du réseau d'acceptation (interbancaire [2] ou privatif [3]) ou la catégorie de carte (carte de débit, carte de crédit, carte commerciale ou carte prépayée) concernée.

1 Cf. *https://www.banque-france.fr/rapport-annuel-2015* (page 12).

2 Qualifie les systèmes de paiement par carte faisant intervenir un nombre élevé de prestataires de services de paiement émetteurs de cartes et acquéreurs de paiements.

3 Qualifie les systèmes de paiement par carte faisant intervenir un nombre restreint de prestataires de services de paiement émetteurs de cartes et acquéreurs de paiements (par exemple, au sein d'un seul groupe bancaire).

Typologie de fraude à la carte de paiement	Forme de la fraude
Carte perdue ou volée	Le fraudeur utilise une carte de paiement à la suite d'une perte ou d'un vol, à l'insu du titulaire légitime.
Carte non parvenue	La carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime. Ce type de fraude se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut difficilement constater qu'un fraudeur est en possession d'une carte lui étant destinée. Dans ce cas de figure, le fraudeur s'attache à exploiter des vulnérabilités dans les procédures d'envoi des cartes.
Carte falsifiée ou contrefaite	La falsification d'une carte de paiement consiste à modifier les données magnétiques, d'embossage [a] ou de programmation d'une carte authentique. La contrefaçon d'une carte suppose, quant à elle, la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou un terminal de paiement de commerçant. Dans les deux cas, le fraudeur s'attache à ce qu'une telle carte supporte les données nécessaires pour tromper le système d'acceptation.
Numéro de carte usurpé	Le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage [b] » et utilisé en vente à distance.
Numéro de carte non affecté	Utilisation d'un numéro de carte (ou PAN – *personnal account number*) cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance.

a Modification de l'impression en relief du numéro de carte.
b Technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de carte pour générer de tels numéros.

Origine des données de fraude

Les données de fraude à la carte de paiement sont collectées par l'Observatoire auprès :

- des membres du Groupement des cartes bancaires CB, de MasterCard et de Visa Europe France par l'intermédiaire de ceux-ci ;
- des principaux émetteurs de cartes privatives actifs en France.

Éléments d'analyse de la fraude

L'analyse de la fraude à la carte de paiement tient compte de plusieurs paramètres : les types de fraude, les canaux d'initiation de paiement, les zones géographiques d'émission et d'utilisation de la carte ou des données qui lui sont attachées et, pour les paiements à distance, les secteurs d'activité du commerçant.

Canal d'utilisation de la carte	Modalités d'utilisation
Paiement de proximité	Paiement réalisé au point de vente ou sur automate, y compris le paiement en mode sans contact.
Paiement à distance	Paiement réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen.
Retrait	Retrait d'espèces à un distributeur automatique de billets.

Zone géographique	Description
Transaction nationale	L'émetteur et l'accepteur sont, tous deux, établis en France. Pour autant, pour les paiements à distance, le fraudeur peut opérer depuis l'étranger.
Transaction internationale France → espace SEPA	L'émetteur est établi en France et l'accepteur est établi à l'étranger dans l'espace SEPA (*single euro payment area*).
Transaction internationale France → hors espace SEPA	L'émetteur est établi en France et l'accepteur est établi à l'étranger hors espace SEPA.
Transaction internationale espace SEPA → France	L'émetteur est établi à l'étranger dans l'espace SEPA et l'accepteur est établi en France.
Transaction internationale hors espace SEPA → France	L'émetteur est établi à l'étranger hors espace SEPA et l'accepteur est établi en France.

Secteur d'activité du commerçant pour les paiements à distance	Description
Alimentation	Épiceries, supermarchés, hypermarchés, etc.
Approvisionnement d'un compte, vente de particulier à particulier	Sites de vente en ligne entre particuliers, etc.
Assurance	Souscription de contrats d'assurance.
Commerce généraliste et semi-généraliste	Textile/habillement, grand magasin, généraliste vente sur catalogue, vente privée, etc.
Équipement de la maison	Vente de produits d'ameublement et de bricolage.
Jeux en ligne	Sites de jeux et de paris en ligne.
Produits techniques et culturels	Matériel et logiciel informatiques, matériel photographique, livre, CD/DVD, etc.
Santé, beauté, hygiène	Vente de produits pharmaceutiques, parapharmaceutiques et cosmétiques.
Services aux particuliers et aux professionnels	Hôtellerie, service de location, billetterie de spectacle, organisme caritatif, matériel de bureau, service de messagerie, etc.
Téléphonie et communication	Matériel et service de télécommunication/téléphonie mobile.
Voyage, transport	Ferroviaire, aérien, maritime.
Divers	

MESURE DE LA FRAUDE AU VIREMENT

Instruments de paiement couverts

La fraude au virement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement émis par le débiteur – appelé donneur d'ordre – afin de transférer des fonds de son compte de paiement ou de monnaie électronique vers le compte d'un bénéficiaire tiers. Cette catégorie recouvre à la fois les virements au format européen SEPA (*SEPA credit transfert* et *SEPA credit transfert inst*) et les virements de clientèle émis via les systèmes de paiement de gros montant (notamment le système Target2 opéré par les banques centrales nationales de l'Eurosystème, ainsi que le système privé paneuropéen Euro1).

Origine des données de fraude

Les données de fraude au virement sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement [4] agréés.

Éléments d'analyse de la fraude

La fraude au virement est analysée à partir des types de fraude, des zones géographiques d'émission et de destination du virement et des canaux d'initiation utilisés.

4 Établissements habilités à tenir des comptes de paiement pour le compte de leur clientèle et émettre des moyens de paiement relevant des statuts suivants au sens des réglementations françaises et européennes :
- établissements de crédit ou assimilés (institutions visées à l'article L. 518-1 du Code monétaire et financier),
- établissements de monnaie électronique et établissements de paiement de droit français ;
- établissements de crédit, établissements de monnaie électronique et établissements de paiement de droit étranger habilités à intervenir sur le territoire français et implantés sur ce dernier.

Typologie de fraude au virement	Forme de la fraude
Faux	Le fraudeur contrefait un ordre de virement, contraint le titulaire légitime à émettre un ordre de virement, ou usurpe les identifiants de la banque en ligne du donneur d'ordre légitime afin d'initier un ordre de paiement. Dans ce cas de figure, les identifiants peuvent notamment être obtenus via des procédés de piratage informatique (*phishing*, *malware*, etc.) ou sous la contrainte.
Falsification	Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime.
Détournement	Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.), le titulaire légitime du compte à émettre régulièrement un virement à destination d'un numéro de compte qui n'est pas celui du bénéficiaire légitime du paiement ou qui ne correspond à aucune réalité économique.

Zone géographique d'émission et de destination du virement	Description
Virement national	Virement émis depuis un compte tenu en France vers un compte tenu en France.
Virement européen	Virement émis depuis un compte tenu en France vers un compte tenu dans un autre pays de l'espace SEPA (*single euro payment area*).
Virement hors espace SEPA	Virement émis depuis un compte tenu en France vers un compte tenu dans un pays étranger hors espace SEPA.

Canal d'initiation utilisé	Modalités d'utilisation
Papier	Ordre de virement transmis par courrier, formulaire, courriel, télécopie ou téléphone.
Internet	Ordre de virement transmis par la banque en ligne ou par une application de paiement mobile.
Télématique	Ordre de virement transmis via d'autres canaux électroniques, hors banque en ligne et application de paiement mobile, tels que par exemple le système EBICS (*electronic banking Internet communication standard*, canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque).

MESURE DE LA FRAUDE AU PRÉLÈVEMENT

Instruments de paiement couverts

La fraude au prélèvement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement donnés par le créancier à son prestataire de services de paiement afin de débiter le compte d'un débiteur conformément à l'autorisation (ou mandat de prélèvement) donnée par ce dernier. Cette catégorie est constituée des prélèvements au format européen SEPA (*SEPA direct debit*), et comprend le prélèvement standard (*SDD Core – SEPA direct debit Core*) et le prélèvement inter-entreprises (*SDD B2B – business to business*).

Typologie de fraude au prélèvement	Forme de la fraude
Faux	Le fraudeur créancier émet des prélèvements vers des numéros de compte qu'il a obtenus illégalement et sans aucune autorisation ou réalité économique sous-jacente.
Détournement	Le fraudeur débiteur usurpe l'identité et l'IBAN (*international bank account number*) d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien.
Rejeu	Le fraudeur créancier émet sciemment des prélèvements déjà émis (qui ont soit déjà été réglés ou ont fait l'objet de rejets pour opposition du débiteur par exemple).

Origine des données de fraude

Les données de fraude au prélèvement sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés.

Éléments d'analyse de la fraude

La fraude au prélèvement est analysée à partir des types de fraude, des zones géographiques d'émission et de destination du prélèvement et des canaux d'autorisation utilisés.

Zone géographique d'émission et de destination du virement	Description
Prélèvement national	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu en France.
Prélèvement européen	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un autre pays de l'espace SEPA.
Prélèvement hors espace SEPA	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un pays étranger, hors espace SEPA.

Canal d'autorisation utilisé	Modalités d'utilisation
Papier	Mandat de prélèvement collecté par courrier, formulaire, courriel, télécopie ou téléphone.
Internet	Mandat de prélèvement émis depuis un canal Internet (site de banque en ligne, site ou application mobile du créancier).
Télématique	Mandat de prélèvement validé via d'autres canaux électroniques, hors site Internet et application mobile de la banque ou du créancier.

MESURE DE LA FRAUDE AU CHÈQUE

Contrairement aux autres moyens de paiement scripturaux, le chèque présente pour particularités de n'exister que sous format papier et d'utiliser la signature du payeur comme seul moyen d'authentification de ce dernier par sa banque. Ces caractéristiques ne permettent pas la mise en œuvre par les acteurs bancaires de dispositifs d'authentification automatiques en amont du paiement.

Périmètre de la fraude

La fraude au chèque, telle que mesurée dans le présent rapport, porte sur les chèques payables en France, en euros ou en devises (pour ces derniers, il s'agit des chèques tirés sur un compte de paiement tenu en devises), répondant au régime juridique fixé aux articles L. 131-1 à 88 du Code monétaire et financier. Plus précisément, il s'agit des chèques tirés par la clientèle de l'établissement bancaire sur des comptes tenus par

celui-ci, ainsi que des chèques reçus des clients de l'établissement pour crédit de ces mêmes comptes.

Cette définition intègre les titres suivants : chèque bancaire, chèque de banque, lettre-chèque pour les entreprises, titre emploi service entreprise (Tese) ; elle exclut les chèques de voyage, ainsi que les titres spéciaux de paiement définis par l'article L. 525-4 du Code monétaire et financier, tels que les chèques-vacances, les chèques ou titres restaurant, les chèques culture ou les chèques emploi-service universels, qui recouvrent des catégories variées de titres dont l'usage est restreint, soit à l'acquisition d'un nombre limité de biens ou de services, soit à un réseau limité d'accepteurs.

Origines des données de fraude

Les données de fraude au chèque sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés. Ces derniers effectuent leur déclaration en qualité d'établissement recevant de son client des chèques à l'encaissement (établissement remettant).

Éléments d'analyse des données de fraude

Les données de fraude au chèque sont analysées à partir des grands types de fraude définis par l'Observatoire. Pour le chèque, le tableau ci-après récapitule les formes de la fraude les plus couramment observées et la typologie à laquelle elles se rattachent.

Typologie de fraude au chèque	Forme de la fraude
Faux (vol, perte, ou apocryphe [a])	Utilisation par le fraudeur d'un chèque perdu ou volé à son titulaire légitime, revêtu d'une fausse signature qui n'est ni celle du titulaire du compte, ni celle de son mandataire. Émission illégitime d'un chèque par un fraudeur utilisant une formule vierge [b] (y compris lorsque l'opération a été effectuée sous la contrainte par le titulaire légitime).
Contrefaçon	Faux chèque créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque.
Falsification	Chèque régulier intercepté par un fraudeur qui l'altère volontairement par grattage, gommage ou effacement.
Détournement/rejeu	Chèque perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l'encaissement. Chèque régulièrement émis, perdu ou volé, intercepté dans le circuit d'acheminement vers le bénéficiaire et encaissé sur un compte différent de celui du bénéficiaire légitime. La formule est correcte, le nom du bénéficiaire est inchangé et la ligne magnétique située en bas du chèque est valide, tout comme la signature du client. Émission volontaire d'un chèque par le titulaire après sa mise en opposition.

a Apocryphe : terme utilisé par certains établissements pour désigner un écrit dont l'authenticité n'est pas établie.
b Formule vierge : formule mise à la disposition du client par la banque teneur de compte.

MESURE DE LA FRAUDE AUX EFFETS DE COMMERCE

Instruments de paiement couverts

La fraude aux effets de commerce, telle que mesurée dans le présent rapport, porte sur deux instruments de paiement :

- la lettre de change relevé (LCR) : instrument de paiement sur support papier ou dématérialisé par lequel le payeur (généralement le fournisseur) donne à son débiteur (son client) l'ordre de lui payer une somme d'argent déterminée ;
- le billet à ordre relevé (BOR) : ordre de paiement dématérialisé par lequel le payeur se reconnaît débiteur du bénéficiaire et promet de payer une certaine somme d'argent à un certain terme, tous deux spécifiés sur le titre.

Typologie et origine des données de fraude

Les types de fraude aux effets de commerce sont les mêmes que ceux définis pour les chèques.

Les données de fraude sur les effets de commerce sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés. Ces derniers effectuent leur déclaration en qualité d'établissement recevant de son client des effets de commerce à l'encaissement (établissement remettant).

DISPOSITIONS SPÉCIFIQUES POUR LA FRAUDE SUR LES TRANSACTIONS EN MONNAIE ÉLECTRONIQUE

La monnaie électronique constitue une valeur monétaire qui est stockée sous une forme électronique, représentant une créance sur l'émetteur qui doit être préalimentée au moyen d'un autre instrument de paiement, et qui peut être acceptée en paiement par une personne physique ou morale autre que l'émetteur de monnaie électronique.

On distingue deux catégories de support de monnaie électronique :

- les supports physiques de type carte prépayée,
- les comptes en ligne tenus par l'établissement émetteur.

Le suivi de la fraude sur les paiements en monnaie électronique par l'Observatoire est intégré à la mesure de la fraude :

- au titre des cartes de paiement pour la monnaie électronique sur support physique (carte prépayée),
- au titre des virements pour la monnaie électronique sous forme de compte en ligne.

A6 DOSSIER STATISTIQUE

VUE D'ENSEMBLE

T1 Cartographie des moyens de paiement scripturaux en 2020

(nombre en millions, montant en milliards d'euros, montant moyen en euros, variation en pourcentage)

	Nombre de transactions		Montant des transactions		Montant moyen
	2020	Variation 2020/2019	2020	Variation 2020/2019	
Paiement carte [a]	13 852	- 4	578	- 4	41
dont sans contact	*5 159*	*+ 37*	*80*	*+ 86*	*15*
Prélèvement	4 622	+ 6	1 684	- 2	364
Virement	4 483	+ 5	32 712	+ 30	7 298
dont VGM [b]	*9*	*- 30*	*19 042*	*+ 65*	*2 201 670*
dont virement instantané (SCT inst)	*45*	*+ 224*	*27*	*+ 276*	*586*
Chèque	1 175	- 26	614	- 25	522
Effet de commerce	71	- 8	197	- 15	2 755
Monnaie électronique	36	- 42	1	+ 23	19
Total	**24 238**		**35 786**		**1 476**
Retrait carte [a]	1 064	- 24	116	- 15	109
Total transactions	**25 302**	**-4**	**35 902**	**+ 25**	**1 418**

a) Cartes émises en France uniquement.
b) VGM : virement de gros montant, émis au travers de systèmes de paiement de montant élevé (Target 2, Euro 1), correspondant exclusivement à des paiements professionnels.

Source : Observatoire de la sécurité des moyens de paiement.

T2 Répartition de la fraude sur les moyens de paiement en montant et en volume en 2020

(montant en euros, volume en unités, part en pourcentage, montant moyen en euros)

	Montant		Volume		Montant moyen
	2020	Part	2020	Part	
Paiement carte [a]	439 489 315	34	7 421 137	95	59
Chèque	538 084 731	42	220 730	3	2 438
Virement	267 102 989	21	35 920	0	7 436
dont sur virement instantané (SCT inst)	*10 562 419*	*0*	*7 131*	*0*	*1 481*
Prélèvement	1 891 051	0	6 485	0	292
Effet de commerce	538 918	0	62	0	8 692
Total paiements	**1 247 107 004**	**97**	**7 684 334**	**98**	**162**
Retrait carte [a]	33 950 879	3	113 067	2	300
Total transactions	**1 281 057 883**	**100**	**7 797 401**	**100**	**164**

a) Cartes émises en France uniquement.

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LES CARTES DE PAIEMENT

Les données de fraude sur la carte de paiement sont collectées par l'Observatoire auprès :

- des cent vingt membres du Groupement des cartes bancaires CB par l'intermédiaire de celui-ci, MasterCard et Visa Europe France ;
- sept émetteurs de cartes privatives : American Express, Oney Bank, Crédit agricole Consumer Finance (Finaref et Sofinco), Cofidis, Franfinance, JCB et UnionPay.

En 2020, le nombre de cartes en circulation s'élève à 94,6 millions dont :

- 89 millions de cartes de type « interbancaire » (CB, MasterCard, Visa, etc.) ;
- 5,6 millions de cartes de type « privatif ».

Le nombre de cartes [1] mises en opposition en 2020 s'élève à 1 437 446.

1 Cartes mises en opposition pour lesquelles au moins une transaction frauduleuse a été enregistrée.

T3 Le marché des cartes de paiement en France – Émission
(volume en millions, valeur en milliards d'euros)

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	10 930,52	409,11	173,77	7,70	36,83	1,95
Paiements à distance hors Internet	41,38	3,15	63,04	1,19	0,95	0,18
Paiements à distance sur Internet	2 000,48	120,38	397,77	18,68	100,55	4,06
Retraits	1 038,43	112,31	14,11	1,82	11,34	1,80
Total	**14 010,81**	**644,95**	**648,68**	**29,39**	**149,68**	**7,99**
Cartes de type « privatif »						
Paiements de proximité et sur automate	48,08	4,65	2,31	0,35	2,28	0,34
Paiements à distance hors Internet	18,87	2,28	9,49	0,71	0,39	0,06
Paiements à distance sur Internet	10,95	1,75	13,71	1,59	0,85	0,10
Retraits	0,21	0,03	0,00	0,00	0,00	0,00
Total	**78,11**	**8,71**	**25,51**	**2,65**	**3,53**	**0,50**
Total général	**14 088,92**	**653,65**	**674,19**	**32,04**	**153,20**	**8,49**

Note : SEPA – *Single Euro Payments Area*.

Source : Observatoire de la sécurité des moyens de paiement.

T4 Le marché des cartes de paiement en France – Acceptation

(volume en millions, valeur en milliards d'euros)

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	10 930,52	409,11	219,50	8,87	81,97	4,29
Paiements à distance hors Internet	41,38	3,15	5,10	0,66	2,58	0,49
Paiements à distance sur Internet	2 000,48	120,38	104,04	7,00	40,87	3,04
Retraits	1 038,43	112,31	14,80	2,65	8,70	1,89
Total	**14 010,81**	**644,95**	**343,44**	**19,19**	**134,12**	**9,71**
Cartes de type « privatif »						
Paiements de proximité et sur automate	48,08	4,65	2,18	0,45	2,19	0,81
Paiements à distance hors Internet	18,87	2,28	1,55	0,31	0,48	0,19
Paiements à distance sur Internet	10,95	1,75	1,21	0,21	0,68	0,17
Retraits	0,21	0,03	0,00	0,00	0,22	0,12
Total	**78,11**	**8,71**	**4,94**	**0,97**	**3,57**	**1,29**
Total général	**14 088,92**	**653,65**	**348,38**	**20,16**	**137,68**	**11,00**

Source : Observatoire de la sécurité des moyens de paiement.

T5 Répartition de la fraude par type de carte

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)					
	2015	2016	2017	2018	2019	2020
Cartes de type « interbancaire »	0,086 (526,8)	0,082 (531,3)	0,070 (482,2)	0,072 (526,5)	0,071 (544,8)	0,073 (517,4)
Cartes de type « privatif »	0,068 (15,5)	0,060 (13,5)	0,043 (11,6)	0,040 (11,0)	0,048 (12,2)	0,056 (7,9)
Total	**0,085 (542,3)**	**0,081 (544,8)**	**0,069 (493,8)**	**0,071 (537,5)**	**0,071 (557,0)**	**0,072 (525,3)**

Source : Observatoire de la sécurité des moyens de paiement.

T6 Répartition de la fraude par zone géographique

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)					
	2015	2016	2017	2018	2019	2020
Transactions nationales (carte française et accepteur français)	0,044 (244,4)	0,042 (244,5)	0,037 (226,5)	0,038 (245,6)	0,040 (270,7)	0,044 (290,7)
Transactions internationales	0,372 (297,9)	0,353 (300,3)	0,281 (267,3)	0,270 (291,9)	0,262 (286,3)	0,327 (234,6)
dont carte française et accepteur hors SEPA	*0,692 (74,5)*	*0,713 (68,0)*	*0,511 (60,3)*	*0,438 (50,3)*	*0,441 (51,7)*	*0,533 (45,3)*
dont carte française et accepteur SEPA	*0,459 (116,8)*	*0,370 (113,9)*	*0,308 (100,7)*	*0,352 (143,3)*	*0,333 (147,5)*	*0,429 (137,5)*
dont carte étrangère hors SEPA et accepteur français	*0,353 (69,7)*	*0,449 (73,7)*	*0,386 (74,1)*	*0,323 (65,5)*	*0,311 (59,9)*	*0,290 (31,9)*
dont carte étrangère SEPA et accepteur français	*0,153 (36,9)*	*0,158 (44,7)*	*0,102 (32,3)*	*0,092 (32,8)*	*0,080 (27,2)*	*0,099 (20,0)*
Total	**0,085 (542,3)**	**0,081 (544,8)**	**0,069 (493,8)**	**0,071 (537,5)**	**0,071 (557,0)**	**0,072 (525,3)**

Source : Observatoire de la sécurité des moyens de paiement.

T7 Répartition de la fraude nationale par type de transaction

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)											
	2015		2016		2017		2018		2019		2020	
Carte française – accepteur français												
Paiements	0,047	(204,5)	0,045	(208,6)	0,039	(191,9)	0,041	(214,7)	0,043	(234,8)	0,048	(258,2)
dont paiements de proximité et sur automate	*0,012*	*(43,4)*	*0,009*	*(33,6)*	*0,009*	*(35,8)*	*0,010*	*(41,4)*	*0,010*	*(44,2)*	*0,009*	*(36,3)*
dont paiements à distance	*0,244*	*(161,1)*	*0,241*	*(175,0)*	*0,190*	*(156,1)*	*0,173*	*(173,3)*	*0,170*	*(190,6)*	*0,174*	*(221,9)*
– dont par courrier / téléphone	*0,372*	*(9,1)*	*0,280*	*(9,3)*	*0,357*	*(7,4)*	*0,351*	*(9,5)*	*0,270*	*(7,5)*	*0,165*	*(8,9)*
– dont sur Internet	*0,239*	*(152,0)*	*0,239*	*(165,7)*	*0,186*	*(148,7)*	*0,168*	*(163,8)*	*0,167*	*(183,1)*	*0,174*	*(213,0)*
Retraits	0,033	(39,9)	0,029	(35,9)	0,027	(34,6)	0,024	(30,9)	0,028	(35,9)	0,029	(32,5)
Total	**0,044**	**(244,4)**	**0,042**	**(244,5)**	**0,037**	**(226,5)**	**0,038**	**245,6**	**0,040**	**(270,7)**	**0,044**	**(290,7)**

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition de la fraude internationale par type de transaction – Cartes françaises

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)									
	2016		2017		2018		2019		2020	
Carte française – accepteur étranger hors SEPA										
Paiements	0,862	(56,2)	0,608	(53,3)	0,534	(44,4)	0,525	(47,1)	0,662	(44,3)
dont paiements de proximité et sur automate	*0,485*	*(22,9)*	*0,252*	*(12,7)*	*0,230*	*(12,9)*	*0,187*	*(11,0)*	*0,164*	*(3,8)*
dont paiements à distance	*1,862*	*(33,3)*	*1,096*	*(40,6)*	*1,168*	*(31,5)*	*1,175*	*(36,1)*	*0,921*	*(40,5)*
– dont par courrier / téléphone	*2,783*	*(9,4)*	*1,499*	*(8,4)*	*1,127*	*(4,8)*	*1,263*	*(4,4)*	*1,409*	*(3,3)*
– dont sur Internet	*1,648*	*(23,9)*	*1,025*	*(32,3)*	*1,175*	*(26,7)*	*1,164*	*(31,7)*	*0,893*	*(37,2)*
Retraits	0,390	(11,8)	0,229	(7,0)	0,184	(5,9)	0,168	(4,6)	0,056	(1,0)
Total	**0,713**	**(68,0)**	**0,511**	**(60,3)**	**0,438**	**50,3**	**0,441**	**(51,7)**	**0,533**	**(45,3)**
Carte française – accepteur étranger SEPA										
Paiements	0,422	(112,9)	0,342	(99,8)	0,385	(142,4)	0,359	(146,4)	0,453	(137,0)
dont paiements de proximité et sur automate	*0,066*	*(8,3)*	*0,075*	*(10,5)*	*0,066*	*(10,2)*	*0,061*	*(9,8)*	*0,099*	*(8,0)*
dont paiements à distance	*0,754*	*(104,5)*	*0,591*	*(89,2)*	*0,617*	*(132,2)*	*0,552*	*(136,6)*	*0,582*	*(129,1)*
– dont par courrier / téléphone	*1,317*	*(19,7)*	*1,489*	*(14,9)*	*0,911*	*(14,2)*	*1,159*	*(19,9)*	*0,767*	*(14,6)*
– dont sur Internet	*0,687*	*(84,9)*	*0,527*	*(74,4)*	*0,594*	*(118,0)*	*0,507*	*(116,7)*	*0,565*	*(114,5)*
Retraits	0,024	(0,9)	0,025	(0,9)	0,025	(0,9)	0,030	(1,1)	0,025	(0,5)
Total	**0,370**	**(113,8)**	**0,308**	**(100,7)**	**0,352**	**(143,3)**	**0,333**	**(147,5)**	**0,429**	**(137,5)**

Source : Observatoire de la sécurité des moyens de paiement.

T9 Répartition de la fraude internationale par type de transaction – Cartes étrangères

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)									
	2016		2017		2018		2019		2020	
Carte étrangère hors SEPA – accepteur français										
Paiements	0,507	(73,2)	0,429	(73,3)	0,357	(64,8)	0,342	(59,3)	0,352	(31,6)
dont paiements de proximité et sur automate	*0,169*	*(17,4)*	*0,135*	*(16,3)*	*0,108*	*(13,7)*	*0,124*	*(15,8)*	*0,077*	*(3,9)*
dont paiements à distance	*1,341*	*(55,8)*	*1,143*	*(57,0)*	*0,947*	*(51,1)*	*0,956*	*(43,5)*	*0,711*	*(27,7)*
– dont par courrier / téléphone	*1,748*	*(18,2)*	*1,488*	*(19,8)*	*0,886*	*(11,5)*	*0,813*	*(10,3)*	*0,844*	*(5,8)*
– dont sur Internet	*1,206*	*(37,7)*	*1,017*	*(37,2)*	*0,967*	*(39,6)*	*1,011*	*(33,2)*	*0,682*	*(21,9)*
Retraits	0,024	(0,5)	0,038	(0,8)	0,031	(0,7)	0,031	(0,6)	0,013	(0,3)
Total	**0,449**	**(73,7)**	**0,386**	**(74,1)**	**0,323**	**(65,5)**	**0,311**	**(59,9)**	**0,290**	**(31,9)**
Carte étrangère SEPA – accepteur français										
Paiements	0,178	(43,8)	0,114	(31,5)	0,102	(32,0)	0,089	(26,4)	0,112	(19,6)
dont paiements de proximité et sur automate	*0,024*	*(3,7)*	*0,018*	*(3,5)*	*0,018*	*(3,4)*	*0,023*	*(4,5)*	*0,029*	*(2,7)*
dont paiements à distance	*0,456*	*(40,0)*	*0,337*	*(28,0)*	*0,229*	*(28,6)*	*0,207*	*(21,9)*	*0,207*	*(17,0)*
– dont par courrier / téléphone	*0,695*	*(11,0)*	*0,564*	*(8,9)*	*0,357*	*(6,2)*	*0,348*	*(5,4)*	*0,298*	*(2,9)*
– dont sur Internet	*0,403*	*(29,0)*	*0,284*	*(19,1)*	*0,208*	*(22,4)*	*0,183*	*(16,5)*	*0,195*	*(14,1)*
Retraits	0,024	(0,9)	0,019	(0,7)	0,019	(0,8)	0,018	(0,8)	0,013	(0,4)
Total	**0,158**	**(44,7)**	**0,102**	**(32,3)**	**0,092**	**(32,8)**	**0,080**	**(27,2)**	**0,099**	**(20,0)**

Source : Observatoire de la sécurité des moyens de paiement.

T10 Répartition de la fraude nationale selon son origine et par type de carte en 2020

(montant en millions d'euros, part en pourcentage)

	Tous types de carte		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	71,7	24,7	71,5	24,9	0,2	6,4
Carte non parvenue	1,1	0,4	1,0	0,4	0,1	1,6
Carte altérée ou contrefaite	3,0	1,0	2,8	1,0	0,1	4,6
Numéro usurpé	212,2	73,1	210,9	73,4	1,3	42,2
Autres	2,4	0,8	1,0	0,3	1,5	45,2
Total	**290,4**	**100,00**	**287,2**	**100,00**	**3,2**	**100,00**

Source : Observatoire de la sécurité des moyens de paiement.

T11 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » – Émission

(volume en milliers, valeur en milliers d'euros)

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**790,4**	**34 655,5**	**150,6**	**7 800,4**	**26,3**	**3 599,3**
Cartes perdues ou volées	734,9	30 934,9	36,5	2 431,4	7,0	1 043,1
Cartes non parvenues	5,9	568,3	0,2	29,7	0,1	13,8
Cartes altérées ou contrefaites	26,6	1 630,7	24,4	1 597,5	9,4	1 349,0
Numéros de cartes usurpés	12,0	737,8	82,0	3 023,2	5,6	726,3
Autres	11,0	783,8	7,5	718,6	4,2	467,1
Paiements à distance hors Internet	**70,9**	**8 278,7**	**307,40**	**13 912,6**	**11,5**	**3 181,7**
Cartes perdues ou volées	4,0	1 080,6	3,4	231,4	0,3	71,4
Cartes non parvenues	0,0	2,5	0,3	16,8	0,0	0,1
Cartes altérées ou contrefaites	0,3	93,1	2,0	183,5	0,2	34,7
Numéros de cartes usurpés	66,5	7 092,0	300,3	13 396,3	10,7	3 064,6
Autres	0,1	10,5	1,4	84,6	0,3	10,9
Paiements à distance sur Internet	**2 844,5**	**212 057,7**	**2 457,7**	**113 305,2**	**701,5**	**36 931,6**
Cartes perdues ou volées	109,5	7 571,8	27,5	2 061,0	11,9	682,5
Cartes non parvenues	0,3	13,0	1,4	52,9	0,3	10,7
Cartes altérées ou contrefaites	24,9	1 105,8	130,2	4 966,7	119,6	3 393,0
Numéros de cartes usurpés	2 708,2	203 192,5	2 294,0	105 977,8	567,6	32 749,7
Autres	1,6	174,6	4,6	246,8	2,1	95,7
Retraits	**103,0**	**32 472,2**	**1,9**	**461,6**	**8,2**	**1 011,9**
Cartes perdues ou volées	101,3	31 991,0	1,4	381,9	1,5	243,5
Cartes non parvenues	1,3	435,7	0,0	9,2	0,0	8,5
Cartes altérées ou contrefaites	0,0	2,8	0,2	9,6	6,0	643,9
Numéros de cartes usurpés	0,1	6,7	0,1	12,8	0,2	41,2
Autres	0,3	35,9	0,2	48,1	0,5	74,8
Total	**3 808,8**	**287 464,2**	**2 917,7**	**135 479,9**	**747,4**	**44 724,5**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » – Acceptation

(volume en milliers, valeur en milliers d'euros)

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**790,4**	**34 655,5**	**24,4**	**2 579,4**	**22,7**	**3 647,0**
Cartes perdues ou volées	734,9	30 934,9	9,2	913,1	9,3	1 317,3
Cartes non parvenues	5,9	568,3	0,1	23,0	0,1	10,6
Cartes altérées ou contrefaites	26,6	1 630,7	3,4	276,4	5,6	1 309,5
Numéros de cartes usurpés	12,0	737,8	11,1	1 186,1	6,3	822,0
Autres	11,0	783,8	0,6	180,8	1,4	187,6
Paiements à distance hors Internet	**70,9**	**8 278,7**	**12,3**	**2 754,5**	**16,6**	**4 757,0**
Cartes perdues ou volées	4,0	1 080,6	0,2	43,0	0,7	198,6
Cartes non parvenues	0,0	2,5	0,0	0,5	0,0	5,0
Cartes altérées ou contrefaites	0,3	93,1	0,5	161,1	1,4	297,2
Numéros de cartes usurpés	66,5	7 092,0	11,6	2544,9	14,4	4 240,0
Autres	0,1	10,5	0,0	5,0	0,1	16,2
Paiements à distance sur Internet	**2 844,5**	**212 057,7**	**126,8**	**13 853,7**	**199,3**	**21 546,6**
Cartes perdues ou volées	109,5	7 571,8	2,0	214,0	6,8	715,2
Cartes non parvenues	0,3	13,0	0,1	9,5	0,2	20,0
Cartes altérées ou contrefaites	24,9	1 105,8	5,1	379,0	16,1	1 406,8
Numéros de cartes usurpés	2 708,2	203 192,5	118,3	13 061,2	167,7	19 198,2
Autres	1,6	174,6	1,3	190,0	1,8	206,4
Retraits	**103,0**	**32 472,2**	**1,3**	**354,4**	**0,7**	**245,1**
Cartes perdues ou volées	101,3	31 991,0	1,2	323,3	0,6	195,7
Cartes non parvenues	1,3	435,7	0,0	3,0	0,0	1,6
Cartes altérées ou contrefaites	0,0	2,8	0,0	9,0	0,1	14,4
Numéros de cartes usurpés	0,1	6,7	0,1	15,3	0,0	11,6
Autres	0,3	35,9	0,0	3,8	0,0	21,8
Total	**3 808,8**	**287 464,2**	**164,7**	**19 542,0**	**239,2**	**30 195,5**

Source : Observatoire de la sécurité des moyens de paiement.

T13 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » – Émission

(volume en milliers, valeur en milliers d'euros)

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**3,0**	**1 624,9**	**0,7**	**156,8**	**1,3**	**157,7**
Cartes perdues ou volées	1,0	148,1	0,4	55,8	0,3	61,4
Cartes non parvenues	0,1	40,2	0,0	4,1	0,0	2,1
Cartes altérées ou contrefaites	0,4	82,8	0,1	46,4	0,5	49,0
Numéros de cartes usurpés	0,1	13,4	0,1	39,0	0,5	40,7
Autres	1,4	1 340,4	0,1	11,5	0,0	4,5
Paiements à distance hors Internet	**3,9**	**685,6**	**15,5**	**686,2**	**2,0**	**154,2**
Cartes perdues ou volées	0,3	40,5	0,8	20,6	0,2	5,2
Cartes non parvenues	0,0	11,7	0,0	2,1	0,0	0,0
Cartes altérées ou contrefaites	0,1	58,6	0,7	22,6	0,0	11,0
Numéros de cartes usurpés	3,4	551,7	13,6	625,0	1,8	136,5
Autres	0,1	23,1	0,2	15,9	0,0	1,5
Paiements à distance sur Internet	**3,2**	**904,9**	**27,4**	**1 149,2**	**3,2**	**246,7**
Cartes perdues ou volées	0,1	10,5	1,1	22,9	0,2	13,1
Cartes non parvenues	0,0	0,3	0,1	3,9	0,0	0,1
Cartes altérées ou contrefaites	0,1	8,1	1,3	26,5	0,2	23,9
Numéros de cartes usurpés	2,9	794,0	24,2	1 017,5	2,8	205,1
Autres	0,1	92,0	0,7	78,4	0,0	4,5
Retraits	**0,0**	**5,2**	**0,0**	**0,0**	**0,0**	**0,0**
Cartes perdues ou volées	0,0	5,2	0,0	0,0	0,0	0,0
Cartes non parvenues	0,0	0,0	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,0	0,0	0,0	0,0	0,0
Numéros de cartes usurpés	0,0	0,0	0,0	0,0	0,0	0,0
Autres	0,0	0,0	0,0	0,0	0,0	0,0
Total	**10,1**	**3 220,6**	**43,6**	**1 992,2**	**6,5**	**558,6**

Source : Observatoire de la sécurité des moyens de paiement.

T14 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » – Acceptation

(volume en milliers, valeur en milliers d'euros)

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**3,0**	**1 625,0**	**0,2**	**78,6**	**0,6**	**297,8**
Cartes perdues ou volées	0,9	148,1	0,1	6,1	0,2	160,2
Cartes non parvenues	0,2	40,2	0,0	0,0	0,0	1,8
Cartes altérées ou contrefaites	0,4	82,8	0,0	0,3	0,2	90,8
Numéros de cartes usurpés	0,1	13,4	0,0	19,8	0,1	38,9
Autres	1,4	1 340,5	0,1	52,4	0,1	6,1
Paiements à distance hors Internet	**3,9**	**685,6**	**0,5**	**144,6**	**1,8**	**1 023,9**
Cartes perdues ou volées	0,3	40,5	0,0	0,7	0,1	14,2
Cartes non parvenues	0,0	11,7	0,0	0,0	0,0	0,6
Cartes altérées ou contrefaites	0,1	58,6	0,0	1,2	0,1	45,9
Numéros de cartes usurpés	3,4	551,7	0,5	135,8	1,6	954,4
Autres	0,1	23,1	0,0	6,8	0,0	8,8
Paiements à distance sur Internet	**3,2**	**904,9**	**1,1**	**231,6**	**1,5**	**371,9**
Cartes perdues ou volées	0,0	10,5	0,0	6,8	0,0	5,4
Cartes non parvenues	0,0	0,3	0,0	23,1	0,0	6,5
Cartes altérées ou contrefaites	0,1	8,1	0,0	0,0	0,1	64,8
Numéros de cartes usurpés	2,9	794,0	1,1	174,3	1,3	289,2
Autres	0,2	92,0	0,0	27,4	0,1	6,0
Retraits	**0,0**	**5,2**	**0,0**	**0,0**	**0,0**	**7,3**
Cartes perdues ou volées	0,0	5,2	0,0	0,0	0,0	0,0
Cartes non parvenues	0,0	0,0	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,0	0,0	0,0	0,0	7,3
Numéros de cartes usurpés	0,0	0,0	0,0	0,0	0,0	0,0
Autres	0,0	0,0	0,0	0,0	0,0	0,0
Total	**10,1**	**3 220,7**	**1,8**	**454,8**	**3,9**	**1 700,9**

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE CHÈQUE

T15 Évolution de la fraude

(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018	2020	Variation 2020/2019
En montant de transactions	**276 716 554**	**296 072 847**	+ 7	**450 108 464**	+ 52	**539 215 175**	+ 20	**538 084 731**	- 0,2
En nombre de transactions	120 295	114 906	- 4	166 421	+ 45	183 488	+ 10	220 730	+ 20

Source : Observatoire de la sécurité des moyens de paiement.

T16 Répartition de la fraude par typologie de fraude

(montant en euros, part entre parenthèses en pourcentage)

	2016		2017		2018		2019		2020	
Détournement, rejeu	5 010 202	(2)	1 002 809	(3)	14 741 262	(3)	20 454 286	(4)	37 103 618	(7)
Vol, perte (faux, apocryphe)	123 537 940	(45)	130 815 653	(44)	252 890 727	(56)	296 367 562	(55)	365 839 356	(68)
Contrefaçon	32 418 849	(11)	28 097 173	(10)	36 739 051	(8)	76 511 582	(14)	32 340 420	(6)
Falsification	115 749 563	(42)	127 157 212	(43)	145 737 424	(33)	145 881 745	(27)	102 801 337	(19)
Total	**276 716 554**	**(100)**	**296 072 847**	**(100)**	**450 108 464**	**(100)**	**539 215 175**	**(100)**	**538 084 731**	**(100)**

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE VIREMENT

T17 Évolution de la fraude

(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018	2020	Variation 2020/2019
En montant de transactions	**86 359 473**	**78 286 492**	- 9	**97 307 108**	+ 24	**161 642 174**	+ 66	**267 102 989**	+ 65
En nombre de transactions	5 585	4 642	- 17	7 731	+ 67	15 934	+ 106	35 261	+ 125

Source : Observatoire de la sécurité des moyens de paiement.

T18 Répartition de la fraude par typologie de fraude

(montant en euros, part entre parenthèses en pourcentage)

	2016		2017		2018		2019		2020	
Faux	63 707 498	(74)	42 008 522	(53)	51 069 661	(52)	98 525 485	(61)	87 087 545	(33)
Falsification	4 477 057	(5)	1 304 143	(2)	485 131	(1)	3 438 923	(2)	3 377 807	(1)
Détournement	14 978 462	(17)	32 966 084	(42)	40 250 639	(41)	56 514 755	(35)	157 426 483	(59)
Autres	3 196 456	(4)	2 007 743	(3)	5 501 677	(6)	3 163 011	(2)	19 211 154	(7)
Total	**86 359 473**	**(100)**	**78 286 492**	**(100)**	**97 307 108**	**(100)**	**161 642 174**	**(100)**	**267 102 989**	**(100)**

Source : Observatoire de la sécurité des moyens de paiement.

T19 Répartition de la fraude par zone géographique
(montant en euros, part en pourcentage)

	2020	
	Montant	Part
France	120 566 249	45
SEPA hors France	111 156 283	42
Hors SEPA	35 380 457	13
Total	**267 102 989**	**100**

Note : SEPA – *Single Euro Payments Area*.

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE PRÉLÈVEMENT

T20 Évolution de la fraude
(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018	2020	Variation 2020/2019
En montant de transactions	**39 935 882**	**8 726 403**	- 78	**58 346 253**	+ 569	**10 990 025**	- 81	**1 891 051**	- 83
En nombre de transactions	1 176	25 806	+ 209	309 377	+ 110	43 519	- 86	6 485	- 85

Source : Observatoire de la sécurité des moyens de paiement.

T21 Répartition de la fraude par typologie de fraude
(montant en euros, part entre parenthèses en pourcentage)

	2016		2017		2018		2019		2020	
Faux	5 270 858	(13)	6 141 836	(71)	58 329 283	(99)	3 961 260	(34)	1 795 478	(95)
Détournement	34 647 562	(87)	2 305 112	(26)	16 703	(0)	6 677 467	(61)	13 864	(1)
Autres	17 462	(0)	8 726 403	(3)	267	(0)	351 298	(3)	63 180	(4)
Total	**39 935 882**	**(100)**	**8 726 403**	**(100)**	**58 346 253**	**(100)**	**10 990 025**	**(100)**	**1 891 051**	**(100)**

Source : Observatoire de la sécurité des moyens de paiement.

T22 Répartition de la fraude par zone géographique
(montant en euros, part en pourcentage)

	2020	
	Montant	Part
France	1 421 187	75
SEPA hors France	469 864	25
Hors SEPA	0	0
Total	**1 891 051**	**100**

Note : SEPA – *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

Éditeur
Banque de France

Directrice de la publication
Nathalie Aufauvre
Directrice générale de la Stabilité financière et des Opérations de marché
Banque de France

Rédactrice en chef
Valérie Fasquelle
Directrice des Infrastructures, de l'Innovation et des Paiements
Banque de France

Secrétariat de rédaction
Pierre Bienvenu, Véronique Bugaj, Olivier Catau, Caroline Corcy, Florian Dintilhac, Christelle Guiheneuc, Trân Huynh, Julien Lasalle

Réalisation
Studio Création
Direction de la Communication

Contact
Observatoire de la sécurité des moyens de paiement
Code courrier : 011-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Impression
Banque de France – SG - DISG

Dépôt légal
Juillet 2021
ISSN 2557-1230 (en ligne)
ISSN 2556-4536 (imprimé)

Internet
www.observatoire-paiements.fr

Le *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement* est en libre téléchargement sur le site internet de la Banque de France (*www.banque-france.fr*).

www.banque-france.fr