CHAPITRE 3

La sécurité des moyens de paiement

Mis à jour en mai 2022

Le présent chapitre vise à décrire les différents enjeux en matière de sécurité des moyens de paiement et les dispositifs mis en place pour déjouer les tentatives de fraude toujours plus complexes. En effet, le développement des moyens de paiement électroniques est étroitement lié au développement des technologies de l'information et de la communication. Les innovations technologiques entraînent en parallèle une sophistication accrue des techniques de fraude, qui rend nécessaire une mise à niveau régulière des dispositifs de sécurité des systèmes attachés aux moyens de paiement.

La sécurité : un enjeu stratégique pour le secteur des paiements

La fraude porte préjudice au développement des activités commerciales dans son ensemble en raison, d'une part, des répercussions en matière d'image et de confiance auprès des utilisateurs et, d'autre part, de la crainte des professionnels de voir leur activité fragilisée en cas d'attaque organisée et de compromission massive de données de paiement. Dans ce contexte, la sécurité des moyens de paiement est une exigence essentielle à la confiance que l'utilisateur porte dans les moyens de paiement.

Du point de vue de l'utilisateur, la valeur ajoutée d'un moyen de paiement peut se résumer par trois caractéristiques : sa simplicité d'utilisation, son faible coût voire sa gratuité, et sa sécurité. Sur ce dernier point, deux risques principaux sont généralement perçus par l'utilisateur : i) le détournement des fonds en cours de paiement, susceptible d'entraîner une fraude immédiate ; et ii) la captation des données bancaires de l'utilisateur, qui pourrait entraîner des fraudes ultérieures.

Cela étant, il peut exister un écart entre la sécurité réelle d'un moyen de paiement et la perception qu'en a l'utilisateur. En effet, pour ce dernier, la sécurité du moyen de paiement sera souvent liée à une absence de perte financière pour lui, et non à l'impossibilité de réaliser des fraudes.

L'adoption d'un moyen de paiement par les consommateurs relève donc d'un équilibre subtil entre le coût du moyen de paiement et sa facilité d'utilisation, d'une part, et les investissements devant être consentis par les prestataires de services de paiement [1] pour en assurer la sécurité, d'autre part. Ainsi, l'utilisateur se détournera d'un moyen de paiement présentant des failles de sécurité qu'il juge excessives, mais il préférera également s'abstenir si les méthodes utilisées pour sécuriser le moyen de paiement se traduisent par une trop grande complexité d'utilisation ou par un coût de transaction trop élevé, ce qui laisse une marge de manœuvre relativement limitée pour le développement de techniques avancées de sécurisation.

Un prestataire de services de paiement souhaitant commercialiser un nouveau moyen de paiement doit donc trouver un juste milieu entre ces deux impératifs. Le modèle économique qui en découlera devra en outre intégrer le coût de la fraude, dans la mesure où le prestataire de services de paiement sera susceptible de subir directement des pertes financières lors de la survenance d'attaques. Dans certains cas, il peut ressortir de cette analyse qu'un risque de fraude accepté mais maîtrisé s'avérera commercialement plus rentable pour le prestataire de services de paiement et plus acceptable par les utilisateurs de son moyen de paiement que la mise en place de mesures permettant d'assurer, à l'extrême, une disparition quasi totale du risque de fraude au prix d'une complexification excessive du « parcours client » susceptible de faire échouer l'acte de paiement.

Dans un premier temps, ce chapitre s'attache à clarifier la notion de fraude aux moyens de paiement en présentant une typologie de la fraude observée et des modes opératoires utilisés par les fraudeurs. Dans un deuxième temps, il présente les mesures mises en place au niveau européen pour assurer le respect des droits des utilisateurs de moyens de paiement et la sécurité des opérations de paiement. Enfin, le chapitre se conclut en décrivant le cadre français de la lutte contre la fraude aux moyens de paiement.

1 Les prestataires de services de paiement (PSP) sont les établissements habilités à tenir des comptes de paiement pour le compte de leur clientèle et à émettre des moyens de paiement. Ils relèvent des statuts suivants, au sens des réglementations française et européenne :

- 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, et prestataires de services d'information sur les comptes de droit français ;
- établissements de crédit, établissements de monnaie électronique et établissements de paiement, et prestataires de services d'information sur les comptes de droit étranger habilités à intervenir sur le territoire français.

1. La fraude aux moyens de paiement

1.1. Définition de la fraude aux moyens de paiement

En France, de nombreux délits du Code pénal (escroqueries, abus de biens sociaux, blanchiment, recel, etc.) peuvent être associés à l'utilisation d'un moyen de paiement sans pour autant que les dispositifs de sécurité mis en place par les prestataires de services de paiement aient été mis en défaut. De telles fraudes ne sont pas considérées, dans le cadre de ce chapitre, comme des fraudes aux moyens de paiement. En effet, la fraude aux moyens de paiement est définie ici de manière plus restrictive comme recouvrant uniquement les utilisations illégitimes d'un moyen de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation :

- **ayant pour conséquence un préjudice financier** : ce préjudice peut affecter 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 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, c'est-à-dire quels que soient :**

  – 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.

1.2. Typologie de la fraude

L'identification des techniques de fraude est, par nature, un objectif permanent dans la mesure où les fraudeurs cherchent de nouvelles failles au fur et à mesure de l'évolution des dispositifs de sécurité. De même, le renforcement des moyens de prévention de la fraude dans un secteur du marché des paiements peut se traduire par un report de la fraude vers d'autres supports moins sécurisés ou vers d'autres zones géographiques. À titre d'exemple, bien que la généralisation des spécifications EMV[2] pour la carte à puce en Europe ait contribué à sensiblement renforcer la sécurité des paiements de proximité, elle a également incité les fraudeurs à cibler les zones géographiques n'ayant pas adopté le standard EMV, mais également à concentrer leurs attaques au sein de la zone euro sur les paiements par carte à distance.

On distingue quatre grands types de fraude aux différents instruments de paiement :

- **faux** : fraude par établissement d'un faux ordre de paiement soit au moyen d'un instrument de paiement physique perdu, volé ou contrefait, soit via le détournement de données ou d'identifiants bancaires ;

- **falsification** : fraude par utilisation d'un instrument de paiement falsifié (instrument

2 EMV (pour Europay, Mastercard, Visa) 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*.

de paiement authentique dont les caractéristiques physiques ou les données attachées ont été modifiées par le fraudeur) 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 un 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) ;

- **utilisation ou contestation abusive** : fraude par répudiation abusive par le titulaire légitime du moyen de paiement d'un ordre de paiement qu'il a régulièrement émis.

Encadré n° 1 : Déclinaison de la typologie de la fraude aux instruments de paiements courants

Les quatre types de fraude ne s'appliquent pas de la même façon aux différents instruments de paiement. Le tableau ci-après récapitule les formes les plus couramment observées.

Les quatre grands types de fraude aux différents instruments de paiement

Typologie de fraude	Carte de paiement	Chèque	Virement	Prélèvement
Faux	Utilisation par le fraudeur d'une carte perdue ou volée à son titulaire légitime, ou d'un numéro de carte usurpé (vente à distance) Fausse carte créée par un fraudeur à partir de données qu'il a recueillies	Utilisation par le fraudeur d'un chèque perdu ou volé à son titulaire légitime Faux chèque, créé de toutes pièces par un fraudeur, émis sur une banque existante ou une fausse banque	Transmission par le fraudeur d'un faux ordre de virement Usurpation des informations de connexion à un espace bancaire en ligne pour initier des virements frauduleux	Émission par le fraudeur d'un ordre de prélèvement sans mandat ou à partir d'un faux mandat
Falsification	Carte authentique dont les données magnétiques, d'embossage [a] ou de programmation ont été modifiées par le fraudeur	Chèque régulier intercepté par le fraudeur qui l'altère volontairement par grattage, gommage ou effacement	Virement régulier intercepté et modifié par le fraudeur	Remplacement des références du compte du créancier légitime par celles du compte du fraudeur sur un ordre ou fichier de prélèvement
Détournement	Paiement ou retrait sous la contrainte	Chèque régulier signé par le titulaire légitime sous la contrainte ou la manipulation	Virement initié, par le titulaire légitime du compte, sous la contrainte ou par la tromperie vers un compte qui n'est pas celui du bénéficiaire légitime ou qui ne correspond à aucune réalité économique	Usurpation par le fraudeur de l'identité et de l'IBAN d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien
Utilisation ou contestation abusive	Contestation par le porteur, de mauvaise foi, d'une transaction de paiement par carte valide qu'il a initiée	Chèque émis par le titulaire légitime, de manière abusive, à partir d'une formule authentique qu'il a préalablement déclarée perdue ou volée	Contestation abusive par le titulaire du compte d'un ordre de virement valide qu'il a initié	Contestation abusive par le débiteur, de mauvaise foi, d'un ordre de prélèvement émis légitimement par le créancier (litige commercial)

a) Modification de l'impression en relief du numéro de carte.

Utilisée dans le cadre des collectes statistiques mises en œuvre par la Banque de France au niveau national, cette typologie sert de socle commun à l'analyse de la fraude par les prestataires de services de paiement. Selon les objectifs poursuivis, cette typologie peut être complétée par une analyse :

- du **moyen de paiement ciblé** : carte de paiement, virement, prélèvement, chèque, autres instruments ;
- des **canaux de paiement** utilisés : paiement de proximité réalisé au point de vente grâce à un terminal de paiement ou sur un automate, paiement à distance sur internet, par courrier, par téléphone ou par tout autre canal ;
- du **préjudice et de sa répartition** entre la banque du bénéficiaire, la banque du payeur, le commerçant, le titulaire du moyen de paiement, les éventuelles assurances, les autres acteurs impliqués ;
- du **secteur d'activité** du commerçant ayant fait l'objet de la fraude pour les paiements à distance : alimentation, jeux en ligne, services aux particuliers, produits techniques et culturels, téléphonie et communication, etc. ;
- des **zones géographiques** d'émission ou d'utilisation des moyens de paiement ou des données qui lui sont attachées, selon que les banques du payeur et du bénéficiaire sont toutes deux établies dans le même pays ou la même zone monétaire ou non.

Encadré n° 2 : La fraude aux moyens de paiement en France

En France, la fraude sur les paiements par carte fait l'objet depuis 2003 d'un suivi statistique et analytique au sein de l'Observatoire de la sécurité des cartes de paiement (OSCP), sur le périmètre des cartes interbancaires et privatives émises par des établissements agréés en France. En 2016, le législateur a élargi le champ de compétences de l'Observatoire à l'ensemble des moyens de paiement scripturaux et transformé l'OSCP en l'Observatoire de la sécurité des moyens de paiement (OSMP [1]). Ce dernier est chargé désormais d'établir des statistiques de fraude sur les différents instruments de paiement scripturaux.

Les données recueillies par l'OSMP pour l'année 2020 font état d'un montant global de fraude aux moyens de paiement scripturaux émis en France de 1,28 milliard d'euros, pour un peu plus de 35 900 milliards d'euros de flux de paiement. La répartition de la fraude par moyen de paiement présente le profil suivant :

- Le chèque est le moyen de paiement le plus fraudé depuis 2018, puisqu'il représente à lui seul 42 % du montant total de la fraude scripturale (soit 538 millions d'euros en 2020), alors même que son usage décroît régulièrement, avec un nombre de chèque émis divisé par près de deux depuis 2014. En 2020, une fraude sur un chèque représente 2 438 euros en moyenne, pour un taux de fraude qui s'établit à 0,088 % en valeur, représentant l'équivalent d'un euro de fraude pour 1 140 euros de paiement, soit le niveau le plus élevé parmi les moyens de paiement scripturaux, pour une utilisation beaucoup moins intensive (moins d'un paiement sur dix) et qui n'est pas exposée au risque de fraude à l'international ;
- La carte de paiement concentre 37 % de la fraude aux moyens de paiement scripturaux (soit 473 millions d'euros en 2020), avec un taux de fraude qui reste maîtrisé, à 0,068 %, représentant l'équivalent d'un euro de fraude pour 1 470 euros de paiement, malgré l'orientation massive des

1 *https://www.banque-france.fr/stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement*

.../...

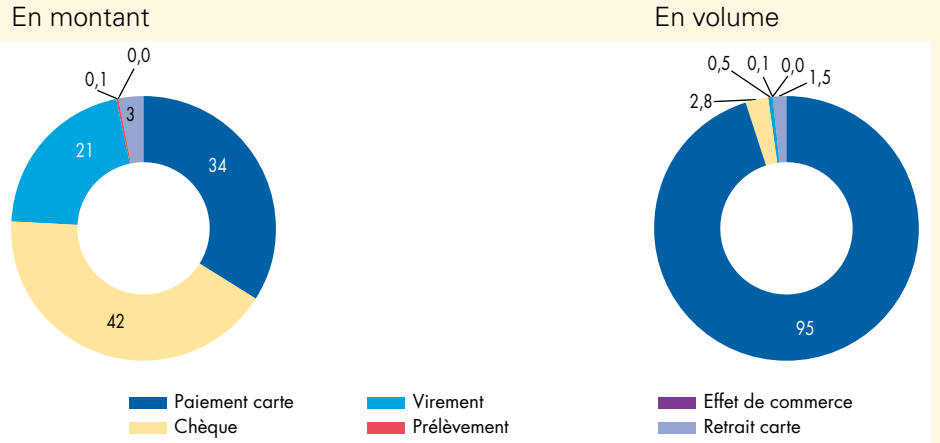
flux vers des pratiques plus sensibles à la fraude comme les paiements sans contact (+ 86 % des flux en valeur par rapport à 2019) et les paiements à distance (+ 13 % des flux en valeur par rapport à 2019). Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,009 %, soit un euro de fraude pour 11 100 euros de paiement), mais plus importante, 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 % des transactions. Avec la croissance du e-commerce, ce constat rend indispensable la généralisation des mesures d'authentification forte prévues par la DSP 2 ;

- Le virement supporte un montant de fraude en progression de 65 % en 2020, à 267 millions d'euros (contre 162 millions en 2019), représentant ainsi 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 du rapport annuel 2020 de l'OSMP), en particulier lorsque le bénéficiaire des fonds sollicite leur envoi sur un compte tenu à l'étranger ;

- Enfin, la fraude sur les prélèvements est très limitée, puisqu'elle représente un montant de 2 millions d'euros, avec un taux de fraude extrêmement bas, à 0,0001 % en 2020.

Répartition de la fraude sur les moyens de paiement scripturaux en 2020

(en %)

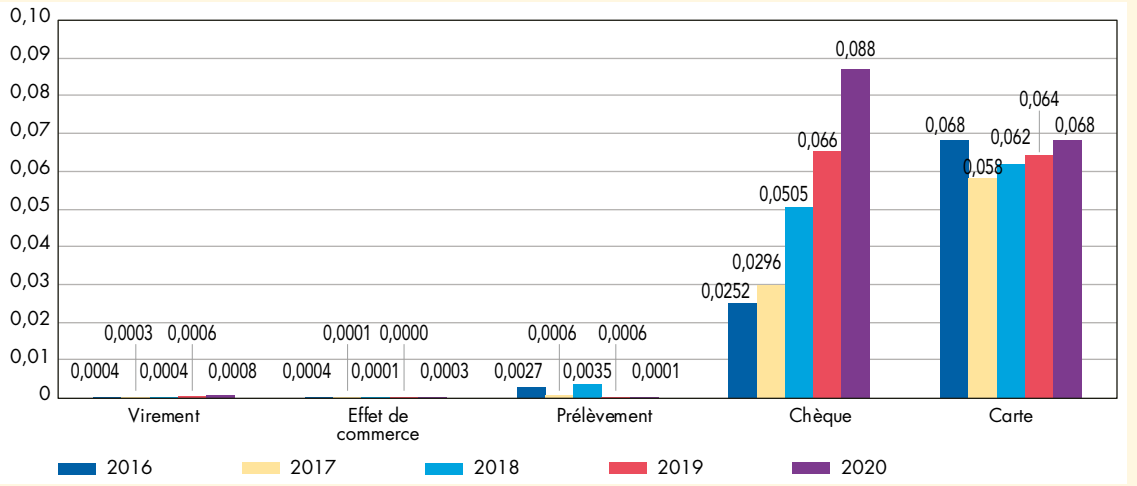


Source : Banque de France (2021), *Observatoire de la sécurité des moyens de paiement. Rapport annuel 2020.*

.../...

Évolution du taux de fraude par moyen de paiement scriptural de 2016 à 2020

(en % des paiements en valeur)



Source : Banque de France (2021), *Observatoire de la sécurité des moyens de paiement. Rapport annuel 2020.*

1.3. Techniques de fraude

Un point central de toute analyse de la fraude est l'identification du mode opératoire utilisé par les fraudeurs. Avec le développement des moyens de paiement électronique, les fraudeurs ciblent de manière croissante les données liées aux moyens de paiement ou à un service de paiement particulier. Une difficulté réside dans le fait que ces données sont véhiculées tout au long de la chaîne de paiement. Cela nécessite par conséquent de déployer des dispositifs efficaces de protection sur l'ensemble de la chaîne et notamment sur tous les points sensibles identifiés.

Les systèmes d'information : il s'agit notamment des équipements informatiques (ordinateurs, smartphones, etc.) des consommateurs ou des commerçants, des bases de données des prestataires de services de paiement et des concentrateurs monétiques pour les transactions liées à des cartes de paiement qui peuvent être victimes d'attaques visant à capturer les données insuffisamment sécurisées. À ce titre, les bases de données constituées aux différents stades de la transaction, et concentrant les données relatives à un grand nombre d'opérations, sont devenues très attractives pour les fraudeurs du fait de l'importance du volume des données susceptibles de faire l'objet d'une utilisation à des fins de fraude.

Ce type d'attaque nécessite, pour être réalisée, l'installation préalable de logiciels malveillants (ou *malwares*) à l'insu de l'utilisateur, ces logiciels étant généralement inoculés au travers de sources apparemment de confiance. Cette technique de fraude vise tant les serveurs des grandes entreprises que les ordinateurs personnels des particuliers, et de manière croissante les téléphones mobiles, qui sont de plus en plus utilisés dans le cadre de transactions de paiement. L'un des *malwares* les plus répandus, connu sous le nom de *keylogger*, permet ainsi d'enregistrer les touches frappées au clavier par la victime.

Internet : un fraudeur peut inciter les utilisateurs à communiquer leurs données personnelles, telles que les données d'une carte de paiement (numéro de carte, date de

validité, cryptogramme visuel situé au dos de la carte) ou d'authentification (par exemple, le numéro de téléphone mobile sur lequel sont envoyés les codes nécessaires à la confirmation d'une opération de paiement). On parle alors d'hameçonnage ou *phishing*. Cette technique de fraude repose généralement sur l'envoi de courriels usurpant des logos et chartes visuelles connus de leurs destinataires (par exemple un établissement de crédit) et invitant les victimes à se connecter à un site qui s'avère frauduleux, dont l'objet est de collecter des informations sensibles. Des variantes existent également sur téléphone mobile (*smishing*, *vishing* pour *voice phishing*), par lesquelles le fraudeur utilise à des fins frauduleuses des messages de type SMS, MMS ou notification du système d'exploitation mobile.

Le dévoiement ou *pharming* consiste, quant à lui, à manipuler les serveurs afin de rediriger l'internaute, sans qu'il s'en aperçoive, vers un site frauduleux, en apparence semblable au site légitime, afin de collecter frauduleusement des fonds ou des données sensibles par ce biais.

Les courriels, fax et conversations téléphoniques : dans le cadre de transactions initiées par courrier, fax ou téléphone comportant une part de traitement manuel, des opérateurs mal intentionnés peuvent enregistrer les données bancaires lors d'un paiement ou d'une réservation en vue de les réutiliser ultérieurement.

Les systèmes d'acceptation ou les réseaux : pour les paiements par carte, le matériel d'acceptation (automates de paiement ou de retrait et terminaux de paiement) ainsi que les réseaux véhiculant les données entre celui-ci et les serveurs d'acquisition peuvent être la cible d'attaques visant à s'approprier des données.

La technique utilisée la plus fréquemment consiste à capturer, à l'insu des porteurs [3], les données écrites sur les pistes magnétiques des cartes (*skimming*). L'ensemble de la façade de l'automate ou sa fente d'insertion peuvent être factices et dissimuler le matériel illégitime. Le dispositif est en outre associé à une caméra vidéo ou à un faux clavier permettant la capture du code confidentiel. Il peut également contenir des systèmes de stockage ou de transmission des données compromises.

Une autre technique consiste à retenir une carte de paiement dans un automate afin de la réutiliser ultérieurement. À cette fin, le fraudeur insère un dispositif dans l'automate, observe la frappe du code confidentiel au clavier, puis il prend possession de la carte après le départ du porteur. Cette technique s'apparente à un vol physique de carte de paiement.

Un fraudeur peut également exploiter des failles de sécurité sur les éléments logiques des automates ou terminaux. L'objectif est alors d'injecter un code malveillant dans les systèmes de ces matériels afin d'en modifier le comportement, voire de prendre le contrôle de leurs différents composants (clavier, écran et imprimante).

Enfin, les réseaux eux-mêmes peuvent être la cible d'attaques lors de l'échange des données entre les matériels d'acceptation, les concentrateurs monétiques le cas échéant et les serveurs acquéreurs.

Les instruments de paiement physiques : le vol physique du moyen de paiement pour l'utiliser en lieu et place de son porteur légitime constitue le principal type d'attaque. Dans le cas des cartes, afin d'optimiser la fraude, le fraudeur tente en général de récupérer le code confidentiel de la carte, ce qui lui permet, à la fois, l'utilisation de la carte dans les distributeurs automatiques de billets, dans les terminaux de paiement et sur internet, pour tous types de transactions.

3 Pour de plus amples développements sur ce thème, cf. Observatoire de la sécurité des cartes de paiement (2010), rapport annuel.

2. La lutte contre la fraude aux moyens de paiement

2.1. L'exercice des missions de surveillance par la Banque de France

La multiplicité des services de paiement et des techniques de fraude requiert une coordination entre institutions et acteurs du secteur privé afin de garantir le bon fonctionnement des services de paiement.

En France, la mission de surveillance des moyens de paiement scripturaux est confiée à la Banque de France depuis la loi sur la sécurité quotidienne de 2001. Elle est codifiée dans les articles L. 141-4 et suivants du Code monétaire et financier. La responsabilité de la Banque de France s'étend à l'ensemble des moyens de paiement scripturaux ainsi qu'aux titres spéciaux de paiement dématérialisés. Le champ de sa surveillance est ainsi défini de manière extensive, l'article L. 311-3 du Code monétaire et financier disposant que « sont considérés comme moyens de paiement tous les instruments de paiement qui permettent à toute personne de transférer des fonds, quel que soit le support et le procédé technique utilisé ».

Pour l'exercice de cette surveillance, la Banque de France s'appuie en particulier sur l'Observatoire de la sécurité des moyens de paiement (OSMP), dont le mandat est triple :

- 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 ;
- établissement des statistiques en matière de fraude ;
- veille technologique, avec pour objet de proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement scripturaux.

Encadré n° 3 : L'Observatoire de la sécurité des moyens de paiement, une spécificité française

L'Observatoire de la sécurité des moyens de paiement (OSMP) est une instance nationale destinée à favoriser l'échange d'informations et la concertation entre tous les acteurs concernés (consommateurs, commerçants et entreprises, autorités publiques et administrations, banques et gestionnaires de moyens de paiement) par le bon fonctionnement des moyens de paiement scripturaux et la lutte contre la fraude.

Institué par la loi n° 2016-1691 du 9 décembre 2016, dite « loi Sapin 2 », l'OSMP a succédé à l'Observatoire de la sécurité des cartes de paiement (OSCP) et a ainsi repris les missions qui lui étaient précédemment dévolues, avec un périmètre étendu à l'ensemble des moyens de paiement scripturaux (virement, prélèvement, carte de paiement, monnaie électronique, chèque et effet de commerce). Le rôle moteur joué par l'Observatoire, depuis sa création en 2002, dans le renforcement de la sécurité des paiements par carte mais aussi le caractère particulièrement protéiforme de l'innovation dans le domaine des paiements, qui ne touche pas la seule carte, ont en effet convaincu les pouvoirs publics français d'élargir son champ de compétences à l'ensemble des moyens de paiement scripturaux.

Présidé par le gouverneur de la Banque de France, l'Observatoire regroupe des représentants de l'État et du Parlement, du surveillant et du superviseur bancaire ainsi que de la Commission nationale de l'informatique et des libertés (CNIL), des émetteurs de moyens de paiement, des opérateurs des systèmes de paiement, des associations de consommateurs, des associations d'entreprises et des associations de commerçants.

.../...

L'Observatoire, dont le secrétariat est assuré par la Banque de France, procède en particulier au suivi des mesures de sécurisation mises en œuvre par les émetteurs, les commerçants et les entreprises, à l'établissement de statistiques de la fraude et à une veille technologique en matière de moyens de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des moyens de paiement. Il établit chaque année un rapport d'activité remis au ministre chargé de l'Économie, des Finances et de l'Industrie et transmis au Parlement [1].

1 Ces rapports sont publiés sur le site de l'Observatoire : *www.observatoire-paiements.fr*

L'objectif principal de la Banque de France dans la conduite de sa mission de surveillance est de maintenir la confiance du public dans l'utilisation des moyens de paiement, en contribuant à la diffusion de bonnes pratiques en matière de sécurité, adressées à l'ensemble des acteurs concernés et de façon homogène sur le territoire. Pour ce faire, elle procède à des analyses de risque pour chaque moyen de paiement et établit des référentiels de sécurité. Au travers de contrôles menés sur pièces ou sur place, elle s'assure de la conformité des acteurs et de leurs prestataires techniques au regard de ces référentiels. Si elle estime qu'un moyen de paiement présente des garanties de sécurité insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier. Si ces recommandations ne sont pas suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au Journal officiel.

Encadré n° 4 : Exemples d'exigences de sécurité inscrites dans les référentiels de sécurité

La sécurité des systèmes d'information

Les dispositifs de lutte contre la fraude doivent intégrer en priorité la protection des données à caractère personnel. Les systèmes d'information doivent ainsi répondre à des standards de sécurité permettant de limiter les risques identifiés de captation des données liées aux moyens de paiement. Les systèmes d'information doivent, d'une manière générale, être protégés contre les menaces internes ou externes et faire l'objet, à ce titre, d'analyses de sécurité visant à mettre en place des mesures de protection adaptées au contexte dans lequel ils évoluent. Leurs gestionnaires doivent ainsi définir une politique de sécurité et réévaluer régulièrement les risques auxquels ils sont exposés. Différentes méthodes leur sont proposées. On citera par exemple Ebios (élaborée et maintenue à jour en France par l'Agence nationale de la sécurité des systèmes d'information) ou la série de normes ISO 27000.

En matière d'attaque contre les bases de données, la directive européenne sur la sécurité des réseaux et de l'information dans l'Union [1], adoptée le 6 juillet 2016, impose en particulier aux banques ainsi qu'aux e-commerçants de mettre en place des systèmes de protection de leurs données adaptés aux risques évalués et de déclarer aux autorités les violations de leurs bases de données contenant des informations sur la clientèle et notamment des informations sur les moyens de paiement.

1 Directive Network and Information System Security (NIS).

.../...

La sécurité des données au moment de leur enregistrement dans les systèmes doit également faire partie intégrante de ces politiques de sécurité. Celles-ci doivent en effet prévoir une traçabilité de l'ensemble des accès au système d'information, ayant pour objet la saisie ou la modification de données nécessaires à la réalisation de la transaction, afin de constituer une piste d'audit fiable. Les compromissions généralement constatées dans ce contexte relèvent de malversations initiées par du personnel indélicat. Des dispositifs d'acceptation limitant l'interaction entre les commerçants et les moyens de paiement doivent donc être privilégiés. Il est en outre important de limiter l'accès aux données au seul personnel réellement habilité et de ne pas conserver de données sensibles dès lors que celles-ci ne sont plus utiles.

La sensibilisation des utilisateurs

La sensibilisation des utilisateurs aux questions de sécurité est de nature à lutter contre les attaques d'ingénierie sociale. Une communication efficace, utilisant l'ensemble des canaux disponibles (courriers, courriels, sites internet, etc.), est souhaitable de la part de l'ensemble des acteurs de la chaîne de paiement et doit ainsi être instaurée afin d'attirer la vigilance des utilisateurs sur les facteurs de risque et les bonnes pratiques à respecter. Les utilisateurs doivent en outre être incités à n'utiliser que des sites de confiance, dont le niveau de sécurité apparaît conforme aux termes de référence cités dans ces communications.

L'identification des transactions à risque

La mise en place de dispositifs reposant sur l'analyse et l'exploitation des données personnelles du payeur constitue un axe de développement clef dans la détection des transactions frauduleuses. Ces dernières années, ces dispositifs ont eu tendance à élargir le nombre et la nature des données collectées lors d'une transaction sur internet afin de vérifier la cohérence entre ces données et d'augmenter le degré de certitude quant à l'identité de la personne initiant la transaction de paiement. Ainsi, aux côtés des données traditionnellement collectées relatives à l'identité et aux coordonnées de la personne initiant la transaction (nom, prénom, adresse postale, adresse de livraison, e-mail, numéro de téléphone, etc.), les outils de lutte contre la fraude ont progressivement intégré :

- les habitudes de consommation du payeur (nombre et détail des commandes, périodicité et montants des achats, ancienneté de la relation commerciale) ;
- sa localisation (par exemple par l'adresse IP de l'ordinateur utilisé) ;
- les outils utilisés pour accéder à internet ;
- des données liées à son comportement (analyse du temps de remplissage de formulaires, type de saisie clavier, etc.).

Si cet élargissement du nombre de critères retenus dans la détermination du score d'une transaction a permis d'atteindre une meilleure fiabilité du niveau de risque évalué, il présente des risques en matière d'atteinte à la vie privée, dans la mesure où les acteurs de la chaîne de paiement sont très largement passés d'une logique déclarative, où le client communiquait ses données, à une logique de collecte automatique, sans que le client en soit systématiquement informé. C'est la raison pour laquelle ces traitements doivent être préalablement autorisés en France par la Commission nationale de l'informatique et des libertés (CNIL), autorité nationale compétente en matière de protection des données personnelles, notamment au titre du règlement général sur la protection des données (RGPD) de l'Union européenne.

La Banque de France peut, dans le cadre de son rôle de surveillant, contrôler tout prestataire de services de paiement (émetteurs, acquéreurs et gestionnaires de moyens de paiement scripturaux) sur le territoire national : établissements bancaires, établissements de paiement et établissements de monnaie électronique. Ces établissements sont agréés et supervisés par l'Autorité de contrôle prudentiel et de résolution (ACPR). La surveillance de la Banque de France peut également s'étendre à un établissement exempté d'agrément par l'ACPR, mais qui gère des moyens de paiement scripturaux dans un réseau limité d'acceptation ou pour un éventail limité de biens et de services.

Au cours des dernières années, la Banque de France a diligenté plusieurs missions de contrôle sur place portant successivement sur i) l'état de la préparation des principaux groupes bancaires français à la migration vers les moyens de paiement SEPA, ii) l'évaluation de la sécurité et le bon fonctionnement de la gestion des activités liées au chèque, et iii) la conformité des processus d'administration et de gestion des paiements sur internet au regard des orientations de l'Autorité bancaire européenne (ABE). Suite à ces différentes missions, la Banque de France a établi une série de recommandations à chacun des différents acteurs, dont les principales portaient sur le renforcement des dispositifs de suivi de la migration à SEPA de la clientèle, sur l'amélioration de la qualité des statistiques de fraude déclarées auprès de la Banque de France ainsi que celles des dispositifs de contrôle interne.

La Banque de France exerce également sa mission en matière de surveillance de la sécurité des moyens de paiement scripturaux par l'émission d'un avis consultatif à l'attention de l'ACPR sur les moyens techniques, informatiques et organisationnels relatifs à la sécurité des moyens de paiement pour les activités envisagées par les sociétés sollicitant un agrément d'établissement de paiement ou d'établissement de monnaie électronique. Cet avis est versé au dossier soumis au collège Banques de l'ACPR, appelé à se prononcer sur la délivrance de l'agrément.

La Banque de France rend compte de son action en matière de surveillance des moyens de paiement scripturaux au travers de rapports de surveillance publiés tous les trois à quatre ans [4].

2.2. Les acteurs de la lutte contre la fraude

En complément de l'action des banques centrales dans leur fonction de surveillance des moyens de paiement, les forces de l'ordre jouent un rôle primordial dans le démantèlement des réseaux de fraude aux moyens de paiement. Ainsi, en France, les forces de l'ordre se sont structurées à différents niveaux, conduisant la police et la gendarmerie nationales à mettre en place un certain nombre d'organismes spécialisés, notamment :

- Au sein de la direction centrale de la police judiciaire, la sous-direction de la lutte contre la criminalité organisée et la délinquance financière (SDLCODF) est chargée du recueil du renseignement, de l'analyse stratégique et des relations avec les administrations concernant, entre autres, la délinquance spécialisée. À ce titre, elle est constituée d'offices centraux parmi lesquels certains ont un rôle actif dans la lutte contre la fraude aux moyens de paiement, comme l'Office central pour la répression de la grande délinquance financière (ORCGDF) et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), sous l'autorité duquel est placée la brigade centrale pour la répression des contrefaçons des cartes de paiement (BCRCCP) ;

- Au sein de la gendarmerie nationale, le service technique de recherches judiciaires et de documentation est constitué notamment de la division financière et de la division de lutte contre la

4 Banque de France (2021), *La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers. Rapport 2020*.

cybercriminalité, en charge de centraliser et d'exploiter les informations judiciaires relatives aux crimes et délits. Ces deux divisions sont fortement impliquées dans la lutte contre la fraude en ce qui concerne les cartes de paiement ;

- Ces services spécialisés sont complétés par des services d'expertises techniques : le service central de l'informatique et des traces technologiques au sein de la police nationale et la division criminalistique ingénierie et numérique au sein de l'institut de recherche criminelle de la gendarmerie nationale, qui réalisent des investigations techniques de haut niveau.

Cette organisation est relayée sur le terrain, tant au niveau de la police que de la gendarmerie, par des enquêteurs en technologies numériques et des investigateurs en cybercriminalité.

Par ailleurs, les établissements bancaires et plus globalement les prestataires de services de paiement, les forces de l'ordre, les organismes de certification et laboratoires d'expertise technique ou encore les autorités bancaires ont éprouvé le besoin de mettre en place des **structures de coopération permanentes**. Enfin, en fonction des thématiques, des organisations externes au secteur bancaire, comme Europol, peuvent être invitées afin d'enrichir les échanges.

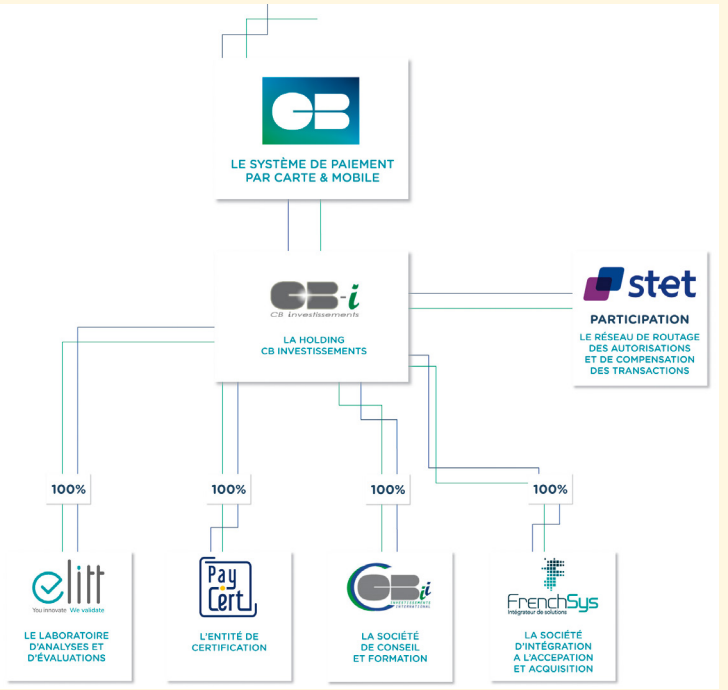
Encadré n° 5 : Le Groupement des Cartes Bancaires CB (GIE CB) et la lutte contre la fraude à la carte de paiement en France

Dans le domaine des paiements par carte, le secteur bancaire français s'est organisé dès 1984 en France autour d'un groupement d'intérêt économique (GIE), le Groupement des Cartes Bancaires CB (GIE CB [8]), autorité de gouvernance du système de paiement par carte « CB » et pôle opérationnel et d'expertise technique du système. La naissance de ce GIE a donc, de fait, accompagné le développement de l'interbancarité en France autour de la carte de paiement, tout en conférant au GIE une position centrale dans la lutte opérationnelle contre la fraude.

Les actions du GIE en la matière s'articulent notamment autour des activités suivantes :

- la mise en place des outils permettant l'identification de transactions potentiellement frauduleuses et la

Organisation du GIE CB et de ses filiales



Source : Groupement des Cartes Bancaires CB (GIE CB).

8 Le GIE CB regroupe environ 130 établissements prestataires de services de paiement. Il assure les missions attachées à la gouvernance, à la sécurité et à la promotion du système CB, et pilote le développement de produits et services ainsi que l'innovation en matière monétique dans le respect des règles législatives et réglementaires. Outre le système CB, l'objet du Groupement s'étend également aux travaux d'étude et de normalisation de sécurité spécifiques aux cartes TRD (support matériel des titres-restaurants dématérialisés).

.../...

détection de points de compromission, par l'analyse en temps réel des données d'activité sur le système CB ;

- une collaboration étroite et régulière avec les forces de l'ordre afin d'apporter des éléments de preuve, notamment dans les enquêtes ;
- l'analyse et l'évaluation de l'ensemble des composants du réseau CB (cartes, terminaux, réseaux, etc.), au travers d'une filiale dédiée, le laboratoire Elitt ;
- la certification des matériels autorisés sur le réseau CB (par exemple, terminaux de paiement, solutions de paiement mobile, etc.), au travers d'une filiale dédiée, PayCert.

À noter que les réseaux internationaux tels que Visa, Mastercard ou encore American Express, ont développé des outils similaires, qui bénéficient à leurs membres.

2.3. L'apport du suivi des innovations dans les moyens de paiement au niveau international

Le Comité sur les paiements et les infrastructures de marché (Committee on Payments and Market Infrastructures, CPMI) de la Banque des règlements internationaux, qui a succédé en 2014 au Comité sur les systèmes de paiement et de règlement (Committee on Payment and Settlement Systems, CPSS), couvre dans son champ d'action les systèmes de paiement de détail et par extension les moyens de paiement. Il s'est ainsi intéressé à l'innovation dans les moyens de paiement et notamment au positionnement des banques centrales dans ce cadre, et a publié un rapport en mai 2012 à ce sujet, dont les constats et recommandations conservent l'essentiel de leur pertinence [5].

Le rapport souligne l'importance qu'attachent les banques centrales à promouvoir l'utilisation de moyens de paiement efficients et sécurisés tout en favorisant l'innovation. Il dresse également un inventaire des freins et problématiques générales liées à l'innovation dans les paiements, comme le rôle de la standardisation, l'influence des usages dans les instruments de paiement pouvant varier d'un pays à l'autre, ainsi que le rôle du régulateur. En matière de sécurité, le rapport souligne l'importance du maintien de la confiance des utilisateurs dans les services de paiement. La technologie doit être au service de l'efficience de l'instrument de paiement. Elle doit aussi améliorer la fluidité de l'acte de paiement sans pour autant introduire des vulnérabilités dans la chaîne de paiement, pouvant être exploitées par des fraudeurs, en particulier au niveau du consentement de l'opération de paiement.

Dans cet esprit, le rapport souligne par exemple les avancées permises par la technologie EMV, qui rendent possible l'authentification de la carte et du terminal de paiement. Concernant les transactions à distance, des points d'attention sont identifiés, relatifs :

- aux conditions de sécurité dans lesquelles sont conservées les données de la carte par le marchand et/ou son prestataire de services de paiement ;
- à la mise en place de mécanismes d'authentification forte afin de lutter efficacement contre la fraude. Le CPSS a constaté à cet égard l'efficacité des mécanismes basés sur au moins deux facteurs d'authentification.

Ces réflexions confortent ainsi les choix réglementaires adoptés au niveau européen, ainsi que les travaux conduits en France par l'Observatoire de la sécurité des moyens de paiement.

5 CPMI (2012), *Innovations in retail payments*.

3. Le cadre européen de sécurité des moyens de paiement

La convergence des réglementations applicables au marché des paiements est une composante essentielle à l'intégration du marché des paiements en Europe, et vient compléter les initiatives politiques majeures telles que l'introduction de l'euro fiduciaire ou la mise en place des moyens de paiement SEPA.

3.1. La 1re directive sur les services de paiement (DSP 1)

La directive sur les services de paiement (DSP) adoptée le 13 novembre 2007 [6], et entrée en application en novembre 2009, a posé des règles communes pour la fourniture de services de paiement en Europe, par l'apport d'un cadre harmonisé en matière de régulation des services de paiement couplé à un renforcement à la fois de la protection du consommateur et de la concurrence sur ce marché.

3.1.1. Les règles applicables aux services de paiement

En définissant des règles pour un ensemble de « services de paiement », notion qui peut être assimilée à celle d'opérations de « mise à disposition ou de gestion de moyens de paiement » (cf. encadré 6), la directive sur les services de paiement présente la particularité de ne pas s'appuyer sur la notion du support utilisé pour l'initiation ou l'acceptation du paiement ou de technologie sous-jacente ; par ailleurs, elle ne différencie pas les règles en fonction du statut juridique de l'établissement fournisseur des services de paiement. Cette approche permet d'assurer une constance des règles applicables aux paiements par rapport aux technologies utilisées et à leur évolution, ou à la nature de leur fournisseur, tout en tenant compte des spécificités des services concernés.

Pour l'application de certaines dispositions, comme en matière de révocation des ordres, de contestation des paiements et d'exécution des opérations, la directive distingue ainsi les services de paiement en fonction de leur mode d'initiation. Elle désigne notamment les paiements par carte sous le vocable « d'opérations initiées via le bénéficiaire ». Les autres types d'opérations sont également désignés de manière générique par les expressions suivantes : « opérations initiées par le payeur » dans le cas des virements, « opérations initiées par le bénéficiaire » dans le cas des prélèvements.

Pour préciser certaines dispositions, la directive s'appuie également sur la notion d'instrument de paiement ou plus précisément sur la notion d'instrument de paiement équipé d'un « dispositif de sécurité personnalisé », c'est-à-dire permettant d'authentifier le payeur. Ces articles visent essentiellement les transactions effectuées par carte, par téléphone portable si l'application de paiement est assortie d'un dispositif de sécurité personnalisé, ainsi que celles effectuées depuis des sites de banque en ligne. Enfin, la directive prévoit pour les instruments de paiement « relatifs à des montants faibles » un allégement réglementaire, notamment en matière d'obligation d'information et de contestation. Ce dispositif ne s'applique qu'à des instruments dont le montant maximal de transaction ne peut, par contrat, dépasser 30 euros.

3.1.2. La contestation des opérations non autorisées

La directive prévoyait deux dispositifs, selon que le paiement contesté a été autorisé par le payeur ou non.

Le premier dispositif concernait les opérations non autorisées, c'est-à-dire en pratique les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement. Le payeur dispose d'un délai de 13 mois suivant la date de débit de son compte pour contester l'opération de paiement non autorisée. Son prestataire de services de paiement doit alors rétablir sans délai le compte dans l'état

6 Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur. *http://eur-lex.europa.eu/legal-content/FR/*

dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Le payeur doit, dès qu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer son prestataire de services de paiement.

Avant l'introduction de l'authentification forte par la deuxième directive, la première directive prévoyait que ce dispositif ne s'applique pas pour les instruments équipés d'un dispositif de sécurité personnalisé, ce qui est notamment le cas des cartes de paiement : le payeur pouvait dans ce cas supporter, à concurrence de 150 euros[7], les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé, ou « si le payeur n'était pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, consécutive au détournement d'un instrument de paiement ». Enfin, dans le cas avéré d'agissement frauduleux ou de négligence grave du titulaire et avant la mise en opposition de la carte, ce dernier ne peut bénéficier de ces dispositions de remboursement.

Le deuxième cas de contestation ouvert par la directive concerne les opérations ayant fait l'objet d'une autorisation générale de la part du payeur, mais sans que le montant précis de l'opération n'ait été indiqué au moment de l'autorisation. Ce dispositif s'applique aux prélèvements et aux paiements par carte, par exemple lors de réservations d'hôtels ou de voitures. Ainsi, lorsque le payeur a donné son consentement à une opération de paiement, il peut, dans un délai de 8 semaines à compter de la date à laquelle les fonds ont été débités, demander un remboursement de cette opération dans le cas où le montant de l'opération finalement exécutée dépasse le montant auquel le payeur pouvait raisonnablement s'attendre compte tenu de ses dépenses passées, des conditions prévues au contrat-cadre ou autres circonstances pertinentes. Dans un délai de 10 jours ouvrables suivant la réception de la demande de remboursement, le prestataire de services de paiement doit alors rembourser le montant total de l'opération de paiement, ou justifier son refus de rembourser en indiquant les organismes que le payeur peut saisir s'il n'accepte pas la justification donnée.

3.1.3. L'harmonisation des obligations d'information dans le cadre de la fourniture de services de paiement

La directive définit les obligations d'information du client à la charge des prestataires à la fois pour les opérations de paiement isolées et pour les opérations relevant d'un « contrat-cadre ». Il s'agit principalement d'informations sur le prestataire de services de paiement (nom et coordonnées), sur l'utilisation du service de paiement (forme et procédure du consentement, délai d'exécution, possibilité de convenir de limites de dépenses pour l'utilisation d'un instrument de paiement), sur les frais (y compris taux d'intérêt et taux de change), sur la communication (fréquence), sur les mesures de protection et les mesures correctives (mesure à prendre pour préserver la sécurité d'un instrument, possibilité de blocage de l'instrument, responsabilité du prestataire et du payeur, conditions de remboursement, etc.), sur la modification et la résiliation d'un contrat (durée du contrat, droit de résiliation) et sur les recours possibles.

La directive encadre également les modalités de modification et de résiliation des contrats passés entre les utilisateurs et les prestataires de services de paiement, ce qui constituait une nouveauté pour les contrats carte français. En ce qui concerne la modification des conditions contractuelles, les dispositions se situaient cependant largement dans la lignée des pratiques françaises en matière de conventions de compte. La directive prévoit ainsi que toute modification doit être proposée par le prestataire de services de paiement au plus tard deux mois avant la date proposée pour son entrée en vigueur. Sauf refus explicite

7 Montant ramené à 50 euros dans le cadre de la DSP 2.

de l'utilisateur avant la date d'entrée en vigueur, la modification est réputée acceptée. Dans le cas où l'utilisateur n'accepterait pas la modification, il a le droit de résilier son contrat immédiatement et sans frais, avant la date d'entrée en vigueur de la modification.

En matière de résiliation, la directive encadre en revanche davantage les pratiques et propose un cadre un peu plus favorable aux utilisateurs de services de paiement que celui qui était précédemment en vigueur en France. Un contrat-cadre peut ainsi être résilié à tout moment par le client à moins que les parties ne soient convenues d'un délai de préavis, celui-ci ne pouvant excéder un mois. Cette résiliation n'emporte pas de frais si le contrat-cadre a été conclu pour une durée déterminée supérieure à 12 mois ou s'il a été conclu pour une durée indéterminée. Dans les autres cas, les frais de résiliation doivent être adaptés et en rapport avec les coûts.

3.2. La 2e directive sur les services de paiement (DSP 2)

3.2.1. Les principales dispositions de la DSP 2

La 2e directive européenne sur les services de paiement (dite « DSP 2 »), adoptée le 25 novembre 2015 et entrée en vigueur le 13 janvier 2018, s'inscrit dans le prolongement de la DSP 1, en élargissant à de nouveaux services et acteurs le champ des services de paiement régulés, tout en renforçant les exigences sécuritaires applicables aux acteurs du marché des paiements. En particulier, la directive généralise l'utilisation de l'authentification forte du payeur pour les opérations de paiement initiées par voie électronique.

Afin de préserver une marge de flexibilité et d'évolutivité dans l'application de la DSP 2, la Commission européenne a choisi une approche reposant sur deux niveaux de textes réglementaires :

- d'une part, la directive elle-même et sa transposition au niveau national, qui fixent le cadre et les principes généraux de la réglementation ;
- d'autre part, des textes de second niveau, soit des orientations dont l'élaboration a été confiée à l'Autorité bancaire européenne (ABE), soit des normes techniques de réglementation préparées par l'ABE et adoptées par la Commission européenne, visant à préciser les conditions de mise en œuvre et les exigences définies par la directive.

En matière de sécurité des services de paiement, l'ABE a ainsi reçu pour mandat d'élaborer ou de préparer, en étroite collaboration avec la Banque centrale européenne (BCE), les textes suivants :

- une norme technique de réglementation (ou *regulatory technical standard,* RTS) qui précise : i) les requis et les exemptions de l'authentification forte du client ; ii) les requis en matière de protection des données de sécurité personnalisées (identifiants de connexion et mots de passe) ; et iii) les modalités techniques et opérationnelles permettant aux prestataires de services de paiement (PSP) gestionnaires de comptes, aux PSP tiers (à l'« initiateur de paiement » et à l'« agrégateur d'informations ») et aux titulaires de compte de communiquer de façon sécurisée [8] ;
- des orientations définissant les mesures de sécurité relatives aux risques opérationnels et de sécurité [9] ;
- des orientations relatives aux notifications des incidents majeurs aux autorités nationales et européennes [10] ;
- des orientations relatives aux statistiques de fraude [11].

Enfin, il est à noter que l'entrée en application de cette nouvelle directive au niveau européen est concomitante de celles, d'une part, du règlement général sur la protection des données à caractère

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

9 Orientations de l'Autorité bancaire européenne du 12 décembre 2017 relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liées aux services de paiement dans le cadre de la directive (UE) 2015/2366 (EBA/GL/2017/17).

10 Orientation de l'Autorité bancaire européenne du 27 juillet 2017 sur la notification des incidents majeurs dans le cadre de la directive (UE) 2015/2366 (EBA/GL/2017/10).

11 En cours d'élaboration.

personnel (RGPD [12]) et, d'autre part, de la directive sur la sécurité des systèmes et des réseaux d'information (souvent appelée « directive NIS » pour *network information security* [13]), dont la transposition en France avait été en partie anticipée au travers de la loi de programmation militaire (LPM) de décembre 2014 et qui sert de cadre aux obligations spécifiques applicables aux opérateurs d'importance vitale (OIV). Ces deux textes réglementaires conditionnent également, dans les domaines qui les concernent, les exigences applicables aux acteurs des moyens de paiement scripturaux.

12 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

13 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Encadré n° 6 : Les services de paiement au sens de la directive

1. Les services permettant de verser des espèces sur un compte de paiement et toutes les opérations qu'exige la gestion d'un compte de paiement.

2. Les services permettant de retirer des espèces d'un compte de paiement et toutes les opérations qu'exige la gestion d'un compte de paiement.

3. L'exécution d'opérations de paiement, y compris les transferts de fonds sur un compte de paiement auprès du prestataire de services de paiement (PSP) de l'utilisateur ou auprès d'un autre PSP :

   a) l'exécution de prélèvements, y compris de prélèvements autorisés unitairement ;

   b) l'exécution d'opérations de paiement à l'aide d'une carte de paiement ou d'un dispositif similaire ;

   c) l'exécution de virements, y compris d'ordres permanents.

4. L'exécution d'opérations de paiement dans le cadre desquelles les fonds sont couverts par une ligne de crédit accordée à l'utilisateur de services de paiement :

   a) l'exécution de prélèvements, y compris de prélèvements autorisés unitairement ;

   b) l'exécution d'opérations de paiement à l'aide d'une carte de paiement ou d'un dispositif similaire ;

   c) l'exécution de virements, y compris d'ordres permanents.

5. L'émission d'instruments de paiement et/ou l'acquisition d'opérations de paiement.

6. Les transmissions de fonds.

7. Les services d'initiation de paiement.

8. Les services d'information sur les comptes.

3.2.2. L'authentification forte des opérations sensibles

La DSP 2 impose le recours à un dispositif d'authentification forte du titulaire de compte lorsque celui-ci accède à son compte de paiement en ligne (pour une simple consultation), initie une opération de paiement électronique (virement ou paiement par carte) ou exécute une action au moyen d'un canal de communication à distance qui présente un risque élevé de fraude (par exemple, enregistrement d'un bénéficiaire de virement).

L'authentification forte, ou authentification à deux facteurs, repose sur l'utilisation de deux éléments ou plus appartenant au 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 PSP : une carte, un smartphone, une montre ou un bracelet connecté, un porte-clefs, etc. ;
- « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique.

La DSP 2 dispose que ces éléments doivent être indépendants : la compromission de l'un ne doit pas remettre en question la fiabilité des autres, de manière à préserver la confidentialité des données d'authentification.

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 clef de validation de l'opération de paiement générée après lecture de l'empreinte devra être également à usage unique.

Ce recours à l'authentification forte ne s'impose que dans le cas d'opérations de paiement intra-européennes, c'est-à-dire pour lesquelles les PSP du payeur et du bénéficiaire sont établis dans l'Union européenne [14] ; dans le cas d'opérations de paiement faisant intervenir un PSP non implanté dans l'Union, les RTS prévoient qu'une authentification forte soit mise en œuvre dans la mesure du possible, sur une base de meilleur effort (ou *best effort*). Dans ce cas, le régime de responsabilité prévu par la directive continue de s'appliquer : le PSP situé dans l'UE qui n'applique pas l'authentification forte supporte les éventuelles pertes financières en cas d'opération de paiement non autorisée.

L'article 2 des RTS prévoit par ailleurs que les PSP sont tenus de mettre en place des dispositifs permettant de détecter les opérations frauduleuses ou suspectes en tenant compte des éléments suivants :

- les éléments d'authentification qui auraient été volés ou compromis ;
- le montant de chaque opération de paiement ;
- les scénarios de fraude connus ;
- la détection des logiciels malveillants (virus ou *malwares*) susceptibles d'affecter les dispositifs informatiques utilisés pour l'authentification ;
- la journalisation des accès des utilisateurs aux services de paiement.

14 Le Royaume-Uni est un cas particulier, puisque la Financial Conduct Authority (FCA) a indiqué que les dispositions prévues par les RTS continueraient d'être appliquées, et ce même dans l'éventualité d'un « no deal » (FCA Policy Stance PS19/26). *https://www.fca.org.uk/publications/policy-statements/*

Quelques exemples de solutions d'authentification

Combinaison de facteurs d'authentifications mis en œuvre	Connaissance	Possession	Inhérence
Inhérence	Saisie d'un code confidentiel + Capture d'une empreinte biométrique	Lecture d'une empreinte biométrique sur un terminal reconnu comme appartenant au payeur	Lecture d'une empreinte biométrique sur un terminal non reconnu comme appartenant au payeur
Possession	Carte ou mobile du payeur + Code confidentiel *ou* Données de paiement + Code à usage unique adressé sur un terminal appartenant au payeur	Lecture de carte, d'un porte-clefs, d'un mobile, etc., sans saisie de code confidentiel ou d'empreinte (exemple : paiement sans contact)	
Connaissance	Identifiant + Code confidentiel		

Solutions d'authentification simple (une seule famille de facteurs)

Solutions d'authentification forte (combinaison de deux familles de facteurs)

3.2.3. Les exemptions à l'authentification forte

Les RTS prévoient toutefois des cas d'exemption à l'authentification forte, qui permettent aux PSP de ne pas appliquer d'authentification forte dans un nombre limité de cas :

- La consultation de comptes après une première authentification forte, pendant une période de 90 jours (article 10) ; à l'issue de cette période, une nouvelle demande d'authentification forte est nécessaire pour permettre l'accès aux comptes par le client ;
- Les paiements de faible montant, avec des plafonds définis par cas d'usage, tel que présenté dans le tableau ci-après :

Le PSP gestionnaire de compte est tenu de veiller à la mise en place des dispositifs techniques permettant d'assurer le respect de ces plafonds : dès l'atteinte de l'un des seuils retenus par le PSP gestionnaire du compte, une authentification forte doit être mise en œuvre ;

- Les paiements aux automates de transport et de parking (article 12) ;
- Les paiements vers un bénéficiaire de confiance (article 13) désigné comme tel par le client auprès de son PSP gestionnaire de comptes ; 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 ;

	Paiements de proximité en mode sans contact (article 11)	Paiements à distance (article 16)
Plafond de paiement en valeur absolue	50 euros / paiement	30 euros / paiement
Plafond de paiement en cumul de transactions successives	5 opérations successives ou[a] 150 euros de paiement cumulé	5 opérations successives ou[a] 100 euros de paiement cumulé

a) En ce qui concerne le seuil relatif au cumul d'opérations successives, il appartient au prestataire de services de paiement (PSP) teneur de compte de choisir le plafond qui lui semblera le plus approprié.

- Les opérations de paiement récurrentes initiées par le payeur (article 14), c'est-à-dire une série d'opérations de paiement de même montant et vers le même bénéficiaire ; dans ce cas, seule l'initiation de la première opération de paiement est soumise à authentification forte (exemples : abonnement, loyer, etc.) ;

- Les virements entre les comptes détenus par la même personne physique ou morale au sein d'un même PSP gestionnaire de comptes (article 15) ;

- Les opérations de paiement d'entreprises recourant à des protocoles de transfert d'ordres de paiement sécurisés (article 17) ;

- Pour les opérations de paiement à distance, lorsque les PSP estiment que le niveau de risque de l'opération de paiement est faible (article 18) au regard de leur dispositif de détection des opérations de paiement suspectes. Le recours à ce motif d'exemption est encadré par des dispositions visant à s'assurer de la qualité de l'évaluation réalisée par les PSP du payeur et du bénéficiaire.

3.2.4. Le plan de migration de la Place française vers l'authentification forte des paiements par carte sur internet

Du point de vue juridique, l'ensemble des exigences en matière d'authentification forte est entré en application le 14 septembre 2019. Toutefois, compte tenu du manque de préparation de marché et du temps nécessaire à la mise à niveau des protocoles et des systèmes tant chez les banques que chez les commerçants, l'Observatoire de la sécurité des moyens de paiement (OSMP) a défini un plan de migration pour la Place française, conformément à l'avis de l'Autorité bancaire européenne du 16 octobre 2019 (EBA-Op-2019-11). Ce plan de migration comprend deux volets :

- un volet à l'attention des consommateurs portant sur 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) comme facteur unique d'authentification ;

- un volet à l'attention des acteurs professionnels de la chaîne des paiements, y compris les e-commerçants, portant sur l'évolution des infrastructures d'authentification, notamment du protocole technique 3D-Secure, afin d'assurer la gestion des règles de responsabilité et d'exemption à l'authentification forte prévues par la DSP 2.

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.

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. L'Observatoire a en même temps décidé d'un certain nombre de mesures complémentaires pour atteindre le plus haut niveau de conformité dans les délais impartis par l'Autorité bancaire européenne.

- Tout d'abord, l'Observatoire a accordé une attention particulière à la disponibilité effective et complète du protocole 3D-Secure dans sa version 2 pour les e-commerçants. La Banque de France a pris l'attache des principaux prestataires d'acceptation technique (PAT), actifs pour le e-commerce en France, pour connaître leur calendrier de mise à niveau de leurs infrastructures.

- Ensuite, l'Observatoire a convenu d'une trajectoire de déploiement du mécanisme de *soft decline* entre septembre 2020 et mars 2021. Ce mécanisme permet à l'émetteur de la carte de rejeter une transaction non conforme à la DSP 2 tout en permettant au e-commerçant de soumettre une nouvelle fois la transaction via 3D-Secure. Il a été introduit comme attendu au 1er avril 2020, sur une base

réduite, puis a connu une montée en régime progressive selon une approche par seuils décroissants [15].

- Enfin, l'Observatoire promeut la nécessaire résilience et qualité des infrastructures servant à la mise en œuvre de l'authentification forte, tant du côté des émetteurs de cartes avec leurs serveurs d'authentification que des schémas interbancaires avec leurs serveurs de routage des flux, dès lors que leur utilisation est appelée à devenir systématique. Un mécanisme de traitement des flux de paiement en cas de défaut de ces infrastructures doit être défini afin d'assurer, dans un cadre normé et commun, l'identification des incidents, le partage d'information au niveau de la Place et l'activation de modes de traitement alternatifs.

En parallèle de ces actions collectives, la Banque de France a également renforcé à partir du deuxième semestre 2020 le suivi des acteurs bancaires les plus en retard sur la trajectoire cible, du côté de l'émission ou de l'acquisition. L'Observatoire a également développé des supports de communication à l'attention des consommateurs, visant à expliquer la nouvelle réglementation et les conditions de la migration. Une fiche pédagogique et une vidéo ont notamment été diffusées en septembre 2020 [16].

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, plus de 50 % 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. 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 second 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 ; ce déploiement doit être achevé à l'automne 2021.

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 dans sa version 2. Elle s'est toutefois accélérée sous l'effet du plan de montée en régime du mécanisme de *soft decline*. Ainsi, à fin juin 2021, 85 % des flux de paiement éligibles

15 À partir du 1er octobre 2020 : rejet des transactions non conformes de plus de 2 000 euros.

À partir du 15 janvier 2021 : rejet des transactions non conformes de plus de 1 000 euros.

À partir du 15 février 2021 : rejet des transactions non conformes de plus de 500 euros.

À partir du 15 mars 2021 : rejet progressif des transactions non conformes de plus de 250 euros (étalé sur 4 semaines).

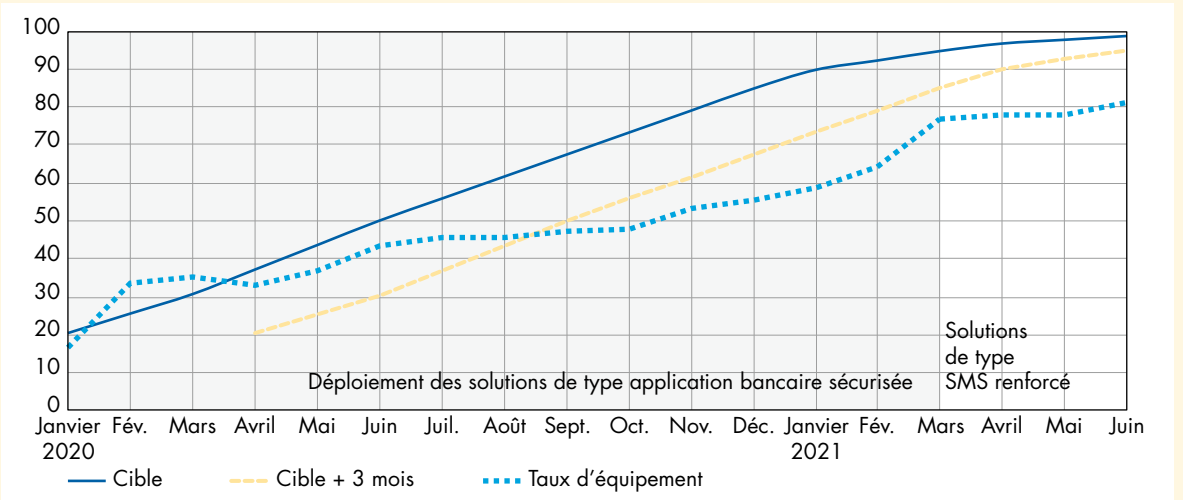
À partir du 15 avril 2021 : rejet progressif des transactions non conformes de plus de 100 euros (étalé sur 4 semaines).

À partir du 15 mai 2021 : rejet progressif de toutes les transactions non conformes (étalé sur 4 semaines).

16 La vidéo est accessible sur la plateforme YouTube via la chaîne de la Banque de France : *www.youtube.com/*

Volet consommateur : taux d'équipement des porteurs effectuant des achats sur internet

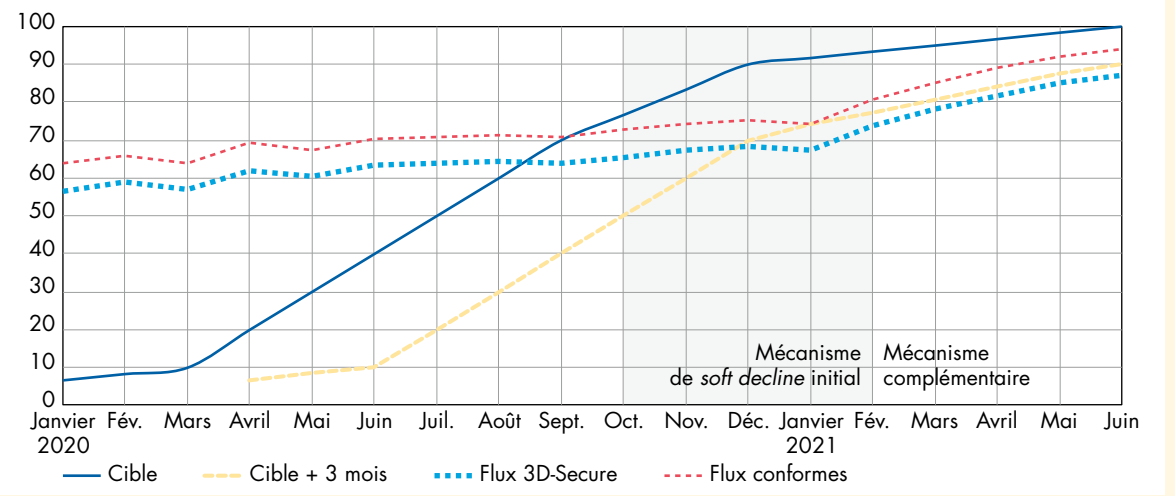
(en % de porteurs actifs enrôlés)



Source : Banque de France (2021), *Observatoire de la sécurité des moyens de paiement. Rapport annuel 2020.*

Volet commerçants : part des flux 3D Secure en valeur

(en %)



Source : Banque de France (2021), *Observatoire de la sécurité des moyens de paiement. Rapport annuel 2020.*

à la DSP 2 transitaient par les protocoles 3D-Secure, ce qui assure leur conformité ; en complément, les flux non 3D-Secure de moins de 30 euros, qui bénéficient d'une exemption a priori, représentaient 7 % des flux. Le taux de conformité à fin juin atteignait ainsi 92 % des flux visés par le périmètre de la DSP 2 en valeur.

3.2.5. La mise en place des interfaces d'accès aux comptes

Dans le cadre de la mise en œuvre de la DSP 2 et du règlement délégué (UE) 2018/389 de la Commission européenne (ou RTS « Authentification forte et normes de communication ») précisant les mesures de sécurité associées, les prestataires de services de paiement gestionnaires de comptes qui offrent un service de consultation des comptes en ligne doivent permettre l'accès aux comptes de paiement de leurs clients par les acteurs tiers agréés (initiateurs de paiement et agrégateur d'informations) à compter du 14 septembre 2019. Trois modalités distinctes sont possibles pour répondre à cette exigence :

- La fourniture d'un accès via le site de banque en ligne avec authentification de l'acteur tiers (donc sans interface dédiée) ;
- La mise à disposition d'une interface dédiée dotée d'un mécanisme de secours en cas d'indisponibilité de l'interface dédiée (via l'accès banque en ligne avec authentification du tiers) ;
- La mise à disposition d'une interface sans mécanisme de secours. Dans ce cas de figure, l'ACPR doit s'être prononcée favorablement sur l'octroi d'une exemption avant le 14 septembre 2019 sous peine de non-conformité.

En complément des RTS, les exigences applicables aux interfaces o>nt fait l'objet de clarifications complémentaires apportées par l'ABE au travers de deux avis :

- L'avis du 3 juin 2018 (EBA-OP-2018-04) sur l'implémentation des RTS, qui apporte des clarifications sur les conditions de mise en place des interfaces sans toutefois apporter une réponse à l'ensemble des questions d'interprétation alors en suspens ;
- L'avis du 4 juin 2020 (EBA-OP-2020-10) sur les obstacles à la fourniture des services tiers, qui identifie les pratiques des établissements gestionnaires de comptes susceptibles de constituer

Encadré nº 6 : La définition d'un standard d'interface pour la Place française

Afin de soutenir l'action de standardisation d'un modèle d'interface communautaire de type API (*application programming interface*) au niveau national tout en veillant au respect des dispositions sécuritaires prévues par les normes techniques de réglementation (*regulatory technical standard*, RTS), la Banque de France et l'ACPR ont proposé de créer au niveau du Comité national des paiements scripturaux (CNPS) un groupe de travail afin de définir les fonctionnalités et requis d'une telle API. Ce groupe de travail, mis en place en avril 2018 et co-animé par la Banque de France et l'ACPR, regroupe l'ensemble des acteurs du marché (PSP tiers, banques, commerçants) ainsi que la société STET, qui a piloté pour le compte de la communauté bancaire française le développement d'un standard d'API répondant aux exigences de la DSP 2.

Le rôle de ce groupe a été d'identifier et de résoudre les points bloquants à la mise en conformité DSP 2 de l'API communautaire, en recherchant des solutions consensuelles entre les PSP tiers d'un côté et les teneurs de compte de l'autre sur les points d'interprétation des textes. Ainsi, dès le 27 juillet 2018, le groupe a validé un document de conclusions qui a servi de base à la version de l'API cible pour l'entrée en application des RTS, soit le 14 septembre 2018.

Les réunions de ce groupe de travail se sont poursuivies à un rythme mensuel jusqu'à la fin de l'année 2020, afin de suivre le déploiement progressif des interfaces par les établissements teneurs de comptes et leur montée en charge par le raccordement des acteurs tiers. Ces réunions ont également permis de relayer et d'expliquer les clarifications apportées au niveau européen.

une entrave à la capacité des acteurs tiers à délivrer leurs services, et qui doivent donc faire l'objet d'une attention particulière de la part des autorités nationales compétentes.

3.3. Le cadre européen de surveillance et ses évolutions

La construction de l'Espace unique des paiements en euros (*Single Euro Payments Area* », SEPA : cf. chapitre 2) confère aux banques centrales nationales une coresponsabilité en matière de sécurité des moyens de paiement d'intérêt commun. L'Eurosystème a ainsi développé, sur la base des dispositions du Traité [17] et des statuts du Système européen de banques centrales (SEBC) et de la BCE [18] sur la promotion du bon fonctionnement des systèmes de paiement, des cadres de surveillance applicables aux moyens de paiement paneuropéens :

- En janvier 2008 [19], un premier cadre de surveillance a été élaboré par l'Eurosystème afin d'évaluer la sécurité et l'efficacité des systèmes de paiement par carte. Il a permis aux banques centrales de l'Eurosystème de mettre en œuvre une surveillance harmonisée et d'obtenir une vision cohérente et standardisée des systèmes de paiement par carte ;

- Les cadres de surveillance relatifs aux prélèvements [20] et virements [21] SEPA ont été établis respectivement en août 2009 et en octobre 2010. Ils s'appuient sur une structure similaire à celle définie pour les systèmes de paiement par carte.

Des guides d'évaluation correspondant à chacun de ces trois cadres de surveillance ont également été publiés afin de préciser les attentes de l'Eurosystème en la matière. Ils ont été mis à jour en 2014 et 2015 en incorporant notamment les recommandations sur la sécurité des paiements sur internet publiées par le Forum européen de la sécurité des moyens de paiement (Forum on the Security of Retail Payments ou forum SecuRe Pay, cf. *infra*), qui ont été reprises dans les orientations émises par l'ABE en décembre 2014.

17 Article 127.2 du TFUE : « Les missions fondamentales relevant du SEBC consistent à : définir et mettre en œuvre la politique monétaire de l'Union ; conduire les opérations de change conformément à l'article 219 ; détenir et gérer les réserves officielles de change des États membres ; promouvoir le bon fonctionnement des systèmes de paiement ».

18 Articles 3.1 et 22 des statuts du SEBC et de la BCE.

19 BCE (2008) *Oversight framework for card payment schemes – Standards*, janvier.

20 BCE (2009) *Oversight framework for direct debit schemes*, août.

21 BCE (2010) *Oversight framework for credit transfer schemes*, octobre.

En s'appuyant sur ces cadres de surveillance, l'Eurosystème mène des exercices de surveillance auprès des acteurs de marché. Les cartes de paiement sont le premier instrument scriptural à avoir bénéficié de cette surveillance commune des banques centrales, avec le lancement dès 2008 de l'évaluation de l'ensemble des systèmes de paiement par carte actifs en Europe, qu'ils soient d'envergure nationale ou internationale ; cet exercice a été reconduit en 2016, suite à la publication des orientations de l'ABE relatives à la sécurité des paiements sur internet, lesquelles ont alors été intégrées au référentiel de sécurité. Plus récemment, l'Eurosystème a finalisé en 2016 un exercice de surveillance portant sur le prélèvement SEPA, et démarré une action de surveillance similaire portant sur les virements SEPA.

Partie intégrante de cette surveillance, une collecte annuelle de statistiques en matière de fraude sur les paiements par carte est organisée au niveau européen par la BCE et les banques centrales nationales auprès de l'ensemble des systèmes de paiement par carte actifs. Elle devrait être complétée dans les années à venir par une collecte de statistiques en matière de fraude sur les virements et les prélèvements.

Encadré n° 7 : Le cadre de surveillance PISA

Le cadre de surveillance PISA a pour ambition d'harmoniser les pratiques en matière de surveillance dans le domaine des paiements, en fusionnant les différents textes existants [1]. Son objectif est double : il s'agit non seulement de définir une approche unifiée pour la surveillance de l'ensemble des parties prenantes en appliquant les mêmes principes et les mêmes procédures à tous, mais également d'inclure un certain nombre de nouveaux acteurs dans le périmètre, à l'instar des solutions digitales ou des portefeuilles électroniques. En effet, la montée en puissance des paiements par téléphone mobile et du e-commerce favorise l'émergence de nouveaux modes d'initiation s'appuyant sur une diversité d'instruments de paiement sous-jacents. Alors que certains de ces nouveaux acteurs enregistrent une forte croissance et pourraient jouer un rôle majeur dans les années à venir, nombre d'entre eux échappent aux cadres de surveillance actuels – c'est par exemple le cas des solutions de paiement telles qu'Apple Pay ou Paylib, à ce jour simplement considérées comme des prestations techniques externalisées par les banques.

Le cadre de surveillance PISA s'appliquera uniquement aux acteurs de taille critique : le périmètre sera défini en s'appuyant sur quatre critères objectifs, reflétant leurs poids respectifs sur le marché européen. Les principaux systèmes de paiement par carte (tels que Visa, Mastercard, American Express, Groupement des Cartes Bancaires CB – GIE CB) et les solutions de paiement les plus répandues (telles que Apple Pay, Google Pay, Paylib, Paypal) devraient y être assujettis. La version finale du cadre de surveillance PISA sera publiée courant 2021.

1 *Harmonised oversight approach and oversight standards for payment instruments* (BCE, février 2009), *Electronic money system security objectives* (BCE, mai 2003), *Oversight framework for card payment schemes – Standards* (BCE, janvier 2008), *Oversight framework for direct debit schemes* (BCE, août 2009), *Oversight framework for credit transfer schemes* (BCE, octobre 2010).

3.4. Les travaux du forum SecuRe Pay

Créé en février 2011, le forum SecuRe Pay est une structure réunissant banquiers centraux et superviseurs. Coprésidée par la BCE et l'ABE, cette instance a pour vocation d'instaurer un dialogue entre les autorités nationales, en vue de parvenir à une approche commune en matière de sécurité des moyens de paiement.

La première série de recommandations publiée par le forum SecuRe Pay en janvier 2013 a porté sur la sécurité des paiements sur internet. Bien que la principale mesure préconisée dans ce premier

document concerne la généralisation de l'authentification renforcée du payeur lors de l'initiation de paiements sur internet, le forum y aborde de nombreux autres aspects susceptibles de renforcer la sécurité des paiements sur internet, dont l'environnement général de contrôle et de sécurité mis en œuvre par les prestataires de services de paiement et la question de la sensibilisation des clients aux risques de fraude, ou encore les modalités de communication entre ces derniers et leurs prestataires de services de paiement.

Enfin, le forum avait également porté son attention sur les risques liés à l'activité de nouveaux acteurs non régulés se positionnant en tant que « tiers de paiement » afin d'offrir des services d'initiation des transactions et d'agrégation d'information de comptes. Les recommandations du forum visant à assurer des conditions de sécurité satisfaisantes pour la mise en place de ces services ont été publiées, à l'issue d'une consultation publique, en mars 2014 [22].

Nombre des recommandations du forum SecuRe Pay ont été reprises lors de la révision de la directive sur les services de paiement (DSP 2). C'est dans le cadre du forum SecuRe Pay que les RTS et *guidelines* confiées à l'ABE pour décliner les exigences de la DSP 2 ont été élaborées.

Afin d'assurer une application uniforme au sein de l'Union européenne, dans la DSP 2, l'ABE a été chargée, en étroite coopération avec la BCE, d'élaborer, outre les normes techniques de réglementation (RTS) évoquées précédemment, des orientations (*guidelines*) couvrant notamment les exigences en matière de gestion des risques opérationnels et sécuritaires en lien avec la mise à disposition de services de paiement, ainsi que la description du cadre de déclaration des incidents majeurs aux autorités compétentes.

22 Recommandations disponibles en anglais sur le site de la BCE : *http://www.ecb.europa.eu/pub/*