CHAPITRE 3

La sécurité des moyens de paiement

Mis à jour le 14 décembre 2018

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 termes 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 : le détournement des fonds en cours de paiement, susceptible d'entraîner une fraude immédiate, et 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 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 et prestataires de services d'information sur les comptes de droit français ;
- établissements de crédit, établissements de monnaie électronique et établissements de paiement de et prestataires de services d'information sur les comptes 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 grandes typologies 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 de paiement authentique dont les caractéristiques physiques ou les

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 & PIN* ».

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

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.

T1 : Les quatre grandes typologies 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 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 l'IBAN d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien
Utilisation/ contestation abusive	• Contestation abusive par le porteur 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 d'un ordre de prélèvement émis légitimement par le créancier (litige commercial)

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

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

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 pas.

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

Les données recueillies par la Banque de France et l'OSMP pour l'année 2017 font état d'un montant global de fraude aux moyens de paiement scripturaux émis en France d'environ 744 millions d'euros pour un peu plus de 27 500 milliards d'euros de flux de paiement. La répartition par moyen de paiement présente le profil suivant :

- Compte tenu de son usage important (près de la moitié des transactions scripturales), la carte de paiement concentre à elle seule près de la moitié de la fraude aux moyens de paiement scripturaux (soit 360 millions d'euros en 2017) avec un taux de fraude de 0,054 %, représentant l'équivalent d'1 euro de fraude pour 1 850 euros de transactions. Cette fraude présente deux caractéristiques principales : d'une part, elle est concentrée sur les paiements à distance, essentiellement sur internet, qui supportent les deux tiers du montant de la fraude alors qu'ils ne représentent que 12 % des transactions ; d'autre part, elle affecte plus fortement les transactions transfrontalières que les transactions nationales, les premières supportant près de 60 % du montant de la fraude alors que leur poids n'est que de 13 % des transactions réalisées.

- Le chèque est le deuxième moyen de paiement le plus touché par la fraude puisqu'il représente un tiers du montant global de la fraude (soit un taux de fraude de 0,029 %, représentant 1 euro de fraude pour 3 500 euros de paiements).

.../...

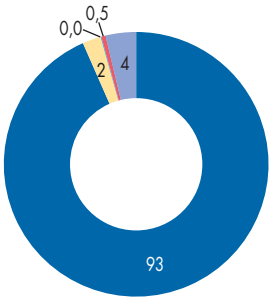
- Le virement supporte un montant de fraude plus faible, de l'ordre de 78 millions d'euros, et est proportionnellement beaucoup moins touché que la carte ou le chèque avec un taux de fraude près de cent fois inférieur à ces derniers.

- Enfin, la fraude sur les prélèvements et les effets de commerce est limitée puisqu'elle représente des montants plus faibles, de l'ordre respectivement de 9 millions d'euros et 0,15 million d'euros en 2017.

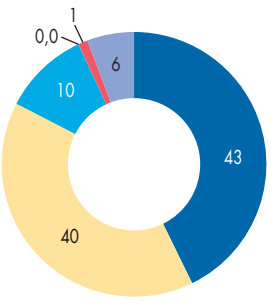
G1 : Répartition de la fraude sur les moyens de paiement scripturaux en 2017

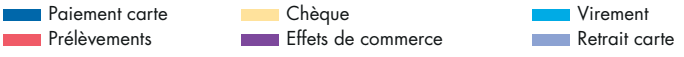
(en %)

a) en volume



b) en montant

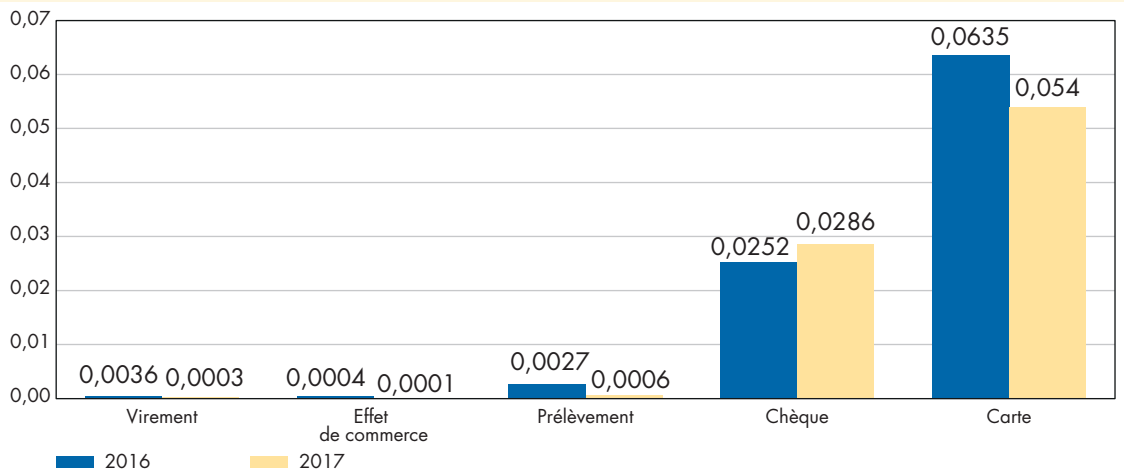




Source : Observatoire de la Sécurité des Moyens de Paiement.

G2 : Évolution du taux de fraude par moyen de paiement, 2016–2017

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

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 électroniques, 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 de « *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 (« *vishing* »), 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 cartes 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.

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.

3 Pour de plus amples développements sur ce thème, se reporter à la partie 5 du rapport 2010 de l'Observatoire de la Sécurité des Cartes de paiement, *https://www.banque-france.fr/sites*

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.

Instituée par la loi n° 2016-1691 du 9 décembre 2016, dite « Loi Sapin 2 », l'OSMP a succédé à l'Observatoire sur 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 n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au Journal officiel.

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

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.

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 indispensable, notamment pour lutter contre les attaques frauduleuses. Une communication efficace, utilisant l'ensemble des canaux disponibles (courriers, courriels, sites Internet, etc.), est donc souhaitable de la part de l'ensemble des acteurs de la chaîne de paiement doit donc 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

1 Network and Information Security (NIS) Directive, *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148.*

.../...

de la personne initiant la transaction (nom, prénom, adresse postale, adresse de livraison, email, 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 termes 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 de protection des données (RGPD) de l'Union européenne entré en application en mai 2018.

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'intention 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 3 à 4 ans [4].

4 *https://www.banque-france.fr/liste-chronologique*

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 autre, 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 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

Encadré n° 5 : Le GIE Cartes Bancaires 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, le GIE Cartes Bancaires [1], 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 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 ;

1 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 et 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 Restaurant Dématérialisés).

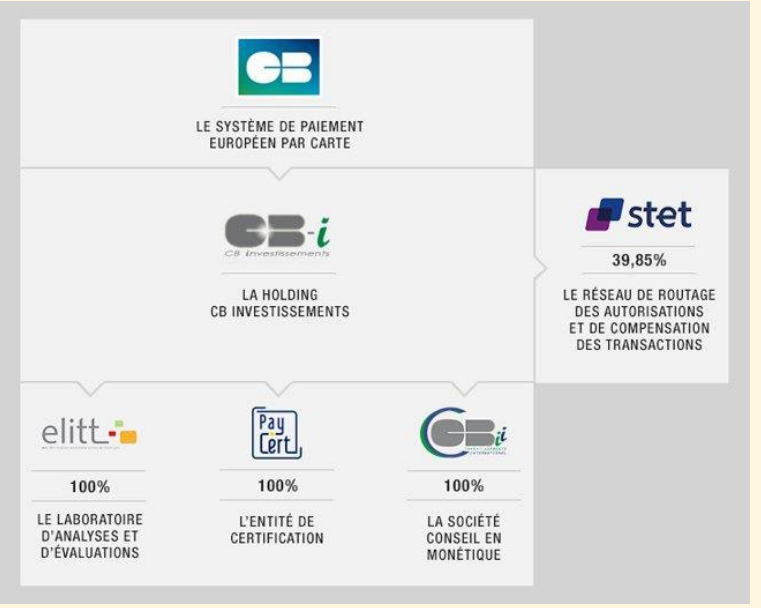
.../...

- 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 Visa, MasterCard ou encore American Express, ont développé des outils similaires qui bénéficient à leurs membres.

Organisation du GIE CB et de ses filiales



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 service 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.

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

Le Comité des paiements et des infrastructures de marché (CPMI) de la Banque des règlements internationaux, qui a succédé en 2014 au Comité des systèmes de paiements et règlements (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 [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

5 *http://www.bis.org/publ/cpss102.htm*

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 ont ainsi contribué à éclairer les choix règlementaires adoptés au niveau européen, ainsi que les travaux conduits en France par l'Observatoire de la Sécurité des Moyens de Paiement Scripturaux.

3. Le cadre européen de sécurité des moyens de paiement

3.1. Le cadre juridique européen applicable aux moyens de paiement

La convergence des règlementations applicables aux moyens et services de paiement 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.

La première directive sur les services de paiement (DSP1)

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.

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 dans le temps 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'opération 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

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*

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.

Encadré n° 6 : Les services de paiement dans la DSP1

La notion de service de paiement ne fait pas l'objet d'une définition en tant que telle dans la DSP1. Celle-ci fixe toutefois une liste limitative des catégories d'activités qui sont considérées comme des services de paiement. Ces catégories, au nombre de 7, sont les suivantes :

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 de l'utilisateur ou auprès d'un autre prestataire de services de paiement :
- l'exécution de prélèvements, y compris de prélèvements autorisés unitairement ;
- l'exécution d'opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire ;
- l'exécution de virements, y compris d'ordres permanents.

4. L'exécution d'opérations de paiement couvertes par une ligne de crédit au bénéfice de l'utilisateur du service de paiement, cela concerne :
- les prélèvements, y compris de prélèvements autorisés unitairement ;
- les opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire ;
- les virements unitaires ou dans le cadre d'un ordre permanent.

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

6. Les transmissions de fonds.

7. L'exécution d'opérations de paiement lorsque le consentement du payeur à une opération de paiement est donné au moyen de tout dispositif de télécommunication, numérique ou informatique et que le paiement est adressé à l'opérateur du système ou du réseau de télécommunication ou informatique, agissant uniquement en qualité d'intermédiaire entre l'utilisateur de services de paiement et le fournisseur de biens ou services.

Sont ainsi exclus du champ d'application de la directive un certain nombre d'instruments de paiement sous forme papier, dont les plus importants sont le chèque, le mandat postal et les lettres de change, ceux-ci étant déjà spécifiquement régis par des conventions internationales.

La liste des services de paiement a toutefois connu une modification à l'occasion de la révision de la directive, dont la deuxième version (DSP2) intègre notamment les services fournis par les tiers de paiement (cf. *infra*).

La contestation des opérations non autorisées : la directive prévoit deux dispositifs, selon que le paiement contesté a été autorisé par le payeur ou non.

Le premier dispositif concerne 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 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.

La directive prévoit toutefois 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 pourra dans ce cas supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé ou, « si le payeur n'est 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 pourra pas 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'hôtel 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.

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 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.

La deuxième directive sur les services de paiement (DSP2)

La deuxième directive européenne sur les services de paiement (dite « DSP2 »), adoptée le 25 novembre 2015 [7], s'inscrit dans le prolongement de la DSP1, en étendant le champ des services de paiement régulés à de nouveaux services et acteurs, tout en renforçant les exigences sécuritaires applicables aux acteurs du marché des paiements Elle est entrée en vigueur en France, comme dans la plupart des États membres, le 13 janvier 2018.

La DSP2 crée un statut de prestataire de services de paiement (PSP) pour les acteurs tiers qui accèdent aux comptes tenus par des PSP dits « gestionnaires de comptes » (principalement les banques) pour initier des paiements ou pour agréger les informations de comptes :

- l'initiateur de paiement est un intermédiaire qui a la capacité d'initier des paiements, le plus souvent des virements, depuis le compte de banque en ligne du client, et propose ces offres de paiement aux commerçants en ligne et à leurs clients comme une alternative possible au paiement par carte ou par portefeuille électronique ;

- le prestataire de services d'information propose un service de consolidation des informations des différents comptes de paiement qu'un client peut détenir auprès d'un ou plusieurs prestataires de services de paiement.

Ces activités, exercées jusqu'alors en dehors de tout cadre réglementaire, présentaient un risque élevé en matière de fraude car elles nécessitaient la communication par les utilisateurs à un tiers des identifiants et codes d'accès des comptes de banque en ligne.

La directive défend également un objectif d'amélioration de la sécurité des paiements, articulé autour des deux axes suivants :

- l'authentification forte du titulaire du compte est requise pour l'accès aux comptes et pour toute action en ligne qui présente des risques importants (par exemple, création d'un nouveau bénéficiaire pour les virements sur un espace de banque en ligne) ;

- l'authentification forte du payeur est requise pour l'initiation de paiements par voie électronique.

7 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, *https://eur-lex.europa.eu/legal- content/FR/TXT/ ?uri=CELEX%3A32015L2366*

Cette obligation de recours à l'authentification forte peut toutefois faire l'objet d'exemptions définies règlementairement dans le cas où les transactions sont considérées comme peu risquées (par exemple, paiement de faible montant ou virement entre plusieurs comptes d'une même personne).

Encadré n° 7 : L'authentification forte du payeur

La question de la sécurisation des paiements sur internet a été soulevée dès 2008, dans l'enceinte de l'Observatoire de la Sécurité des Cartes de Paiement (OSCP) sous l'impulsion de la Banque de France. Les recommandations émises par l'Observatoire dans son rapport annuel 2009 définissaient le concept d'authentification forte du payeur, et invitaient les acteurs du marché français des cartes de paiement à développer et mettre en œuvre des solutions d'authentification répondant à cette définition.

L'exemple français a inspiré les travaux conduits au niveau européen, tout d'abord dans le cadre du forum européen *SecuRe Pay* (cf. *infra*), puis de la Commission européenne en préparation de la DSP2. La nouvelle directive définit ainsi l'authentification forte comme un ensemble de procédures fondées sur l'utilisation d'au moins deux éléments parmi les trois suivants :

1. élément connu du seul payeur (facteur de connaissance) :
Il s'agit d'un élément que le payeur est le seul à connaitre, comme un mot de passe, un code d'identification personnel (« code PIN »), etc. ;

2. élément en la possession du seul payeur (facteur de possession) :
Il s'agit d'un élément dont le payeur est le seul détenteur, comme un « *token* », un téléphone mobile, une carte à micro-processeur (« carte à puce »), etc. ;

3. Élément lié à la personne elle-même (facteur d'inhérence) :
Il s'agit d'une caractéristique biométrique du payeur telle que l'empreinte digitale ou la voix par exemple.

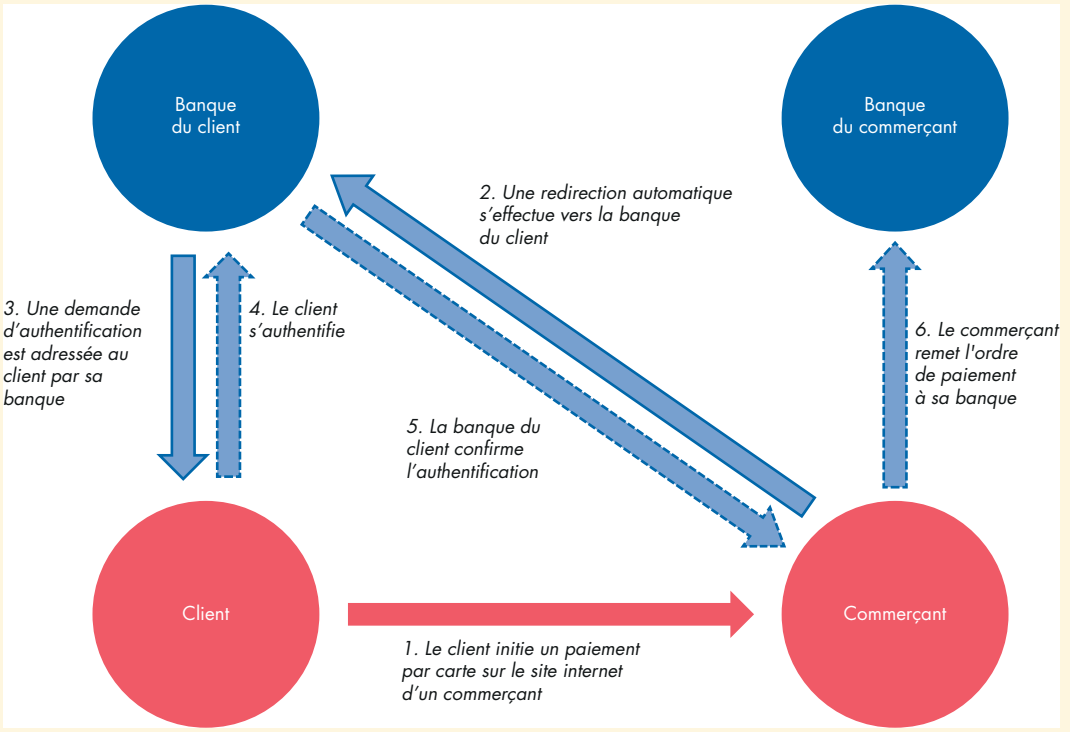
Les éléments retenus doivent être mutuellement indépendants, au sens où la compromission de l'un ne doit pas mettre en danger la sécurité des autres. En outre, l'un des éléments choisis au moins doit être non rejouable et non reproductible, c'est-à-dire ne pas être réutilisable à l'identique pour deux opérations de paiements différents, excepté pour ce qui concerne le recours à la biométrie. Enfin, la procédure d'authentification forte doit assurer la protection de la confidentialité des données d'authentification.

Le dispositif d'authentification forte le plus répandu actuellement pour les paiements sur internet repose sur un code à usage unique tel un OTP (« *OneTime Password* ») communiqué au payeur selon divers canaux possibles (envoi d'un SMS sur son téléphone portable, génération sur le site de banque en ligne du payeur, par un lecteur de carte physique, un dispositif autonome de génération de code (ou *token*) intégré à un porte-clefs, etc.) [1]. Lors du paiement, la page de paiement en ligne met en relation le payeur avec la banque qui a émis la carte pour qu'elle puisse l'authentifier, en s'appuyant sur le protocole « 3D-Secure » dont le fonctionnement est synthétisé dans le schéma ci-après.

1 Le rapport annuel 2015 de l'Observatoire de la sécurité des cartes de paiement présente un état des lieux des techniques d'authentification renforcée les plus couramment utilisées en France : *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2015.pdf*

.../...

Fonctionnement du protocole « 3D-Secure »



Dans ce nouveau cadre, le texte prévoit que les identifiants bancaires puissent être partagés avec les PSP tiers, tout en assurant leur protection, notamment par chiffrement des données. Il est également prévu que les PSP tiers et les PSP gestionnaires de comptes, ainsi que les utilisateurs communiquent de façon sécurisée en utilisant une interface dont les principes sont spécifiés par un texte règlementaire dit de niveau 2 associé à la directive, les normes techniques de règlementation (*Regulatory Technical Standards* – RTS).

L'Autorité bancaire européenne (ABE) a ainsi reçu pour mandat d'élaborer, en étroite collaboration avec la Banque centrale européenne (BCE), des normes techniques de réglementation qui précisent : i) les requis et les exemptions de l'authentification forte des clients pour la sécurisation des transactions et des accès aux comptes ; ii) les requis en matière de protection des identifiants de connexion ; et iii) les modalités techniques et opérationnelles permettant aux banques, aux PSP tiers et à leurs clients de communiquer de façon sécurisée. Pour permettre aux acteurs d'adapter leurs systèmes informatiques et aux autorités compétentes de préparer la mise en place des dispositifs de contrôles associés, la directive dispose que les exigences fixées par ces normes techniques de règlementation seront applicables 18 mois après leur adoption et leur publication, soit à compter du 14 septembre 2019.

Encadré n° 8 : Les dispositions des RTS

À la suite de travaux conduits sous l'égide du Forum européen sur la sécurité des paiements (SecuRe Pay, voir *infra*) marqués par un souhait d'interaction forte avec le marché (publication d'un *discussion paper*, puis d'une consultation publique), les normes techniques de réglementation (RTS) de la DSP2 ont été adoptées par la Commission Européenne le 27 novembre 2017, le Parlement européen et le Conseil disposant alors de 3 mois pour les examiner. À l'issue de cette période d'examen, le règlement délégué (UR) 2018/389 relatif aux RTS a été publié au Journal Officiel de l'Union européenne du 13 mars 2018 [1], date qui constitue le point de départ du délai de 18 mois pour leur entrée en application, soit le 14 septembre 2019.

En matière d'authentification forte, les RTS retiennent plusieurs cas d'exemption :

- la consultation de comptes (après une première authentification forte) ;
- les paiements de faible montant (jusqu'à 50 euros en proximité et 30 euros à distance) ;
- les paiements aux automates de transport et de parking ;
- les paiements vers un bénéficiaire de confiance ;
- les transactions récurrentes (sauf pour l'initiation de la première transaction) ;
- les paiements d'entreprises recourant à des protocoles de transfert d'ordres sécurisés ;
- et les transactions pour lesquelles le niveau de risque est jugé faible par l'établissement teneur de compte du débiteur.

Dans ce dernier cas de figure, le PSP devra veiller à ce que les taux de fraude observés sur les transactions bénéficiant de l'exemption restent inférieurs à des seuils inscrits dans les RTS, en fonction du moyen de paiement utilisé et de la tranche de montants :

T2 : Taux de fraude maximal

(en %)

	Sur les paiements par carte à distance	Sur les virements initiés à distance
De 250 à 500 euros	0,01	0,005
De 100 à 250 euros	0,06	0,010
De 0 euros à 100 euros	0,13	0,015

Ainsi, au-delà de 500 euros, les transactions ne pourront pas bénéficier de cette exemption. Par ailleurs, en cas de dépassement des seuils fixés durant deux trimestres consécutifs, le PSP ne sera plus autorisé à bénéficier de cette exemption tant que les taux de fraude mesurés ne seront pas revenus en-deçà des seuils.

En ce qui concerne la **sécurisation des interfaces d'échange entre PSP teneurs de comptes et PSP tiers**, les RTS entérinent l'obligation de mise en place et d'utilisation d'une interface dédiée permettant i) l'identification du PSP tiers par le PSP teneur de comptes au moyen de certificats qualifiés au sens du règlement européen eIDAS, ii) de s'appuyer sur le mécanisme d'authentification de l'utilisateur proposé par l'établissement teneur de compte, et iii) l'initiation d'ordre de paiement et la réception d'informations relatives à l'exécution des opération de paiement initiées.

Les RTS prévoient une période de test de l'interface de 6 mois avant la date d'application des RTS. Les PSP gestionnaires de comptes ont le choix de développer une interface dédiée ou de permettre un accès *via* l'interface utilisateur avec une identification du PSP tiers.

1 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 : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ :L :2018 :069 :TOC

.../...

Dans le cas où un PSP gestionnaire de comptes choisit de fournir une interface dédiée, les RTS prévoient un certain nombre de dispositions :

- L'interface dédiée doit présenter un niveau de performance équivalent à l'interface utilisateur. Des indicateurs de performances doivent être développés à cet effet par les PSP gestionnaires de comptes. Les autorités nationales compétentes veillent alors à ce que les PSP tiers respectent à tout moment l'obligation d'accès *via* ces interfaces ;

- En cas d'indisponibilité de l'interface dédiée (dégradation de performance), les PSP gestionnaires de comptes doivent permettre aux PSP tiers d'utiliser l'interface utilisateur (selon donc des méthodes de *web scrapping* ou *screen scraping*), avec un mécanisme d'identification du PSP tiers. Ceci doit être possible dès lors qu'une demande d'accès est refusée 5 fois de suite dans un délai de 30 secondes. En cas d'utilisation de cette interface de repli, les PSP tiers doivent pouvoir le justifier auprès de leur autorité nationale compétente et conserver la liste des accès afin de les communiquer sur demande à leur autorité nationale compétente ;

- Toutefois, les autorités nationales compétentes peuvent exempter les PSP gestionnaires de comptes d'interface de repli, après consultation de l'ABE, si l'interface dédiée répond aux exigences du RTS, en particulier si elle a été testée pendant la période de 6 mois spécifiée et si elle a été utilisée pendant 3 mois. Cette exemption doit être retirée par l'autorité nationale compétente si l'interface ne respecte plus les exigences du RTS et si le PSP gestionnaire de comptes n'est plus capable de résoudre les dysfonctionnements pendant une période de 2 semaines. Dans ce cas, le PSP gestionnaire de comptes doit fournir une interface de repli sous un délai de 2 mois.

3.2. Le cadre européen de surveillance et ses évolutions

La construction de l'Espace unique des paiements en euros (« *Single Euro Payments Area* » ; 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 [8] et des statuts du Système européen de banques centrales et de la BCE [9] sur la promotion du bon fonctionnement des systèmes de paiement, des cadres de surveillance applicables aux moyens de paiement paneuropéens :

- En janvier 2008 [10], 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 [11] et virements [12] 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'évaluations 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* », forum *SecuRe Pay*, cf. *infra*) qui ont été reprises dans les orientations émises par l'Autorité bancaire européenne (ABE) en décembre 2014.

8 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 ».

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

10 *Oversight framework for card payment scheme standards*, January 2008, http://www.ecb.europa.eu/pub

11 *Oversight framework for direct debit schemes*, August 2009, http://www.ecb.europa.eu/pub

12 *Oversight framework for credit transfer schemes*, October 2010, http://www.ecb.europa.eu/pub

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'Autorité bancaire européenne 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.

3.3. 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 [13].

Nombre des recommandations du forum *SecuRe Pay* ont été reprises lors de la révision de la directive sur les services de paiement (DSP2). C'est dans le cadre du forum *SecuRePay*, que les RTS et *guidelines* confiés à l'ABE pour décliner les exigences de la DSP2 ont été élaborés.

Afin d'assurer une application uniforme au sein de l'Union européenne, dans la DSP2, 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.

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