Rapport annuel
de l'Observatoire de la sécurité des moyens de paiement

2017

BANQUE DE FRANCE
EUROSYSTÈME

bservatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

Rapport annuel 2017
de l'Observatoire de la sécurité des moyens de paiement

adressé à

Monsieur le ministre de l'Économie et des Finances
Monsieur le président du Sénat
Monsieur le président de l'Assemblée nationale

par

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

L'Observatoire de la sécurité des moyens de paiement, mentionné au I de l'article L. 141-4 du Code monétaire et financier, a été créé par la loi n° 2016-1691 du 9 décembre 2016. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, entreprises, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des moyens de paiement scripturaux.

Conformément à l'alinéa 7 de cet article, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'Économie et des Finances et transmis au Parlement.

Synthèse

Ce deuxième rapport annuel de l'Observatoire de la sécurité des moyens de paiement rend compte de progrès significatifs en matière de lutte contre la fraude.

Ces progrès s'illustrent d'abord par une baisse significative à 744 millions d'euros en 2017 du montant annuel de la fraude sur les moyens de paiement émis en France, soit 54 millions d'euros de moins qu'en 2016. Cette évolution est détaillée dans le ***chapitre 2****. Tous les moyens de paiement modernes, électroniques ou dématérialisés (reposant sur la carte, le virement ou le prélèvement), bénéficient de cette tendance baissière de la fraude, dans un contexte de croissance des flux de paiements.*

• Si la carte conforte sa position de moyen de paiement scriptural le plus utilisé, sa fraude (361 millions d'euros, soit 48 % de la fraude aux paiements scripturaux) connaît un repli significatif, notamment pour les paiements à distance auprès de commerçants français. En effet, le taux de fraude sur ces paiements s'établit en net retrait pour la sixième année consécutive, et atteint ainsi un plus bas historique à 0,161 %. Ce taux de fraude reste néanmoins supérieur à celui des transactions au point de vente (0,008 %), du paiement sans contact (0,020 %) ou des retraits aux distributeurs (0,027 %), tous trois quasiment stables. La baisse du taux de fraude sur les paiements à distance, associée à la croissance des flux de paiement, explique la quasi-totalité de la baisse de la fraude sur les paiements par carte au niveau national, qui diminue de 18 millions d'euros pour atteindre un total de 200 millions d'euros. Cette baisse permet ainsi de ramener le taux de fraude à 0,033 %, son plus bas niveau depuis 2010.

• Les transactions internationales par carte affichent également des progrès significatifs en matière de réduction de la fraude : pour la première fois depuis 2011, la fraude sur les paiements internationaux par carte s'affiche en baisse, et ce tant pour les transactions intraeuropéennes que pour les transactions avec le reste du monde. Pour les porteurs français, le montant de fraude subi sur les transactions transfrontalières s'est ainsi réduit de 21 millions d'euros en un an, pour se situer à 161 millions d'euros, soit un taux de fraude ramené à 0,281 %, son plus bas niveau historique.

• Le prélèvement connaît également une baisse spectaculaire de la fraude, ramenée de 40 millions d'euros à 9 millions d'euros en un an. Un mouvement analogue, quoique de

moindre ampleur, est également observé sur le virement, dont la fraude se réduit de 86 millions d'euros à 78 millions d'euros entre 2016 et 2017. Ces moyens de paiement présentent ainsi des taux de fraude extrêmement bas, à respectivement 0,0006 % et 0,0003 %.

À l'inverse des moyens de paiement modernes, le chèque fait face à une croissance de la fraude de près de 25 millions d'euros, à 296 millions d'euros en 2017, contre 272 millions d'euros un an plus tôt. Cette évolution, associée à une réduction de l'usage du chèque de 7 % en montant entre 2016 et 2017, entraîne une progression du taux de fraude sur le chèque à 0,029 %, contre 0,025 % en 2016. Si le chèque reste le deuxième moyen de paiement le plus touché par la fraude, sa part dans le montant global de fraude aux paiements scripturaux augmente à 40 % en 2017 (contre 34 % en 2016) et se rapproche de celle de la carte (48 % en 2017), pour une utilisation pourtant beaucoup moins intensive : seulement 8 % du nombre des transactions scripturales se font par chèque, contre 58 % par carte.

Ce constat vient conforter les axes de la stratégie nationale des paiements scripturaux, en faveur du développement de moyens de paiement innovants et de la promotion de solutions sécurisées de paiement qui puissent être des alternatives au chèque, telles la carte ou le virement, et bientôt le virement instantané.

Les progrès significatifs observés sur les moyens de paiement électroniques ou dématérialisés résultent en grande partie des progrès en matière de prévention de la fraude quand, a contrario, *le chèque offre des vulnérabilités liées à la difficulté de mettre en place des dispositifs de prévention de la fraude sur cet instrument. Les principaux vecteurs des progrès constatés sur les moyens de paiement électroniques sont :*

- *le recours croissant à l'authentification du payeur lors des transactions sur internet, notamment* via *le protocole 3D-Secure pour les paiements par carte ;*

- *le développement de dispositifs de* scoring, *c'est-à-dire de systèmes experts capables d'évaluer le niveau de risque d'une transaction donnée sur la base de certaines de ses caractéristiques (telles que les habitudes du client, sa localisation, le matériel utilisé, etc.), tant par les acteurs du secteur des paiements que par les commerçants.*

Ces outils de prévention de la fraude, dont le développement a été promu depuis 2008 par l'Observatoire, font aujourd'hui partie intégrante des exigences prévues par la deuxième directive européenne sur les services de paiement (dite DSP2), entrée en application

en janvier 2018 dans l'ensemble de l'Union européenne. Si la France bénéficie d'ores et déjà d'acquis en la matière, le caractère plus systématique de mise en application de ces dispositifs, ainsi que l'harmonisation des pratiques en Europe, ouvrent des perspectives très positives en matière de réduction supplémentaire de la fraude à la fois au niveau national et au sein de l'Union européenne.

Outre la sécurisation des paiements sur internet, la DSP2 prévoit également la mise en place d'un cadre sécurisé pour la fourniture de services de paiement innovants, tels que l'initiation de paiement ou l'agrégation d'information sur les comptes. Compte tenu du caractère structurant de ces apports de la DSP2 en matière de sécurité des paiements, le ***chapitre 1*** *de ce rapport en propose une lecture accessible et opérationnelle, visant notamment à clarifier les conditions de mise en œuvre d'un certain nombre de dispositions.*

Enfin, de façon complémentaire aux actions conduites par l'Observatoire au cours des années précédentes en matière de veille technologique sur la sécurité des dispositifs techniques, associés aux cartes (terminaux de paiement, paiements sur internet, sans contact, solutions mobiles, etc.), le ***chapitre 3*** *établit cette année une analyse des dispositifs de sécurisation des moyens de paiement SEPA (virement et prélèvement). L'Observatoire note en particulier, outre la nécessité d'assurer la bonne application des exigences prévues par la DSP2 (authentification,* scoring *des transactions), des problématiques spécifiques en matière de sécurisation des données de paiement telles que le numéro de compte (ou IBAN) et de sensibilisation des utilisateurs en la matière. L'Observatoire invite les acteurs de marché à en tenir plus particulièrement compte dans la définition des solutions de paiement reposant sur les instruments SEPA.*

1 Les apports de la DSP2 en matière de sécurité des paiements

1.1 Introduction

La convergence des réglementations applicables au marché des paiements est une composante essentielle à l'intégration du marché des paiements en Europe. Elle vient compléter les initiatives politiques majeures telles que l'introduction de l'euro fiduciaire ou la mise en place des moyens de paiement SEPA [1]. La première directive européenne sur les services de paiement et les deux directives européennes sur la monnaie électronique, adoptées dans les années 2000, visaient à apporter un cadre harmonisé en matière de régulation des opérations de paiement en Europe, tout en renforçant à la fois la protection du consommateur et la concurrence sur ce marché.

La deuxième directive européenne sur les services de paiement (dite « DSP2 »), adoptée le 25 novembre 2015 et entrée en vigueur le 13 janvier 2018, s'inscrit dans le prolongement de ces textes, 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 DSP2, 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 RTS – *regulatory technical standard*) 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

1 *Single euro payments area.*

et opérationnelles permettant aux prestataires de services de paiement (PSP) gestionnaires de comptes, aux PSP tiers (« initiateur de paiement » et « agrégateur d'informations ») et aux titulaires de compte de communiquer de façon sécurisée [2] ;

• des orientations définissant les mesures de sécurité relatives aux risques opérationnels et de sécurité [3] ;

• des orientations relatives aux notifications des incidents majeurs aux autorités nationales et européennes [4] ;

• des orientations relatives aux statistiques de fraude [5].

Enfin, il est à noter que l'entrée en application de cette nouvelle directive au niveau européen est concomitante avec celles, d'une part, du règlement général sur la protection des données à caractère personnel (RGPD) [6], 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*) [7], 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.

1.2 Le cadre général de la DSP2

Opérations couvertes par la DSP2

L'article 2 de la DSP2 définit le champ d'application de la directive. Il couvre la fourniture de services de paiement au sein de l'Union européenne (UE). Son cadre réglementaire s'applique :

• aux opérations de paiement électronique dans une devise d'un État membre lorsque les PSP du bénéficiaire et du payeur sont localisés dans l'Union européenne ;

• aux opérations de paiement électronique dans une devise d'un État non membre lorsque les PSP du bénéficiaire et du payeur sont localisés dans l'Union européenne ;

• de façon partielle, aux opérations de paiement électronique dans toute devise lorsqu'un seul des prestataires de services de paiement (celui du bénéficiaire ou celui du payeur) est localisé dans l'Union européenne, pour la partie de l'opération de paiement qui se situe dans l'Union (par exemple une opération de paiement libellée en dollars effectuée entre deux PSP, dont le premier est situé en France et le second aux États-Unis).

La directive distingue donc les opérations intraeuropéennes,

2 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.

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

4 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).

5 En cours d'élaboration.

6 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).

7 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 européenne.

c'est-à-dire s'appuyant sur des PSP tous localisés dans l'Union européenne, dites *two legs* (premier et deuxième cas), des opérations faisant intervenir un PSP non établi dans l'Union, dites *one leg* (troisième cas). Compte tenu des difficultés à imposer des exigences réglementaires à des acteurs non établis en Europe, les dispositions de la DSP2 concernant les procédures d'authentification forte ne s'appliquent pas aux opérations de paiement *one leg*, et ce quel que soit l'instrument de paiement utilisé.

De nouveaux acteurs et services de paiement

La DSP2 étend le statut de PSP aux acteurs tiers qui accèdent aux comptes tenus par les PSP gestionnaires de comptes (principalement les banques) pour fournir les services d'initiation de paiement ou d'information sur les comptes (« agrégation » d'informations).

• L'initiateur de paiement agit comme un intermédiaire ayant la capacité d'initier des paiements, le plus souvent des virements, depuis l'espace de gestion de compte en ligne du titulaire pour le compte de ce dernier. Il propose sa solution de paiement aux commerçants et aux créanciers comme une alternative possible au paiement par carte ou par portefeuille électronique.

• L'agrégateur d'informations propose un service de consolidation des informations des différents comptes de paiement qu'un titulaire de compte peut détenir auprès d'autres PSP gestionnaires de comptes.

Encadré 1

Services de paiement au sens de la directive

On dénombre huit services de paiement au sens de la deuxième directive européenne sur les services de paiement (DSP2).

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 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.

Ces activités, exercées jusqu'alors en dehors de tout cadre réglementaire relatif aux paiements, présentaient un risque élevé en matière de fraude dans la mesure où elles nécessitaient la communication par les utilisateurs à un tiers des données de sécurité personnalisées permettant d'accéder aux comptes de paiement en ligne. Dans ce nouveau cadre, la directive met en place un dispositif sécurisant la communication de données entre PSP et la confidentialité des données de sécurité personnalisées des utilisateurs. Les requis réglementaires du point de vue technique et sécuritaire sont énoncés dans les normes techniques réglementaires présentées au paragraphe « L'interface sécurisée », dans la section « Les exigences de sécurité inscrites dans les RTS ».

Le cadre d'exercice des nouveaux acteurs

La fourniture de services d'initiation de paiement ou d'information sur les comptes est soumise à l'approbation de l'autorité de supervision compétente : en France, cette mission est confiée à l'Autorité de contrôle prudentiel et de résolution (ACPR) et à la Banque de France en ce qui concerne l'analyse du respect des exigences de sécurité applicables aux services de paiement envisagés.

Le dépôt de dossier auprès de l'ACPR se fait selon deux procédures distinctes :

- les prestataires de service d'initiation de paiement (PSIP) doivent obtenir un agrément d'établissement de paiement, pour lequel l'absence de réponse sous trois mois à compter du dépôt de dossier de demande d'agrément vaut décision implicite de rejet ;

- les prestataires de services d'informations sur les comptes (PSIC) doivent, quant à eux, adresser une demande d'enregistrement, le silence de l'ACPR dans un délai de trois mois valant approbation.

Dans les deux cas, sur saisine de l'ACPR, la Banque de France doit délivrer un avis sur la sécurité des services proposés, qui comporte trois volets d'analyse :

- les conditions de sécurisation des moyens techniques envisagés ;

- les moyens humains et organisationnels envisagés ou mis en œuvre pour lutter contre la fraude ;

- les moyens déployés pour assurer la continuité de l'activité.

Au-delà des aspects sécuritaires, agrégateurs et initiateurs de paiement doivent se conformer, vis-à-vis de l'ACPR, à des exigences prudentielles définies par le Code monétaire et financier et précisées par un arrêté du ministre des Finances [8]. Ces exigences prudentielles sont proportionnées et donc limitées puisque ces établissements n'entrent pas en possession de fonds. Ils sont également tenus de souscrire à une assurance en responsabilité professionnelle, du fait des risques de cybersécurité spécifiques auxquels ils doivent faire face.

Il est à noter que les services d'initiation de paiement et d'information sur les comptes peuvent également être fournis par les établissements de crédit, mais aussi les établissements de paiement et de monnaie électronique qui doivent quant à eux se soumettre à une procédure d'extension d'agrément. Enfin, les établissements agréés pour ces services de paiement par un autre pays membre de l'Espace économique européen (EEE) sont

8 Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

également habilités à exercer leurs activités en France, sous réserve que leur autorité compétente transmette à l'ACPR un dossier de notification : c'est le principe du passeport financier européen.

Les établissements agréés par l'ACPR pour fournir ces services, ainsi que ceux pour lesquels l'ACPR a reçu une notification au titre du passeport européen, sont répertoriés dans le registre des agents financiers [9].

De la même manière que les établissements de paiement, les PSIP et les PSIC peuvent voir leur agrément/enregistrement révoqué s'ils cessent d'exercer leur activité, mais aussi et surtout si cette autorisation a été obtenue sur la base d'informations erronées, ou bien si l'établissement ne remplit plus les conditions auxquelles était subordonné son agrément/enregistrement. Ainsi, en cas de modification des conditions d'exercice de l'activité, le PSP doit en notifier l'ACPR pour un réexamen de sa situation.

L'ACPR publie chaque mois dans son registre officiel la liste des établissements concernés par un retrait d'agrément ou d'enregistrement [10].

9 Cf. *https://acpr.banque-france.fr/autoriser/registre-des-agents-financiers*

10 Cf. *https://acpr.banque-france.fr/page-tableau-filtre/registre-officiel*

Encadré 2

Éléments constitutifs d'un dossier d'agrément d'établissement de paiement

Les éléments constitutifs d'un dossier d'agrément ou d'enregistrement d'un prestataire de services de paiement (PSP) ont été définis dans des orientations dédiées de l'Autorité bancaire européenne [1], qui ont été déclinées dans le modèle de dossier type utilisé en France.

Ainsi, après avoir présenté son projet à la direction des autorisations de l'ACPR, tout établissement français souhaitant obtenir le statut d'établissement de paiement doit remplir un modèle de dossier fourni par l'ACPR, et y joindre les documents justificatifs suivants :

1. un programme d'activité * indiquant le type de services de paiement envisagés ;
2. un plan d'affaires incluant un calcul budgétaire prévisionnel pour les trois premiers exercices * ;
3. la preuve que l'établissement de paiement dispose des exigences en capital initial (50 000 euros pour le service d'initiation de paiement) ;

* Informations à fournir dans le cadre d'une demande d'enregistrement en tant que PSIC. Cette démarche bénéficie d'un cadre allégé.

1 Cf. *https://www.eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+ %28EBA-GL-2017-09 %29.pdf*

.../...

4. pour les établissements concernés, c'est-à-dire les établissements proposant un ou plusieurs des services de paiement 1 à 6 (cf. encadré 1), une description des mesures prises pour protéger les fonds des utilisateurs de services de paiement ;

5. une description du dispositif de gouvernance d'entreprise et des mécanismes de contrôle interne * ;

6. une description de la procédure en place pour assurer la surveillance, le traitement et le suivi des incidents de sécurité et des réclamations de clients liées à la sécurité * ;

7. une description du processus en place pour enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles, et conserver la trace de ces accès * ;

8. une description des dispositions en matière de continuité des activités, prévoyant notamment de soumettre ces plans à des tests périodiques * ;

9. une description des principes et des définitions appliqués pour la collecte de données statistiques relatives aux performances, aux opérations et à la fraude ;

10. un document relatif à la politique de sécurité, comprenant une analyse détaillée des risques liés aux services proposés, et une description des mesures de maîtrise correspondantes * ;

11. une description des mécanismes de contrôle interne liés aux obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ;

12. une description de l'organisation structurelle du demandeur, de ses éventuels accords de participation à un système international et/ou d'externalisation, et des mesures de contrôle de ses agents le cas échéant * ;

13. l'identité des personnes détenant une participation qualifiée dans le capital du demandeur, la taille de leur participation ainsi que la preuve de leur qualité ;

14. l'identité des dirigeants et des personnes responsables de la gestion de l'établissement (critères d'honorabilité, de compétence et d'expérience) et, le cas échéant, de la personne responsable de la gestion des activités de services de paiement * ;

15. le cas échéant, l'identité du/des commissaires aux comptes ;

16. la forme juridique et les statuts du demandeur * ;

17. l'adresse du siège social du demandeur * ;

18. une description de ses dispositions en matière d'audit et des dispositions organisationnelles* (cf. points 4, 5, 6 et 12).

* Informations à fournir dans le cadre d'une demande d'enregistrement en tant que PSIC. Cette démarche bénéficie d'un cadre allégé.

Le tableau ci-contre récapitule les différentes modalités selon lesquelles les acteurs financiers sont autorisés à fournir des services d'initiation de paiement et d'information sur les comptes en France.

Situation du demandeur	Procédure	Démarches
Nouvel acteur	Demande d'agrément en tant qu'établissement de paiement (services d'initiation de paiement) ou d'enregistrement (services d'information sur les comptes)	Dépôt du dossier auprès de l'ACPR, qui procède à l'instruction de la demande conjointement avec la Banque de France dans un délai de trois mois
Acteur agréé par l'ACPR en tant qu'établissement de crédit	Déjà habilité à proposer ces services	Pas de démarches supplémentaires
Acteur agréé par l'ACPR en tant qu'établissement de paiement ou établissement de monnaie électronique	Demande d'extension d'agrément	Dépôt d'un dossier d'extension d'agrément auprès de l'ACPR, qui procède à l'instruction de la demande conjointement avec la Banque de France dans un délai de trois mois
Acteur agréé en tant que PSP ou d'informations sur les comptes dans un pays membre de l'EEE	Procédure de libre prestation de services	Dépôt du dossier auprès de l'autorité compétente du pays membre, qui l'examine et décide de sa transmission à l'ACPR le cas échéant

Note de lecture : ACPR : Autorité de contrôle prudentiel et de résolution, PSP : prestataire de services de paiement et EEE : Espace économique européen.

Les mesures de protection des consommateurs

La protection des consommateurs est un objectif majeur de la directive notamment en ce qui concerne le droit à remboursement du payeur en cas d'opération de paiement non autorisée, lequel incombe aux PSP gestionnaires de comptes : lorsque le payeur (le titulaire d'un compte) constate qu'une opération de paiement qu'il n'a pas autorisée est débitée sur son compte, il doit en informer sans tarder son PSP gestionnaire de compte, et au plus tard dans un délai de treize mois à compter de la date du débit. Sauf en cas de fraude du payeur ou de négligence avérée de sa part, il sera remboursé par son PSP gestionnaire de compte. Afin d'inciter le payeur à signaler au plus vite les opérations de paiement non autorisées, son PSP peut lui faire supporter les pertes financières causées par ces opérations frauduleuses avant opposition jusqu'à concurrence de cinquante euros. Cependant, cette « franchise » ne peut pas être appliquée si : i) l'instrument de paiement perdu ou volé a été utilisé sans utilisation des données de sécurité personnalisées, ou ii) la perte, le vol ou le détournement de l'instrument de paiement ne pouvait être détecté par le payeur en amont, ou iii) les opérations contestées sont dues à des actes ou une négligence d'une personne dont le PSP est responsable.

Le remboursement doit s'effectuer au plus tard à la fin du jour ouvré suivant la notification sauf si le PSP gestionnaire de compte a de bonnes raisons de soupçonner une fraude du payeur. Dans ce cas, le PSP gestionnaire de compte peut effectuer certaines vérifications avant de rembourser ou non le payeur. Afin d'éviter tout abus, les PSP gestionnaires de comptes doivent notifier à la Banque de France les raisons pour lesquelles ils ne remboursent pas immédiatement.

Dans un souci de simplification des démarches de remboursement, le PSP gestionnaire de compte assure la fonction de point de contact unique du client en cas d'opération non autorisée impliquant un prestataire de services d'initiation de paiement (PSIP). Le PSP gestionnaire de compte est en charge du remboursement du payeur et se retourne vers le PSIP s'il estime que la responsabilité de l'opération de paiement pèse sur ce dernier. Le PSIP doit

alors indemniser le PSP gestionnaire de compte du payeur. S'il conteste sa responsabilité, il doit fournir la preuve que l'opération en question a bien été authentifiée et enregistrée, et qu'elle n'a pas été affectée par une déficience technique.

Par ailleurs, si le bénéficiaire de l'opération de paiement ou son PSP a demandé à ne pas recourir à la procédure d'authentification forte proposée par le PSP gestionnaire du compte, il est tenu de rembourser les préjudices subis par le PSP du payeur. Le PSP du payeur est en revanche responsable s'il a lui-même choisi de ne pas appliquer de procédure d'authentification forte.

La directive prévoit que les PSP mettent à la disposition de leurs clients des procédures de réclamation efficaces, leur permettant d'exercer leurs droits au regard de la DSP2 et garantissant une réponse sous un délai maximal de quinze jours. Une procédure de réclamation auprès des autorités – en France, auprès de l'ACPR – visant à signaler d'éventuels manquements à la DSP2 doit également être mise en place.

En cas d'échec des procédures de réclamation proposées à son client, le PSP doit l'informer de l'existence d'au moins une instance extrajudiciaire compétente pour traiter le litige. Enfin, le règlement extrajudiciaire des litiges doit faire l'objet de procédures indépendantes, impartiales, transparentes et efficaces.

Encadré 3

La deuxième directive européenne sur les services de paiement (DSP2) et le règlement général sur la protection des données (RGPD) : focus sur le consentement, l'information et les droits des personnes

Le RGPD s'applique dans son intégralité aux traitements de données à caractère personnel effectués par les prestataires de services de paiement (PSP) [1], que ces traitements relèvent ou non de la DSP2. Par exemple, les PSP doivent se conformer aux obligations de documentation (registre et étude d'impact relative à la protection des données, le cas échéant), de pertinence des données par rapport à l'objectif poursuivi, ou encore d'information préalable quant aux caractéristiques des traitements, et enfin de respect des droits d'accès, d'opposition, etc.

Dans la mesure où le RGPD constitue le cadre réglementaire général applicable à la protection des données à caractère personnel, les dispositions de la DSP2 en la matière doivent être interprétées au regard de ce cadre général. Or, certaines dispositions présentes dans la DSP2, telles que celles relatives au consentement explicite de l'utilisateur mentionné à l'article 94, semblent renvoyer à des obligations de nature différente de celles prévues par le RGPD en la matière. Un éclairage par les instances compétentes sur ces points d'articulation entre les deux réglementations, en premier lieu au niveau européen, apparaît souhaitable en vue d'assurer une mise en œuvre opérationnelle homogène par les acteurs du marché.

1 Le considérant 89 de la DSP2 rappelle que « *La fourniture de services de paiement par les prestataires de services de paiement peut comporter le traitement de données à caractère personnel. La directive 95/46/CE du Parlement européen et du Conseil* [abrogée par le RGPD], *les dispositions de droit national transposant cette directive et le règlement (CE) n° 45/2001 du Parlement européen et du Conseil s'appliquent au traitement des données à caractère personnel aux fins de la présente directive* ».

1.3 Les exigences de sécurité inscrites dans les RTS

L'article 98 de la DSP2 dispose que « *L'ABE, en étroite coopération avec la BCE et après avoir consulté toutes les parties concernées, y compris sur le marché des services de paiement, représentant tous les intérêts en présence, élabore des projets de normes techniques de réglementation à l'intention des PSP* […] *précisant :*

- *les exigences relatives à l'authentification forte du client* […] *;*

- *les dérogations à l'application de l'authentification forte du client* […] *;*

- *les exigences auxquelles doivent satisfaire les mesures de sécurité* […] *afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement ; et*

- *les exigences applicables aux normes ouvertes communes et sécurisées de communication aux fins de l'identification, de l'authentification, de la notification et de l'information, ainsi que pour la mise en œuvre des mesures de sécurité, entre les PSP gestionnaires du compte, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement.* »

Ces normes techniques réglementaires, ou RTS (pour *regulatory technical standards*) précisent ainsi les exigences de sécurité encadrant la fourniture des services de paiement, adaptées aux évolutions récentes du marché des paiements. Conformément à la DSP2, l'élaboration de ces RTS, conduite sous l'égide du Forum européen sur la sécurité des paiements (SecuRe Pay), a fait l'objet d'une interaction forte et régulière avec le marché (publication d'un *discussion paper*, puis d'une consultation publique), tout en respectant un principe de neutralité technologique et commercial.

La version finale des RTS a été rendue publique par la Commission européenne le 27 novembre 2017, puis publiée formellement au Journal officiel de la Commission européenne le 13 mars 2018. Compte tenu des délais prévus par la directive, ces RTS seront applicables à compter du 14 septembre 2019 – à l'exception des clauses concernant la mise à disposition de la documentation technique et des dispositifs d'essai des interfaces sécurisées, qui entreront en vigueur à partir du 14 mars 2019.

L'authentification forte

La DSP2 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 de bénéficiaire de virement).

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

- « connaissance » : une information que seul l'utilisateur connaît, par exemple, un code confidentiel, un mot de passe ou une information personnelle ;

- « possession » : un objet que seul l'utilisateur possède, et qui peut être reconnu sans risque d'erreur par le PSP : une carte, un *smartphone*, une montre ou un bracelet connecté, un porte-clés, etc. ;

Encadré 4

Quelques exemples de solutions d'authentification

Combinaison de facteur(s) d'authentification 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	Lecture de carte, d'un porte-clés, 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)

Quel statut pour l'authentification par mot de passe à usage unique au regard de la DSP2 ?

La principale solution d'authentification des paiements par carte sur internet déployée en France repose sur l'envoi d'un code confidentiel à usage unique par SMS (appelé SMS-OTP, pour *one time password*) au porteur de la carte, en complément de la saisie des données de carte de paiement (numéro, date d'expiration, cryptogramme, voire nom et prénom du porteur). La saisie de ce code confidentiel au travers du protocole 3D-Secure, dans une fenêtre dédiée du navigateur internet, permet de valider l'opération de paiement.

Dans son Opinion sur l'implémentation des RTS *(regulatory technical standards)* publiée le 13 juin 2018 [1], l'Autorité bancaire européenne (ABE) retient que ce mode d'authentification ne repose que sur un seul facteur : la possession du mobile du porteur, qui sert à recevoir le code de validation ; les données de carte nécessaires à l'initiation de la transaction ne peuvent être considérées comme un second facteur [2]. Ce mode d'authentification ne faisant ainsi intervenir en règle générale ni facteur biométrique, ni facteur de connaissance, il devrait être considéré comme un mode d'authentification non conforme au requis de la deuxième directive européenne sur les services de paiement (DSP2), qui prévoit le recours à deux familles différentes de facteurs d'authentification.

Le statut dominant en France de l'authentification par SMS-OTP, qui permet des gains notables en termes de lutte contre la fraude aux paiements sur internet (cf. chapitre 2), pose la question de la migration vers d'autres solutions d'authentification pleinement compatibles avec les requis de la DSP2 et des RTS. Au-delà de l'interprétation apportée par l'ABE, une mobilisation des acteurs au sein de l'Observatoire apparaît ainsi nécessaire en vue de définir une feuille de route concernant les modalités de cette migration, tant du point de vue technique que de l'accompagnement des acteurs, commerçants comme consommateurs.

1 Cf. Opinion EBA-Op-2018-04 : *https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf*

2 Le numéro de carte, le cryptogramme et la date d'expiration ne peuvent pas être considérés comme des éléments de connaissance, dans la mesure où ils sont imprimés sur la carte et peuvent être aisément répliqués. Par ailleurs, la présence physique de la carte n'étant pas requise pour un paiement à distance, la carte ne peut être considérée comme un facteur de possession dans ce cas d'usage.

• « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique.

La DSP2 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 DSP2 ajoute un requis supplémentaire : les données d'authentification doivent être liées à l'opération de paiement, de sorte qu'elles ne peuvent être réutilisées pour une opération de paiement ultérieure :

• le code d'authentification généré pour l'opération est spécifique au montant de l'opération et au bénéficiaire identifié ;

• toute modification du montant ou du bénéficiaire invalide le code d'authentification.

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

Ce recours à l'authentification forte ne s'impose que dans le cas d'opérations de paiement intraeuropéennes, c'est-à-dire pour lesquelles les PSP du payeur et du bénéficiaire sont établis dans l'Union européenne ; 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.

Les exemptions à l'authentification forte

Les RTS prévoient 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 *infra*. Le PSP gestionnaire de compte est tenu de veiller à la mise en place des dispositifs techniques permettant d'assurer le respect

	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 PSP teneur de compte de choisir le plafond qui lui semblera le plus approprié.

des plafonds fixés : 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 compte. 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.

• 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 (cf. *supra* « L'authentification forte » au sein de cette section). 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.

Le recours à ces différentes possibilités d'exemption est conditionné par le suivi, par les PSP, du taux de fraude observé pour chacun des motifs d'exemption à l'authentification forte et pour les opérations de paiement ayant bénéficié d'une authentification forte. Ce suivi doit être réalisé sur une base trimestrielle, par instrument de paiement, et en distinguant les opérations de paiement initiées en proximité des opérations de paiement initiées à distance. La remontée aux autorités nationales de données statistiques périodiques portant sur ces éléments est également prévue par la DSP2 (cf. article 3-c).

En outre, le PSP doit également veiller à ce que les taux de fraude globaux mesurés sur l'ensemble des opérations de paiement à distance, authentifiées ou non, respectent les plafonds par tranche de montant tels que présentés dans l'encadré 5.

Encadré 5

Conditions de mise en œuvre de l'exemption au titre de l'analyse des risques (article 18)

L'article 18 des RTS *(regulatory technical standards)* définit des conditions nécessaires à l'identification d'un faible niveau de risque.

• Le taux de fraude mesuré par le prestataire de services de paiement (PSP) pour le type d'opération de paiement concerné (c'est-à-dire au regard de l'instrument de paiement utilisé et du montant de l'opération de paiement) doit être inférieur aux taux affichés dans le tableau ci-après :

Taux de fraude maximal autorisé pour le recours à l'exemption au titre de l'article 18

(en %)

Montant de l'opération de paiement	Paiements électroniques à distance liés à une carte	Virements électroniques à distance
Plus de 500 euros	Exemption au titre de l'article 18 non autorisée	
250 à 500 euros	0,01	0,0050
100 à 250 euros	0,06	0,0100
0 à 100 euros	0,13	0,0150
Pour mémoire, taux de fraude moyen en 2016	0,161 pour les opérations en France > 0,3 pour les opérations transfrontalières	0,0003

• Le PSP n'a décelé, sur la base d'une analyse en temps réel, aucun facteur d'aggravation de risque, parmi lesquels :

- des dépenses ou un comportement anormal du payeur,
- des informations inhabituelles concernant le dispositif matériel ou logiciel utilisé par le payeur,
- des signes d'infection par un logiciel malveillant sur la page de paiement,
- la reconnaissance d'un scénario de fraude connu dans les paramètres de l'opération de paiement,
- une localisation anormale du payeur,
- une localisation du bénéficiaire présentant des risques élevés.

Dans l'hypothèse où les taux de fraude mesurés par le PSP viendraient à excéder les taux maximaux autorisés durant deux trimestres consécutifs, le PSP perdrait le bénéfice de cette exemption pour la tranche de montants considérée, et devrait donc recourir systématiquement à l'authentification forte du payeur, sauf dans les cas où une autre exemption pourrait s'appliquer. Cette exclusion prend fin dès que le PSP présente à nouveau, durant au moins un trimestre, des taux compatibles avec les maxima autorisés.

Encadré 6

Clarifications apportées sur les modalités de mise en application de certains facteurs d'exemption

Les conditions de recours aux différents cas d'exemption à l'authentification forte ont fait l'objet de clarifications apportées par l'Autorité bancaire européenne (ABE) au travers d'une Opinion [1] publiée le 13 juin 2018.

• Si la pertinence ou non d'appliquer un facteur d'exemption peut être appréciée par le prestataire de services de paiement (PSP) du payeur comme par celui du bénéficiaire, voire par le bénéficiaire lui-même, l'ABE précise que le choix d'activer ou non le recours à l'authentification forte n'appartient qu'aux PSP parties prenantes au paiement ; en outre, le PSP du payeur doit toujours pouvoir choisir, en dernier lieu, d'activer s'il le juge nécessaire le recours à l'authentification forte. Le tableau ci-après précise les cas dans lesquels les PSP peuvent proposer l'application d'un facteur d'exemption :

Référence dans les RTS	Facteur d'exemption	PSP du payeur	PSP du bénéficiaire	
			Virement	Carte
Article 10	Consultation des comptes	Oui	Sans objet	
Article 11	Paiement sans contact	Oui	Non	Oui [a]
Article 12	Automates de transport et de parking	Oui	Non	Oui [a]
Article 13	Bénéficiaire de confiance	Oui	Non	Non
Article 14	Transactions récurrentes	Oui	Non	Oui [a]
Article 15	Virement à soi-même	Oui	Non	nd
Article 16	Paiements de faible montant	Oui	Non	Oui [a]
Article 17	Protocoles de transferts d'ordres sécurisés	Oui	Non	nd
Article 18	Analyse de risque	Oui	Non	Oui [a]

a) Le PSP du payeur doit être en situation de décideur ultime, et doit donc pouvoir imposer le recours à l'authentification forte même dans le cas où le PSP du bénéficiaire estime que le paiement relève d'un facteur d'exemption.
Note : nd : non disponible.

• Le PSP chargé d'assurer l'authentification forte est par définition le PSP du payeur, qui a toutefois la faculté de déléguer contractuellement la mise en œuvre de cette authentification forte à un ou plusieurs acteurs tiers, tels que par exemple des PSP initiateurs de paiement ou des fournisseurs de portefeuilles d'instruments de paiement (ou *wallets*). Dans ce cas de figure, le PSP du payeur reste toutefois responsable du respect par ses délégataires des exigences définies dans la deuxième directive européenne sur les services de paiement (DSP2) et dans les *regulatory technical standards* (RTS) en matière d'authentification forte.

• L'exemption au titre de l'article 13 (bénéficiaires de confiance) n'est pas limitée au virement, et pourrait également s'appliquer pour les paiements par carte, dès lors que le PSP du porteur est en capacité d'assurer la gestion d'une liste de bénéficiaires de confiance validée par le porteur. Toutefois, l'ABE précise que cette exemption est à l'usage exclusif du PSP du payeur, comme précisé dans le tableau précédent.

1 Cf. *Opinion EBA-Op-2018-04 : https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf*

.../...

Comment appliquer les exemptions à l'authentification forte à certaines pratiques de paiement existantes ?

Les paiements fractionnés et les abonnements à options : de nombreux commerçants proposent aujourd'hui à leurs clients des facilités de paiement en plusieurs fois (dits paiements fractionnés), dont les montants peuvent varier dans le temps (par exemple, paiement de la moitié en une fois puis solde réparti sur quatre échéances, ou panier contenant plusieurs biens présentant des échéanciers de paiement de durées différentes). De façon similaire, certains services numériques ou culturels (chaînes de télévision, services de musique ou de vidéo à la demande, etc.) proposés sous forme d'abonnements sur mesure, en fonction de la consommation du client (par exemple, souscription à une chaîne télévisuelle pendant deux mois, puis retour à l'abonnement standard ensuite) donnent lieu à des facturations à une fréquence prédéfinie, mais de montant variable.

L'utilisation de la carte de paiement comme instrument de support à ces opérations nécessite que ces dernières soient initiées par l'intermédiaire du commerçant ou de fournisseur du service d'abonnement, dans un processus dit « *offline* » ne faisant pas intervenir le payeur en dehors de l'acte initial de souscription de la facilité de paiement ou de l'abonnement. De ce fait, la mise en œuvre d'une authentification forte à chaque opération de paiement unitaire apparaît difficilement réalisable.

Or, du fait du montant variable de ces paiements, et en dépit de leur caractère périodique, ils ne peuvent bénéficier de l'exemption à l'authentification forte au titre de l'article 14 (paiements récurrents), qui ne s'applique qu'en cas d'opérations de paiement successives de même montant. Le recours à d'autres critères d'exemption peut toutefois être envisagé, sous réserve que certaines conditions soient remplies.

• Au titre de l'article 13, sous réserve que le commerçant soit enregistré par le payeur comme bénéficiaire de confiance auprès de son PSP gestionnaire de compte.

• Au titre de l'article 16, dans l'hypothèse où les opérations de paiement (notamment dans le cas d'abonnements) seraient d'un montant unitaire inférieur à trente euros. Cette contrainte limite toutefois le prix maximal des options supplémentaires que le payeur peut souscrire ; en outre, certaines échéances pourraient être rejetées dès lors que le payeur aurait atteint le plafond de paiements consécutifs définis dans l'article 16.

• Au titre de l'article 18, dès lors que les opérations de paiement sont reconnues comme à faible niveau de risque par le PSP du payeur, ce qui suppose notamment que les taux de fraude mesurés pour le commerçant soient vus par le PSP du payeur comme suffisamment faibles, le recours à cette exemption étant conditionné par la capacité de ce PSP à maîtriser sur une base durable son niveau de fraude.

Les pratiques de régularisation de l'industrie du tourisme : une pratique courante du secteur du tourisme consiste à utiliser le numéro de carte de paiement du client en vue d'initier des opérations de paiement de régularisation de prestations supplémentaires au fonctionnement standard des services souscrits, par exemple : annulation tardive de réservation, consommations non prévues au forfait et non déclarées par le payeur au moment de

.../...

la facturation (minibar de chambre d'hôtel, restaurant, accès à des services annexes, etc.), ou encore dégâts matériels constatés *a posteriori* (locations de véhicules, mobilier, etc.).

Ces opérations de paiement sont généralement initiées en l'absence du payeur, et ne font donc pas l'objet d'une authentification forte. Or, ces pratiques ne font pas explicitement l'objet d'une exemption dans les RTS [2], et pourraient être de fait considérées comme incompatibles avec la DSP2, sauf si le recours à un facteur d'exemption pouvait être invoqué. À ce titre, les exemptions au titre de l'article 13 (commerçant enregistré par le payeur comme bénéficiaire de confiance) ou de l'article 18 (transactions reconnues comme à faible niveau de risque par le PSP du payeur) apparaissent les plus appropriées ; toutefois, compte tenu de l'objet de ces paiements, les contestations par le payeur sont *a priori* relativement courantes, et devraient constituer un frein au recours à ces deux cas d'exemptions.

Compte tenu des difficultés à identifier un cadre d'exemption approprié pour ces opérations de paiement, ou au contraire à acter de leur non-conformité à la DSP2, la question du régime applicable à ce cas d'usage a été soumise à l'Autorité bancaire européenne, qui devrait y apporter une réponse dans le cadre d'une future liste de questions/réponses portant sur l'interprétation des textes de niveau 2, dont la publication est attendue au deuxième semestre 2018.

2 Notamment du fait qu'elles ne peuvent être assimilées à des transactions de type MOTO (*mail order/telephone order*) non soumises à l'obligation d'authentification forte.

Encadré 7

Modification majeure du schéma de décision en matière d'authentification pour le *e-commerce*

En instituant par défaut le principe d'authentification forte des opérations de paiement et en permettant au prestataire de services de paiement (PSP) gestionnaire de comptes de décider en dernier ressort de l'application ou non d'une exemption, la deuxième directive européenne sur les services de paiement (DSP2) constitue une évolution majeure dans le processus de décision en matière d'authentification dans le cadre de la vente en ligne.

En effet, dans le cadre actuel, les e-commerçants ont l'initiative du déclenchement de l'authentification forte, en choisissant de faire appel au dispositif d'authentification (dans le cas général, le protocole 3D-Secure) dans le cas où leur propre analyse identifie une opération de paiement comme risquée.

Les dispositions de la DSP2 relatives à l'authentification forte qui s'appliqueront à partir du 14 septembre 2019 (à l'expiration du délai de mise en œuvre des *regulatory technical standards* – RTS) prévoient que le recours à l'authentification forte soit à la main du PSP du payeur, et ce même dans une situation où l'opération de

.../...

paiement entre du point de vue du commerçant dans un cas d'exemption (par exemple, pour une opération de paiement de faible montant). En effet, si le PSP du payeur juge qu'une opération de paiement est risquée, il peut décider d'appliquer l'authentification forte même dans l'hypothèse où les conditions d'application d'une autre exemption sont remplies.

Cette évolution du schéma de décision associé à la mise en œuvre de l'authentification forte peut inciter à l'échange d'informations entre e-commerçant et PSP du payeur : en effet, sur la base des dispositifs d'évaluation du niveau de risque d'ores et déjà en place, le e-commerçant est capable d'identifier des facteurs de réduction du risque (tels que les habitudes d'achat de son client sur son site en ligne, ou encore l'utilisation d'une adresse de livraison déjà utilisée) qui pourraient justifier de son point de vue le recours à l'exemption au titre de l'article 18 des RTS (c'est-à-dire, niveau de risque faible). Cette information, si elle peut être techniquement partagée avec le PSP du payeur comme cela est prévu notamment dans les spécifications du protocole 3D-Secure 2.0, pourrait être utilisée pour alimenter le dispositif d'évaluation des risques de ce dernier, et donc faciliter l'application d'une exemption.

S'agissant de la protection des données personnelles, des garanties doivent toutefois être prévues afin que les échanges réalisés dans ce contexte se limitent à un partage d'expertises et de critères de détection d'anomalies ou d'incohérences pouvant révéler une fraude ou une tentative de fraude, à l'exclusion de toute communication de données personnelles susceptibles de permettre l'identification directe ou indirecte (notamment par recoupement d'informations), de l'auteur d'une fraude ou d'une tentative de fraude entre des professionnels relevant de secteurs d'activité différents ou appartenant à des groupes différents au sein d'un même secteur (principe de sectorisation de la mise en œuvre et de l'accès aux fichiers d'exclusion).

L'interface sécurisée

Les RTS précisent les modalités de communication ouvertes et sécurisées prévues par la DSP2 qui concerne l'obligation de mise en place et d'utilisation d'une interface sécurisée (ou API – *application programming interface*) permettant i) l'identification du PSP tiers (c'est-à-dire l'initiateur de paiement ou l'agrégateur d'information sur les comptes) par le PSP gestionnaire de comptes au moyen de certificats qualifiés au sens du règlement européen eIDAS [11], ii) de s'appuyer sur le mécanisme d'authentification forte de l'utilisateur proposé par le PSP gestionnaire de comptes, et iii) l'initiation d'ordre de paiement et la réception d'informations relatives à l'exécution des opérations de paiement initiées.

Les RTS prévoient une période de test de l'interface d'une durée de six mois avant la date d'entrée en application. Les PSP gestionnaires de comptes ont le choix de développer une interface dédiée aux prestataires tiers (c'est-à-dire différente de l'interface client), ou de permettre un accès *via* l'interface client enrichie par des mécanismes techniques permettant la reconnaissance et l'identification des PSP tiers.

11 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Encadré 8

Clarifications apportées par l'Autorité bancaire européenne sur les modalités de fonctionnement de l'interface sécurisée

Le périmètre de données et de services accessibles au travers de l'interface sécurisé et les conditions de connexion par les prestataires de services de paiement (PSP) tiers ont fait l'objet de clarifications apportées par l'Autorité bancaire européenne au travers d'une Opinion [1] publiée le 13 juin 2018.

- Au titre du service d'information sur les comptes, l'interface dédiée doit permettre l'accès à l'ensemble de données relatives aux comptes de paiement disponibles *via* les interfaces utilisateurs (site web, application mobile, etc.). Dans l'hypothèse où ces interfaces ne présenteraient pas la même profondeur de données, l'interface sécurisée doit permettre l'accès au périmètre de données le plus étendu.
- Au titre du service d'initiation de paiement, l'interface doit permettre l'accès à l'ensemble de la gamme d'instruments de paiement proposés par le PSP gestionnaire de compte au travers de ses interfaces utilisateurs.
- À l'exception du nom du titulaire du compte, les informations transmises par le PSP gestionnaire de compte au prestataire de services d'information sur les comptes (PSIC) ou au prestataire de services d'initiation de paiement (PSIP), dans le cadre de la fourniture des services encadrés par la DSP2, ne doivent pas comporter d'autre information relative à l'identité du titulaire du compte (date de naissance, adresse, etc.), sans préjudice du respect des principes généraux relatifs à la protection des données personnelles prévus par le règlement général sur la protection des données (RGPD) et des droits des personnes.
- En dehors des périodes de connexion active de l'utilisateur aux services du PSIC (par exemple, au travers du site internet du PSP tiers ou de son application mobile), le PSIC dispose d'un accès à l'interface sécurisée limité à quatre connexions par jour, sauf arrangement contractuellement avec le PSP gestionnaire de compte autorisant une plus grande fréquence de connexion, voire le recours à un mode de communication active (dit mode *push*) par lequel le PSP gestionnaire de compte informe le PSIC de tout nouveau mouvement imputé sur le compte de paiement de l'utilisateur.

1 Cf. Opinion EBA-Op-2018-04 : *https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf*

Encadré 9

Recherche d'une standardisation des interfaces au niveau français

Dans le cadre des travaux du Comité national des paiements scripturaux, la mise en place d'interfaces spécifiques à chaque prestataire de services de paiement (PSP) gestionnaire de compte a été identifiée comme un facteur de fragmentation du marché de l'accès aux comptes de paiement et à leurs informations, susceptible de pénaliser le développement de services innovants en matière d'agrégation ou d'initiation de paiement.

Afin de favoriser le développement d'un modèle d'interface commun au niveau de la Place française, un groupe de travail a été constitué afin de définir les fonctionnalités d'une interface de programmation applicative (ou API – *application programming interface*) sécurisée répondant aux exigences de la DSP2 et, de façon la plus consensuelle possible aux besoins exprimés tant par les PSP gestionnaires de comptes que par les prestataires de services d'information sur les comptes (PSIC) et les prestataires de services d'initiation de paiement (PSIP).

Dans le cas où un PSP gestionnaire de compte choisit de fournir une interface dédiée, les RTS prévoient un certain nombre d'exigences et de conditions.

• 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'utiliser cette interface, et n'utilisent donc pas les interfaces dédiées aux clients du PSP gestionnaire de compte.

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

• 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 des RTS, et après avoir été testée pendant la période de six mois spécifiée et utilisée pendant trois mois. Cette exemption peut être retirée par l'autorité nationale compétente si l'interface ne respecte plus les exigences des RTS et si le PSP gestionnaire de comptes n'est plus capable de résoudre les dysfonctionnements constatés sous un délai de deux semaines. Dans ce cas, le PSP gestionnaire de compte doit fournir une interface de repli sous un délai de deux mois.

Encadré 10

Protection des identifiants personnels dans le cadre des nouveaux services de paiement

En cas d'utilisation d'une interface dédiée, l'utilisateur de services d'information sur les comptes n'aura plus nécessairement à fournir ses données de sécurité personnalisées (identifiant et mot de passe de banque en ligne). La connexion sera automatiquement sécurisée entre les prestataires de services d'information sur les comptes (PSIC, les agrégateurs d'informations) et les prestataires de services de paiement (PSP) gestionnaires de comptes (les banques). De manière proportionnée aux risques sur les droits et libertés des personnes concernées, les mesures choisies pourront notamment être l'authentification mutuelle des serveurs, le chiffrement du canal de communication, l'envoi d'un récépissé à l'utilisateur, une voie de recours en cas de litige, la gestion de traces appropriées et accessibles par l'utilisateur, etc.

En tout état de cause, il faut retenir que l'obligation de « mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques » (article 32-1 du règlement général sur la protection des données – RGPD) s'applique à l'ensemble des PSP, en tant que responsable du traitement des données des utilisateurs. La Commission nationale de l'informatique et des libertés (Cnil) reste pleinement compétente pour agir en cas de manquement.

1.4 Les orientations de l'Autorité bancaire européenne

Orientations relatives aux mesures de sécurité pour les risques opérationnels et de sécurité

L'article 95 de la DSP2 prévoit que « *Les États membres veillent à ce que les PSP établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité, liés aux services de paiement qu'ils fournissent.* […] *L'ABE, en étroite coopération avec la BCE et après avoir consulté toutes les parties concernées, y compris sur le marché des services de paiement, représentant tous les intérêts en présence, émet des orientations* [...] *concernant l'établissement, la mise en œuvre et le suivi des mesures de sécurité, y compris, le cas échéant, des procédures de certification.* »

Les neuf orientations sur les risques opérationnels et de sécurité, publiées par l'Autorité bancaire européenne le 12 décembre 2017, visent ainsi à définir des lignes directrices s'imposant aux PSP en matière de gestion de leurs risques.

L'orientation 1 définit un principe général de proportionnalité applicable aux huit autres orientations, en énonçant que le cadre de gestion des risques du PSP doit être proportionné à sa taille et à son profil de risques.

L'orientation 2 demande aux PSP de définir formellement un cadre de gouvernance dédié à la gestion des risques, prévoyant notamment la rédaction d'une politique de sécurité, l'identification des rôles et responsabilités au sein de l'établissement, ainsi que les procédures et systèmes nécessaires pour identifier, mesurer, suivre et gérer l'ensemble des risques résultant des activités liées au paiement du PSP. Ce cadre doit répondre aux impératifs suivants :

- il doit être dûment documenté et régulièrement actualisé, notamment en cas de modification majeure d'infrastructure, de procédés ou de procédures et après chaque incident majeur opérationnel ou de sécurité ayant une incidence sur la sécurité des services de paiement ;

- le modèle de gestion des risques doit être supporté par un dispositif de contrôle interne ;

- en cas d'externalisation d'activités, les PSP doivent veiller à ce que les activités sous-traitées soient correctement couvertes par le cadre de gouvernance des risques ; à cet effet, les exigences applicables au sous-traitant doivent être définies contractuellement.

L'orientation 3 impose aux PSP d'évaluer leurs risques opérationnels et de sécurité. À cette fin, ils sont tenus d'identifier et d'ordonner leurs différentes fonctions, ressources et systèmes d'information internes par profil de risque.

L'orientation 4 prévoit la mise en place par les PSP de mesures de sécurité visant à le prémunir contre les risques opérationnels et de sécurité identifiés, notamment au travers de mesures de protection des actifs logiques et physiques ainsi que de dispositifs de contrôle.

L'orientation 5 invite les PSP à mettre en place des dispositifs de suivi continu des activités et de détection des incidents opérationnels et de sécurité, ainsi que les modalités d'information et de résolution opérationnelle de ces derniers.

L'orientation 6 prévoit la mise en place d'un cadre de gestion de la continuité d'activité, basée sur l'identification de scénarios de crise et de plans de communication et de continuité associés, ainsi que le test de la capacité de mise en œuvre de ces plans.

L'orientation 7 invite les PSP à mettre en place un cadre de test de l'ensemble des mesures de sécurité prévues dans le cadre de gestion des risques opérationnels et de sécurité, sur une base périodique ainsi qu'en cas d'évolution des systèmes d'information ou des procédures ou suite à la survenance d'incidents majeurs.

L'orientation 8 prescrit la mise en place de dispositifs permettant d'assurer la sensibilisation des équipes du PSP aux risques opérationnels et au cadre de gestion mis en place au sein de l'établissement.

Enfin, l'orientation 9 invite les PSP à sensibiliser leurs clients aux risques de sécurité associés aux services de paiement proposés, ainsi qu'aux mesures de prévention déployées, notamment en termes de restriction d'utilisation (par exemple, plafonds de paiement, etc.), de dispositifs d'authentification proposés et de point de contact à utiliser en cas d'alerte.

Orientations sur la notification des incidents majeurs

L'article 96 de la DSP2 définit des exigences en matière de déclaration des incidents majeurs opérationnels (y compris de sécurité) rencontrés par les PSP :

- d'une part, les PSP doivent notifier les incidents majeurs à leur autorité nationale compétente (ANC), soit, pour les PSP français, à la Banque de France pour les incidents de sécurité et à l'ACPR pour les incidents opérationnels ;

- d'autre part, les ANC sont, à leur tour, tenues de rapporter ces incidents aux autorités européennes compétentes : l'Autorité bancaire européenne (ABE) et la Banque centrale européenne (BCE).

Conformément à l'article 96 de la DSP2, les modalités de mise en œuvre de ces exigences ont été précisées par des orientations de l'ABE, qui spécifient également la méthodologie de qualification des incidents et la nature des informations à transmettre par les PSP.

Qualification des incidents

Un incident opérationnel ou de sécurité est défini comme « *un événement unique ou une série d'événements liés, non planifiés par le PSP, qui a ou aura probablement une incidence négative sur l'intégrité, la disponibilité, la confidentialité,*

Seuils critères	Niveau d'impact inférieur	Niveau d'impact supérieur
Opérations affectées	> 10 % du volume habituel des opérations du PSP (en nombre d'opérations) et > 100 000 euros	> 25 % du volume habituel des opérations du PSP (en nombre d'opérations) ou > 5 millions euros
Utilisateurs de services de paiement affectés	> 5 000 utilisateurs de services de paiement du PSP et > 10 % des utilisateurs de services de paiement du PSP	> 5 000 utilisateurs de services de paiement du PSP ou > 25 % des utilisateurs de services de paiement du PSP
Interruption du service	> 2 heures	Sans objet
Impact économique	Sans objet	> Max. (0,1 % des fonds propres de catégorie 1 [a], 200 000 euros) ou > 5 millions euros
Niveau élevé d'escalade interne	Oui	Oui, et un mode de « crise » (ou équivalent) est susceptible d'être déclenché
Autres PSP ou infrastructures pertinentes potentiellement affectés	Oui	Sans objet
Impact en termes de réputation	Oui	Sans objet

a) Fonds propres de catégorie 1 tels que définis à l'article 25 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012.

l'authenticité et/ou la continuité des services liés au paiement ».

Un incident est qualifié de « majeur » lorsqu'il remplit un ou plusieurs critères pouvant avoir un « niveau d'impact élevé » (ci-dessous : « impact supérieur ») ou trois critères ou plus pouvant avoir un « niveau d'impact plus faible » (ci-dessous : « impact inférieur »).

La mesure des impacts pour chaque critère est réalisée par rapport à des seuils dont les montants sont précisés dans le tableau *supra*. Les PSP peuvent avoir recours à des estimations s'ils ne disposent pas de données réelles leur permettant de juger si un seuil donné a été ou sera probablement atteint avant la résolution de l'incident (par exemple, pendant la phase d'enquête initiale).

Suivi du cycle de vie des incidents

Les rapports d'incidents sont constitués d'un ensemble de champs structurés, et répartis en trois grandes sections (A, B et C), qui correspondent aux différentes étapes du cycle de vie de l'incident.

• Rapport initial (section A) : il doit être transmis par le PSP dans les 4 heures qui suivent la détection d'un incident par le PSP impacté, et contient a minima les informations décrites dans la section A.

• Rapport(s) intermédiaire(s) (section B) : le premier rapport intermédiaire doit être remis au maximum dans les trois jours suivant l'émission du rapport initial. Un nouveau rapport pourra être soumis autant de fois que nécessaire suivant l'évolution de l'incident ou sur demande de la Banque de France. Elle contient au minimum les informations décrites dans la section B. Si un incident est résolu dans les 4 heures suivant la période de détection, les données du rapport intermédiaire pourront être remises soit dans le rapport initial,

Encadré 11

Incidents majeurs et violation de données à caractère personnel : un point d'intersection entre la DSP2 et le RGPD (article 33)

Dans certains cas, les organismes ont aussi une obligation de notifier les violations de données à caractère personnel à l'autorité de protection des données personnelles (en France il s'agira de la Commission nationale de l'informatique et des libertés – Cnil – en cas de traitement transfrontalier il s'agira de l'autorité de protection désignée « chef de file ») et, dans certains cas, de les communiquer aux personnes concernées.

Concrètement, dès qu'un incident concerne des données à caractère personnel (accès non autorisé, modification non désirée ou disparition de données), il s'agit d'une violation, emportant les actions suivantes :

• l'organisme doit l'inscrire, en interne, dans un registre des violations ;

• si cette violation engendre des risques sur les droits et libertés des personnes concernées, il doit en notifier l'autorité de contrôle, si possible dans les 72 heures suivant la prise de connaissance de la violation ;

• si ces risques sont élevés, il doit informer, dans les meilleurs délais, les personnes concernées de la violation.

Les échelles d'impacts utilisées par les organismes devraient donc intégrer ceux sur les droits et libertés des personnes concernées. De plus, la gestion des violations devrait être intégrée dans le processus de gestion des incidents des organismes.

soit dans un rapport intermédiaire soumis au maximum 4 heures après la résolution de l'incident.

• Rapport final (section C) : il doit être remis au maximum dans les deux semaines après que la situation soit revenue à la normale. Il contient au minimum les informations décrites dans la section C. Si un incident est résolu dans les 4 heures suivant la période de détection, un rapport unique contenant toutes les informations des sections A, B et C pourra être soumis.

Chacun de ces rapports peut être accompagné, si le PSP le juge opportun, de documents complémentaires transmis sous format libre.

Enfin, dans le cas d'une délégation de la déclaration des incidents à un sous-traitant commun à plusieurs PSP, de dernier peut émettre un rapport consolidé couvrant plusieurs PSP. Dans ce cas de figure, la structure du rapport demeure la même, avec l'ajout d'un tableau complémentaire récapitulant la liste des PSP impactés.

Orientations sur les statistiques de fraude

La réduction de la fraude est l'un des objectifs essentiels de la DSP2. C'est à ce titre qu'elle requiert la fourniture par les PSP aux États membres – sur une base annuelle a minima – de données statistiques liées à la fraude aux moyens de paiement.

L'objectif de cette collecte est double pour les autorités européennes :

• mesurer dans le temps l'efficacité des mesures européennes de lutte contre la fraude ;

• s'assurer que les PSP bénéficiant de l'exemption d'application des procédures d'authentification forte au titre de l'article 18 (appréciation d'un faible niveau de risque des opérations de paiement) respectent les plafonds de taux de fraude fixés par les RTS, faute de quoi la faculté de recours à ce motif d'exemption pourra leur être retirée.

Or, au moment de l'entrée en application de la DSP2, les pratiques de collecte de données sur la fraude aux moyens de paiement parmi les États membres étaient disparates, voire limitées à certains moyens de paiement (essentiellement la carte). Cette situation, qui était de nature à complexifier l'agrégation de données de fraude à l'échelle européenne, justifiait l'harmonisation des modalités de remontée de données statistiques aux autorités nationales et européennes.

Les orientations de l'Autorité bancaire européenne définissent un cadre de référence, qui prévoit de collecter les statistiques de fraude sur une base annuelle/semestrielle selon un certain nombre d'axes d'analyse :

• par moyen de paiement (carte, virement, prélèvement, monnaie électronique) ;

• par canal de paiement (en proximité ou à distance) ;

• par typologie de fraude,

• par mode d'authentification (avec ou sans authentification forte) et par facteur d'exemption en cas d'absence d'authentification forte ;

• par zone géographique (transaction nationale, intraeuropéenne ou extraeuropéenne).

Ce cadre est globalement cohérent à celui qui préexistait en France au titre de la mission de surveillance de la Banque de France et des travaux statistiques de l'Observatoire, tel que présenté en annexe 5.

2 État de la fraude en 2017

2.1 Vue d'ensemble

Cartographie des moyens de paiement

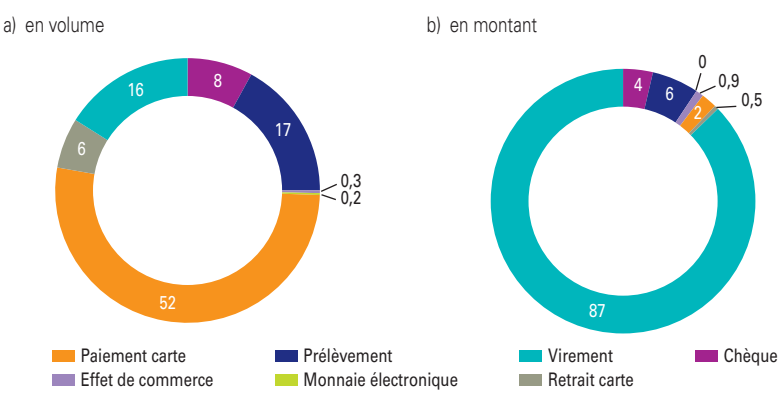
En 2017, ce sont 24,1 milliards de transactions scripturales qui ont été réalisées par les clients (particuliers et entreprises) des banques et prestataires de services de paiement français pour un montant total de 27 575 milliards d'euros, ce qui représente une progression de 6,6 % de nombre de transactions et de 1,5 % des montants échangés par rapport à l'année 2016.

Le paiement par carte conforte sa place de mode de paiement privilégié des Français, qui l'utilisent désormais dans 52 % des paiements scripturaux pour un montant total de 530 milliards d'euros en 2017. En complément, les retraits par carte ont représenté 1 481 millions d'opérations en 2017, pour 135 milliards d'euros.

Le virement reste l'instrument privilégié pour les paiements de

G1 Usage des moyens de paiement scripturaux en France en 2017

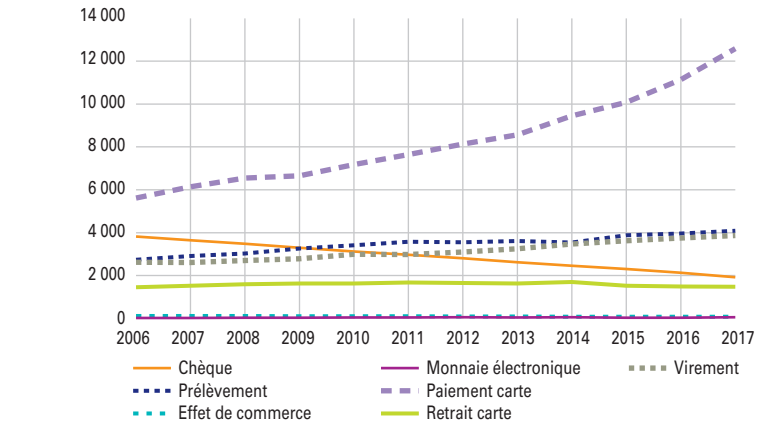
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G2 Usage des moyens de paiement scripturaux en France depuis 2006

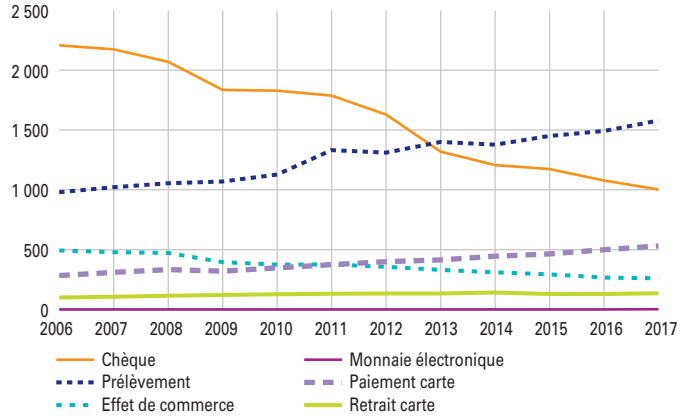
(en millions d'opérations)



Source : Observatoire de la sécurité des moyens de paiement.

G3 Montant des transactions hors virements en France depuis 2006

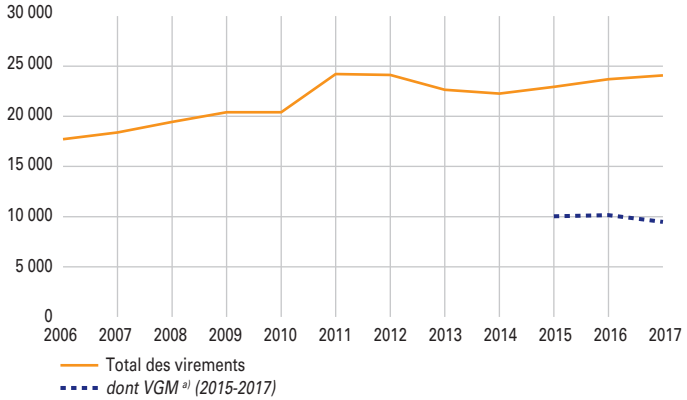
(en milliards d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G4 Montant des virements en France depuis 2006

(en milliards d'euros)



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

montant élevé (paiements des salaires et pensions, paiements interentreprises, etc.) et représente 87 % du montant total des transactions scripturales. En nombre d'opérations, il conserve la troisième position (16 %), juste après la carte et le prélèvement. Les virements sont principalement nationaux (79 % des virements globaux), contre 21 % à destination de l'étranger (espace SEPA – *single euro payments area* – et en-dehors). Plus d'un tiers des virements émis en montant (39 %) transite *via* des infrastructures dédiées aux paiements de gros montant. Ils correspondent exclusivement à des paiements interentreprises dont le montant moyen s'établit à près d'un million d'euros. Le solde correspond pour l'essentiel au virement SEPA, accessible tant à la clientèle professionnelle qu'aux particuliers, et dont le montant unitaire moyen est de 3 780 euros. Dans une moindre mesure, le solde comprend également d'autres formes de virement (notamment, les virements internationaux hors Union européenne).

Le prélèvement conserve le second rang des instruments de paiement scripturaux les plus utilisés, tant en volume qu'en montant. Il représente 17 % des transactions en nombre et un peu moins de 6 % du montant total des transactions en 2017. Son utilisation est presque exclusivement nationale, les prélèvements SEPA transfrontaliers ne représentant que 2 % de l'ensemble des flux émis.

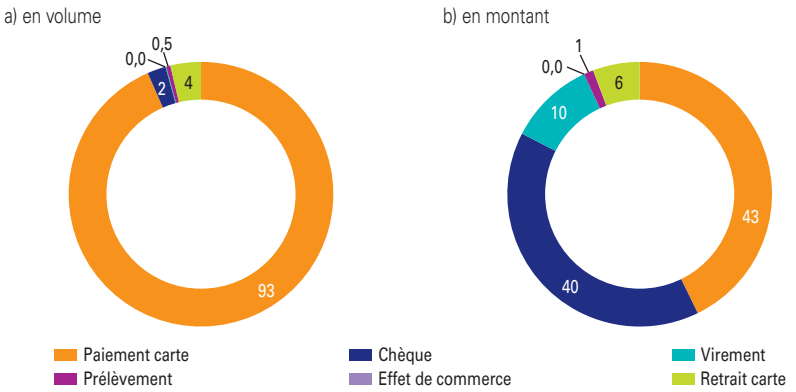
Le déclin continu du **chèque**, observé depuis plusieurs années, s'est poursuivi en 2017, tant en nombre d'opérations (– 10 %) que de leur valeur (– 7 %), soit une émission de 1,9 milliard de chèques en 2017, pour un montant global de 1 001 milliards d'euros.

Les effets de commerce (lettres de change relevé et billets à ordre relevé), qui représentent moins de 1 % des transactions scripturales tant en nombre d'opérations (0,3 %) qu'en valeur (0,9 %), confirment en 2017 le déclin observé depuis plusieurs années.

Enfin, bien que l'utilisation de **la monnaie électronique** reste encore marginale en 2017, elle connaît une nette tendance à la hausse en 2017, pour atteindre 55 millions de transactions (+ 44 %) et une valeur totale de 898 millions d'euros (+ 52 %), portée par le développement de solutions de paiements entre particuliers.

G5 Répartition de la fraude sur les moyens de paiement scripturaux en 2017

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Fraude aux moyens de paiement

En 2017, la fraude aux transactions scripturales représente un montant global de 744 millions d'euros pour 5,1 millions de transactions frauduleuses, contre 798 millions d'euros et 4,8 millions de cas en 2016.

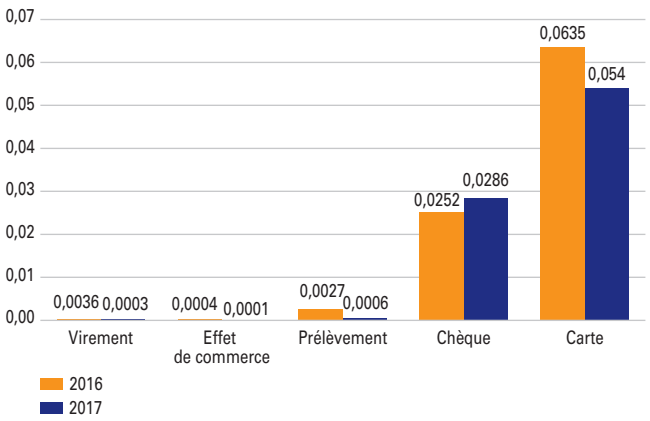
La **carte de paiement** [1] concentre près de la moitié de la fraude en montant, soit 361 millions d'euros en cumulant les transactions de paiement et de retrait, et représente la quasi-totalité (97 %) du nombre de transactions frauduleuses. Néanmoins, le montant de fraude global sur les cartes émises en France diminue en 2017 pour la deuxième année consécutive. Ainsi, après plusieurs années de stagnation, le taux de fraude sur les opérations par carte diminue pour s'établir à 0,054 %, soit environ un euro de fraude pour 1 850 euros de transactions. Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,008 % soit un euro de fraude pour 12 500 euros de paiement) mais plus significative sur les paiements à distance (0,161 %, soit un euro de fraude pour 620 euros de paiement), en dépit d'une nouvelle baisse remarquable de la fraude sur ce canal.

Le **chèque** reste le second moyen de paiement le plus fraudé, avec un montant annuel de fraude en hausse qui atteint 296 millions d'euros en 2017, et ce alors que son utilisation

1 Cartes émises en France.

G6 Évolution du taux de fraude par moyen de paiement, 2016–2017

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

continue à se réduire. Son taux de fraude progresse pour s'établir à 0,0286 %, soit un euro de fraude pour 3 500 euros de paiement.

Le montant annuel de fraude au **virement** est toujours très inférieur à celui de la carte et du chèque (78 millions d'euros en 2017), et de surcroît en baisse significative par rapport à 2016 (– 17 %). Son taux de fraude reste le plus faible parmi les moyens de paiement accessibles aux particuliers. Il s'établit à 0,0003 %, soit l'équivalent d'un euro de fraude pour 300 000 euros de paiement.

Le **prélèvement** représente à nouveau le montant annuel de fraude le plus limité parmi les moyens de paiement scripturaux accessibles aux particuliers (9 millions d'euros en 2017), en baisse très significative par rapport à 2016 (– 78 %). Son taux de fraude connaît également un repli significatif pour s'établir à 0,0006 %, soit l'équivalent d'un euro de fraude pour 180 000 euros de prélèvements émis.

Enfin, les **effets de commerce** restent épargnés par la fraude, avec un montant de l'ordre de 153 000 euros en 2017 pour trois cas de fraude, et un taux de fraude de 0,0001 % équivalent à un euro de fraude pour plus de 1 700 000 euros de paiement.

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

Vue d'ensemble

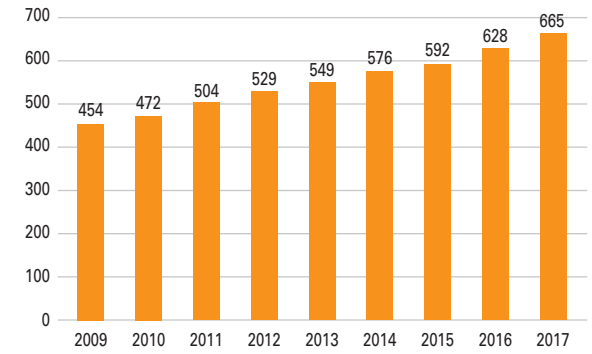
Le montant total de la fraude sur les transactions de paiement et de retrait effectuées en France et à l'étranger avec des cartes françaises a de nouveau reculé en 2017 (9,6 % par rapport à 2016). Il s'établit à 360,7 millions d'euros, et cela alors même que le montant total des transactions augmente sensiblement (5,8 %), à 664,6 milliards d'euros.

En conséquence, le taux de fraude sur les cartes de paiement françaises s'établit désormais à 0,054 %, contre 0,064 % en 2016, soit son plus bas niveau sur la période 2009-2017 (cf. graphique 9 *infra*).

En tenant compte également de la fraude enregistrée sur les transactions réalisées en France avec des cartes émises dans d'autres pays, la même tendance est observée avec une baisse de 9,8 %, par rapport à 2016, du montant total de la fraude. Celui-ci s'élève à 467 millions d'euros en 2017, pour un montant total de transactions atteignant 715,4 milliards d'euros, en progression de 6,3 % par rapport à 2016.

G7 Montant total des transactions des cartes françaises

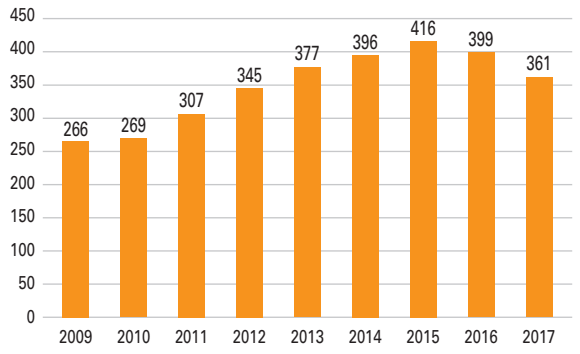
(en milliards d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G8 Montant total de la fraude des cartes françaises

(en millions d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

Encadré 1

Statistiques de fraude sur les cartes : les contributeurs

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

Les statistiques calculées par l'Observatoire pour l'année 2017 portent ainsi sur :

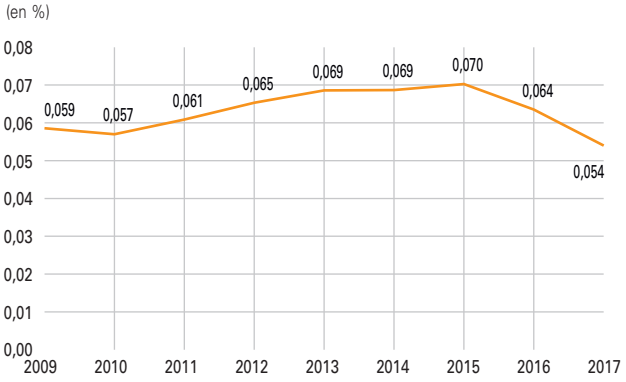
- 644,7 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 76,1 millions de cartes de type « interbancaire » émises en France (dont 51,2 millions de cartes sans contact) ;
- 19,9 milliards d'euros de transactions réalisées (principalement en France) avec 9,9 millions de cartes de type « privatif » émises en France ;
- 50,7 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».

Les données recueillies proviennent :

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

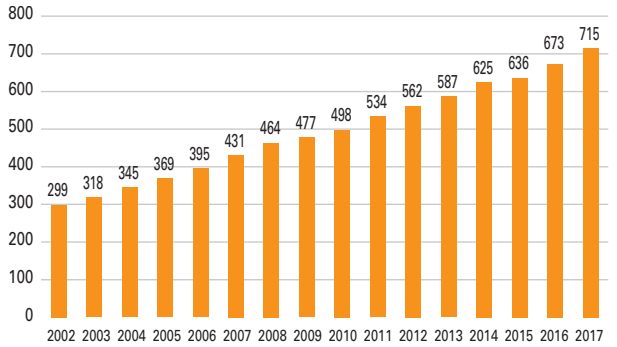
1 Les systèmes de paiement par carte dits « interbancaires » correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. À l'inverse, les systèmes privatifs sont ceux pour lesquels il existe un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs.

G9 Taux de fraude des cartes françaises



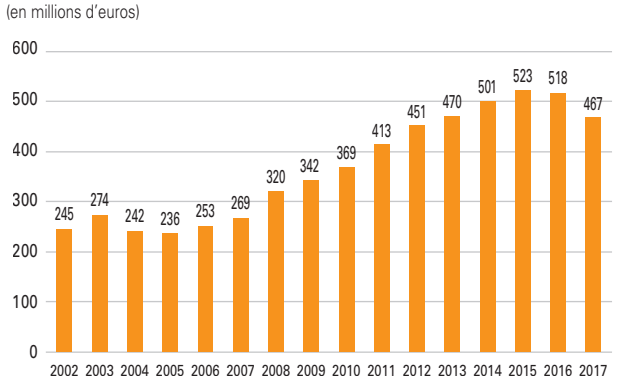
Source : Observatoire de la sécurité des moyens de paiement.

G10 Montant des transactions traitées dans les systèmes français, cartes françaises et étrangères



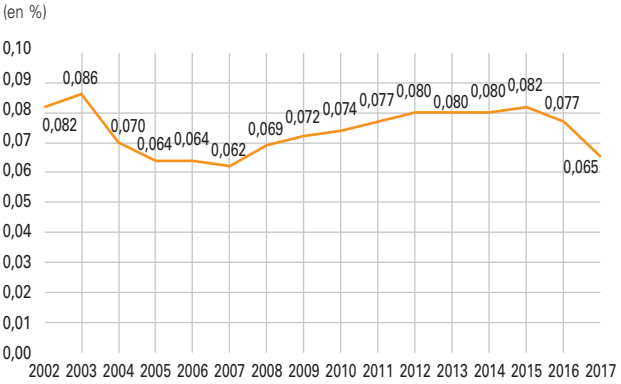
Source : Observatoire de la sécurité des moyens de paiement.

G11 Montant de la fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères



Source : Observatoire de la sécurité des moyens de paiement.

G12 Taux de fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères



Source : Observatoire de la sécurité des moyens de paiement.

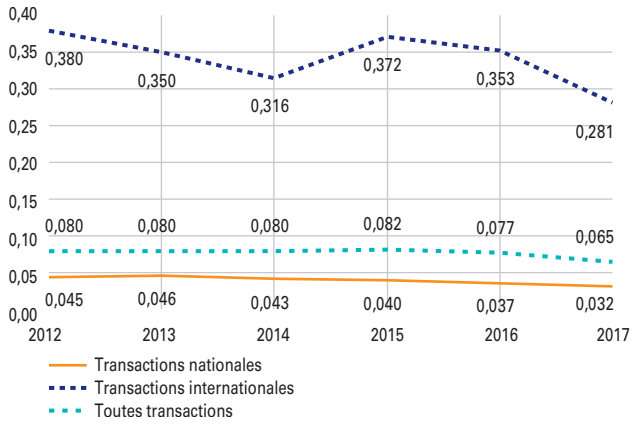
Sur la base de ces éléments, le taux de fraude global sur les transactions par carte traitées dans les systèmes monétiques français, comprenant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises ainsi que ceux effectués en France avec des cartes étrangères, se replie sensiblement à 0,065 %, contre 0,077 % en 2016, soit son plus bas niveau depuis 2008 (cf. graphique 12 *supra*).

Enfin, le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2017 s'élève à 1 213 008, ce qui représente une progression

de 6,5 % par rapport à 2016. Cette hausse s'accompagne toutefois d'une baisse significative du montant unitaire des cas de fraude à 84 euros en 2017, contre 95 euros en 2016. Le phénomène s'explique par une meilleure performance des mesures déployées pour sécuriser les paiements par carte (authentification renforcée des paiements en ligne, systèmes d'analyse de risque et de *scoring* des transactions, alertes SMS aux porteurs, etc.), et donc une détection et une désactivation plus rapides des cartes compromises. Ce renforcement de mesures de prévention a conduit les fraudeurs à devoir multiplier les tentatives de fraude, tout en réduisant leur montant unitaire pour tenter d'échapper aux mécanismes de détection.

G13 Taux de fraude par zone géographique

(en %)



Source : Observatoire de la sécurité des moyens de paiement

Répartition de la fraude par zone géographique

La tendance à la baisse de la fraude sur les transactions nationales, amorcée en 2014, se poursuit en 2017. Le montant de la fraude sur les transactions de paiement et de retrait effectuées en France avec des cartes françaises a diminué de 17,5 millions d'euros (soit – 8,1 % par rapport à 2016), ramené ainsi à 199,7 millions d'euros. Le taux de fraude sur les transactions nationales s'établit à un niveau bas de 0,032 %, contre 0,037 % en 2016.

En ce qui concerne les transactions internationales [2], la fraude est également en recul de 11 % par rapport à 2016, avec un montant total de fraude s'élevant à 267,3 millions d'euros. Le taux de fraude sur les transactions internationales ressort à 0,281 %, contre 0,353 % en 2016. C'est son plus bas niveau sur la période 2012–2017, et cela en parallèle d'une croissance des transactions internationales de l'ordre de 12 % par rapport à 2016. Néanmoins, ce taux de fraude reste toujours élevé au regard du montant des opérations concernées. Ainsi, les transactions internationales représentent 57 % du montant total de la fraude alors qu'elles ne comptent que pour 13 % de la valeur totale des transactions. Par ailleurs, on continue d'observer, pour les transactions internationales, une meilleure maîtrise de la fraude sur les opérations réalisées au sein de la zone SEPA [3] que sur celles effectuées avec les pays situés hors de celle-ci :

- pour les cartes françaises, le taux de fraude sur les transactions effectuées

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

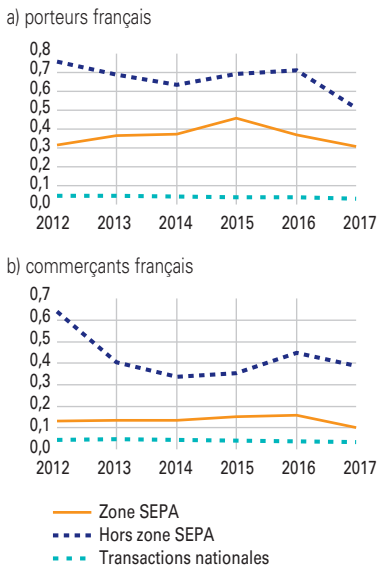
3 La zone SEPA comprend les 28 pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande et Saint-Martin.

hors de l'espace européen SEPA (0,511 %) est plus d'une fois et demie supérieur à celui des transactions réalisées au sein de la zone SEPA (0,308 %) ;

• pour les cartes étrangères, le taux de fraude sur les transactions effectuées en France avec des cartes émises hors de l'espace européen SEPA (0,386 %) est près de quatre fois supérieur à celui des transactions réalisées en France avec des cartes émises au sein de la zone SEPA (0,102 %).

G14 Taux de fraude par zone géographique

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Ces résultats récompensent les efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et terminaux de paiement vers le standard EMV (Europay Mastercard VISA) [4] et pour renforcer la sécurité des paiements sur internet [5].

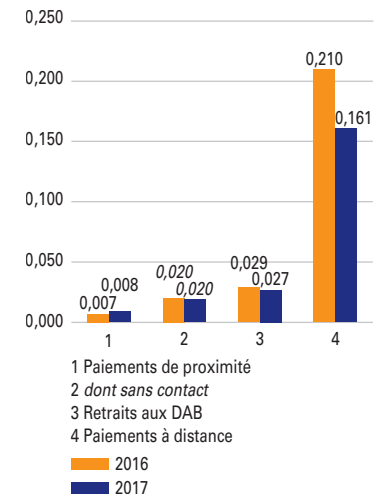
Répartition de la fraude par type de transaction

Fraude sur les transactions nationales

La baisse de la fraude sur les transactions nationales résulte principalement de celle enregistrée sur les paiements à distance, soit une diminution de 13,3 % par rapport à 2016, alors que le montant des transactions à distance progresse de 15,7 % en 2017. Le taux de fraude sur les paiements à distance s'inscrit donc en forte baisse, pour la sixième année consécutive à 0,161 %, contre 0,210 % en 2016. Cette amélioration continue résulte des efforts de sécurisation des émetteurs et des commerçants pour déployer des dispositifs d'authentification forte (tels 3D-Secure), ainsi que des outils d'analyse de risque et de *scoring* des transactions. Néanmoins, si la fraude sur les paiements à distance diminue, elle représente toujours la majeure partie de la fraude nationale (66,1 % du montant total), avec un taux de fraude qui reste près de vingt fois supérieur à celui sur les paiements de proximité.

G15 Comparaison des taux de fraude par type de transaction, transactions nationales

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

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

5 Les orientations de l'Autorité bancaire européenne visant au renforcement de la sécurité des paiements sur internet sont entrées en vigueur en août 2015.

Encadré 2

Fraude aux paiements sans contact

Les paiements sans contact sont en plein essor au niveau national, avec une multiplication par deux du nombre et des montants de transactions entre 2016 et 2017. Ainsi, sur l'ensemble de l'année 2017, un peu plus 1,2 milliard de paiement sans contact ont été enregistrés (contre 628,5 millions en 2016) pour un montant total de 12,9 milliards d'euros (contre 6,5 milliards d'euros en 2016). Cela représente 12 % en volume et 3 % en valeur des paiements par carte en situation de proximité. Le montant moyen d'un paiement sans contact s'établit à 10,2 euros en 2017.

Si l'on ajoute aux paiements nationaux sans contact ceux réalisés en France au moyen de cartes étrangères et ceux effectués avec des cartes françaises à l'étranger, le montant total des transactions sans contact s'élève à 13,8 milliards d'euros pour 1,3 milliard d'opérations.

Cette évolution s'est accompagnée d'une confirmation de la stabilité du taux de fraude sur les transactions nationales à 0,020 %, avec un montant total de fraude de près de 2,8 millions d'euros. Le taux de fraude sur les paiements sans contact se situe toujours à un niveau intermédiaire entre celui des paiements de proximité (0,008 %) et celui des retraits (0,027 %), bien en-deçà de celui des paiements à distance (0,161 %). Si l'on ajoute à cette fraude nationale celle engendrée sur les paiements sans contact effectués par des cartes françaises à l'étranger et ceux réalisés par des cartes françaises à l'étranger, le taux de fraude ressort au même niveau, soit à 0,020 %.

En 2017, la fraude sur les paiements sans contact résulte seulement du vol ou de la perte de la carte. En effet, les émetteurs de carte fixent des plafonds sur le montant d'une transaction unitaire (montant maximum généralement fixé entre 20 et 30 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (cumul généralement fixé à 100 euros). Ces mesures permettent de limiter le préjudice subi en cas de perte ou de vol d'une carte. Il est d'ailleurs rappelé que le porteur est protégé par la loi en cas de fraude et ne supporte aucune perte (cf. annexe 2).

Ces données intègrent les paiements par mobile, qui progressent également bien que leur part dans les transactions de proximité demeure encore marginale (0,03 % des transactions nationales de proximité). En 2017, les transactions nationales par mobile représentent ainsi 4,4 millions d'opérations, soit quinze fois le volume de 2016, et un montant total de près de 83,5 millions d'euros, contre 4,4 millions d'euros en 2016. Avec les transactions effectuées en France par des mobiles étrangers et celles réalisées à l'étranger par des mobiles français, le montant total des transactions par mobile s'élève à près de 123 millions d'euros pour 6,3 millions d'opérations.

En 2017, aucune fraude n'a été enregistrée sur les transactions nationales par mobile. Pour les transactions internationales, des cas de fraude ont été enregistrés, pour un montant total toutefois peu significatif de 31 715 euros. Le taux de fraude sur le paiement mobile, toutes zones confondues, s'établit ainsi à un niveau quasiment équivalent à celui des paiements sans contact par carte, à 0,026 %.

Encadré 3

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

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

Répartition de la fraude par secteur d'activité

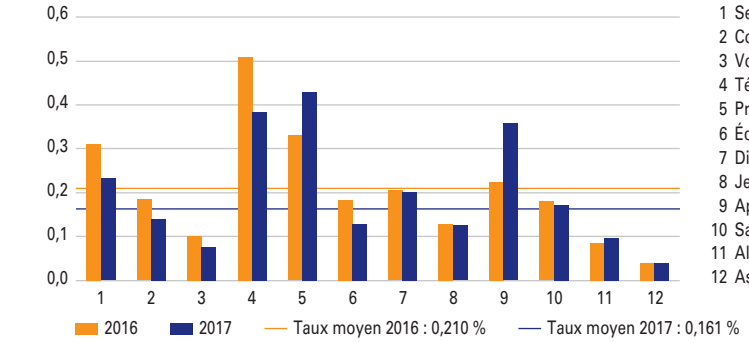
(montant en millions d'euros, part en pourcentage)

		Montant	Part
1	Services aux particuliers et aux professionnels	32,6	24,7
2	Commerce généraliste et semi-généraliste	28,4	21,5
3	Voyage, transport	19,7	14,9
4	Téléphonie et communication	19,0	14,4
5	Produits techniques et culturels	10,6	8,0
6	Équipement de la maison, ameublement, bricolage	6,5	4,9
7	Divers	5,0	3,8
8	Jeu en ligne	4,2	3,2
9	Approvisionnement d'un compte, vente de particulier à particulier	2,9	2,2
10	Santé, beauté, hygiène	1,3	1,0
11	Alimentation	1,2	0,9
12	Assurance	0,5	0,4
Total		**131,9**	**100,0**

Les secteurs « Services aux particuliers et aux professionnels », « Commerce généraliste et semi-généraliste », « Voyage et transport » et « Téléphonie et communication » demeurent toujours les plus exposés, concentrant à eux seuls 75,5 % du montant total de la fraude en vente à distance. Néanmoins, ces quatre secteurs affichent des taux de fraude en baisse par rapport à 2016. Si le secteur « Téléphonie et communication » conserve quant à lui un taux de fraude très supérieur à la moyenne (0,384 %), ce dernier est bien inférieur aux taux observés en 2015 et 2016 (soit plus de 0,5 %). Le secteur « Produits techniques et culturels » affiche un taux de fraude en hausse pour s'établir à 0,429 %, soit au niveau le plus élevé par rapport à tous les secteurs.

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

(en %)



1 Services aux particuliers et aux professionnels
2 Commerce généraliste et semi-généraliste
3 Voyage, transport
4 Téléphonie et communication
5 Produits techniques et culturels
6 Équipement de la maison, ameublement, bricolage
7 Divers
8 Jeu en ligne
9 Approvisionnement d'un compte, vente de particulier à particulier
10 Santé, beauté, hygiène
11 Alimentation
12 Assurance

Source : Observatoire de la sécurité des moyens de paiement.

En ce qui concerne les retraits, le taux de fraude est en léger recul pour s'établir à 0,027 %, contre 0,029 % en 2016. Cette baisse s'explique principalement par la forte diminution du nombre de piratages de distributeurs automatiques de billets en 2017 (63, contre 301 en 2016), en particulier avec la technique du *skimming* [6] suite à la migration de certains pays vers la norme EMV. Ces appareils restant cependant toujours des cibles privilégiées pour les réseaux de fraude organisés, l'Observatoire maintient ses conseils de prudence aux porteurs et rappelle les bonnes pratiques à suivre lors d'une opération de paiement chez un commerçant ou lors d'un retrait (cf. annexe 1).

À l'inverse, la fraude sur les paiements de proximité et sur automate enregistre une légère progression par rapport à 2016, avec un taux de fraude qui reste toutefois très faible à 0,008 %, contre 0,007 % en 2016. La légère hausse observée est en partie imputable à la croissance des paiements sans contact, dont le taux de fraude est sensiblement plus élevé (cf. encadré 2 *supra*). Ces paiements représentent près des deux tiers du montant des transactions nationales (66 %), pour seulement 17,7 % du montant de la fraude nationale.

Fraude sur les transactions internationales

La fraude sur les transactions réalisées par les cartes françaises à l'étranger enregistre un repli pour la deuxième année consécutive.

- Le montant total de la fraude baisse de 11,6 % pour celles effectuées au sein de l'espace européen SEPA (100,6 millions d'euros, contre 113,8 millions d'euros en 2016). Toutefois, les évolutions par type de transaction sont contrastées : le taux de fraude sur les paiements à distance s'est amélioré (0,591 % en 2017, contre 0,754 % en 2016), tandis que celui sur les paiements de proximité et sur automate s'est dégradé, passant de 0,066 % en 2016 à 0,075 % en 2017. Pour les paiements à distance, la diminution de la fraude s'explique par la perspective de l'entrée en vigueur, en janvier 2018, de la deuxième directive sur les services de paiement qui prévoit le recours systématique à l'authentification forte du porteur (cf. chapitre 1), comme par la généralisation des systèmes d'analyse de risque et de *scoring* des transactions.

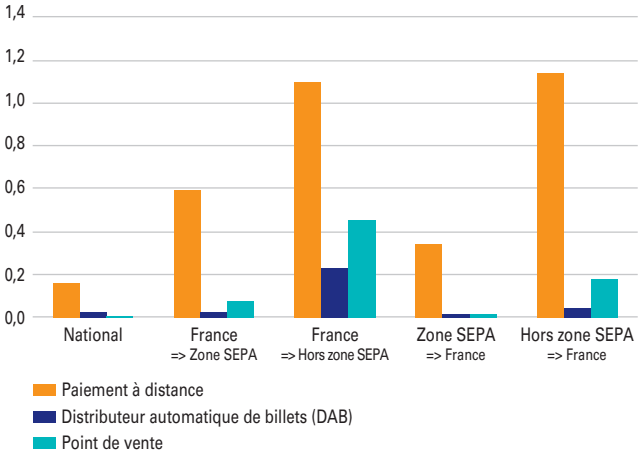
- La même tendance à la baisse est observée pour les transactions réalisées par les cartes françaises en dehors de l'espace européen SEPA, avec un montant total de fraude en diminution de 11,3 % (60,3 millions d'euros contre 68 millions d'euros en 2016). Les taux de fraude sont en recul pour l'ensemble des types de transaction et celui portant sur les paiements à distance demeure le plus élevé (1,096 %).

Par ailleurs, concernant les transactions réalisées en France par des cartes étrangères, on observe un taux de fraude particulièrement élevé (1,143 %) pour les paiements à distance effectués avec des cartes émises hors de l'espace européen SEPA.

6 La technique du *skimming* consiste à capturer les données magnétiques des cartes au moyen d'un module additionnel (appelé *skimmer*) installé par le fraudeur dans les DAB (ou dans des terminaux de paiement isolés, comme par exemple des distributeurs de carburant, péages, etc.). Le code PIN du porteur n'étant pas écrit sur la piste magnétique, le *skimming* s'accompagne le plus souvent de dispositifs (caméras ou claviers modifiés par exemple) permettant d'obtenir frauduleusement le PIN du porteur de la carte lors de sa saisie. Ces données capturées sont ensuite utilisées par le fraudeur, soit en réalisant des transactions à distance dans des pays ou des sites ne demandant pas systématiquement la saisie du cryptogramme visuel situé au dos de la carte ou une authentification renforcée du porteur, soit en réalisant des transactions de proximité ou des retraits dans les pays où la norme EMV n'a pas été déployée.

G16 Taux de fraude par type de transaction et origine géographique

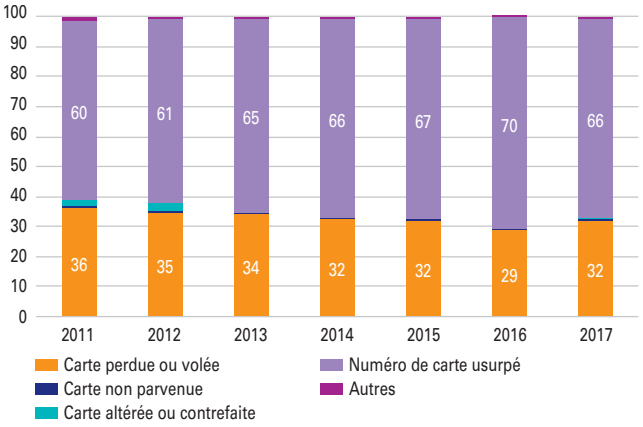
(en %)



Note de lecture : Cf. annexe 5.
Source : Observatoire de la sécurité des moyens de paiement.

G17 Répartition de la fraude aux paiements par carte selon sa typologie

(en %)



Note : Transactions nationales hors retraits, en valeur.
Source : Observatoire de la sécurité des moyens de paiement.

Répartition de la fraude par type de transaction

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux reste toujours la principale origine de la fraude (66 % en montant), en baisse toutefois par rapport à 2016. Les techniques de fraude les plus utilisées pour usurper les numéros de cartes demeurent celles de l'hameçonnage ou *phishing* [7], et des logiciels malveillants (*malwares*) [8]. On note que, en raison des mesures prises par les banques et les opérateurs de téléphonie, celles reposant sur les *swaps* de carte SIM [9]

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

8 Les logiciels malveillants visent 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. Ces logiciels malveillants son généralement inoculés, à l'insu de l'utilisateur, au travers de sources apparemment de confiance.

9 Le *swap* de carte SIM est la technique du *phishing* où le fraudeur simule le site d'un opérateur mobile pour détourner la ligne téléphonique de la victime afin de se faire remettre une nouvelle carte SIM qui lui permettra de recevoir les SMS d'authentification des paiements.

Encadré 4

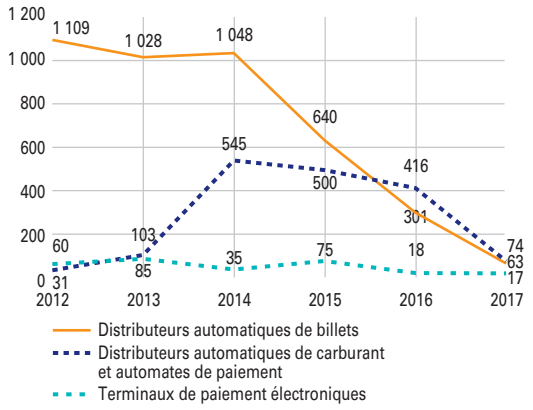
Indicateurs des services de police et de gendarmerie

Le nombre de piratages de distributeurs automatiques de billets (DAB) est en très forte baisse en 2017, avec 63 cas (contre 301 cas en 2016) confirmant ainsi la baisse amorcée en 2015 après des niveaux particulièrement élevés enregistrés les années précédentes (environ 1 000 cas par an entre 2012 et 2014). En 2017, il est observé une forte réduction des compromissions de DAB par la technique du « *skimming* » au profit d'une autre appelée « *jackpotting* ». Celle-ci consiste à prendre le contrôle d'un distributeur en y connectant un ordinateur portable et ainsi accéder aux données du calculateur du distributeur ou lui injecter un *malware*.

À ces attaques de DAB s'ajoutent 91 piratages ciblant les points de vente (contre 434 en 2016), dont 74 piratages de distributeurs automatiques de carburant (DAC) et 17 de terminaux de paiement chez les commerçants et automates de paiement (tels les bornes de parking).

Nombre d'infractions constatées sur les distributeurs et terminaux

(en unités)



Source : Observatoire de la sécurité des moyens de paiement.

La baisse du nombre d'infractions sur l'ensemble des points de compromission s'explique par la migration vers la norme EMV de plus de pays situés hors de la zone Europe ainsi que par le renforcement significatif des mesures de sécurité physique sur les terminaux.

sont en diminution. La perte ou vol de carte constitue la deuxième origine de la fraude et représente près du tiers de la fraude sur les transactions nationales (32 %).

La contrefaçon de cartes n'est à l'origine que de 1 % des paiements nationaux frauduleux. Ce niveau très bas s'explique principalement par l'adoption de technologies de cartes à puce par le plus grand nombre de systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes.

Suivi du déploiement de l'authentification forte

Le développement du commerce en ligne a entraîné un usage croissant de la carte pour les paiements à distance, configuration dans laquelle l'impossibilité de recourir à la sécurité embarquée physiquement dans la carte (lecture de la puce et saisie du code confidentiel) nécessite la mise en œuvre d'autres mécanismes de protection des transactions. Dans ce contexte, les recommandations émises dès 2008 par l'Observatoire de la sécurité des

cartes de paiement afin de renforcer la sécurité du paiement à distance portent sur la généralisation des dispositifs d'authentification forte. Ces recommandations font l'objet d'un suivi statistique depuis 2011.

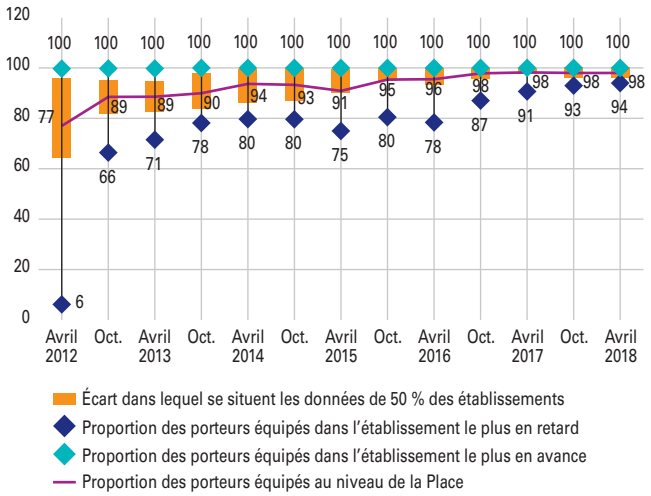
Pour la période de novembre 2017 à avril 2018, le suivi statistique du déploiement des solutions d'authentification réalisé par l'Observatoire auprès des principaux établissements bancaires porte sur un volume de 64,5 millions de cartes de paiement et 55 milliards d'euros de transactions en valeur (dont 22,7 milliards d'euros sécurisés par le dispositif « 3D-Secure ») permettant de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification renforcée.

L'année 2018 vient confirmer l'achèvement du processus d'équipement des porteurs en authentification forte constaté l'année précédente, avec un taux moyen en 2017 de 98 %, permettant de couvrir la totalité des porteurs susceptibles de réaliser des transactions sur internet.

Du côté des e-commerçants, le taux d'équipement en dispositif d'authentification forte continue à progresser pour s'établir à 72,8 %, dans le

G18 Distribution du taux d'équipement des porteurs en dispositif d'authentification forte

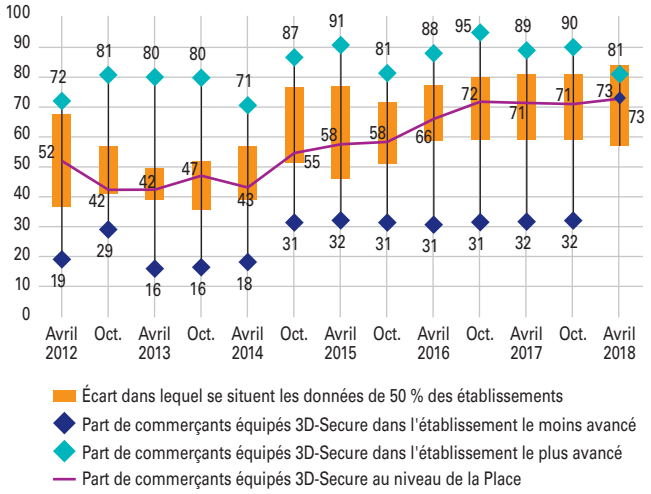
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G19 Distribution du taux d'équipement des commerçants en dispositif 3D-Secure

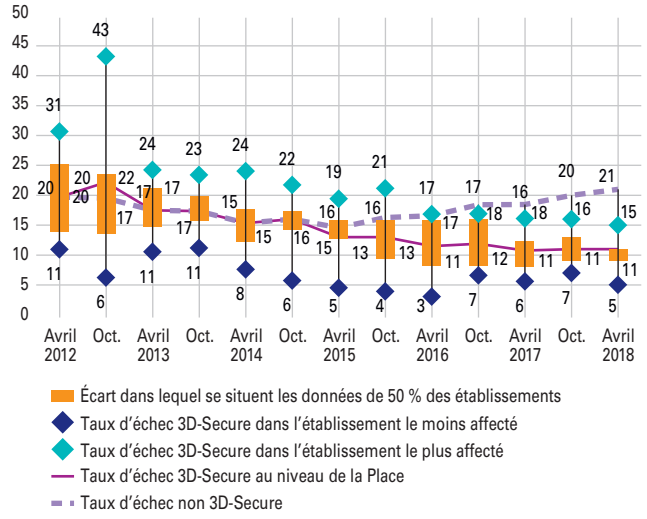
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G20 Distribution du taux d'échec 3D-Secure

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

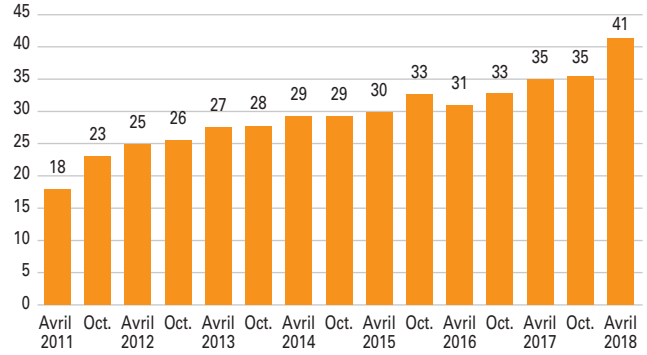
prolongement des hausses constatées au cours des trois dernières années.

L'Observatoire constate une poursuite de la baisse du taux d'échec sur les transactions authentifiées qui devient inférieur à 11 % et reste sensiblement inférieur à celui des transactions non authentifiées, ce qui permet de souligner la bonne appropriation de ces dispositifs par les particuliers. Cela reflète également la plus grande efficacité des contrôles réalisés sur les sites équipés de l'authentification forte, laquelle pousse les fraudeurs à privilégier par défaut des sites non équipés.

Compte tenu de ces différentes évolutions favorables au développement du recours à l'authentification forte, la proportion de paiements en ligne authentifiés 3D-Secure poursuit une progression continue depuis 2011, pour atteindre 41 % des montants de paiement par carte à distance.

G21 Part du montant total des paiements en ligne authentifiés par 3D-Secure

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Le taux de fraude sur les transactions nationales authentifiées par le protocole 3D-Secure ressort à 0,06 % pour l'année 2017. Ce niveau est plus proche du taux de fraude observé sur la totalité des transactions nationales y compris de proximité (0,032 %), que du taux de fraude sur l'ensemble des paiements à distance (0,161 %). Cette hiérarchie des taux de fraude conforte la stratégie de recours à l'authentification forte du porteur promue depuis 2008 par l'Observatoire. Par ailleurs, cette stratégie est inscrite dans les exigences de la deuxième directive européenne sur les services de paiement (DSP2), entrée en vigueur

en France le 13 janvier 2018 et dont les dispositions sur ce sujet prendront effet en septembre 2019 (cf. chapitre 1).

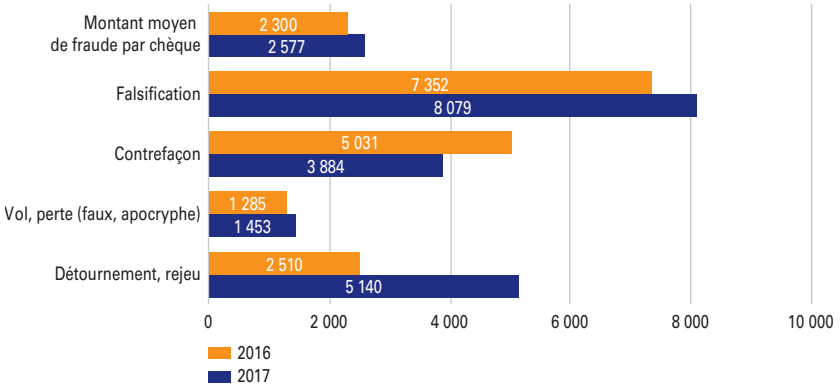
2.3 État de la fraude sur le chèque

Vue d'ensemble

En 2017, le chèque est le seul moyen de paiement à connaître une hausse des montants fraudés, lesquels atteignent 296 millions d'euros, soit une progression annuelle de 9 %. Dans un contexte de diminution des flux de paiement par chèque, le taux de fraude enregistre une hausse : il est à 0,029 % en 2017, contre 0,025 % en 2016. Ces données consolident la place du chèque comme deuxième moyen de paiement le plus fraudé après la carte de paiement (respectivement 40 % et 48 % de la fraude aux moyens de paiement scripturaux en montant), pour une utilisation pourtant beaucoup moins intensive. En effet, le chèque n'est que le quatrième moyen de paiement scriptural en nombre de paiements

G23 Montant unitaire de fraude par chèque, par typologie de fraude, 2016–2017

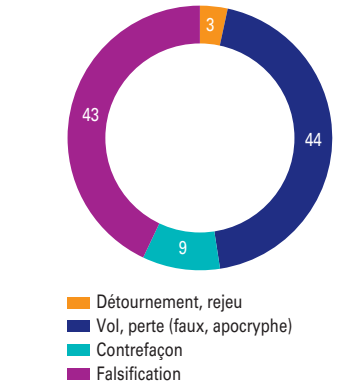
(en euros)



Source : Observatoire de la sécurité des moyens de paiement.

G22 Répartition de la fraude par chèque en montant par typologie de fraude

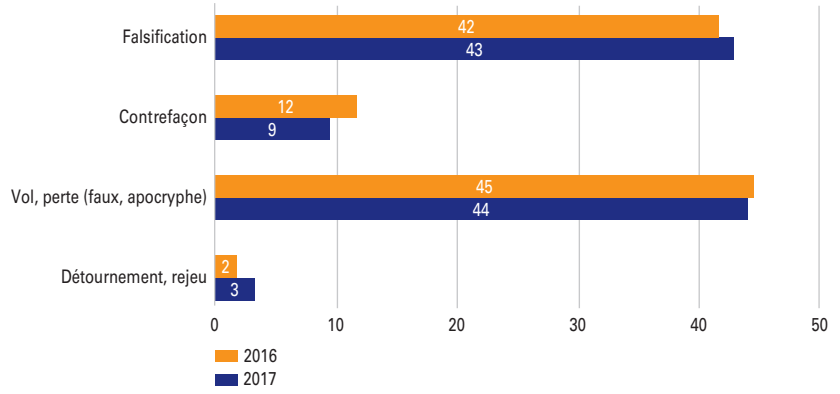
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G24 Répartition de la fraude par chèque en montant, par typologie de fraude, 2016–2017

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Principaux cas de fraude	Mesures de prévention
Vol de chéquiers dans les circuits de distribution : les circuits de distribution font intervenir de nombreux prestataires extérieurs aux banques, notamment pendant le transport ou lors de la remise au client. Le vol de chéquiers ou de formules de chèques vierges peut se produire à deux niveaux : • en amont de la délivrance au client : chez les prestataires fabricants et/ou expéditeurs, chez les prestataires transporteurs ou distributeurs vers les agences bancaires, dans les boîtes à lettres des clients bénéficiaires, • lors de la remise en agences bancaires, les fraudeurs utilisent des pièces d'identité volées ou falsifiées pour se faire remettre un chéquier. **Vol de chéquiers lors de la détention par le client lui-même** faisant suite à un cambriolage, au vol ou à la perte de son chéquier.	**Traçabilité des envois** de chéquiers et lettres chèques durant les phases de transport. **Information par la banque de la mise à disposition d'un chéquier**, soit en agence bancaire, soit par pli postal selon l'option définie par le client lors de la souscription au moyen de paiement, et indication d'un délai attendu de mise à disposition, permettant au client d'informer sa banque en cas de retard constaté. **Rappel régulier par les banques des obligations de vigilance** des détenteurs de chéquiers et lettres chèques et de l'obligation de déclaration en cas de perte ou de vol, même en cas de souscription d'une assurance couvrant ces événements.
Falsification d'un chèque régulier intercepté par les fraudeurs, consistant à altérer le chèque subtilisé par grattage, gommage ou effacement, se manifeste par le fait que, concrètement, les fraudeurs tirent profit des vulnérabilités présentes sur le chèque subtilisé pour le modifier, par exemple : • en substituant, par grattage ou gommage, le nom du bénéficiaire légitime inscrit avec une encre faible, • en réécrivant un nom de bénéficiaire sur celui du bénéficiaire légitime, • en ajoutant une mention (par exemple nom ou sigle, tampon de société, etc.) après celui du bénéficiaire légitime sur l'espace libre de la ligne non remplie, • en ajoutant un montant en lettres et/ou en chiffres sur l'espace libre laissé avant ou après la mention manuscrite.	**Examen systématique du chèque et des mentions portées, ainsi que de leur cohérence avec l'identité du payeur.** Il s'agit de réaliser un examen physique du chèque afin d'identifier les éventuelles altérations avant son acceptation, ainsi que de contrôler l'identité du payeur, *via* la demande par exemple d'une pièce d'identité ou d'un justificatif de domicile. **Les commerçants peuvent se prémunir des chèques irréguliers en accédant au fichier national des chèques irréguliers (FNCI)** de la Banque de France, service officiel de prévention des impayés chèques [1].
Contrefaçon de chèque, en créant un faux chèque de toutes pièces, émis sur une banque existante ou une fausse banque.	**Examen physique approfondi du chèque et des documents d'identité du payeur** (cf. ci-dessus).
Techniques de fraude dérivées du processus dit de « **cavalerie** » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement de virements des fonds crédités, et visant principalement les comptes de professionnels et d'entrepreneurs bénéficiant de mécanismes de crédit en compte immédiat des chèques remis à l'encaissement.	**Identification des flux d'encaissement atypiques** au regard du profil du client afin de suspendre, le cas échéant, les opérations de retrait ou de transfert des fonds vers un autre établissement, immédiatement consécutives à une remise de chèques.

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

annuel. Par ailleurs, il est utilisé 6,5 fois moins souvent que la carte. Dans ce contexte, l'Observatoire réitère ses recommandations, reprises ci-dessous, afin de limiter la fraude sur ce moyen de paiement. Comme en 2016, deux catégories de fraude concentrent à parts égales la majeure partie des montants

fraudés en 2017 : d'une part, l'utilisation frauduleuse de chèques perdus ou volés (44 % du total de la fraude sur le chèque), et d'autre part la falsification d'un chèque régulièrement émis (43 %). La fraude par contrefaçon de chèques et celle par détournement/rejeu continuent de s'inscrire à des niveaux bien moindres (respectivement 9 % et 3 % de la fraude chèque).

Le montant moyen d'un chèque fraudé remis à l'encaissement est en légère progression, à 2 577 euros, contre 2 300 euros en 2016. En-dehors de la contrefaçon de chèque, dont le montant unitaire moyen est en baisse, la fraude au chèque se caractérise par une progression des montants unitaires, soit 8 079 euros pour les chèques détournés (contre 7 352 euros en 2016) et 1 453 euros pour les chèques perdus et/ou volés (contre 1 285 euros en 2016).

2.4 État de la fraude sur le virement

Vue d'ensemble

En 2017, le montant total de la fraude sur les virements émis depuis un compte tenu en France s'élève à 78 millions d'euros, en baisse de 9 %, dans un contexte de croissance modérée des flux de paiement associés. En conséquence, le taux de fraude en montant pour ce moyen de paiement s'établit à 0,0003 %, contre 0,0004 % en 2016. Ces données confirment que le virement est le moyen de paiement scriptural le moins fraudé en proportion, alors qu'il est celui qui véhicule les montants globaux les plus importants (87 % du total des paiements scripturaux émis en France). Le montant moyen d'un virement frauduleux s'établit à 16 884 euros, soit un montant en légère progression par rapport à 2016 (15 500 euros).

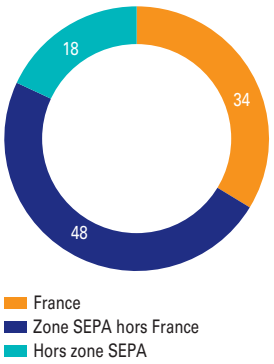
Les virements transfrontaliers subissent en proportion une fraude plus importante que les virements nationaux, et représentent près de 66 % des montants fraudés alors que les transactions transfrontalières ne comptent que pour 30 % des virements émis en montant.

La catégorisation des virements frauduleux a fait l'objet de travaux méthodologiques permettant d'assurer une meilleure comptabilisation des données (cf. annexe 5). Sur ces bases, le faux virement, c'est-à-dire l'émission d'un ordre de virement par le fraudeur au moyen d'attaques informatiques, reste le type de fraude prédominant (54 % du montant total de la fraude aux virements), suivi par le détournement (42 %).

La fraude au virement est répartie de façon relativement équilibrée entre les différents canaux d'utilisation de ce moyen de paiement : l'initiation de virement depuis l'espace de banque en ligne (sur internet ou *via* application mobile) reste le canal le plus

G25 Répartition de la fraude au virement en montant, par zone géographique

(en %)



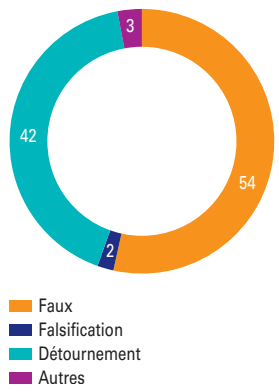
Source : Observatoire de la sécurité des moyens de paiement.

Cas de fraude rencontrés	Mesures de prévention
En 2017, la fraude de type **détournement au moyen de techniques d'ingénierie sociale** a revêtu essentiellement les formes exposées ci-après. • **La fraude au président :** le fraudeur usurpe l'identité d'un haut responsable de l'entreprise pour obtenir d'un collaborateur la réalisation d'un virement urgent et confidentiel à destination de l'étranger. Pour ce faire, le fraudeur utilise des informations recueillies sur l'entreprise et ses dirigeants sur internet ou directement auprès des services de l'entreprise. • **La fraude aux coordonnées bancaires :** le fraudeur usurpe l'identité d'un fournisseur, bailleur ou autre créancier, et prétexte auprès du client, locataire ou débiteur, un changement de coordonnées bancaires aux fins de détourner le paiement des factures ou loyers. Le fraudeur envoie les nouvelles coordonnées bancaires par courrier électronique ou avec un courrier en bonne et due forme du créancier. • **La fraude au faux technicien :** le fraudeur usurpe l'identité d'un technicien informatique (de la banque, par exemple) pour effectuer des faux tests dans le but de récupérer des identifiants de connexion, provoquer des virements frauduleux ou encore procéder à l'installation de logiciels malveillants. • **La fraude au faux conseiller bancaire :** le fraudeur usurpe le numéro de téléphone du conseiller bancaire, généralement en période d'absence de ce dernier, et contacte le client pour obtenir des informations.	**Outils de surveillance et de détection des transactions à caractère inhabituel** qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison par exemple de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Un contre-appel auprès du client peut alors être fait afin de vérifier le bien-fondé de l'ordre de virement. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des entreprises et des particuliers.
Les **attaques informatiques** ont principalement visé en 2017 les sites de banque en ligne et les canaux télématiques, tels que par exemple le système EBICS – *electronic banking internet communication standard* (canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque) et ont été réalisées essentiellement par deux moyens. • ***Malwares*** : des logiciels malveillants (tels que les troyens, les *spammeurs*, les virus, etc.) qui s'installent sur l'ordinateur d'une entreprise ou d'un particulier à son insu lors de l'ouverture d'un courriel frauduleux, de la navigation sur des sites infectés ou encore lors de la connexion de périphériques infectés (clé USB par exemple). Ces *malwares* permettent à des fraudeurs d'analyser et de collecter les données transitant par l'ordinateur ou le système d'information du client. Ainsi, lors de la connexion au site de banque en ligne d'un client, le *malware* récupère les identifiant et mot de passe que le client a saisis puis les réutilise pour s'y connecter lui-même, faire une demande d'ajout de bénéficiaire et initier un ordre de virement frauduleux. • ***Phishing* ou hameçonnage** : technique permettant de collecter des données personnelles et bancaires à partir de courriels non sollicités invitant leurs destinataires à cliquer sur un lien renvoyant vers un faux site (celui d'une banque en ligne ou d'un marchand en ligne) lequel le plus souvent demande à l'internaute de communiquer ses coordonnées bancaires. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide (facture à régler sous peine de la suspension d'un service, régularisation d'une interdiction bancaire ou encore une mise à jour sécuritaire). Des variantes du *phishing* sur d'autres canaux sont également mises en œuvre, comme le *smishing* par SMS.	**Déploiement d'un dispositif d'authentification forte pour la validation des ordres de virement** saisis en ligne. **Mise en place d'une temporisation ou d'une authentification forte du client pour l'ajout de nouveaux bénéficiaires** de virement depuis le site de banque en ligne. **Fixation de plafonds maximaux de virements** sur le site de banque en ligne. **Mise à disposition aux clients de solutions informatiques de sécurisation** permettant la recherche d'infections de type *malware* sur les postes de la clientèle. **Outils de surveillance et de détection** des transactions à caractère inhabituel qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison, par exemple, de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Une alerte peut être adressée au client pour lui permettre de faire opposition à la transaction, le cas échéant, pendant la durée de temporisation. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des particuliers.

touché mais dans des proportions moindres qu'en 2016 (38 % des montants fraudés en valeur en 2017, contre 48 % en 2016), le solde étant réparti à parts égales entre les canaux télématiques sécurisés et les virements sur support papier (courrier, fax, etc.), soit 31 % des montants fraudés pour chacun de ces deux canaux. Toutefois, compte tenu d'un usage désormais très limité du support papier, qui représente moins de 10 % des émissions de virements en montant, le taux de fraude sur les ordres de virement papier ressort à 0,0011 %, soit un niveau 4,4 fois supérieur à celui des virements émis *via* un canal électronique (0,0002 %).

G26 Répartition de la fraude au virement en montant, par typologie de fraude

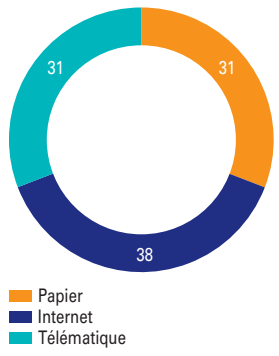
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G27 Répartition de la fraude au virement en montant, par canal de transmission

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Principaux cas de fraude en 2017 et mesures de prévention

Les principales techniques de fraude sur le virement constatées en 2017 sont la fraude par ingénierie sociale [10] et les attaques informatiques par *malware* et *phishing*. Après observation d'une baisse du nombre de cas de *phishing* en 2016, les établissements bancaires ont noté une inversion de tendance en 2017. Ainsi, malgré une amélioration des dispositifs de détection, les mails des fraudeurs sont désormais de meilleure qualité et peuvent plus facilement tromper les titulaires de comptes.

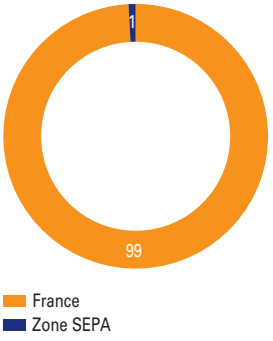
2.5 État de la fraude sur le prélèvement

Vue d'ensemble

En 2017, les prélèvements frauduleux émis au débit d'un compte tenu en France se sont chiffrés en montant à 9 millions d'euros contre 40 millions d'euros en 2016, soit une baisse conséquente de 78 %. Dans un contexte de croissance des flux de paiement, le taux de fraude pour le prélèvement s'établit ainsi en net repli à 0,0006 %, contre 0,0027 %, soit l'équivalent d'un euro de fraude pour environ

G28 Répartition de la fraude au prélèvement en montant par zone géographique

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

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

180 000 euros de prélèvements émis. Le montant moyen d'un prélèvement frauduleux s'établit également en très forte baisse, à 340 euros contre 34 000 euros en 2016.

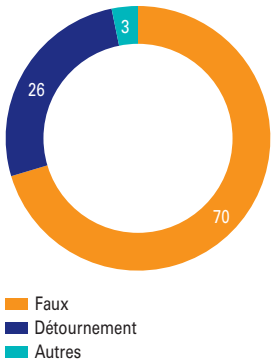
Si l'année 2016 avait été marquée par quelques cas ciblés de fraude de montant élevé, qui avaient impacté à la hausse le taux de fraude, cette baisse témoigne également de la mise en place de mécanismes avancés d'identification des ordres de prélèvement atypiques émis par des créanciers frauduleux.

La catégorisation des prélèvements frauduleux a fait l'objet de travaux méthodologiques permettant d'assurer une meilleure comptabilisation des données (cf. annexe 5). Sur ces bases, la fraude est largement imputable à l'émission de faux prélèvements (c'est-à-dire l'émission d'ordre de prélèvement sans mandat par des créanciers frauduleux) qui représentent 70 % du montant total de la fraude, le solde étant principalement constitué de cas de détournement (26 % des montants fraudés).

Enfin, la fraude sur le prélèvement reste concentrée sur les transactions nationales et reste toujours marginale sur les transactions transfrontalières avec la zone SEPA.

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

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

Principaux cas de fraude en 2017 et mesures de prévention

La principale technique de fraude sur le prélèvement constatée en 2017 est le faux prélèvement, qui consiste en l'émission d'ordres de prélèvement de façon illégitime et sans aucune autorisation ou réalité économique. Deux autres techniques de fraude ont été constatées mais dans une moindre mesure : il s'agit de l'usurpation de l'identité et de l'IBAN [11] d'un tiers par un fraudeur pour la souscription d'un service et de l'entente frauduleuse entre créancier et débiteur.

11 *International bank account number.*

Cas de fraude rencontrés	Mesures de prévention
Émission illégitime d'ordres de prélèvement (faux prélèvement) : le créancier fraudeur s'enregistre en tant qu'émetteur de prélèvement auprès d'un prestataire de services de paiement et émet massivement des prélèvements vers des IBAN qu'il a obtenus illégalement et sans aucune autorisation.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire. **Envoi d'une alerte aux clients débiteur** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »).
Usurpation d'IBAN pour la souscription de service (détournement) : le débiteur fraudeur communique à son créancier les coordonnées bancaires d'un tiers lors de la signature du mandat de prélèvement et bénéficie ainsi du service, sans avoir à en honorer les règlements prévus.	**Envoi d'une alerte aux clients débiteur** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays, ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »).
Entente frauduleuse entre créancier et débiteur : un créancier fraudeur émet des prélèvements sur un compte détenu par un débiteur complice de façon régulière et en augmentant progressivement les montants. Un peu avant la fin de la période de rétraction légale (de 13 mois après le paiement du prélèvement), le débiteur conteste les prélèvements qui ont été débités sur son compte, au motif qu'il n'a pas signé de mandats de prélèvement correspondants. Au moment des rejets des prélèvements, le solde du compte du créancier fraudeur ne permet plus le remboursement des opérations contestées car les fonds ont été transférés vers un compte tenu à l'étranger.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire.

3 La sécurité des moyens de paiement SEPA

3.1 Introduction

Les virements et les prélèvements paneuropéens SEPA [1] sont des moyens de paiement récents, dans la mesure où ils ont été introduits en 2013. Depuis le mois de février 2016 [2], ils se sont substitués entièrement et définitivement aux moyens de paiement équivalents qui existaient dans les différents pays de l'espace SEPA [3].

Les données statistiques collectées depuis 2016 par l'Observatoire permettent de souligner les faibles taux de fraude observés sur ces moyens de paiement (cf. chapitre 2, « L'état de la fraude en 2017 »). La fraude observée sur les instruments SEPA présente toutefois des spécificités. D'une part, ces instruments apparaissent plus exposés à la fraude transfrontalière qu'à la fraude domestique, à l'instar des cartes de paiement. D'autre part, ces moyens de paiement étant notamment utilisés pour les transactions des entreprises (telles que les paiements de salaire, les règlements des fournisseurs, etc.), les montants unitaires des transactions sont significativement plus élevés que pour le chèque et la carte. Cette caractéristique se répercute très logiquement sur les montants unitaires des cas de fraude.

Dans le cadre des travaux de promotion de l'usage des moyens de paiement SEPA comme alternative au chèque, le Comité national des paiements scripturaux (CNPS) a saisi l'Observatoire d'une étude de veille sur les dispositifs mis en œuvre pour en assurer la sécurité, au travers de deux axes d'analyse :

- le premier, en termes d'authentification du payeur dans la perspective de l'entrée en vigueur, à compter du 13 janvier 2018, de la deuxième directive européenne sur les services de paiement (DSP2), qui vise notamment à systématiser le recours aux dispositifs d'authentification forte pour toute opération de paiement initiée électroniquement par le payeur ;

- le second, au regard des dispositifs complémentaires de sécurité déployés par les émetteurs de moyens de paiement, tels que la protection des identifiants et des données sensibles, les mesures de temporisation appliquées à certaines opérations, ou encore la mise en place de solutions d'évaluation du niveau de risque des transactions.

Enfin, cette étude constitue le pendant, pour les instruments de paiement SEPA, des travaux conduits en 2015 et 2016 par l'Observatoire de la sécurité des cartes de paiement concernant respectivement les techniques d'authentification biométriques et les nouvelles technologies d'authentification pour les transactions par carte.

1 *Single euro payments area.*

2 Pour mémoire, la migration vers les instruments SEPA au niveau européen a été conduite en deux temps :

- la migration des virements et prélèvements nationaux, qui s'est achevée au 1er août 2014 ;

- la migration des produits dits « de niche », c'est-à-dire apparentés à des virements et des prélèvements et représentant moins de 10 % des volumes de paiement nationaux (en France, le titre interbancaire de paiement – TIP – et le télérèglement), qui s'est terminée au 1er février 2016.

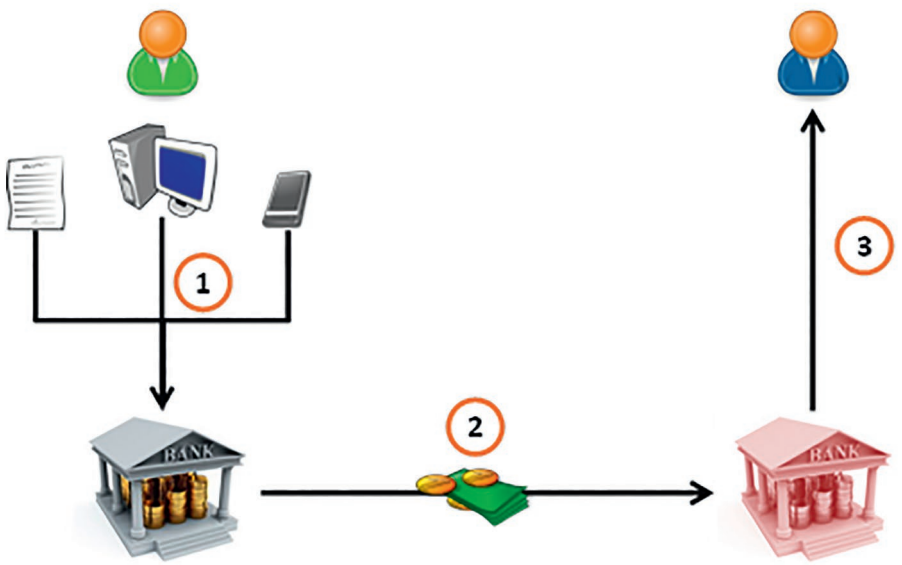
3 L'espace SEPA comprend les 31 membres de l'Espace économique européen (Union européenne, Liechtenstein, Islande et Norvège), ainsi que la Suisse, la Principauté de Monaco et Saint-Marin.

Le virement SEPA

Le virement SEPA, aussi appelé *SEPA credit transfer* (SCT), est un moyen de paiement fourni par l'établissement teneur du compte de paiement du payeur. Il consiste à créditer, sur la base d'une instruction du payeur ou d'un mandataire, le compte de paiement d'un bénéficiaire par une opération (virement unitaire) ou une série d'opérations (virement récurrent) réalisées à partir du compte de paiement du payeur.

Encadré 1

Cinématique d'utilisation du virement SEPA



1. Le payeur, titulaire du compte ou mandataire, établit l'ordre de virement indiquant notamment le compte à débiter, le numéro de compte (ou IBAN – *international bank account number*) à créditer, le montant, la date et la fréquence de l'opération si nécessaire et le transmet à son établissement teneur de compte.

2. L'ordre de virement est échangé dans les circuits de paiement interbancaire, entraînant le règlement des fonds vers l'établissement teneur du compte du bénéficiaire.

3. L'établissement teneur du compte du bénéficiaire crédite le compte destinataire identifié dans l'ordre de virement.

Une opération de virement ne donne pas droit à une garantie à remboursement systématique, c'est-à-dire la possibilité pour le payeur d'annuler *a posteriori* un ordre qu'il aurait lui-même validé. Seule exception, un droit à remboursement sous treize mois peut être exercé dans le cas d'une « opération non autorisée » [4] et considérée comme frauduleuse.

Depuis novembre 2017, les établissements européens ont la possibilité de proposer à leurs clients une variante du virement SEPA, appelée virement instantané (SCT Inst). Cet instrument, dont le fonctionnement est analogue à celui du virement SEPA, prévoit une confirmation des opérations sous 10 secondes à compter de l'échange de l'ordre de paiement et le crédit en compte immédiat du bénéficiaire.

Le prélèvement SEPA

Le prélèvement est un moyen de paiement dont la cinématique de fonctionnement est inversée par rapport au virement (cf. encadré 2) : les ordres de prélèvement sont émis par le payé – dénommé généralement « créancier » dans le cadre de ce moyen de paiement –, lequel doit préalablement s'assurer du consentement du payeur par la signature d'un mandat de prélèvement définissant les conditions d'émission des ordres de paiement par le créancier. Le mandat peut ainsi fixer des limitations en termes de montant ou de périodicité. À titre d'exemple, le titre interbancaire de paiement (TIP), ancien instrument de paiement national dont le fonctionnement s'apparentait pour l'utilisateur à la signature d'un chèque pré-rempli, a majoritairement été remplacé par un mandat de prélèvement SEPA à usage unique et montant prédéfini, toujours sous format papier, à retourner signé au créancier et désigné sous l'appellation commerciale « TIP SEPA ».

Le prélèvement SEPA, aussi appelé *SEPA direct debit* (SDD), se décline en deux instruments distincts, à savoir le prélèvement standard (ou SDD core), utilisé tant par les particuliers que les entreprises, et le prélèvement interentreprises (ou SDD B2B pour « *business to business* »), strictement réservé aux paiements entre professionnels.

Ces deux instruments, s'ils partagent une base technique commune, diffèrent sur plusieurs aspects, notamment en ce qui concerne leurs modalités de remboursement (cf. tableau *supra*).

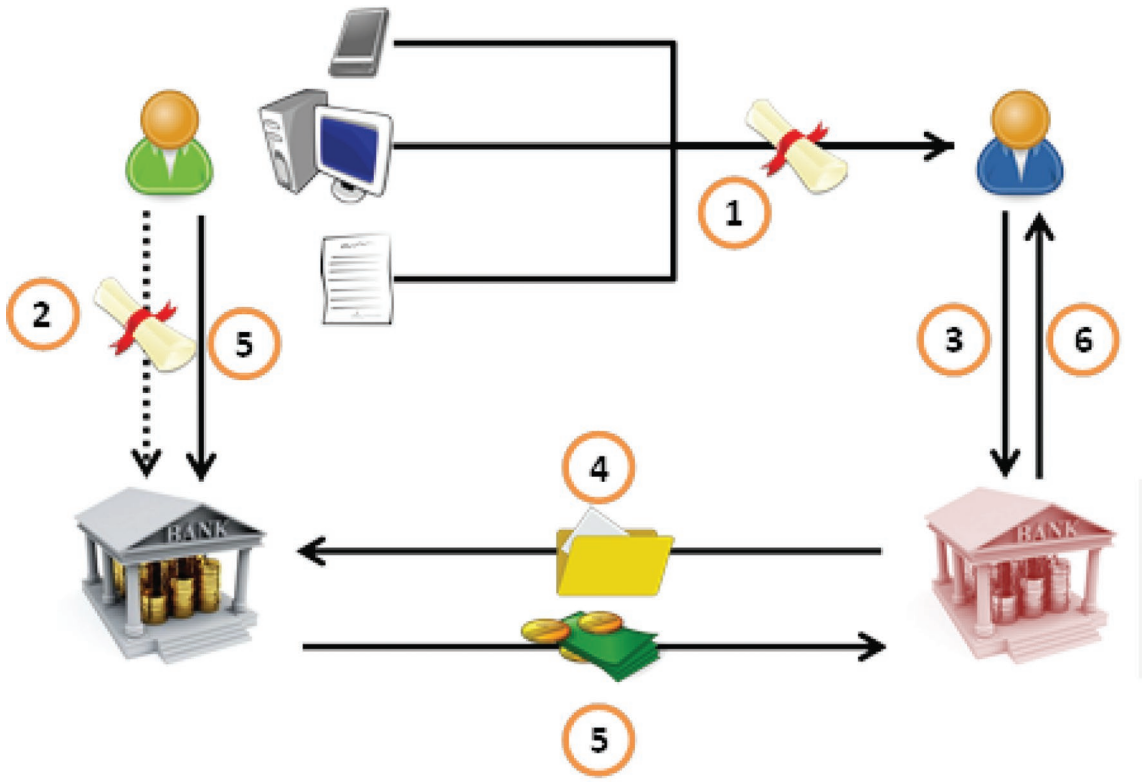
	SDD core	SDD B2B
Délai de contestation du débiteur	8 semaines qui suivent le débit	Aucun : le débiteur renonce par la signature du mandat B2B à contester les SDD reçus du créancier
Délai de contestation du débiteur pour absence de consentement	13 mois [a]	13 mois [b]

a) Une franchise de 50 euros (seuil de la DSP2 abaissé lors de la transposition) peut être appliquée en cas de contestation d'une opération.
b) Cette situation ne devrait pas se produire, sauf cas de faux mandat, dans la mesure où le débiteur doit préalablement fournir le mandat de prélèvement à son établissement teneur de compte.

4 L'article L. 133-6 du Code monétaire et financier explicite cette notion : « *Une opération de paiement est autorisée si le payeur a donné son consentement à son exécution* ». En complément, l'article L. 133-7 précise que « *Le consentement est donné sous la forme convenue entre le payeur et son prestataire de services de paiement.* » Une « opération non autorisée » est une opération à laquelle l'utilisateur de l'instrument de paiement n'a pas consenti et pour laquelle l'établissement teneur de compte n'est pas en mesure de certifier qu'elle a été ordonnée par le titulaire du compte ou l'un de ses mandataires. Ces opérations comprennent notamment les cas de perte ou vol (avec ou sans authentification forte), le détournement de l'instrument de paiement ou des données et le manque d'information permettant le blocage de l'instrument de paiement.

Encadré 2

Cinématique d'utilisation du prélèvement SEPA



1. Le payeur, titulaire du compte à débiter, remplit à la demande du créancier le mandat de prélèvement SEPA et le lui retourne signé (de façon manuscrite ou électronique). Le mandat doit comporter obligatoirement :

   • une référence unique de mandat (RUM) [1], propre à ce mandat et attribuée par le créancier en vue d'identifier toutes les opérations de prélèvement qui y seront associées,

   • ainsi que l'identifiant de créancier SEPA (ICS) [2] nécessaire pour émettre des ordres de prélèvement.

1 Dans quelques cas particuliers, tels que la signature de mandat lors de la souscription d'abonnements par voie postale, le mandat est signé au moment de la souscription sur un format générique, dont la RUM est attribuée par le créancier à réception et communiquée en retour à son client.
2 En France, l'ICS est attribué au créancier par la Banque de France, par l'intermédiaire de son établissement bancaire. Dans le cas de créanciers multibancarisés, une seule demande est nécessaire, l'ICS attribué pouvant être utilisé pour l'émission d'ordres de prélèvement *via* les différentes banques du créancier.

.../...

À cette étape, le créancier est tenu de présenter au payeur les éléments permettant d'apprécier les dates et montants des opérations à venir (sous forme d'échéancier), qui pourront être modifiés le cas échéant (par exemple, en cas de surconsommation par rapport à un service prévu initialement), sous réserve d'en alerter le payeur, par exemple par la remise d'un échéancier amendé ou d'une facture.

2. Uniquement dans le cas du prélèvement interentreprises (SDD B2B pour « *business to business* ») : le payeur transmet à son établissement teneur de compte la copie de son mandat de prélèvement.
3. Le créancier transmet à son établissement teneur de compte l'ordre de prélèvement.
4. L'ordre de prélèvement est échangé dans les circuits de paiement interbancaire avant la date d'exécution [3].
5. À la date d'exécution, l'établissement du payeur débite le compte de ce dernier, et le règlement des fonds est effectué à destination de l'établissement teneur du compte du créancier.
6. L'établissement du créancier crédite le compte mentionné dans l'ordre de prélèvement.

3 Les règles applicables au SDD imposent un délai minimum d'un jour entre la transmission de l'ordre à l'établissement débité et la date d'exécution de l'ordre.

3.2 L'authentification forte

Définition et cadre juridique

« *L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté* [5]*. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.* » [6] S'il est aisé de définir l'authentification statique par l'utilisation d'un simple mot de passe, l'authentification forte fait appel à des concepts qu'il convient de préciser.

Dans la DSP2, l'authentification forte du client est définie comme « *une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification* ».

La DSP2 prévoit le recours systématique à l'authentification forte du payeur pour toute transaction initiée électroniquement à l'initiative du payeur, à l'exception

5 Par exemple, dans la sphère des paiements : un identifiant ou un code personnel, un numéro de compte ou un numéro de carte.

6 Définition de l'Agence nationale de sécurité des systèmes d'information : *http://www.ssi.gouv.fr/entreprise/glossaire/a/*

d'un nombre limitatif de cas d'exemption définis dans les normes techniques règlementaires de sécurité associées à la directive (cf. chapitre 1, « Les apports de la DSP2 en matière de sécurité »). Elle précise par ailleurs, dans son article 3, que cette obligation « *ne s'applique pas* […] *aux opérations de paiement fondées sur* […] *une traite sur support papier* ». Les chèques, les ordres de virement papier et les prélèvements, notamment, sont donc exclus du champ d'application de cette disposition.

Par ailleurs, l'article 97 de la DSP2 précise que « *pour les opérations de paiement électronique à distance, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés* ».

De la même manière que les établissements teneurs de comptes, les établissements qui fournissent des services d'information sur les comptes ou d'initiation de paiement sont soumis à ces mêmes obligations et doivent notamment permettre aux établissements teneur de compte d'authentifier leurs clients.

Les solutions d'authentification applicables au virement

Les solutions d'authentification appliquées ou envisageables pour sécuriser l'initiation d'un virement peuvent s'appuyer sur les trois familles de facteurs définis par la directive comme constitutives de l'authentification forte.

Facteur appartenant à la catégorie « connaissance »

La mise en œuvre d'un facteur de connaissance fait appel à l'utilisation d'une donnée connue exclusivement du titulaire du moyen de paiement. Dans le cas général, il s'agit donc d'un mot de passe statique et/ou d'un code confidentiel ; plus rarement, le facteur d'authentification peut être une information liée à l'utilisateur : date de naissance ou de mariage, nom d'un animal de compagnie, modèle de voiture, etc. Toutefois, compte tenu de la facilité croissante à collecter des données personnelles au travers des réseaux sociaux ou d'internet, le recours à ce type d'information pour initier des paiements devrait être proscrit, sauf en solution de secours en cas d'indisponibilité technique avérée des autres services d'authentification.

Dans le cadre du virement, il est fréquent de devoir saisir un facteur de « connaissance » lors de la connexion à la banque en ligne ou à l'ouverture d'une application bancaire sur mobile. Ce facteur est ensuite complété par un autre type de facteur au moment de la validation de l'ordre de virement.

Facteur appartenant à la catégorie « possession »

La mise en œuvre d'un facteur de possession se fonde sur le recours à un dispositif physique personnel dont l'émetteur du virement est le seul détenteur.

La solution d'authentification forte la plus utilisée par les établissements du marché français pour les particuliers consiste à conditionner la validation d'une opération sur internet à la saisie d'un code à usage unique (OTP – *one-time password*) transmis par SMS sur le téléphone portable du titulaire du compte (SMS OTP). Cette solution repose sur la possession du téléphone mobile enregistré par l'établissement. Elle peut aussi être déclinée en transmettant l'OTP par courrier électronique ou par un serveur vocal interactif [7].

7 Dans ce cas, un serveur vocal appelle sur le téléphone du titulaire de la carte et lui dicte l'OTP à utiliser pour valider la transaction en cours.

Cependant, comme relevé dans le rapport annuel 2013 de l'Observatoire de la sécurité des cartes de paiement, cette technique présente plusieurs faiblesses en termes de sécurité :

• le canal de communication utilisé lors de l'envoi du SMS ne fait pas l'objet de mesures de sécurité adaptées à la transmission de données sensibles ;

• la possibilité, sous certaines conditions [8], d'usurper la ligne de téléphonie mobile du titulaire du compte, peut permettre au fraudeur de recevoir les SMS d'authentification sans que le titulaire du compte ne s'en aperçoive.

En alternative à l'envoi d'un OTP par SMS, courrier électronique ou serveur vocal, certains émetteurs utilisent une application pour téléphone mobile multifonctions (*smartphone*) de façon à authentifier l'utilisateur lors d'une opération en lui demandant de valider qu'il est bien en train d'enregistrer un ordre de virement. Le fonctionnement de ces applications peut différer suivant les choix de l'émetteur, par exemple sur l'utilisation éventuelle d'un OTP transmis ou généré par l'application et par la nécessité ou non :

• d'allumer l'écran de son *smartphone* pour commencer l'authentification,

• de saisir un code confidentiel (élément de connaissance) pour accéder à l'application,

• de saisir un code confidentiel sur la page d'enregistrement du virement pour finaliser l'authentification.

Ces solutions bancaires permettent de mettre en œuvre des mesures complémentaires pour sécuriser la transmission du code d'authentification, tout en gardant une cinématique proche de celle dont les utilisateurs ont l'habitude au travers du SMS OTP.

De la même manière, les opérateurs de téléphonie mobile ont développé un standard appelé *mobile connect* pour la mise en place d'une application sécurisée sur la carte SIM dédiée à l'authentification de l'utilisateur avec un élément de possession et éventuellement un élément de connaissance. Cette application d'authentification est à destination de différents types de fournisseurs de services (service de paiement mais aussi transports en commun, billetterie de spectacles, etc.) et devrait être compatible avec les exigences de la DSP2 et des normes techniques réglementaires (RTS – *regulatory technical standards*). L'activation de ce mode d'authentification, pour une carte SIM et un mobile donnés, requiert une phase préalable d'enrôlement de l'utilisateur légitime du service.

Ces différents dispositifs d'authentification s'appuyant sur les téléphones mobiles sont vulnérables à la présence d'un logiciel malveillant installé sur le téléphone, qui peut compromettre la sécurité du dispositif [9]. L'environnement technique des téléphones mobiles continue toutefois d'évoluer pour offrir des fonctionnalités améliorant leur sécurité, notamment à travers la sécurisation des systèmes d'exploitation mobiles afin de prévenir l'exécution d'applications malveillantes, sur une base proche des techniques de sécurisation déployées pour les postes informatiques (antivirus, pare-feu, anti-*spyware*…).

8 Ce mécanisme de fraude, communément désigné sous le terme *SIM swapping*, consiste pour le fraudeur à usurper l'identité du titulaire de la ligne de téléphonie mobile auprès de l'opérateur de téléphonie en vue de se faire remettre une nouvelle carte SIM (en prétextant par exemple, le vol ou la perte du mobile ou un besoin de changement de format de carte SIM). Il s'appuie sur le contournement des procédures d'identification du client mises en place par les opérateurs de téléphonie mobile ou leurs réseaux de distribution.

9 D'une manière plus générale, l'utilisation du téléphone mobile pose un problème d'indépendance entre le canal SMS et le canal de navigation sur internet à partir du même téléphone mobile.

Lorsqu'ils n'ont pas la possibilité de recourir à l'envoi d'un OTP ou à une application sur *smartphone*, par exemple pour les clients ne disposant pas d'une ligne de téléphonie mobile ou pour la clientèle professionnelle, les établissements teneurs de comptes peuvent mettre à disposition de leur clientèle un dispositif matériel, appelé jeton d'authentification ou *token*, affichant un code à validité temporaire, synchronisé avec un serveur d'authentification distant, et incrémenté selon une fréquence prédéfinie (par exemple, toutes les 60 secondes). Ce code doit être saisi lors du processus d'enregistrement de l'ordre de virement.

Des dispositifs plus avancés, dotés d'un clavier numérique, permettent une interaction supplémentaire : dans ce cas, un code à usage unique valide ne peut être obtenu qu'après saisie, selon les cas, d'un code confidentiel connu seulement du porteur du dispositif ou d'un code affiché sur la page d'enregistrement de l'ordre de virement.

Cependant, ce dispositif présente des limites du fait de l'utilisation d'un *token* :

- en situation de mobilité, les utilisateurs n'ont pas toujours le *token* avec eux ;
- le *token* est souvent conservé à proximité directe de l'ordinateur utilisé pour effectuer des virements sur internet, sans la surveillance équivalente à celle d'une carte de paiement mise dans son portefeuille ;
- pour plusieurs solutions de ce type, notamment celles n'utilisant pas de clavier, l'établissement d'un lien dynamique entre l'opération, le montant et le bénéficiaire donnés [10], peut s'avérer difficile à mettre en œuvre.

Pour répondre à ces limites, certains acteurs proposent des solutions reposant sur la lecture d'une carte à puce, telle qu'une carte de paiement ou une carte d'identité, voire un bracelet connecté, à utiliser avec un lecteur dédié à l'authentification de son porteur, par la saisie d'un code confidentiel. Ce type de solution, peu utilisé en France mais très commun par exemple en Belgique, présente cependant un coût de déploiement élevé, car nécessitant la mise à disposition d'un lecteur et, éventuellement, d'un logiciel spécifique pour assurer un niveau de sécurisation équivalent à celui d'un terminal de paiement électronique acceptant les paiements par carte.

Enfin, et principalement pour la clientèle professionnelle, les établissements utilisent également comme facteur d'authentification

Jeton d'authentification simple

Jeton d'authentification avec clavier de saisie

10 Notamment dans le cas de codes à validité temporaire pouvant servir à plusieurs transactions.

de possession la reconnaissance de certificats électroniques qui permettent d'authentifier l'utilisateur à partir de l'équipement utilisé (serveur, poste informatique, etc.) ou à partir d'un outil connecté à celui-ci tel, qu'une clé USB sécurisée ou un lecteur de carte à puce.

Facteur appartenant à la catégorie « inhérence » (biométrie)

La biométrie est définie comme [11] « *l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales* » par la Commission nationale de l'informatique et des libertés (Cnil) [12], qui précise que « *Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.)* ». Comme explicité dans cette définition, la sensibilité des données biométriques repose notamment sur la possibilité d'identifier quelqu'un sans son consentement. Cependant, l'usage qui en est fait dans le milieu des paiements électroniques consiste à valider l'identité d'une personne, c'est-à-dire de l'authentifier. Au lieu de comparer les données d'une personne avec toutes les données d'une base d'utilisateurs, comme dans le cadre de l'identification, l'authentification consiste à ne comparer les données d'une personne qu'avec ses données de référence enregistrées au préalable.

Le recours à des dispositifs biométriques comme facteurs d'authentification pour l'émission de virements suppose que le terminal utilisé pour valider les ordres de paiement soit lui-même équipé d'un capteur de reconnaissance biométrique. En règle générale, les dispositifs utilisés à ce jour sont de deux natures :

- d'une part, les lecteurs d'empreintes biométriques dédiés intégrés aux terminaux utilisés, tels que les lecteurs d'empreinte digitale présents sur un nombre croissant de *smartphones*, de tablettes et d'ordinateurs ;

- d'autre part, les dispositifs de reconnaissance biométrique reposant sur l'exploitation de capteurs non dédiés, par exemple l'appareil photo ou le microphone intégré au terminal utilisé, à des fins de reconnaissance faciale ou vocale.

Un nombre croissant de constructeurs de *smartphones* et d'ordinateurs portables ont intégré de tels dispositifs de reconnaissance biométrique à leurs produits. La commercialisation à grande échelle de ces nouveaux modèles concourt à la familiarisation des techniques biométriques auprès du public et présente une opportunité de déploiement et d'utilisation des technologies biométriques dans le domaine des paiements.

La biométrie revêt un aspect pratique certain lorsqu'elle permet de simplifier la procédure d'initiation d'un paiement, d'en raccourcir la durée, voire de pouvoir répondre à la demande des personnes qui rencontrent des difficultés à mémoriser un mot de passe ou un code confidentiel. Cependant, l'emploi de la biométrie soulève plusieurs problématiques spécifiques.

- Le caractère définitif de la compromission d'une empreinte : la compromission d'une empreinte biométrique (par exemple, une empreinte digitale), dans quelque contexte que ce soit (y compris en

11 Cf. *https://www.cnil.fr/fr/definition/biometrie*

12 La Cnil est l'autorité publique chargée de veiller à la protection des données individuelles.

dehors du domaine des paiements), est irrémédiable et ne devrait pas permettre une réutilisation de l'empreinte compromise à des fins d'authentification pour des opérations de paiement.

• Les limites à l'universalité du dispositif biométrique : certaines personnes peuvent se trouver dans l'incapacité d'utiliser leurs empreintes biométriques de manière temporaire (usure, salissure, blessure, etc.), voire permanente (caractéristiques physiques incompatibles avec le dispositif biométrique, handicap, etc.).

• La difficulté à définir le réglage du niveau de tolérance du dispositif biométrique qui influencera le taux d'erreur : deux types de taux sont principalement mesurés en biométrie, ceux de faux rejets (*false rejection rate* – FRR[13]) et de fausses acceptations (*false acceptation rate* – FAR[14]), pour traduire respectivement le niveau d'exigence et celui de permissivité du dispositif envers l'empreinte biométrique prise et comparée à l'empreinte de référence. Ainsi, des coupures, brûlures aux doigts, voire la simple transpiration, peuvent conduire à un rejet, de la même manière que du bruit ambiant peut altérer une analyse vocale. Ces taux peuvent varier de manière plus ou moins importante selon la caractéristique physique analysée, la qualité du lecteur biométrique et l'algorithme utilisé. La difficulté vient du fait que si un réglage du niveau de tolérance est possible, les taux de faux rejets et de fausses acceptations évoluent généralement de manière opposée. Il n'existe aucune donnée publique concernant les taux de faux rejets et ceux de fausses acceptations pour les dispositifs actuellement disponibles, ce qui rend difficile l'évaluation du niveau de sécurité de l'algorithme utilisé.

• La difficulté à évaluer le niveau de sécurité intrinsèque d'un dispositif : en complément de la sécurité liée au réglage des paramètres de l'algorithme utilisé, il est nécessaire de mesurer la résistance de ces dispositifs face aux techniques de leurrage (consistant à présenter une fausse empreinte copiant celle de l'utilisateur légitime) et face aux attaques sur son déploiement. Si, aujourd'hui, aucun dispositif accessible ne peut être certifié comme résistant à l'ensemble des techniques communes de leurrage, des tests périodiques dans un laboratoire spécialisé peuvent permettre de s'assurer de la robustesse des dispositifs face aux techniques les plus connues.

La signature du mandat de prélèvement

Le fonctionnement du prélèvement SEPA repose sur la signature d'un mandat par le débiteur. Cette signature atteste du consentement du payeur aux ordres de prélèvements qui seront émis par la suite, dans la limite des mentions portées au mandat. Dans le cadre de la DSP2, la signature d'un mandat sous forme électronique n'est pas expressément assujettie à l'obligation d'authentification forte du payeur, mais constitue toutefois un axe fort en matière de sécurisation du prélèvement SEPA.

L'établissement bancaire du payeur n'étant pas directement partie prenante à la signature d'un mandat par son client (sauf dans le cas du SDD B2B), la mise en œuvre de l'authentification forte revient au créancier, et peut recourir ou non aux dispositifs mis en œuvre par les banques pour la sécurisation d'autres moyens de paiement électroniques, tels que les virements.

13 Le FRR est la probabilité que le système biométrique rejette à tort une tentative d'accès par un utilisateur autorisé.

14 Le FAR est la probabilité que le système biométrique accepte une tentative d'authentification par un utilisateur non autorisé.

Encadré 3

Règlementation applicable aux dispositifs de reconnaissance biométrique

Jusqu'à la mise en application du règlement général sur la protection des données (RGPD), le 25 mai 2018, les dispositifs de reconnaissance biométrique étaient soumis à l'autorisation préalable de la Commission nationale de l'informatique et des libertés (Cnil) conformément à l'article 25-I-6° de la loi « Informatique et Libertés ».

La Cnil a ainsi, notamment, eu l'occasion d'autoriser des organismes à utiliser la biométrie en tant que facteur d'authentification pour accéder à des moyens de paiement ou effectuer des opérations de paiement à distance.

Sur la base des dossiers qu'elle a eu à examiner et en tenant compte du contexte économique, ainsi que du paysage législatif en évolution tant au niveau national qu'européen, la Cnil s'est attachée à dégager des principes directeurs applicables aux dispositifs biométriques.

Bien que la biométrie à destination du grand public (hors du cadre professionnel) ne fasse pas l'objet de cadre de référence, permettant d'alléger les formalités des organismes, certaines constantes peuvent être soulignées.

Ainsi, dans une démarche de protection des données (dès la conception, et par défaut), et conformément au droit à l'autodétermination informationnelle, la Cnil marque sa volonté de ne pas voir imposer la biométrie dans tous les usages du quotidien et de garantir aux personnes concernées la maîtrise de leurs données biométriques.

L'utilisateur du service doit par ailleurs être en mesure de choisir une technique équivalente en termes de facilité d'usage, présentant les mêmes conditions d'accès qu'un dispositif biométrique (le choix d'une autre technologie ne doit pas avoir pour effet, par exemple, d'ajouter des contraintes en termes de délai ou de coût).

De plus, le RGPD consacre les données biométriques comme des données « sensibles » (article 9) et interdit par principe leur utilisation. Si cette interdiction peut être levée dans certaines conditions, la seule applicable au cas d'espèce est celle du consentement explicite des personnes concernées. Pour être valable, le consentement doit être libre, spécifique, éclairé et univoque, ce qui suppose l'existence d'un dispositif d'authentification alternatif. Cela suppose en outre que les personnes concernées puissent revenir à tout moment sur leur choix et obtenir, le cas échéant, la suppression de leur gabarit biométrique.

Par ailleurs, les traitements à grande échelle de données « sensibles » au sens de l'article 9 du RGPD, devront faire l'objet d'une analyse d'impacts relative à la protection des données, conformément à l'article 35-3-b du RGPD. Cette analyse devra, notamment, mentionner :

- sur le principe de pertinence et de proportionnalité : la justification du recours à un dispositif biométrique (obligation légale, lutte contre la fraude, etc.) et les raisons ayant conduit à ne pas s'appuyer sur d'autres facteurs d'authentification ;

.../...

- les garanties et les mesures de sécurité adaptées aux risques mises en œuvre compte tenu de la sensibilité des données biométriques (suppression immédiate des données brutes dès enrôlement et du gabarit dès comparaison ou stockage à la main de l'utilisateur, etc.).

Sur ce dernier point, la maîtrise par les personnes concernées de leurs données biométriques est indéniablement réduite lorsque le gabarit biométrique est stocké dans des serveurs distants et non sur un support placé sous leur contrôle exclusif. La compromission du support individuel emporte en effet des conséquences bien moins importantes que celle d'une base centralisant plusieurs gabarits.

C'est pourquoi, la Cnil invite à privilégier le stockage des gabarits biométriques sous le contrôle exclusif de la personne concernée (sur un support individuel ou en base centrale sous une forme chiffrée par une clé de chiffrement/déchiffrement uniquement détenue par la personne concernée).

En outre, de nombreux acteurs sont susceptibles d'intervenir sur la chaîne de traitement liée à l'authentification biométrique (par exemple, en fournissant/gérant le support de stockage des gabarits ou en proposant l'utilisation du facteur d'authentification biométrique).

Une attention accrue est donc nécessaire pour clarifier la répartition des responsabilités et prendre en compte les règles de protection des données dès la conception des services concernés.

Enfin, dans certains cas, la Cnil considère que le traitement biométrique entre dans la définition de l'exemption domestique prévue aux articles 2 de la loi « Informatique et Libertés » et du RGPD (cf. *https://www.cnil.fr/fr/biometrie-dans-les-smartphones-loi-informatique-et-libertes-exemption-ou-autorisation*).

En France, la signature électronique des mandats de prélèvement connaît, à l'initiative des créanciers, un fort développement depuis la migration SEPA, et repose sur deux principaux modèles.

• En situation de proximité, la principale modalité de numérisation du mandat consiste à recourir à la signature manuscrite sur tablette (généralement en agence ou au domicile du payeur) de contrats de prestations qui incluent un mandat de prélèvement. Ces solutions ne permettent toutefois pas d'authentifier de manière automatisée le signataire, comme le titulaire du compte à débiter, et s'appuient, par conséquent, sur la reconnaissance visuelle par le créancier (par exemple, à partir de la carte d'identité du signataire).

• En situation d'entrée en relation ou de contractualisation à distance, la validation du mandat par le payeur s'appuie sur un processus de signature électronique, qui assure un scellement chiffré des données d'authentification du signataire et des données du mandat. Dans ce cas de figure, l'authentification du payeur s'appuie généralement sur la transmission d'un code de validation à usage unique. Ceci nécessite que le créancier dispose préalablement du numéro de téléphone ou de l'adresse électronique ou physique de son client, collectés de façon suffisamment sécurisée. À titre d'exemple, la direction générale

des Finances publiques a ajouté des codes images bidimensionnels (ou QR codes) sur ses avis de paiement. Le contribuable peut alors générer sur son téléphone mobile un mandat de prélèvement à usage unique en scannant ce code *via* l'application mobile *impots.gouv*, dans laquelle il se sera préalablement enrôlé (identification personnelle et IBAN – *international bank account number*), et le valider.

Pour répondre à la problématique d'authentification lors de la signature de mandats à distance, certains pays européens s'appuient sur des architectures publiques ou dédiées.

• Les pays européens ayant mis en place des cartes nationales d'identité équipées d'une puce, comme la Belgique et l'Espagne par exemple, peuvent s'appuyer sur les mécanismes d'authentification associés, en utilisant un lecteur de carte mis à la disposition des payeurs, pour authentifier la signature d'un mandat de prélèvement en ligne.

• Aux Pays-Bas, en Autriche et au Portugal, il existe des fournisseurs de services de mandat interbancaires qui proposent un mécanisme de signature de mandat électronique en ligne. Le débiteur choisit d'abord sa banque ; il est ensuite redirigé vers le site de celle-ci pour qu'elle puisse l'authentifier et lui faire valider les données du mandat. Ce type de système est appelé « à quatre coins » puisque le créancier, le fournisseur de la solution de mandat, le débiteur et sa banque sont mis à contribution.

• Un prestataire de services auprès de la sphère bancaire propose en Italie un système dit « à quatre coins », c'est-à-dire assurant la mise en relation de la banque du créancier et de la banque du débiteur lors de la signature du mandat. Ce dispositif procède à ce qui s'apparente à une demande d'autorisation vers la banque teneur de compte et authentifie le titulaire du compte à partir de son numéro de téléphone.

Dans le cadre de ces solutions, le titulaire du compte est authentifié par la banque teneur de compte qui peut alors mettre en œuvre les moyens d'authentification décrits dans le cadre du virement. Par ailleurs, l'établissement teneur de compte connaît les éléments du mandat avant de recevoir l'ordre de prélèvement, et dispose ainsi de la faculté d'identifier les créanciers autorisés à émettre des prélèvements sur le compte du client. Ce partage d'informations permet ainsi à l'établissement teneur de compte de bénéficier pour le SDD core d'une visibilité sur les mandats équivalente à celle dont il dispose au titre des mandats B2B.

3.3 Les mesures de sécurité complémentaires associées aux moyens de paiement SEPA

Au-delà des mécanismes d'authentification du payeur, d'autres mesures peuvent être mises en place par les acteurs de la chaîne des paiements, en vue de réduire le risque de fraude ou la sensibilité des données échangées.

La protection des identifiants bancaires

Les virements et les prélèvements s'appuient sur l'utilisation du numéro d'identification des comptes bancaires, ou IBAN, qui sert à définir, dans les ordres de paiements, les comptes à créditer et à débiter. Avec le passage aux instruments SEPA, l'IBAN est devenu en Europe la donnée centrale pour l'émission de virements ou de prélèvements, tant pour les opérations nationales que pour les opérations transfrontalières.

Encadré 4

La structure des IBAN français

Pour les comptes tenus en France, l'IBAN (*international bank account number*) est constitué de 27 caractères, commençant par le code pays FR suivi de 2 caractères formant une première clé puis des 23 chiffres de l'ancien relevé d'identité bancaire (RIB) français utilisé avant la migration SEPA (code de l'établissement bancaire, code du guichet, numéro de compte et clé RIB).

Composition du code IBAN

L'IBAN est toutefois de taille variable selon les pays, et peut contenir jusqu'à 34 caractères au maximum.

L'IBAN est considéré en France comme une donnée pouvant faire l'objet de détournements frauduleux, notamment dans le cas d'un prélèvement faux, c'est-à-dire lorsqu'un fraudeur usurpe un IBAN pour bénéficier d'un bien ou d'un service réglé par le détenteur du compte dont l'IBAN a été détourné.

À ce titre, il est recommandé aux détenteurs d'un compte courant de ne pas communiquer leur IBAN, sauf à un créancier bénéficiaire d'un prélèvement ou à un tiers émetteur d'un virement. À cet effet, il est fortement conseillé au détenteur du compte de s'assurer, en amont de toute transaction, de la bonne foi des contacts auxquels est transmis un IBAN [15].

15 Cf. annexe 1, « Conseil de prudence pour l'utilisation des moyens de paiement ».

Encadré 5

Dans quels cas faut-il considérer l'IBAN comme une donnée de paiement sensible au regard de la DSP2 ?

La directive européenne sur les services de paiement (DSP2) prévoit que l'IBAN (*international bank account number*) et le nom du titulaire du compte ne sont pas considérés comme des données de paiement sensibles en ce qui concerne l'activité des prestataires de services d'initiation de paiement (PSIP) ou d'information sur les comptes (PSIC) [1]. Cette disposition se justifie par le fait que la communication de ces données à ces prestataires

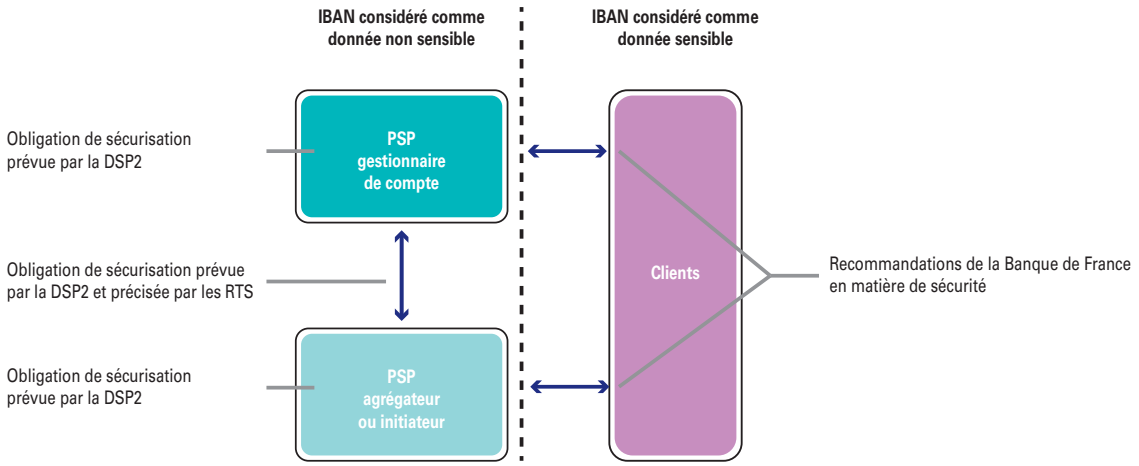
1 Article 4-32 de la DSP2.

.../...

de services de paiement (PSP) peut être nécessaire à la fourniture de leurs services de paiement. En dehors de ces cas d'utilisation bien définis par la DSP2, l'IBAN doit être considéré comme une donnée sensible de paiement.

En conséquence, la DSP2 encadre strictement l'utilisation des IBAN par l'ensemble des acteurs, qu'ils soient PSP gestionnaires de comptes, PSIC ou PSIP. Différents cas sont à distinguer :

- **traitement « interne » des IBAN par des PSIP et des PSIC :** la DSP2 les autorise à stocker cette donnée tout en imposant la mise en place d'un processus sécurisé pour « *enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles et garder la trace de cet accès* » et une politique de sécurité pour limiter les risques d'« *utilisation illicite des données sensibles* » [2] ;
- **traitement « interne » par les PSP gestionnaires de comptes :** ces PSP peuvent stocker des IBAN mais doivent appliquer le même cadre de sécurisation que mentionné pour les PSIC et les PSIP ;
- **traitement dans les échanges entre PSP gestionnaires de comptes et PSIP ou PSIC :** l'IBAN n'est pas une donnée sensible de paiement et peut donc être communiqué entre ces PSP ; toutefois, l'échange de données entre eux doit être sécurisé [3] ;
- **traitement dans le cadre de la relation PSIP ou PSIC et leurs clients :** l'IBAN est une donnée de paiement sensible ; la Banque de France recommande donc une diffusion restreinte et le masquage des IBAN s'ils sont affichés dans l'espace utilisateur ;
- **traitement dans le cadre de la relation PSP gestionnaires de comptes et leurs clients :** l'IBAN est une donnée de paiement sensible ; la Banque de France recommande donc une diffusion restreinte et le masquage des IBAN s'ils apparaissent dans l'espace de banque en ligne de l'utilisateur.



2 Article 5-1-g et j de la DSP2.
3 Utilisation d'une interface sécurisée dédiée prévue à l'article 98 de la DSP2 et précisée par des normes techniques règlementaires (cf. chapitre 1, « Les apports de la DSP2 en matière de sécurité des paiements »).

Les risques de fraude liés à la communication des IBAN

Le SDD B2B présente peu de risque du fait de la nécessité de communiquer en amont le mandat à la banque qui tient le compte à débiter ; à l'inverse, le SDD core présente un risque réel [16] dans deux schémas.

- Client frauduleux : un fraudeur peut remplir un mandat de prélèvement SDD core avec un IBAN usurpé auprès d'une victime. On parle alors d'usurpation d'IBAN pour la souscription d'un service.

- Créancier frauduleux : un fraudeur se fait enregistrer en tant que créancier par une banque et demande un identifiant de créancier SEPA (ICS), qui lui permet ensuite d'initier des prélèvements illégitimes sur la base d'IBAN collectés frauduleusement.

16 Le numéro de compte est encore utilisé par de rares établissements pour se connecter aux services de banque à distance mais ce cas de figure ne sera pas abordé ici, d'autant que la connaissance de cette donnée n'est pas suffisante pour accéder au site.

Encadré 6

Règlementation applicable en matière de protection des données personnelles de paiement, dont l'IBAN

L'IBAN [1] est une donnée à caractère personnel, tant au sens de la définition prévue par la loi « Informatique et Libertés » (article 2), que du règlement général sur la protection des données (RGPD, article 4-1).

Cette typologie de données n'est toutefois pas qualifiée « données sensibles » dans les textes précités et ne fait donc pas l'objet d'un encadrement spécifique.

En premier lieu, comme la présente étude le démontre, les principaux points de vigilance liés au traitement de l'IBAN correspondent aux modalités de sécurité entourant les transactions.

Plus précisément, il conviendra de prévoir des garanties de sécurité adaptées au niveau de risque propre à chaque type de transaction et de veiller à ce que ces mesures soient actualisées tant au regard des technologies ou dispositifs utilisés que des typologies de fraudes.

En second lieu, l'encadrement du traitement de l'IBAN dépendra de l'objectif dudit traitement et du niveau de risque qu'il présente pour les personnes concernées, titulaires du compte. Ce niveau de risque peut être estimé de manière empirique dans un premier temps, notamment en fonction des critères dégagés par le groupe de travail « article 29 » (groupe des autorités de protection des données européennes) dans ses lignes directrices 2016/679 relatives aux études d'impact sur la protection des données. Pour rappel, ces études permettent d'évaluer le risque présenté par le traitement et d'adopter des mesures appropriées pour limiter ses impacts pour les droits et libertés des personnes. La Cnil a également mis à disposition, sur son site, différents guides expliquant la méthodologie de l'étude d'impact ainsi qu'un outil permettant de le réaliser.

1 *International bank account number.*

Dans ce type de montage, le fraudeur émet les ordres de prélèvement et transfère les fonds reçus le plus tôt possible afin d'éviter que les flux ne soient retournés suite à des réclamations ou des plaintes des victimes. On parle alors d'émission illégitime d'ordres de prélèvement.

Les risques liés aux bases de données et aux ordres de paiement

Le virement présente peu de risque de fraude par l'utilisation d'un IBAN volé, puisque l'opération est au bénéfice du titulaire du compte, et non à son débit. Cependant, un grand volume de virements provient de l'activité des entreprises. Ces ordres sont principalement générés à partir d'IBAN présents dans des bases de données. Ainsi, une faiblesse dans le système de sécurité d'une base pourrait permettre à une personne malintentionnée de substituer à un ou plusieurs IBAN légitimes celui de son propre compte, voire ceux de complices. De cette manière, les fichiers d'ordres générés permettront au fraudeur de détourner les fonds à destination des IBAN substitués dans la base.

De manière similaire, un fraudeur en capacité d'accéder au système d'information d'une entreprise pourrait être en mesure d'altérer les ordres de virement en attente de transmission pour en modifier le compte destinataire.

Les mesures de protection du stockage des IBAN

Il n'existe pas à ce jour de certification *ad hoc* visant à garantir un niveau de sécurité cible du stockage des IBAN, des ordres de virement et des données de connexion aux services de banque en ligne. Cependant, en reprenant les bonnes pratiques communes à la protection des données sensibles, plusieurs mesures de sécurité peuvent être envisagées, notamment par les professionnels.

En entreprise, les ordres de paiement sont couramment générés par des logiciels spécialisés qui doivent garantir un développement sécurisé avec des mises à jour régulières, un mécanisme de gestion des droits d'accès et un système de suivi de l'activité permettant de l'analyser et, si nécessaire, de détecter les comportements suspects. Cela inclut une limitation de l'exposition des IBAN, par exemple en les masquant partiellement dès lors que la connaissance complète de la donnée n'est pas nécessaire. Par ailleurs, ces logiciels doivent assurer un stockage sécurisé des IBAN pour en assurer la confidentialité et l'intégrité, notamment en les chiffrant.

En complément, les entreprises et les établissements teneurs de comptes sont invités à porter une attention particulière à leurs règles de communication autour de l'IBAN, afin d'éviter toute exposition inutile (par exemple, dans les conditions générales de vente, dans les signatures professionnelles, dans le papier à en-tête, dans les bons de commande, etc.). Quand cela est opportun en termes de volumétrie et de coût, les entreprises peuvent également se prémunir du risque de fraude en disposant de comptes dédiés à certains usages (par exemple, compte dédié aux paiements par chèque rejetant tout autre moyen de paiement, compte dédié aux prélèvements clientèle, etc.).

Enfin, pour limiter le risque portant sur la circulation des IBAN, il peut être envisagé de faire appel à un mécanisme déjà utilisé dans le cadre de la protection des numéros de cartes de paiement, appelé « tokenisation ». Ce procédé consiste à utiliser, dans un contexte défini (une opération unique, un type d'opération, un canal d'initiation ou

dans un délai limité), un alias en lieu et place de la donnée à protéger. Ainsi, l'alias présent dans un message intercepté par un fraudeur ne sera pas réutilisable par ce dernier en dehors du périmètre d'utilisation restreint. Un établissement français a mis en œuvre cette technique dans le cadre d'un service interbancaire.

Cinématique et autres mesures de sécurité

Un établissement teneur de compte étant légalement contraint d'exécuter rapidement les ordres de virement qu'il reçoit, les mesures visant à lutter contre la fraude doivent donc être mises en œuvre avant la validation des ordres.

L'analyse du niveau de risque des transactions

Dans ce cadre, et en complément des solutions d'authentification forte, les techniques d'évaluation du niveau de risque des transactions, ou *scoring*, consistent à associer une cotation à une opération pour déterminer si celle-ci doit être bloquée, temporisée ou exécutée. Les outils de *scoring* s'appuient généralement sur des règles créées à partir des scénarios de fraude connus. Par exemple, dans le cadre du virement, les règles peuvent prendre en compte les données du virement (type de compte à débiter, montant, nouveau compte à créditer ou non, etc.), le profil du titulaire de compte et les données recueillies par l'établissement sur les habitudes du titulaire de compte (utilisation fréquente ou non du canal de communication utilisé, montant des précédents virements, intensité d'utilisation du moyen de paiement, etc.).

Les normes techniques réglementaires associées à la DSP2 citent notamment les critères suivants comme pouvant être utilisés à des fins d'analyse de risque [17] :

- l'identification d'un comportement ou d'une dépense anormale,
- la détection d'informations inhabituelles concernant l'appareil ou le logiciel utilisé,
- l'identification d'un virus lors d'une session qui a nécessité une authentification client,
- l'identification d'un scénario de fraude,
- une localisation anormale ou à haut risque du titulaire.

Au-delà de l'analyse unitaire des flux, les établissements teneurs de comptes peuvent utiliser des informations concernant les flux observés (taux de rejet pour les prélèvements, destinations ou bénéficiaires inhabituels pour les virements, etc.) sur l'ensemble de leurs clients. En plus de faciliter la détection des tentatives de fraude, ce croisement d'informations permet aux établissements de prévenir, si nécessaire, certains clients de la survenance d'opérations identifiées comme probablement suspectes.

Les paramètres des outils permettent d'affiner les règles en modifiant l'influence des données mises en œuvre. Une fois les règles de *scoring* en place, le système peut déterminer, à partir de la « note calculée », s'il est nécessaire de mettre en œuvre un niveau d'authentification supplémentaire ou d'alerter le titulaire du compte pour une validation complémentaire, au moyen par exemple d'un contre-appel.

17 Ces données sont également répertoriées dans le dispositif d'autorisation unique défini en France par la Cnil pour encadrer les traitements de données ayant pour finalité la lutte contre la fraude externe dans le secteur bancaire et financier : *https://www.cnil.fr/fr/declaration/au-054-lutte-contre-la-fraude-externe-dans-le-secteur-bancaire-et-financier*

L'utilisation de base de correspondance interbancaire entre IBAN et identité du titulaire du compte

Pour se prémunir de cas de fraude à l'usurpation d'identifiants bancaires, en amont de l'émission d'ordres de virement ou de prélèvements, il peut être efficace de s'appuyer sur des mécanismes permettant de tester la cohérence entre l'IBAN déclaré et l'identité de la contrepartie (nom ou raison sociale, adresse, etc.). De tels services, existant sur une base nationale dans certains pays d'Europe dont la France, seront d'autant plus efficaces qu'ils couvriront une base bancaire large.

Les mesures de temporisation des virements

Les sites de banque en ligne permettent à leurs utilisateurs de gérer une liste de bénéficiaires, ce qui évite de saisir à nouveau l'IBAN du destinataire pour chaque nouvel ordre de virement, et permet de mettre en place des mesures de lutte contre la fraude à l'enregistrement d'un nouveau compte bénéficiaire. La mesure la plus répandue consiste à valider l'enregistrement d'un nouveau compte sous un délai prédéfini de un à trois jours, durant lequel aucun paiement vers le nouveau bénéficiaire ne peut être émis. Cette mesure présente deux avantages en matière de lutte contre la fraude :

- elle permet d'informer le client par un autre canal (par exemple, courrier électronique ou SMS) sur l'ajout en cours d'un nouveau bénéficiaire et lui donne le temps de réagir le cas échéant ;

- elle constitue une mesure efficace pour les mécanismes de fraude automatisés, de type *malware* ou *phishing*, par lesquels les fraudeurs tentent généralement d'initier un virement frauduleux dès la première connexion à l'espace de banque en ligne de leur victime.

Ces mesures de temporisation représentent toutefois une gêne pour l'utilisateur dans l'accès à ses moyens de paiement, et sont susceptibles de constituer un obstacle à l'activité des initiateurs de paiement (cf. chapitre 1, « Les apports de la DSP2 en matière de sécurité ») ou au développement du virement instantané.

Dans ce contexte, et comme d'ailleurs déjà initié par de nombreux établissements, il apparaît nécessaire de développer des moyens de substitution sécurisés à ce délai, par exemple par le recours à un canal de communication supplémentaire, tel qu'une application mobile permettant à l'utilisateur de valider un ajout de bénéficiaire après une authentification forte. L'émergence de systèmes de *scoring* performants et fonctionnant en temps réel, y compris pour les virements, paraît également appropriée pour pallier ces mesures de temporisation.

Les mesures de sécurité propres au prélèvement

Un ordre de SDD B2B présente un risque limité dans la mesure où le titulaire du compte à débiter doit remettre *ex-ante* le mandat à son établissement teneur de compte. *A contrario*, comme précisé précédemment, le prélèvement standard présente un réel risque de fraude qui doit pouvoir être pris en compte par l'établissement teneur de compte avant l'exécution de l'opération. C'est pourquoi un SDD core doit parvenir à la banque du débiteur *a minima* la veille de sa date d'échéance. Ce délai peut être mis à profit par les établissements teneurs de comptes pour vérifier la légitimité du prélèvement auprès du titulaire du compte ou d'un mandataire, par un mécanisme

d'alerte (par courrier électronique ou SMS) ou de contre-appel.

La réglementation sur le SDD core impose aux établissements teneurs de comptes de permettre à leurs clients de mettre en place une liste de créanciers autorisés (ou non autorisés). La mise en place de cette liste sur un compte implique qu'un prélèvement à destination d'un autre créancier fera l'objet d'un refus de la part de l'établissement teneur de compte. À noter qu'il est aussi possible de demander à son établissement teneur de compte de bloquer l'exécution de certains types d'opération sur un compte donné.

3.4 Conclusion et recommandations de l'Observatoire

L'Observatoire note que les moyens de paiement SEPA, bien que relativement récents, disposent d'ores et déjà de solutions de sécurisation performantes, qui permettent d'assurer des taux de fraude particulièrement faibles au regard des taux constatés sur les autres instruments de paiement.

L'authentification renforcée des opérations

Des solutions d'authentification existent et ont été déployées pour sécuriser les émissions d'ordres de virement électroniques par les clients, et ce pour les différents canaux disponibles : site de banque en ligne, application mobile, messagerie sécurisée interentreprises, etc. L'Observatoire invite les établissements teneurs de comptes à poursuivre le développement de ces solutions, qui s'inscrivent dans le prolongement à la fois de la stratégie nationale des paiements et des exigences règlementaires en matière d'authentification des paiements. À ce titre, les établissements sont invités à préparer la mise en conformité des solutions déployées avec les requis inscrits dans les normes techniques règlementaires attachées à la DSP2. Une attention particulière devra également être portée au respect des exigences spécifiques applicables à la biométrie pour les acteurs qui souhaiteraient développer des solutions de ce type.

En ce qui concerne le prélèvement, l'Observatoire note les efforts consentis par les créanciers français pour promouvoir des solutions dématérialisées de signature des mandats. À cet égard, l'Observatoire invite les créanciers à mettre en œuvre des solutions d'authentification forte dans ces nouveaux processus dématérialisés, et accueille favorablement le développement de solutions interbancaires proposant aux créanciers de vérifier l'identité du titulaire d'un compte. L'Observatoire rappelle également que les établissements sont tenus de proposer à leurs clients la gestion d'une liste de mandats autorisés, ou non autorisés, à débiter leur compte, et invite les particuliers et entreprises à s'approprier ces dispositifs quand cela est pertinent.

Le développement d'outils d'évaluation du risque

Par ailleurs, l'Observatoire souligne son attachement à la mise en place de mesures de protection complémentaires aux dispositifs d'authentification, telles que la mise en place de systèmes d'évaluation du niveau de risque d'une transaction permettant d'adapter le niveau d'authentification requis lors du paiement ou d'alerter le client le cas échéant.

En particulier, l'amélioration des techniques de *scoring* et d'authentification doit permettre de lever les mesures de temporisation des ordres émis vers de nouveaux bénéficiaires, lesquelles, outre leur caractère contraignant pour l'utilisateur, constituent un obstacle à la mise en place du service d'initiation de paiement prévu par la DSP2 et au déploiement des solutions de paiement reposant sur le virement instantané.

La sécurisation des données sensibles

La protection des numéros de compte (IBAN) constitue également une pierre angulaire de la sécurité des moyens de paiement SEPA. La mise en place par les acteurs professionnels de mécanismes permettant de sécuriser ces informations, tant dans les bases de données que dans les canaux d'échange de toute nature (fichiers d'ordres de paiement, messagerie électronique, etc.), par chiffrement, voire « tokenisation » quand cela est possible, apparait nécessaire pour limiter les risques d'interception ou de substitution à des fins frauduleuses.

La nécessaire vigilance de l'ensemble des utilisateurs

Enfin, l'Observatoire invite les utilisateurs des moyens de paiement SEPA, qu'ils soient particuliers ou entreprises, à être eux-mêmes acteurs de la sécurité de leurs moyens de paiement, en veillant en particulier à conserver secrètement, et de manière sécurisée dans le cas des entreprises, toute donnée de paiement susceptible d'être utilisée à des fins frauduleuses. Une attention particulière doit également être portée au suivi des opérations imputées sur leur compte. À cet égard, le respect des conseils de prudence, rappelés en annexe 1 du présent rapport, contribue directement à la prévention du risque de fraude. De manière plus générale, l'utilisation à des fins de paiement d'équipements grand public, tels que les *smartphones*, nécessite que chaque utilisateur prenne soin de se protéger contre les attaques potentielles, notamment en suivant les précautions élémentaires et les bonnes pratiques en la matière, telles que diffusées notamment par l'Agence nationale de la sécurité des systèmes d'information[18].

En conclusion, l'Observatoire souligne la nécessité de disposer d'une évaluation globale du niveau de sécurité offert par les solutions mises en œuvre, ainsi que des contraintes qu'elles génèrent pour leurs utilisateurs (ergonomie pour les consommateurs, implémentation et gestion pour les entreprises). Il invite en particulier les prestataires de services de paiement à porter une attention particulière à la protection des utilisateurs durant les phases d'expérimentation de nouvelles solutions de sécurité.

18 Cf. *https://www.ssi.gouv.fr/particulier/guide/recommandations-de-securite-relatives-aux-ordiphones/*

A1 Conseils de prudence pour l'utilisation des moyens de paiement

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

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

- **la fraude par établissement de faux ordres de paiement,** soit après le vol ou la contrefaçon d'un instrument physique, soit par détournement de données ou d'identifiants bancaires par un tiers ;

- **la fraude par détournement ou falsification d'un ordre de paiement régulier,** en dupliquant un ordre de paiement émis par son porteur légitime ou en modifiant ses attributs (montant, nom du bénéficiaire ou du donneur d'ordre, etc.) ;

- **la fraude par utilisation ou répudiation abusive** par le titulaire légitime d'un moyen de paiement, caractérisée par la contestation infondée d'un ordre de paiement valablement émis, aboutissant ainsi à l'annulation de l'encaissement des fonds.

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

Votre comportement concourt directement à la sécurité de leur utilisation.

Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

Soyez responsables

- Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, même pas à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.

- Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile, etc.), gardez-le secret, ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui.

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

- Lorsque vous composez un code ou un mot de passe confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal, du distributeur ou du téléphone avec votre autre main.

- Vérifiez régulièrement et attentivement vos relevés de compte.

- Pensez à consulter régulièrement les consignes de sécurité publiées sur le site de votre banque et assurez-vous qu'elle dispose de vos coordonnées afin de vous contacter rapidement en cas d'opérations douteuses sur votre compte. En cas de contact de votre banque, par téléphone ou par courriel pour de telles opérations, rappelez-vous que vous n'avez pas à lui communiquer vos mots de passe et identifiants personnels.

- N'acceptez jamais de payer un vendeur ou loueur de biens que vous ne connaissez pas par transfert d'argent préalable à la mise à disposition ou la livraison du bien ; il peut s'agir de fraudeurs qui, après avoir récupéré les fonds transférés, font disparaître tout lien de communication (adresse email, compte de réseau social, etc.).

Soyez attentifs

Lors des paiements à un professionnel ou à un particulier

- Vérifiez l'utilisation qui est faite de votre carte bancaire par le commerçant. Ne la quittez pas des yeux.

- Pensez à vérifier le montant affiché par le terminal avant de valider une transaction.

- Lorsqu'un chèque est automatiquement rempli par le commerçant, soyez attentif aux mentions indiquées avant de le signer et vérifier plus particulièrement le montant.

- Quelques précautions lors du remplissage d'un chèque permettent de réduire les risques de fraude : évitez les ratures ou surcharges, inscrivez le nom du bénéficiaire du chèque et les montants en chiffres et en lettres sans laisser d'espace libre, puis tirez un trait sur l'espace restant non utilisé. Le lieu de paiement et la date doivent être renseignés en même temps que les autres mentions. La signature du chèque ne doit pas déborder sur la ligne de chiffres en bas du chèque. En aucun cas, la signature ne doit être apposée seule sur un chèque, c'est-à-dire sans les mentions relatives au montant et au bénéficiaire préalablement renseignées.

Lors des retraits sur les distributeurs de billets

- Vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.

- Suivez exclusivement les consignes indiquées à l'écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.

- Mettez immédiatement en opposition votre carte si elle a été avalée par l'automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l'agence.

Lors des paiements sur internet

- Ne stockez pas de coordonnées bancaires sur votre ordinateur (numéro de carte, numéro de compte, relevé d'identité bancaire, etc.), évitez de les transmettre par simple courriel et vérifiez la sécurisation du site du commerçant en cas de saisie en ligne (cadenas en bas de la fenêtre, adresse commençant par « https », etc.).

- Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les mentions légales du commerçant ainsi que ses conditions générales de vente.

- Ne répondez pas à un courrier électronique, SMS, appel téléphonique ou autre invitation qui vous paraisse douteuse. En particulier, ne cliquez jamais sur un lien inclus dans un message référençant un site bancaire.

- Protégez votre ordinateur, en activant les mises à jour de sécurité proposées par les éditeurs de logiciel (en règle générale gratuites) et en l'équipant d'un antivirus et d'un pare-feu.

- Changez régulièrement vos mots de passe, et évitez d'utiliser la fonction d'enregistrement pour des utilisations ultérieures (une usurpation de vos identifiants et de vos coordonnées bancaires vous expose à des fraudes sur tous vos moyens de paiement).

- N'utilisez pas un mot de passe commun pour l'utilisation de vos moyens de paiement, l'accès à votre banque en ligne et l'accès aux autres sites internet sur lesquels vous avez un compte client.

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

- Lors de la réception d'un mandat de prélèvement, vérifiez que les informations relatives au créancier (nom/raison sociale, adresse) sont en cohérence avec vos engagements contractuels. Si votre banque a mis en place une liste des créanciers autorisés à effectuer des prélèvements sur votre compte (appelée aussi « liste blanche »), pensez à la mettre à jour.

- Si vous êtes bénéficiaire d'un paiement à distance et que vous ne connaissez pas personnellement le payeur (par exemple, en situation de vente sur internet), vérifiez la cohérence des informations fournies (nom, adresse, identifiant du payeur, etc.) avant de donner votre accord à la transaction. En cas de doute, vérifiez auprès de la banque du payeur la régularité du moyen de paiement proposé et la qualité du payeur.

- Si vous êtes bénéficiaire d'un chèque de banque (par exemple, en cas de vente d'un véhicule), contactez la banque émettrice en recherchant par vous-mêmes ses coordonnées (sans vous fier aux mentions présentes sur le chèque) pour en confirmer la validité avant de finaliser la transaction.

- Vérifiez la présence effective des mentions obligatoires d'un chèque, notamment la signature de l'émetteur du chèque, le nom de la banque qui doit payer, une indication de la date et du lieu où le chèque est établi, ainsi que la cohérence des informations (bénéficiaire, montant, zone numéro de chèque de la ligne magnétique) et l'absence de ratures ou surcharges pouvant indiquer une origine frauduleuse.

Lors de vos déplacements à l'étranger

- Renseignez-vous sur les précautions à prendre et contactez avant votre départ l'établissement émetteur de votre carte, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.

- Pensez à vous munir des numéros internationaux de mise en opposition de vos moyens de paiement.

Sachez réagir

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

- Faites immédiatement opposition en appelant le numéro que vous a communiqué votre banque ou l'émetteur de votre moyen de paiement. Pensez à le faire pour toutes vos cartes, chéquiers ou appareils mobiles comportant une application de paiement qui ont été perdus ou volés. De même contactez votre banque si vous avez communiqué vos coordonnées bancaires (numéro de compte, relevé d'identité bancaire, etc.) à un tiers qui vous parait douteux.

- En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 150 euros. Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

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

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

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

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

Si, dans un délai de 13 mois à compter de la date de débit de l'opération contestée (délai fixé par la loi), vous déposez une réclamation auprès de votre établissement teneur de compte, les sommes contestées doivent vous être immédiatement remboursées sans frais. Dans ces conditions, votre responsabilité ne peut être

engagée. Néanmoins ceci ne vaut pas en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir) ou en cas de non respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir). Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l'opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir néanmoins dépasser 120 jours.

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

A2 Protection du payeur en cas de paiement non autorisé

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

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

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

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

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

Opérations nationales ou intracommunautaires

Ces dispositions de protection du payeur couvrent :

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

et réalisées en euros ou dans la devise nationale de l'un de ces États.

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

Avant information aux fins de blocage de l'instrument de paiement

Avant l'information aux fins de blocage de l'instrument de paiement, le payeur pourra supporter, à concurrence de cinquante euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de l'instrument de paiement. Toutefois, si l'opération de paiement est effectuée sans utilisation des données de sécurité

2 L'ordonnance du 9 août 2017 transposant la DSP2 prévoit qu'une large part de ses dispositions s'applique à la Nouvelle-Calédonie, à la Polynésie française et au territoire des îles Wallis et Futuna.

personnalisées ou que le payeur ne pouvait pas détecter la perte ou le vol de son instrument de paiement, ou que la perte résulte d'une action d'une personne placée sous la responsabilité du PSP, le payeur ne voit pas sa responsabilité engagée et ne supporte aucune perte financière (même en-deçà de cinquante euros).

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

En revanche, le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à ses obligations de sécurité, d'utilisation ou de blocage de l'instrument de paiement, convenues avec son PSP.

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

Après information aux fins de blocage de l'instrument de paiement

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

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

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

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

Opérations extraeuropéennes

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

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

- l'émetteur est situé à Saint-Pierre-et-Miquelon ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le PSP est situé dans un État non européen [3], quelle que soit la devise dans laquelle l'opération de paiement est réalisée,

- l'émetteur est situé en Nouvelle-Calédonie, en Polynésie française ou à Wallis-et-Futuna, au profit d'un bénéficiaire dont le PSP est situé dans un État autre que la République française, quelle que soit la devise utilisée.

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

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

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

A3 Missions et organisation de l'Observatoire

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

Périmètre concerné

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

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

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

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

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

- les cartes de débit sont des cartes associées à un compte de paiement permettant à son titulaire d'effectuer des paiements ou retraits qui seront débités selon un délai fixé par le contrat de délivrance de la carte ;

- les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai. L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

- les cartes commerciales, délivrées à des entreprises, à des organismes publics ou à des personnes physiques exerçant une activité indépendante, ont une utilisation limitée aux frais professionnels, les paiements effectués au moyen de ce type de cartes étant directement facturés au compte de l'entreprise, de l'organisme public ou de la personne physique exerçant une activité indépendante ;

- les cartes prépayées permettent de stocker de la monnaie électronique.

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

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

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

Attributions

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

- Il assure le suivi de la mise en œuvre des mesures adoptées par les émetteurs, les commerçants et les entreprises pour renforcer la sécurité des moyens de paiement.

- Il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de moyens de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents moyens de paiement scripturaux.

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

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

Composition

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

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

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

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

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

Modalités de fonctionnement

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

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

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

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

A4 Liste nominative des membres de l'Observatoire

En application de l'article R. 142-22 du Code monétaire et financier, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre de l'Économie et des Finances. Le dernier arrêté de nomination date du 16 juin 2017.

Président
François VILLEROY de GALHAU
Gouverneur de la Banque de France

Représentants des assemblées

Éric BOCQUET
Sénat
Rémy REBEYROTTE
Assemblée nationale

Représentant du secrétariat général de l'Autorité de contrôle prudentiel et de résolution

Édouard FERNANDEZ-BOLLO
Secrétaire général

Nathalie BEAUDEMOULIN
Geoffroy GOFFINET

Représentants des administrations

Sur proposition du secrétariat général de la Défense et de la Sécurité nationale :

- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  Guillaume POUPARD
  Vincent STRUBEL

Sur proposition du ministre de l'Économie et des Finances :

- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Christian DUFOUR
  Yuksel AYDIN
  Philippe PAPILLON

- Le directeur général du Trésor
  ou son représentant :
  Odile RENAUD-BASSO
  Arnaud DELAUNAY

- Le directeur général des Entreprises
  ou son représentant :
  Pascal FAURE
  Loïc DUFLOT
  Geoffroy HERMANN

- Le directeur général de la Concurrence,
  de la Consommation et de la Répression
  des fraudes ou son représentant :
  Éric MAURUS
  Madly MERI

Sur proposition du garde des Sceaux,
ministre de la Justice :

- Le directeur des Affaires criminelles
  et des Grâces ou son représentant :
  Guillaume LEFEVRE-PONTALIS
  Adélaïde BARRY-DELONGCHAMPS
  Raphaëlle OLIVE

Sur proposition du ministre de l'Intérieur :

- Le chef de l'Office central de lutte contre la
  criminalité liée aux technologies
  de l'information et de la communication
  ou son représentant :
  François-Xavier MASSON

Sur proposition du ministre de la Défense :

- Le directeur général de la Gendarmerie
  nationale ou son représentant :
  Nicolas DUVINAGE
  Cyril PIAT

Sur proposition de la Commission nationale
de l'informatique et des libertés

- Le chef du service des Affaires économiques
  ou son représentant :
  Clémence SCOTTEZ
  David RUIZ

Représentants des émetteurs de moyens de paiement et des opérateurs de systèmes de paiement

Andrée BERTRAND
Membre du bureau
Association française
des établissements de paiement
et de monnaie électronique (Afepame)

Nathalie CHABERT
Responsable communication
et relations institutionnelles
Association française
du multimédia mobile (AFMM)

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

Jean-Marie DRAGON
Responsable Monétique et Paiements innovants
BNP Paribas (BNPP)

Olivier DURAND
Directeur en charge des projets de place
Office de coordination bancaire
et financière (OCBF)

Caroline GAYE
Directeur général
American Express France (Amex)

Solveig HONORÉ HATTON
Vice-présidente *Business development*
MasterCard France

Philippe LAULANIE
Administrateur
Groupement des cartes bancaires (GCB)

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

Gérard NÉBOUY
Directeur régional
Visa Europe France

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

Caroline SELLIER
Directeur – *Risk management*
et Lutte contre la fraude
Natixis Payment Solutions

Jean-Marie VALLÉE
Directeur général
STET

Narinda YOU
Directeur – Stratégie et Relations de place
Crédit Agricole

Représentants des entreprises

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

Delphine KOSSER-GLORIES
Responsable du département
des Affaires économiques
Mouvement des entreprises de France (Medef)

Christophe LESOBRE
Président de la Commission monétique
et moyens de paiement
Association française
des trésoriers d'entreprises (AFTE)

Représentants du collège « consommateurs » du Conseil national de la consommation

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

Morgane LENAIN
Juriste
Union nationale des associations familiales (Unaf)

Mathieu ROBIN
Chargé de mission Banque Assurance
UFC – Que choisir

Hervé MONDANGE
Juriste
Association Force ouvrière consommateurs (Afoc)

Ariane POMMERY
Juriste
Association de défense d'éducation
et d'information du consommateur (Adeic)

Représentants des organisations professionnelles de commerçants

Jean-Michel CHANAVAS
Délégué général
Mercatel

Vincent DEPRIESTER
Membre du groupe Finances
Fédération du commerce
et de la distribution (FCD)

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

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

Philippe SOLIGNAC
Vice-président
Chambre de commerce et d'industrie
de Paris – Île de France (CCIP)

Personnalités qualifiées en raison de leurs compétences

Claude FRANCE
Directeur général des opérations France
Worldline

David NACCACHE
Professeur
École normale supérieure (ENS)

A5 Méthodologie de mesure de la fraude aux moyens de paiement scripturaux

Cadre général

Définition de la fraude aux moyens de paiement

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

• **ayant pour conséquence un préjudice financier** : pour l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire du moyen de paiement, le bénéficiaire légitime des fonds (l'accepteur et/ou créancier), un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ;

• **quel que soit le mode opératoire retenu** :

– les moyens employés pour récupérer, sans motif légitime, les données ou le support du moyen de paiement (vol, détournement du support ou des données, piratage d'un équipement d'acceptation, etc.),

– les modalités d'utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait, en situation de proximité ou à distance, par utilisation physique de l'instrument de paiement ou des données qui lui sont attachées, etc.),

– la zone géographique d'émission ou d'utilisation du moyen de paiement ou des données qui lui sont attachées ;

• **et quelle que soit l'identité du fraudeur** : un tiers, l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

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

- les tentatives de fraude (auquel cas la fraude est stoppée avant exécution de l'opération) ;

- les utilisations irrégulières d'un moyen de paiement du seul fait d'un défaut de provision suffisante et se traduisant notamment par un impayé ;

- l'utilisation d'une fausse identité ou d'une identité usurpée pour ouvrir un compte et/ou pour obtenir un moyen de paiement en vue de réaliser des paiements.

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

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

Typologie de la fraude aux moyens de paiement

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

1 Cf. *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2015.pdf#page=11*

• **faux** (vol, perte, contrefaçon) : fraude par l'établissement d'un faux ordre de paiement soit au moyen d'un instrument de paiement physique (carte, chéquier, etc.) volé, perdu ou contrefait, soit *via* le détournement de données ou d'identifiants bancaires ;

• **falsification** : fraude par l'utilisation d'un instrument de paiement falsifié (instrument de paiement authentique dont les caractéristiques physiques ou les données attachées ont été modifiées par le fraudeur ou par un complice) ou par altération d'un ordre de paiement régulièrement émis en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.) ;

• **détournement** : fraude visant à utiliser l'instrument de paiement ou l'ordre de paiement sans altération ou modification d'attribut (à titre d'exemple, un fraudeur encaisse un chèque non altéré sur un compte qui n'est pas détenu par le bénéficiaire légitime du chèque) ;

• **rejeu** : fraude par l'utilisation abusive d'un instrument de paiement par son titulaire légitime après la déclaration de sa perte ou de son vol ou par la contestation de mauvaise foi d'un ordre de paiement valablement émis par le titulaire légitime de l'instrument de paiement, ou par la réutilisation d'un ordre de paiement déjà traité.

Mesure de la fraude à la carte de paiement

Transactions couvertes

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

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

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

Origine des données de fraude

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

- du Groupement des cartes bancaires CB, de MasterCard et de Visa pour ce qui concerne les opérations réalisées par leurs membres ;
- des émetteurs de cartes privatives actifs en France.

Éléments d'analyse de la fraude

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

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

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

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

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

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

Mesure de la fraude au virement

Instruments de paiement couverts

La fraude sur le virement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement émis par le débiteur – appelé donneur d'ordre – afin de transférer des fonds de son compte de paiement ou de monnaie électronique vers le compte d'un bénéficiaire tiers. Cette catégorie recouvre à la fois les virements au format européen SEPA (*SEPA credit transfert et SEPA credit transfert inst*) et les virements de clientèle émis *via* les systèmes de paiement de gros montant (notamment le système Target 2 opéré par les banques centrales nationales de l'Eurosystème, ainsi que le système privé paneuropéen Euro1).

Origine des données de fraude

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

Éléments d'analyse de la fraude

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

Typologies de fraude sur le virement	Forme de la fraude
Faux	Le fraudeur contrefait un ordre de virement, contraint le titulaire légitime à émettre un ordre de virement, ou usurpe les identifiants de la banque en ligne du donneur d'ordre légitime afin d'initier un ordre de paiement (dans ce cas de figure, les identifiants peuvent notamment être obtenus *via* des procédés de piratage informatique (*phishing*, *malware,* etc.) ou sous la contrainte.
Falsification	Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime.
Détournement	Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.), le titulaire légitime du compte à émettre régulièrement un virement
Zone géographique d'émission et de destination du virement	**Description**
Virement national :	Virement émis depuis un compte tenu en France vers un compte tenu en France.
Virement européen	Virement émis depuis un compte tenu en France vers un compte tenu dans un autre pays de la zone SEPA.
Virements hors zone SEPA	Virement émis depuis un compte tenu en France vers un compte tenu dans un pays étranger hors zone SEPA.
Canaux d'initiation utilisés	**Modalités d'utilisation**
Papier	Ordre de virement transmis par courrier, formulaire, courriel, télécopie ou téléphone.
Internet	Ordre de virement transmis par la banque en ligne ou par une application de paiement mobile.
Télématique	Ordre de virement transmis *via* d'autres canaux électroniques hors banque en ligne et application de paiement mobile, tels que par exemple le système EBICS (*electronic banking internet communication standard*, canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque).

4 Établissements habilités à tenir des comptes de paiement pour le compte de leur clientèle et émettre des moyens de paiement relevant des statuts suivants au sens des réglementations françaises et européennes :

- établissements de crédit ou assimilés (institutions visées à l'article L. 518-1 du Code monétaire et financier), établissements de monnaie électronique et établissements de paiement de droit français ;
- établissements de crédit, établissements de monnaie électronique et établissements de paiement de droit étranger habilités à intervenir sur le territoire français et implantés sur ce dernier.

Le fraudeur contrefait un ordre de virement, contraint le titulaire légitime à émettre un ordre de virement, ou usurpe les identifiants de la banque en ligne du donneur d'ordre légitime afin d'initier un ordre de paiement (dans ce cas de figure, les identifiants peuvent notamment être obtenus *via* des procédés de piratage informatique (*phishing*, *malware*, etc.) ou sous la contrainte.

Mesure de la fraude au prélèvement

Instruments de paiement couverts

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

Origine des données de fraude

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

Éléments d'analyse de la fraude

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

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

Zones géographiques d'émission et de destination du prélèvement	Description
Prélèvement national	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu en France.
Prélèvement européen	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un autre pays de la zone SEPA.
Prélèvement hors zone SEPA	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un pays étranger, hors zone SEPA.

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

Mesure de la fraude sur le chèque

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

Périmètre de la fraude

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

Cette définition intègre les titres suivants : chèque bancaire, chèque de banque, lettre-chèque pour les entreprises, titre de travail simplifié aux entreprises (TTS) ; elle exclut les chèques de voyage, ainsi que les titres spéciaux de paiement définis par l'article L. 525-4 du code monétaire et financier, tels que les

chèques-vacances, les chèques ou titres restaurant, les chèques culture, les chèques emploi-service universels, etc., qui recouvrent des catégories variées de titres dont l'usage est restreint, soit à l'acquisition d'un nombre limité de biens ou de services, soit à un réseau limité d'accepteurs.

Origines des données de fraude

Les données de fraude sur le chèque sont fournies par la Banque de France et proviennent des déclarations règlementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés. Ces derniers effectuent leur déclaration soit en qualité d'établissement recevant de son client des chèques à l'encaissement (établissement remettant), soit en qualité d'établissement qui tient le compte du payeur (établissement tiré).

Éléments d'analyse des données de fraude

Les données de fraude sur le chèque sont analysées à partir des grandes typologies de fraude définies par l'Observatoire.

Pour le chèque, le tableau ci-après récapitule les formes de la fraude les plus couramment observées et la typologie à laquelle elles se rattachent.

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

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

Mesure de la fraude aux effets de commerce

Instruments de paiement couverts

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

- la lettre de change relevé (LCR) : instrument de paiement sur support papier ou dématérialisé par lequel le payeur (généralement, le fournisseur) donne à son débiteur (son client) l'ordre de lui payer une somme d'argent déterminée ;

- le billet à ordre relevé (BOR) : ordre de paiement dématérialisé par lequel le payeur se reconnaît débiteur du bénéficiaire et promet de payer une certaine somme d'argent à un certain terme, tous deux spécifiés sur le titre.

Typologie et origine des données de fraude

Les typologies de fraude sur les effets de commerce sont les mêmes que celles définies pour les chèques.

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

Dispositions spécifiques pour la fraude sur les transactions en monnaie électronique

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

On distingue deux catégories de support de monnaie électronique :

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

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

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

A6 Dossier statistique

Note de l'éditeur : du fait d'une révision *a posteriori* au moment de la collecte des données 2017, certaines données 2016 présentées dans le chapitre 2 et dans la présente annexe diffèrent des données publiées dans le rapport annuel 2016 de l'Observatoire. Les corrections portent sur la ventilation des paiements par carte par canal d'initiation, entre paiements de proximité et paiements à distance.

Vue d'ensemble

T1 Cartographie des moyens de paiement scripturaux en 2017

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

	Nombre de transactions		Montant des transactions		Montant moyen
	2017	Variation 2017/2016	2017	Variation 2017/2016	
Paiement carte [a]	12 581	+ 13	530	+ 6	42
Prélèvement	4 091	+ 3	1 579	+ 6	386
Virement	3 870	+ 3	24 069	+ 2	6 220
dont VGM [b]	*10*	*+ 5*	*9 482*	*- 6*	*977 085*
Chèque	1 927	- 10	1 002	- 7	520
Effet de commerce	81	- 2	260	- 2	3 217
Monnaie électronique	55	+ 45	1	+ 52	16
Total	**22 605**	**+ 7**	**27 441**	**2**	**1 213**
Retrait carte [a]	1 481	- 1	135	+ 4	91
Total transactions	**24 086**	**+7**	**27 576**	**+ 2**	**1 145**

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

T2 Répartition de la fraude sur les moyens de paiement en montant et en volume en 2017

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

	Montant		Volume		Montant moyen
	2017	Part	2017	Part	
Paiement carte [a]	318 126 046	43	4 749 201	93	67
Chèque	296 072 847	40	114 906	2	2 577
Virement	78 286 492	10	4 642	0	16 864
Prélèvement	8 753 357	1	25 806	1	339
Effet de commerce	153 100	0	3	0	51 033
Total paiements	**701 391 842**	**94**	**4 894 558**	**96**	**143**
Retrait carte [a]	42 455 967	6	189 730	4	224
Total transactions	**743 847 809**	**100**	**5 084 288**	**100**	**146**

a) Cartes émises en France uniquement.
Source : Observatoire de la sécurité des moyens de paiement.

Statistiques de fraude sur les cartes de paiement

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

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

En 2017, le nombre de cartes en circulation s'élève à 86 millions dont :

- 76,1 millions de cartes de type « interbancaire » (CB, MasterCard, Visa, etc.) ;
- 9,9 millions de cartes de type « privatif ».

Le nombre de cartes [1] mises en opposition en 2017 est d'environ 1 213 008.

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

T3 Le marché des cartes de paiement en France – Émission

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

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	10 521,34	395,5	256,74	12,89	52,86	4,06
Paiements à distance hors internet	22,09	1,63	12	0,96	7,28	0,52
Paiements à distance sur internet	1 257,26	78,27	220,11	13,19	67,16	2,96
Retraits	1 426,30	128,12	32,30	3,57	20,6	3,04
Total	**13 226,99**	**603,52**	**521,15**	**30,61**	**147,90**	**10,58**
Cartes de type « privatif »						
Paiements de proximité et sur automate	124,31	14,07	8,64	1,16	6,03	1,01
Paiements à distance hors internet	4,20	0,44	2,95	0,04	0,25	0,03
Paiements à distance sur internet	10,82	1,87	5,90	0,92	1,14	0,19
Retraits	2,28	0,20	0,00	0,00	0,00	0,00
Total	**141,60**	**16,58**	**17,49**	**2,12**	**7,42**	**1,23**
Total général	**13 368,59**	**620,10**	**538,64**	**32,73**	**155,32**	**11,81**

Source : Observatoire de la sécurité des moyens de paiement.

T4 Le marché des cartes de paiement en France - Acceptation

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	10 521,34	395,50	329,12	17,64	81,64	7,66
Paiements à distance hors internet	22,09	1,63	9,66	1,56	4,99	1,33
Paiements à distance sur internet	1 257,26	78,27	64,27	6,44	22,15	3,44
Retraits	1 426,30	128,12	23,63	3,94	7,69	1,83
Total	**13 226,99**	**603,52**	**426,68**	**29,57**	**116,47**	**14,26**
Cartes de type « privatif »						
Paiements de proximité et sur automate	124,31	14,07	9,49	1,63	10,33	4,44
Paiements à distance hors internet	4,20	0,44	0,40	0,02	0,23	0,00
Paiements à distance sur internet	10,82	1,87	2,04	0,29	0,82	0,22
Retraits	2,28	0,20	0,00	0,00	0,62	0,28
Total	**141,60**	**16,58**	**11,93**	**1,94**	**12,00**	**4,94**
Total général	**13 368,59**	**620,11**	**438,61**	**31,51**	**128,47**	**19,19**

Source : Observatoire de la sécurité des moyens de paiement.

T5 Répartition de la fraude par type de carte

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

	Taux de fraude (et montant)											
	2012		2013		2014		2015		2016		2017	
Cartes de type « interbancaire »	0,080	(434,4)	0,080	(455,8)	0,080	(486,4)	0,083	(507,2)	0,077	(504,0)	0,066	(459,3)
Cartes de type « privatif »	0,076	(16,3)	0,065	(14,0)	0,062	(14,2)	0,068	(15,5)	0,060	(13,5)	0,043	(11,6)
Total	**0,080**	**(450,7)**	**0,080**	**(469,9)**	**0,080**	**(500,6)**	**0,082**	**(522,7)**	**0,077**	**(517,5)**	**0,065**	**(467,0)**

Source : Observatoire de la sécurité des moyens de paiement.

T6 Répartition de la fraude par zone géographique

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

	Taux de fraude (et montant)											
	2012		2013		2014		2015		2016		2017	
Transactions nationales	0,045	(226,4)	0,046	(238,6)	0,043	(234,6)	0,040	(225,0)	0,037	(217,2)	0,032	(199,7)
Transactions internationales	0,380	(224,3)	0,350	(231,3)	0,316	(266,0)	0,372	(297,9)	0,353	(300,3)	0,281	(267,3)
dont carte française et accepteur hors SEPA	*0,759*	*(62,5)*	*0,688*	*(70,2)*	*0,636*	*(70,0)*	*0,692*	*(74,5)*	*0,713*	*(68,0)*	*0,511*	*(60,3)*
dont carte française et accepteur SEPA	*0,316*	*(56,3)*	*0,366*	*(67,9)*	*0,374*	*(91,0)*	*0,459*	*(116,8)*	*0,370*	*(113,9)*	*0,308*	*(100,7)*
dont carte étrangère hors SEPA et accepteur français	*0,639*	*(78,2)*	*0,404*	*(64,1)*	*0,336*	*(65,6)*	*0,353*	*(69,7)*	*0,449*	*(73,7)*	*0,386*	*(74,1)*
dont carte étrangère SEPA et accepteur français	*0,132*	*(27,3)*	*0,135*	*(29,1)*	*0,134*	*(39,3)*	*0,153*	*(36,9)*	*0,158*	*(44,7)*	*0,102*	*(32,3)*
Total	**0,080**	**(450,7)**	**0,080**	**(469,9)**	**0,080**	**(500,6)**	**0,082**	**(522,9)**	**0,077**	**(517,5)**	**0,066**	**(467,0)**

Source : Observatoire de la sécurité des moyens de paiement.

T7 Répartition de la fraude nationale par type de transaction

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

	Taux de fraude (et montant)											
	2012		2013		2014		2015		2016		2017	
Paiements	0,049	(190,0)	0,050	(199,9)	0,046	(193,2)	0,043	(185,1)	0,039	(181,5)	0,034	(165,1)
dont paiements de proximité et sur automate	*0,015*	*(51,2)*	*0,013*	*(45,8)*	*0,010*	*(37,1)*	*0,009*	*(34,7)*	*0,007*	*(29,2)*	*0,008*	*(33,1)*
dont paiements à distance	*0,299*	*(138,8)*	*0,269*	*(154,2)*	*0,248*	*(156,0)*	*0,228*	*(150,4)*	*0,210*	*(152,3)*	*0,161*	*(132,0)*
– dont par courrier / téléphone	*0,338*	*(29,4)*	*1,122*	*(29,2)*	*0,147*	*(2,8)* [a]	*0,208*	*(5,1)*	*0,176*	*(5,8)*	*0,218*	*(4,5)*
– dont sur internet	*0,290*	*(109,4)*	*0,229*	*(125,0)*	*0,251*	*(153,2)* [a]	*0,229*	*(145,3)*	*0,211*	*(146,5)*	*0,159*	*(127,5)*
Retraits	0,031	(36,4)	0,033	(38,6)	0,034	(41,5)	0,033	(39,9)	0,029	(35,7)	0,027	(34,6)
Total	**0,045**	**(226,4)**	**0,046**	**(238,6)**	**0,043**	**(234,6)**	**0,040**	**(225,0)**	**0,037**	**(217,2)**	**0,032**	**(199,7)**

a) La diminution très importante entre 2013 et 2014, du montant de la fraude sur les paiements à distance effectués par courrier ou par téléphone, et à l'inverse l'augmentation de celle sur les paiements sur internet, s'expliquent pour grande partie par une modification de la méthodologie statistique utilisée par le Groupement des cartes bancaires CB. Un ajustement plus léger a également été effectué en 2015. Voir le rapport annuel 2014 pour plus de détails.
Source : Observatoire de la sécurité des moyens de paiement

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

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

	Taux de fraude (et montant)				
	2013	2014	2015	2016	2017
Carte française – accepteur étranger hors SEPA					
Paiements	0,547 (40,3)	0,532 (41,7)	0,735 (56,3)	0,862 (56,2)	0,608 (53,4)
dont paiements de proximité et sur automate	*0,377 (17,7)*	*0,350 (19,2)*	*0,509 (25,8)*	*0,485 (23,0)*	*0,252 (12,7)*
dont paiements à distance	*0,848 (22,6)*	*0,960 (22,5)*	*1,174 (30,5)*	*1,862 (33,3)*	*1,096 (40,6)*
– dont par courrier / téléphone	*1,234 (6,4)*	*4,955 (7,5)*	*2,345 (9,5)*	*2,783 (9,4)*	*1,499 (8,4)*
– dont sur internet	*0,755 (16,2)*	*0,682 (14,9)*	*0,959 (21,1)*	*1,648 (23,9)*	*1,025 (32,3)*
Retraits	1,054 (29,9)	0,890 (28,3)	0,586 (18,1)	0,390 (11,8)	0,229 (7,0)
Total	**0,688 (70,2)**	**0,636 (70,0)**	**0,692 (74,5)**	**0,713 (68,0)**	**0,511 (60,3)**
Carte française – accepteur étranger SEPA					
Paiements	0,434 (66,8)	0,434 (89,8)	0,526 (115,7)	0,422 (112,9)	0,342 (99,8)
dont paiements de proximité et sur automate	*0,089 (8,2)*	*0,067 (7,8)*	*0,071 (8,0)*	*0,066 (8,4)*	*0,075 (10,5)*
dont paiements à distance	*0,937 (58,6)*	*0,910 (82,0)*	*1,004 (107,7)*	*0,754 (104,5)*	*0,591 (89,2)*
– dont par courrier / téléphone	*1,566 (11,3)*	*1,317 (13,9)*	*1,399 (18,7)*	*1,317 (19,7)*	*1,489 (14,9)*
– dont sur internet	*0,856 (47,3)*	*0,856 (68,1)*	*0,948 (89,0)*	*0,687 (84,9)*	*0,527 (74,4)*
Retraits	0,036 (1,1)	0,033 (1,2)	0,033 (1,1)	0,024 (0,9)	0,025 (0,9)
Total	**0,366 (67,9)**	**0,374 (91,0)**	**0,459 (116,8)**	**0,370 (113,8)**	**0,308 (100,7)**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	Taux de fraude (et montant)				
	2013	2014	2015	2016	2017
Carte étrangère hors SEPA – accepteur français					
Paiements	0,451 (63,2)	0,380 (65,0)	0,391 (68,1)	0,507 (73,2)	0,429 (73,3)
dont paiements de proximité et sur automate	*0,230 (25,3)*	*0,162 (21,9)*	*0,168 (22,8)*	*0,169 (17,4)*	*0,135 (16,3)*
dont paiements à distance	*1,268 (37,9)*	*1,213 (43,1)*	*1,185 (45,3)*	*1,341 (55,8)*	*1,143 (57,0)*
– dont par courrier / téléphone	*0,930 (9,2)*	*1,018 (7,7)*	*1,159 (10,8)*	*1,748 (18,2)*	*1,488 (19,8)*
– dont sur internet	*1,436 (28,7)*	*1,265 (35,4)*	*1,193 (34,5)*	*1,206 (37,7)*	*1,017 (37,2)*
Retraits	0,051 (0,9)	0,026 (0,6)	0,069 (1,6)	0,024 (0,5)	0,038 (0,8)
Total	**0,404 (64,1)**	**0,336 (65,6)**	**0,353 (69,7)**	**0,449 (73,7)**	**0,386 (74,1)**
Carte étrangère SEPA – accepteur français					
Paiements	0,158 (28,2)	0,156 (38,5)	0,175 (36,0)	0,178 (43,8)	0,114 (31,5)
dont paiements de proximité et sur automate	*0,039 (4,9)*	*0,026 (5,1)*	*0,033 (4,8)*	*0,024 (3,7)*	*0,018 (3,5)*
dont paiements à distance	*0,458 (23,2)*	*0,476 (33,1)*	*0,528 (31,3)*	*0,456 (40,0)*	*0,337 (28,0)*
– dont par courrier / téléphone	*0,308 (3,8)*	*0,397 (4,8)*	*0,734 (7,7)*	*0,695 (11,0)*	*0,564 (8,9)*
– dont sur internet	*0,506 (19,4)*	*0,492 (28,6)*	*0,484 (23,6)*	*0,403 (29,0)*	*0,284 (19,1)*
Retraits	0,025 (0,9)	0,018 (0,9)	0,025 (0,9)	0,024 (0,9)	0,019 (0,7)
Total	**0,135 (29,1)**	**0,134 (39,3)**	**0,153 (36,9)**	**0,158 (44,7)**	**0,102 (32,3)**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

2017	Tous types de carte		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	64,2	32,2	63,8	32,5	0,4	14,1
Carte non parvenue	0,9	0,4	0,6	0,3	0,3	9,9
Carte altérée ou contrefaite	1,2	0,6	1,0	0,5	0,2	4,9
Numéro usurpé	132,0	66,1	130,9	66,6	1,1	33,5
Autres	1,4	0,7	0,2	0,1	1,2	37,6
Total	**199,7**	**100,0**	**196,5**	**100,0**	**3,2**	**100,0**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	720,0	31 257,1	137,1	10 046,8	81,6	12 205,2
Cartes perdues ou volées	694,3	30 128,1	60,0	3 926,8	16,8	2 643,6
Cartes non parvenues	9,8	371,0	0,5	54,0	0,1	11,5
Cartes altérées ou contrefaites	13,5	562,4	14,8	1 900,4	46,0	6 802,4
Numéros de cartes usurpés	0,7	113,2	54,0	3 439,9	11,9	1 866,7
Autres	1,7	82,4	7,8	725,7	6,8	881,0
Paiements à distance hors internet	35,7	3 911,7	189,6	14 440,3	59,8	8 095,6
Cartes perdues ou volées	0,2	4,7	10,5	1 625,1	4,7	700,5
Cartes non parvenues	0,0	0,2	0,1	6,0	0,1	4,5
Cartes altérées ou contrefaites	0,0	4,1	4,5	349,3	1,7	280,4
Numéros de cartes usurpés	35,3	3 896,3	174,1	12 430,9	53,0	7 087,5
Autres	0,2	6,5	0,4	29,1	0,3	22,7
Paiements à distance sur internet	1 747,7	126 919,3	1 264,7	73 381,8	472,3	31 799,8
Cartes perdues ou volées	0,6	22,3	42,9	2 880,2	19,6	1 376,8
Cartes non parvenues	0,0	0,1	0,3	21,3	0,2	16,8
Cartes altérées ou contrefaites	0,1	5,7	20,9	1 456,9	10,6	863,5
Numéros de cartes usurpés	1 746,6	126 879,4	1 198,7	68 866,8	438,4	29 369,3
Autres	0,2	11,9	1,9	156,6	3,5	173,4
Retraits	132,6	34 395,8	4,4	889,3	51,5	6 967,8
Cartes perdues ou volées	118,7	33 629,5	3,0	681,8	3,7	579,8
Cartes non parvenues	0,7	197,9	0,0	3,2	0,1	8,5
Cartes altérées ou contrefaites	12,4	469,2	0,8	121,1	45,5	6 089,3
Numéros de cartes usurpés	0,0	1,1	0,1	9,7	0,6	79,9
Autres	0,8	98,0	0,5	73,6	1,6	210,3
Total	**2 636,0**	**196 483,9**	**1 595,8**	**98 758,2**	**665,1**	**59 068,3**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	720,0	31 257,1	26,8	3 347,1	66,7	14 761,5
Cartes perdues ou volées	694,3	30 128,1	15,2	1 851,4	24,8	6 063,1
Cartes non parvenues	9,8	371,0	0,4	41,8	0,2	70,4
Cartes altérées ou contrefaites	13,5	562,4	2,8	235,5	30,2	5 390,9
Numéros de cartes usurpés	0,7	113,2	7,6	894,3	10,3	2 311,9
Autres	1,82	82,4	0,8	324,1	1,2	925,2
Paiements à distance hors internet	35,7	3 911,7	29,6	8 413,3	42,9	18 535,2
Cartes perdues ou volées	0,2	4,6	0,9	142,7	1,8	509,5
Cartes non parvenues	0,0	0,2	0,0	12,4	0,0	12,6
Cartes altérées ou contrefaites	0,0	4,1	1,3	372,5	2,4	782,0
Numéros de cartes usurpés	35,3	3 896,3	27,3	7 865,1	38,5	17 148,0
Autres	0,2	6,5	0,1	20,6	0,2	83,1
Paiements à distance sur internet	1 747,7	126 919,3	119,8	18 564,6	192,0	36 023,5
Cartes perdues ou volées	0,6	22,2	2,2	237,9	8,5	1 086,0
Cartes non parvenues	0,0	0,1	0,1	25,4	0,2	30,2
Cartes altérées ou contrefaites	0,1	5,7	2,3	303,4	13,2	2 085,4
Numéros de cartes usurpés	1 746,6	126 879,4	114,4	17 771,3	168,1	32 233,8
Autres	0,3	11,9	0,8	226,6	2,0	588,0
Retraits	132,6	34 395,8	3,2	749,4	2,2	669,5
Cartes perdues ou volées	118,7	33 629,6	3,0	698,5	0,9	247,7
Cartes non parvenues	0,7	197,9	0,0	6,6	0,0	2,8
Cartes altérées ou contrefaites	12,4	469,2	0,1	22,9	1,0	248,1
Numéros de cartes usurpés	0,0	1,1	0,1	13,0	0,2	57,4
Autres	0,8	98,0	0,0	8,4	0,1	113,5
Total	**2 636,0**	**196 483,9**	**179,5**	**31 074,3**	**303,9**	**69 989,6**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	3,6	1 815,5	1,1	479,1	3,3	533,8
Cartes perdues ou volées	0,9	253,8	0,3	47,7	0,7	202,7
Cartes non parvenues	0,8	254,8	0,1	91,0	0,0	1,7
Cartes altérées ou contrefaites	0,1	147,6	0,2	105,5	2,0	161,9
Numéros de cartes usurpés	0,3	40,6	0,4	220,7	0,5	160,4
Autres	1,5	1 118,7	0,1	14,2	0,1	7,1
Paiements à distance hors internet	2,3	597,2	8,6	414,9	2,9	263,9
Cartes perdues ou volées	0,1	6,2	0,2	8,7	0,0	3,1
Cartes non parvenues	0,0	3,0	0,0	0,4	0,0	0,0
Cartes altérées ou contrefaites	0,0	5,7	0,1	17,1	0,1	12,9
Numéros de cartes usurpés	2,1	527,5	8,3	380,6	2,8	244,7
Autres	0,1	54,8	0,0	8,1	0,0	3,2
Paiements à distance sur internet	1,7	585,6	13,7	999,8	3,5	459,6
Cartes perdues ou volées	0,1	33,4	0,1	4,5	0,0	1,7
Cartes non parvenues	0,0	15,7	0,0	1,4	0,0	0,1
Cartes altérées ou contrefaites	0,0	3,3	0,1	3,4	0,0	12,0
Numéros de cartes usurpés	1,5	504,1	13,4	968,7	3,5	443,6
Autres	0,1	29,1	0,1	21,8	0,0	2,2
Retraits	1,3	203,1	0,0	0,0	0,0	0,0
Cartes perdues ou volées	1,1	159,0	0,0	0,0	0,0	0,0
Cartes non parvenues	0,2	42,1	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,9	0,0	0,0	0,0	0,0
Numéros de cartes usurpés	0,0	1,1	0,0	0,0	0,0	0,0
Autres	0,0	0,0	0,0	0,0	0,0	0,0
Total	**8,9**	**3 201,3**	**23,4**	**1 893,8**	**9,7**	**1 257,3**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	3,6	1 815,5	0,7	167,5	3,2	1 546,8
Cartes perdues ou volées	0,9	253,8	0,2	55,9	0,8	498,2
Cartes non parvenues	0,8	254,8	0,2	26,7	0,0	15,1
Cartes altérées ou contrefaites	0,1	147,6	0,1	33,9	1,9	861,5
Numéros de cartes usurpés	0,3	40,6	0,1	39,0	0,3	90,6
Autres	1,5	1 118,7	0,1	12,0	0,2	81,3
Paiements à distance hors internet	2,3	597,2	0,9	483,9	2,7	1 238,9
Cartes perdues ou volées	0,1	6,2	0,0	16,2	0,1	21,5
Cartes non parvenues	0,0	3,0	0,0	6,1	0,0	1,0
Cartes altérées ou contrefaites	0,0	5,7	0,0	11,6	0,3	128,9
Numéros de cartes usurpés	2,0	527,5	0,9	450,0	2,2	1 053,5
Autres	0,2	54,8	0,0	0,0	0,1	34,0
Paiements à distance sur internet	1,7	585,6	1,5	527,2	4,2	1 160,7
Cartes perdues ou volées	0,1	33,4	0,0	3,6	0,2	61,6
Cartes non parvenues	0,0	15,7	0,0	3,7	0,0	9,8
Cartes altérées ou contrefaites	0,0	3,3	0,1	19,0	0,3	149,9
Numéros de cartes usurpés	1,5	504,1	1,4	490,8	3,7	929,0
Autres	0,1	29,1	0,0	10,1	0,0	10,4
Retraits	1,3	203,1	0,0	0,0	0,4	141,1
Cartes perdues ou volées	1,1	159,0	0,0	0,0	0,0	3,7
Cartes non parvenues	0,2	42,1	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,9	0,0	0,0	0,4	135,7
Numéros de cartes usurpés	0,0	1,1	0,0	0,0	0,0	0,0
Autres	0,0	0,0	0,0	0,0	0,0	1,7
Total	**8,9**	**3 201,3**	**3,2**	**1 178,6**	**10,5**	**4 087,5**

Source : Observatoire de la sécurité des moyens de paiement.

Statistiques de fraude sur le virement

T15 Répartition de la fraude au virement par zone géographique

(montant en euros, part en pourcentage)

	2017	
	Montant	Part
France	26 376 140	34
SEPA hors France	37 774 404	48
Hors SEPA	14 135 948	18
Total	**78 286 492**	**100**

Source : Observatoire de la sécurité des moyens de paiement.

Statistiques de fraude sur les prélèvements

T16 Répartition de la fraude au prélèvement par zone géographique

(montant en euros, part en pourcentage)

	2017	
	Montant	Part
France	8 650 490	99
SEPA hors France	75 913	1
Total	**8 726 403**	**100**

Source : Observatoire de la sécurité des moyens de paiement.

Statistiques de fraude sur le chèque

T17 Répartition par typologie de fraude en 2017

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

	Montant	Part	Volume	Montant moyen
Détournement, rejeu	10 002 809	3	1 946	5 140
Vol, perte (faux, apocryphe)	130 815 653	44	89 988	1 453
Contrefaçon	28 097 173	10	7 234	3 884
Falsification	127 157 212	43	15 738	8 079
Total	**296 072 847**	**100**	**114 906**	**2 577**

Source : Observatoire de la sécurité des moyens de paiement.

Éditeur
Banque de France
39 rue Croix-des-Petits-Champs
75001 Paris

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

Rédactrice en chef
Emmanuelle Assouan,
Directrice des Systèmes de paiement
et Infrastructures de marché
Banque de France

Secrétariat de rédaction
Véronique Bugaj, Olivier Catau, Guylène Chotard,
Caroline Corcy, Bernard Darrius, Florian Dintilhac,
Christelle Guiheneuc, Julien Lasalle,
Alexandra Madeline, Lucas Nozahic,
Alexandre Stervinou, Mathieu Vileyn

Réalisation
Studio Création
Direction de la Communication
de la Banque de France

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

Impression
Banque de France – SG - DISG

Dépôt légal
Juillet 2018

Internet
www.observatoire-paiements.fr

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