2014 | RAPPORT ANNUEL

DE L'OBSERVATOIRE DE LA SÉCURITÉ DES CARTES DE PAIEMENT

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

Observatoire
de la sécurité
des cartes de paiement

31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01
Code Courrier : 11-2323

Rapport annuel 2014
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Monsieur le ministre de l'Économie,
de l'Industrie et du Numérique
Monsieur le ministre des Finances et des Comptes publics
Monsieur le président du Sénat
Monsieur le président de l'Assemblée nationale

par

Christian Noyer,
gouverneur de la Banque de France,
président de l'Observatoire de la sécurité des cartes de paiement

L'Observatoire de la sécurité des cartes de paiement, mentionné au I de l'article L141-4 du Code monétaire et financier*, a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des systèmes de paiement par carte.*

Conformément à l'alinéa 6 de cet article, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'économie et au ministre chargé des finances et transmis au Parlement.

NB : Pour ses travaux, l'Observatoire distingue les systèmes de paiement par carte de type « interbancaire » et ceux de type « privatif ». Les premiers correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. Les seconds correspondent à ceux dans lesquels il existe un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs.

À ce titre, certains secteurs d'activité, notamment celui de la téléphonie et des communications, présentent des taux de fraude pour les transactions en ligne nettement supérieurs à l'ensemble des e-commerçants, appelant à une vigilance renforcée des acteurs concernés.

À l'inverse, le taux de fraude sur les retraits continue à progresser (0,034 %, après 0,033 % en 2013), dans un contexte où le piratage de distributeurs de billets et le vol de cartes avec code restent des malversations prisées des réseaux de fraude organisés.

Par ailleurs, les premières données statistiques relatives aux paiements en mode sans contact font ressortir un taux de fraude limité sur les neuf derniers mois de 2014, à 0,015 %, soit un niveau intermédiaire entre celui des paiements de proximité et celui des retraits aux distributeurs automatiques de billets. Cette fraude a presque exclusivement pour origine le vol ou la perte de la carte, confirmant ainsi l'analyse faite par l'Observatoire qu'un risque de fraude liée à la technologie sans contact demeure très limité.

- *La fraude sur les transactions internationales continue d'augmenter, à 266 millions d'euros (contre 231,3 millions en 2013), mais en raison d'une croissance forte de l'activité, le taux de fraude sur les transactions internationales est orienté à la baisse, à 0,456 %, après 0,480 % en 2013. Il reste toujours plus de dix fois supérieur à celui des transactions nationales. De ce fait, les transactions internationales représentent 41 % du montant total de la fraude sur les cartes émises en France, alors qu'elles ne comptent que pour 6 % de la valeur totale des transactions réalisées.*

  En particulier, les taux de fraude sur les paiements à distance de cartes françaises dans ou hors zone SEPA restent à des niveaux élevés (respectivement 0,910 % et 0,960 %), notamment sous l'effet d'une meilleure sécurisation des transactions à distance sur les sites français et donc d'un report des fraudeurs vers des sites situés à l'étranger. L'entrée en vigueur à l'été 2015 des orientations de l'Autorité bancaire européenne prévoyant la généralisation du recours à l'authentification renforcée des payeurs devrait permettre de lutter plus efficacement contre la fraude sur les paiements à distance dans la zone SEPA.

3e partie : travaux de veille technologique sur l'usage de la biométrie comme facteur d'authentification

Certains modes d'authentification reposant sur la biométrie, déjà utilisée quotidiennement par une part croissante du grand public, pourraient venir renforcer la sécurisation d'opérations de paiement par carte, qu'elles soient à distance ou de proximité, ou de retrait. De ce fait, l'Observatoire a souhaité faire un état des lieux de ces techniques d'authentification et de leurs conditions de mise en œuvre.

L'utilisation de techniques biométriques étant strictement encadrée en France par la loi Informatique et Libertés, l'Observatoire rappelle que leur application au sein de solutions de paiement requiert le dépôt d'une demande d'autorisation auprès de la CNIL.

L'Observatoire constate que les expérimentations menées en France visent en priorité à tester l'ergonomie des dispositifs biométriques. Avant tout déploiement à grande échelle, l'Observatoire estime nécessaire qu'une analyse des risques liés à l'usage de l'authentification biométrique soit conduite afin que le niveau de protection des solutions mises en œuvre soit au moins équivalent à celui offert par les techniques déjà en place (code confidentiel et carte à puce pour le paiement de proximité, code non rejouable pour le paiement à distance).

Par ailleurs, soulignant le manque d'éléments d'appréciation du niveau de sécurité des dispositifs biométriques par rapport aux technologies actuellement en œuvre (carte à puce, carte SIM des téléphones portables, etc.), l'Observatoire appelle les acteurs à développer des référentiels de sécurité permettant de qualifier les solutions proposées en prenant en compte l'ensemble de leurs composants et paramètres (matériels de capture de l'empreinte biométrique et de traitement, algorithmes, cas d'usage).

L'Observatoire appelle également les acteurs à être vigilants durant les phases d'expérimentation de solutions fondées sur la biométrie, la compromission d'empreintes biométriques utilisées par celles-ci pouvant mettre en cause le déploiement de solutions futures à plus grande échelle.

Enfin, du fait des limitations inhérentes à la biométrie et du manque de maturité de l'évaluation sécuritaire de ces dispositifs, l'Observatoire recommande de toujours conserver un moyen d'authentification alternatif capable de se substituer au dispositif biométrique.

4e partie : synthèse de la conférence « Les nouveaux moyens de paiement : de nouveaux enjeux de sécurité » du 22 octobre 2014

La Banque de France a organisé le 22 octobre 2014 à Paris, en collaboration avec la Banque centrale européenne, une conférence internationale sur les nouveaux défis en matière de sécurité des moyens de paiement. Cette journée a été l'occasion de développer un dialogue entre institutions européennes, autorités nationales et acteurs de marché autour de ces sujets. Trois grands axes qui conditionneront l'avenir des travaux sur la sécurité des moyens de paiement se sont ainsi dégagés des échanges.

En premier lieu, la coopération à la fois entre les différentes autorités concernées au niveau européen, au travers d'enceintes telles que le forum européen Secure Pay [1]*, mais aussi entre ces autorités et les nombreuses parties prenantes du marché des paiements (banques, entreprises, fournisseurs de solutions, consommateurs…), est apparue comme une réponse efficace au besoin d'un développement cohérent des exigences sécuritaires sur le marché européen.*

1 Le forum européen *SecuRe Pay*, coprésidé par la BCE et l'ABE, réunit les banques centrales et superviseurs bancaires nationaux sur les sujets relatifs à la sécurité des moyens de paiement scripturaux.

Ensuite, la prise en compte en permanence des évolutions du marché, dans un contexte où l'innovation fait évoluer rapidement les usages des consommateurs, doit faire partie intégrante du fonctionnement des autorités européennes. À ce titre, les travaux conduits au niveau du forum SecuRe Pay *et de l'Autorité bancaire européenne concernant la sécurité des paiements sur internet illustrent cette volonté d'investir les segments les plus innovants en matière de développement de services de paiement sûrs et efficaces.*

Enfin, dans un secteur en forte évolution, la recherche d'un équilibre entre innovation et sécurité est également un paramètre à intégrer dans l'action des autorités, qui doivent veiller à ce que les exigences règlementaires ne constituent pas une barrière au développement de nouveaux services. Les réflexions conduites dans le cadre de la révision de la directive sur les services de paiement, concernant en particulier l'encadrement des activités des tiers de paiement et de leurs conditions de sécurité, illustrent cette volonté de permettre l'ouverture du marché des paiements à l'innovation tout en maîtrisant les risques pour l'ensemble des acteurs et les consommateurs.

Le recours systématique à l'authentification renforcée pour les paiements par internet sera en outre pris en compte dans la révision de la directive sur les services de paiement (dite DSP2), dont la publication est prévue au second semestre 2015 et qui nécessitera une transposition en droit national [5].

2|3 Les Assises nationales des paiements ont reconnu le rôle de l'authentification renforcée pour développer des moyens de paiement faciles et sûrs à utiliser

Les Assises nationales des paiements, organisées sous l'égide du ministre des Finances et des Comptes publics, Michel Sapin, et du ministre de l'Économie, de l'Industrie et du Numérique, Emmanuel Macron, se sont tenues le 2 juin 2015. Elles visaient à définir les contours d'une stratégie nationale de modernisation des moyens de paiement avec pour objectifs, d'une part, de répondre aux besoins des utilisateurs en terme de rapidité, de sécurité et d'accessibilité des moyens de paiement, et, d'autre part, de développer l'usage de moyens de paiement innovants et la compétitivité de l'industrie nationale des paiements.

La généralisation des dispositifs d'authentification renforcée des payeurs lors de paiements à distance s'inscrit ainsi dans la perspective du développement de moyens de paiement faciles et sûrs à utiliser, au regard à la fois de la part très importante que représente la fraude sur les paiements à distance dans le total de la fraude constatée pour les paiements par carte, et de la dynamique de développement du commerce en ligne.

Les propositions formulées dans le cadre des travaux préparatoires aux Assises nationales des paiements préconisent notamment d'encourager les initiatives permettant une meilleure diffusion de l'authentification renforcée, en intensifiant les efforts de communication et d'éducation menés auprès des commerçants et des utilisateurs, et le développement de solutions d'authentification renforcée dites de « deuxième génération », dont certaines présentent l'avantage de ne pas nécessiter un équipement spécifique des commerçants en ligne ou par exemple fondées sur l'usage de la biométrie. L'avènement de ces dispositifs nouveaux viserait notamment à répondre aux préoccupations exprimées par les e-commerçants, en particulier au regard du fort développement des paiements par téléphone mobile et au manque d'ergonomie des solutions existantes sur ce type de terminal. À ce titre, les nouvelles solutions qui réussiront à s'imposer dans les prochaines années seront vraisemblablement celles qui allieront facilité d'utilisation et sécurité, tout en reposant sur des modèles économiques viables.

3| Conclusion

L'Observatoire appelle l'ensemble des acteurs du paiement à poursuivre le renforcement de la sécurité des paiements par internet. Au regard de l'augmentation significative de la part des sites d'e-commerce équipés (près de 60 % à avril 2015), l'Observatoire note que la généralisation des dispositifs d'authentification renforcée est bien amorcée mais doit rester une priorité, permettant de se conformer aux recommandations de l'Eurosystème et de l'Autorité bancaire européenne relatives à la sécurité des moyens de paiement sur internet, qui entrent en vigueur au 1er août 2015.

5 Voir précisions sur le dispositif réglementaire de la DSP2 au chapitre 4.

Encadré 2

Fraude aux paiements par carte sans contact

L'Observatoire a collecté, pour la première fois cette année, les données permettant d'évaluer le taux de fraude sur les paiements sans contact. Ainsi, sur l'ensemble de l'année 2014, 72,2 millions de paiements sans contact ont été enregistrés pour un montant total de 780,9 millions d'euros, soit un montant moyen de 11 euros par opération. Les données de fraude, quant à elles, sont collectées de manière exhaustive depuis le 1er avril 2014. Sur les neuf derniers mois de l'année 2014, 9 600 paiements frauduleux ont été recensés pour un montant total de 108 000 euros. Le taux de fraude sur les transactions sans contact peut être estimé à 0,015 % sur cette période, et s'établirait donc à un niveau intermédiaire entre le taux de fraude des paiements de proximité tous modes confondus (0,010 %), et celui des retraits (0,034 %).

La fraude aux paiements sans contact a pour origine quasi exclusive le vol ou la perte de la carte ; la technologie sans contact elle-même ne semble donc pas avoir présenté de faille exploitable pour les fraudeurs (de type écoute passive des données de carte lors d'une transaction, ou activation à distance de la carte dans des lieux publics, par exemple), confirmant ainsi l'analyse des risques conduite par l'Observatoire et publiée dans son rapport annuel 2012. En outre, la mise en place par les émetteurs de carte de plafonds sur le montant maximum d'une transaction unitaire (généralement fixé à 20 ou 25 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (généralement fixé à 100 euros), permet de limiter le préjudice subi en cas de perte ou de vol d'une carte.

On rappellera à cette occasion que le porteur est protégé par la loi en cas de fraude. Il dispose en France de treize mois [1] pour contester les transactions non autorisées auprès de son prestataire de services de paiement, qui doit alors le rembourser dans les plus brefs délais. Les porteurs sont par ailleurs invités à faire opposition le plus rapidement possible auprès de l'établissement émetteur de la carte lorsque celle-ci est perdue ou volée. Dans le cas de fraudes résultant d'un paiement effectué en mode sans contact suite à une perte ou un vol de sa carte, on notera que le porteur ne supportera aucune perte liée à cette opération de paiement non autorisée [2].

Dans un contexte de fort développement du taux d'équipement des porteurs, avec plus de 30 millions de cartes disposant de la fonctionnalité de paiement sans contact en circulation à fin décembre 2014, l'Observatoire appelle les émetteurs à toute la vigilance nécessaire, et rappelle les engagements pris concernant la possibilité de désactiver la fonction sans contact des cartes, soit en mettant des étuis de protection [3] à la disposition des utilisateurs, soit en mettant en œuvre la désactivation à distance de la fonction sans contact [4], soit en permettant le remplacement, à la demande du porteur, d'une carte sans contact par une carte dépourvue de cette fonctionnalité.

La Banque de France dans son rôle de surveillant des moyens de paiements scripturaux assure un suivi de la mise en œuvre de ces mesures.

1 *Voir détails en annexe 2.*
2 *Voir annexe 1 : une opération de paiement par carte en mode sans contact est en effet effectuée sans l'utilisation du dispositif personnalisé de sécurité de la carte (absence de saisie de code), ce qui signifie que même avant opposition suite à la perte ou vol du moyen de paiement, le porteur ne peut pas supporter de pertes liées à un paiement non autorisé.*
3 *Étuis de carte bloquant les ondes de communications de type NFC, permettant d'éviter toute activation non sollicitée de la carte.*
4 *La fonction sans contact est alors désactivée par l'exécution d'un script EMV sur la carte, qui est réalisée au moment de l'insertion dans un distributeur automatique de billets ou un terminal de paiement électronique.*

En ce qui concerne les transactions internationales (cf. tableaux 4), on remarque que la fraude sur les paiements à distance réalisés par les cartes françaises auprès des e-commerçants étrangers a très fortement augmenté en 2014 (104,5 millions d'euros, contre 81,2 millions d'euros en 2013). Ce phénomène peut s'expliquer par l'adoption progressive par les sites de commerce en ligne situés en France de dispositifs de sécurisation des paiements sur internet, et par le report des fraudeurs vers des sites étrangers moins sécurisés.

On constate ainsi des taux de fraude sur les paiements à distance particulièrement élevés à la fois hors zone SEPA (0,960 %) et en zone SEPA (0,910 %). Le déploiement de dispositifs d'authentification renforcée, sous l'impulsion notamment des recommandations du forum européen *SecuRe Pay* sur la sécurité des moyens de paiement et des orientations de l'Autorité bancaire européenne (cf. chapitre 1) devrait toutefois permettre d'infirmer cette tendance en zone SEPA.

Enfin, on note la poursuite de la diminution de la fraude sur les paiements de proximité et les retraits réalisés par les cartes françaises dans la zone SEPA, où l'utilisation d'EMV est désormais généralisée. On notera en particulier que le taux de fraude sur les retraits effectués en zone SEPA (0,033 %) est près de 25 fois inférieur à celui des retraits effectués hors zone SEPA (0,890 %), où la piste magnétique est encore très utilisée dans certains pays.

Tableau 4a

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

(taux en %, montants en millions d'euros)

Carte française – Accepteur étranger hors SEPA	**2011**	**2012**	**2013**	**2014**
Paiements	0,561	0,687	0,547	0,532
	(30,5)	(37,8)	(40,3)	(41,7)
– dont paiements de proximité et sur automate	0,369	0,456	0,377	0,350
	(16,0)	(19,8)	(17,7)	(19,2)
– dont paiements à distance	1,320	1,551	0,848	0,960
	(14,5)	(18,0)	(22,6)	(22,5)
– dont par courrier/téléphone	*1,011*	*1,150*	*1,234*	*4,955*
	(3,1)	*(4,0)*	*(6,4)*	*(7,5)*
– dont sur internet	*1,440*	*1,720*	*0,755*	*0,682*
	(11,4)	*(14,1)*	*(16,2)*	*(14,9)*
Retraits	0,800	0,904	1,054	0,890
	(20,5)	(24,7)	(29,9)	(28,3)
Total	**0,638**	**0,759**	**0,688**	**0,636**
	(51,0)	**(62,5)**	**(70,2)**	**(70,0)**
Carte française – Accepteur étranger SEPA				
Paiements	0,300	0,372	0,434	0,434
	(43,1)	(55,3)	(66,8)	(89,8)
– dont paiements de proximité et sur automate	0,140	0,131	0,089	0,067
	(12,6)	(11,7)	(8,2)	(7,8)
– dont paiements à distance	0,571	0,735	0,937	0,910
	(30,5)	(43,6)	(58,6)	(82,0)
– dont par courrier/téléphone	*0,643*	*0,532*	*1,566*	*1,317*
	(5,6)	*(6,5)*	*(11,3)*	*(13,9)*
– dont sur internet	*0,557*	*0,788*	*0,856*	*0,856*
	(24,9)	*(37,1)*	*(47,3)*	*(68,1)*
Retraits	0,040	0,036	0,036	0,033
	(1,2)	(1,1)	(1,1)	(1,2)
Total	**0,255**	**0,316**	**0,366**	**0,374**
	(44,3)	**(56,3)**	**(67,9)**	**(91,0)**

Source : Observatoire de la sécurité des cartes de paiement.

Encadré 3

Fraude domestique en vente à distance selon le secteur d'activité

L'Observatoire a collecté des données permettant de fournir des indications sur la répartition [1] de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions domestiques.

Tableau

Ventilation de la fraude domestique sur les paiements à distance par secteur d'activité

(montants en millions d'euros, part en %)

Secteur	Montant de fraude	Part du secteur dans la fraude
Services aux particuliers et aux professionnels	31,8	20,4
Voyage, transport	30,8	19,7
Commerce généraliste et semi-généraliste	29,5	18,9
Téléphonie et communication	26,7	17,1
Équipement de la maison, ameublement, bricolage	12,7	8,2
Produits techniques et culturels	8,0	5,1
Divers	6,0	3,8
Jeu en ligne	3,2	2,0
Alimentation	2,6	1,7
Approvisionnement d'un compte, vente de particulier à particulier	2,5	1,6
Santé, Beauté, Hygiène	1,8	1,1
Assurance	0,4	0,3
Total	**155,9**	**100,0**

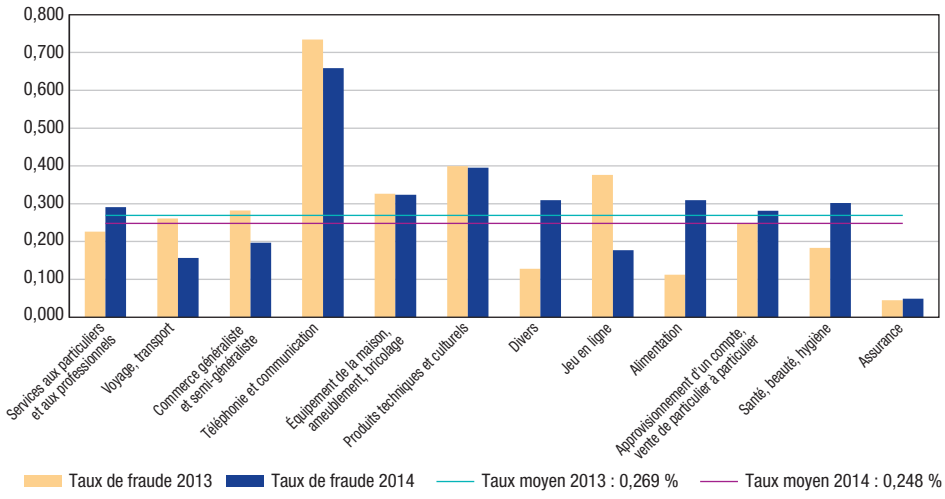
Les secteurs « Services aux particuliers et aux professionnels », « Voyage/transport », « Commerce généraliste et semi-généraliste » et « Téléphonie et communication » représentent 76 % du montant de la fraude en vente à distance, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, tels les « Produits techniques et culturels », qui comptent pour une plus faible part du total de la fraude, subissent toutefois une exposition élevée.

On note que les taux de fraude par secteur sont presque tous proches voire inférieurs au taux de fraude moyen, à l'exception notable du secteur « Téléphonie et communication » qui connaît de manière durable un taux de fraude très supérieur à la moyenne. L'Observatoire appelle tout particulièrement les acteurs de ce secteur à renforcer les mesures visant à lutter contre la fraude.

Graphique

Taux de fraude domestique sur les paiements à distance par secteur d'activité

(en %)

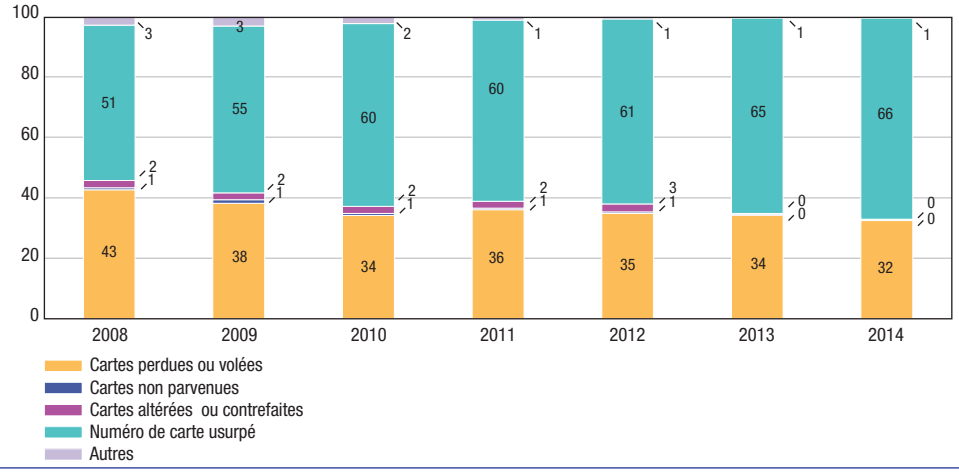


1 *Cf. annexe 6 pour une description des secteurs retenus.*

Graphique 7

Répartition de la fraude selon son origine (transactions domestiques en valeur)

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

Le graphique 7 indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements et n'inclut donc pas les retraits).

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux à distance reste la principale origine de la fraude (66,4 % des montants), en augmentation par rapport à 2013 (64,6 %).

La fraude liée aux pertes et vols de cartes représente toujours près du tiers de la fraude sur les transactions domestiques (32,5 %), mais sa part est en diminution continue (34,2 % en 2013) depuis trois années.

La contrefaçon de cartes n'est à l'origine que de 0,1 % des paiements domestiques frauduleux, en diminution sensible depuis plusieurs années (elle s'élevait à 2,6 % en 2011). Cette diminution s'explique principalement par l'adoption de technologies de cartes à puce par un nombre croissant de systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes [2].

Tableau 5

Répartition de la fraude domestique selon son origine et par type de carte en 2014

(montants en millions d'euros, part en %)

	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	76,3	32,5	75,6	32,8	0,7	17,3
Carte non parvenue	0,9	0,4	0,5	0,2	0,4	9,6
Carte altérée ou contrefaite	0,2	0,1	0,1	0,1	0,1	1,5
Numéro usurpé	155,9	66,4	154,3	66,9	1,6	40,0
Autres	1,4	0,6	0,1	0,1	1,3	31,6
Total	234,6	100,0	230,6	100,0	4,0	100,0

Source : Observatoire de la sécurité des cartes de paiement.

2 Migration de la technologie d'authentification des cartes du *Static Data Authentication* (SDA) vers le *Dynamic Data Authentication* (DDA).

Encadré

Point de vue de la CNIL sur l'authentification biométrique

L'utilisation de la biométrie en tant que facteur d'authentification pour accéder à des moyens de paiement, ou effectuer des opérations à distance, n'a jusqu'à présent été autorisée par la CNIL que dans le cadre d'expérimentations. L'objectif des autorisations temporaires accordées à ce titre est de mesurer l'intérêt porté à la solution par les clients, ainsi que la fiabilité de la technologie biométrique utilisée lorsqu'elle est couplée à un moyen de paiement sur internet.

L'expérimentation permet ainsi d'identifier les problèmes rencontrés afin de définir de nouvelles pistes d'amélioration. Les expérimentations ont une durée limitée au temps nécessaire à l'obtention de résultats concluants, et la CNIL exige qu'un bilan détaillé lui soit remis à leur issue. En outre, elles ne sont possibles que sur la base du volontariat, le système biométrique ne pouvant en tout état de cause être imposé aux utilisateurs.

Sur la base des bilans remis par les organismes et en tenant compte du paysage législatif en évolution tant au niveau national (proposition de loi visant à limiter l'usage des techniques biométriques en cours d'examen) qu'au niveau européen (proposition de règlement européen relatif à la protection des données), la CNIL s'attache à dégager des principes directeurs applicables aux dispositifs biométriques.

Bien que la biométrie « grand public » (hors du cadre professionnel) n'ait pas encore fait l'objet de cadre de référence, certaines constantes peuvent être soulignées. Le positionnement de 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.

Ainsi, le recours à la biométrie ne saurait être le seul moyen d'accéder à un service mais doit pouvoir être utilisé de manière alternative à un autre moyen. L'utilisateur du service doit donc être en mesure de choisir une technique équivalente en termes de facilité d'usage, présentant les mêmes conditions d'accès que le dispositif biométrique (le choix d'une autre technologie ne doit pas avoir pour effet, par exemple, d'ajouter des contraintes telles qu'un délai, un coût, etc.).

De plus, la maîtrise par les personnes de leurs données biométriques est indéniablement réduite lorsque le gabarit [1] biométrique est stocké dans des serveurs distants et non sur un support placé sous le contrôle exclusif de la personne concernée. La compromission du support individuel emporte des conséquences bien moins importantes que celle d'une base centralisant plusieurs gabarits. Sur la base de ces premiers constats, la CNIL marque une préférence pour le stockage de la biométrie sur support individuel, placé sous le contrôle exclusif de la personne concernée.

Par ailleurs, la CNIL exige une information renforcée des personnes notamment sur le dispositif biométrique, son caractère facultatif (l'existence d'un dispositif alternatif), les modalités de stockage de la donnée ; les personnes doivent avoir la possibilité de revenir à tout moment sur leur choix et d'obtenir la suppression de leur gabarit biométrique le cas échéant.

Enfin, de nombreux acteurs sont susceptibles d'intervenir sur la chaîne de traitement liée à l'authentification biométrique (par exemple, que ce soit 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.

1 Ensemble des données biométriques servant de référence lors d'une authentification.

Encadré

Programme de la conférence du 22 octobre 2014

Discours d'ouverture
Christian Noyer (gouverneur, Banque de France)

Présentation introductive
Benoît Coeuré (membre du directoire, Banque centrale européenne)

Thème I : La coopération entre autorités européennes dans le domaine de la sécurité des moyens de paiement de détail

Table ronde
Modérateur : Pierre Petit (coprésident, forum SecuRe Pay*)*
Mario Nava (directeur en charge des institutions financières, Commission européenne)
Adam Farkas (directeur exécutif, Autorité bancaire européenne)

Thème II : Les attentes en matière de sécurité sur les moyens de paiement

Table ronde sur les paiements mobiles
Modérateur : Hanna Franiak (conseiller au département des Systèmes de paiement, Banque nationale de Pologne)
Pierre Chassigneux (responsable Risques et Audit, Groupement des Cartes Bancaires)
Rob Marrewijk (manager du programme sécurité des terminaux, Brightsight)
Santiago Minguito Santos (directeur de la Sécurité de l'information, Banco Sabadell)
Edwin Aoki (architecte en chef, PayPal)

Présentation introductive
Adam Farkas (directeur exécutif, Autorité bancaire européenne)

Table ronde sur les paiements en ligne
Modérateur : Dirk Haubrich (responsable de l'unité de Protection des consommateurs, Autorité bancaire européenne)
Dirk Schrade (adjoint au chef du département des Systèmes de paiement et de Règlement, Banque fédérale d'Allemagne)
Ingrid Lauterbach (responsable de la sécurité client au sein du groupe de cyber-sécurité, Deutsche Bank)
Paul Alfing (président, Comité des e-paiements)
Monique Goyens (directeur général, Organisation des consommateurs européens)

Thème III : Acteurs tiers – comment réguler ?

Présentation introductive
Mario Nava (directeur en charge des institutions financières, Commission européenne)

Table ronde sur les tiers de paiement
Modérateur : Denis Beau (directeur général des Opérations, Banque de France)
Pierre Petit (coprésident, forum SecuRe Pay*)*
Irmfried Schwimann (directeur des Services financiers, Commission européenne)
Massimo Doria (responsable de la division des Services et Instruments de paiement, Banque d'Italie)
Jean Clamon (directeur général, BNP Paribas)
Georg Schardt (adjoint au président directeur général, SOFORT AG)

Conclusion de la conférence
Denis Beau (directeur général des Opérations, Banque de France)

Annexes

Ainsi, les opérations de paiement concernées par ces adaptations sont les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer [3], à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un État non européen [4], quelle que soit la devise dans laquelle l'opération est réalisée. Sont également concernées les opérations effectuées avec une carte dont l'émetteur est situé à Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française ou à Wallis et Futuna, au profit d'un bénéficiaire dont le prestataire est situé dans un État autre que la République française, quelle que soit la devise utilisée.

Dans ces cas, le plafond de 150 euros trouve à s'appliquer pour les opérations non autorisées en cas de perte ou de vol de la carte, même si l'opération a été réalisée sans utilisation du dispositif personnalisé de sécurité.

Par ailleurs, le délai maximal de contestation de l'opération est ramené à 70 jours et conventionnellement étendu à 120 jours. En revanche, le remboursement immédiat de l'opération non autorisée est étendu.

3 Y compris Mayotte depuis le 31 mars 2011.
4 Qui n'est pas partie à l'accord sur l'EEE (UE + Liechtenstein, Norvège et Islande).

Ces cartes peuvent offrir des fonctions diverses qui conduisent à la typologie fonctionnelle suivante en matière de cartes de paiement :

• les cartes de débit sont des cartes associées à un compte de paiement [5] permettant à son titulaire d'effectuer des retraits ou des paiements qui seront débités selon un délai fixé par le contrat de délivrance de la carte. Ce débit peut être immédiat (retrait ou paiement) ou différé (paiement) ;

• 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 (supérieur à quarante jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

• les cartes nationales permettent d'effectuer des paiements ou des retraits exclusivement auprès d'accepteurs établis sur le territoire français ;

• les cartes internationales permettent d'effectuer des paiements et des retraits dans tous les points d'acceptation, nationaux ou internationaux, de la marque ou d'émetteurs partenaires avec lesquels le système de paiement par carte a signé des accords ;

• les porte-monnaie électroniques sont des cartes sur lesquelles sont stockées des unités de monnaie électronique. Aux termes de l'article L.315-1 du *Code monétaire et financier*, *« la monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L.133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique »*.

La typologie fonctionnelle rappelée ci-dessus inclut également les paiements sans contact.

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 cartes de paiement sont de trois ordres :

• il suit la mise en œuvre des mesures adoptées par les émetteurs et les commerçants pour renforcer la sécurité des cartes de paiement. Il se tient informé des principes adoptés en matière de sécurité ainsi que des principales évolutions ;

• il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de cartes 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 types de cartes de paiement ;

• il assure une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des cartes 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.

5 Les comptes de paiement qui sont, aux termes du I de l'article L. 314-1 du *Code monétaire et financier*, des comptes détenus au nom d'une ou plusieurs personnes, utilisés aux fins de l'exécution d'opérations de paiement, correspondent aux comptes de dépôts à vue ouverts sur les livres des banques et aux comptes ouverts sur les livres des autres prestataires de services de paiement.

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 ;
- dix représentants des émetteurs de cartes de paiement, notamment de cartes bancaires, de cartes privatives et de porte-monnaie électroniques ;
- cinq représentants du collège consommateurs du Conseil national de la consommation ;
- cinq représentants des commerçants issus notamment du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;
- trois personnalités qualifiées en raison de leurs compétences.

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 Christian Noyer, gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

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 en 2003 un règlement intérieur qui précise les conditions de son fonctionnement.

A10

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 cartes 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 cartes 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 cartes de paiement. En 2010, l'Observatoire a décidé la création d'un groupe de travail dédié à la problématique du déploiement de la technologie « 3D-Secure ».

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.

Représentants des émetteurs de cartes de paiement

Frédéric COLLARDEAU
Directeur de la filière des paiements
La Banque Postale
Gilbert ARIRA
Administrateur
Groupement des Cartes Bancaires
Jean DIACONO
Administrateur
American Express France
Willy DUBOST
Directeur Systèmes et Moyens de paiement
Fédération bancaire française
Caroline SELLIER
Directeur Risk management et Lutte contre la fraude
Natixis Paiements
François LANGLOIS
Directeur des Relations institutionnelles
BNP Paribas Personal Finance
Frédéric MAZURIER
Directeur administratif et financier
Carrefour Banque
Gérard NEBOUY
Directeur général
Visa Europe France
Régis FOLBAUM
Président directeur général
MasterCard France
Narinda YOU
Directeur
Stratégie et pilotage interbancaire
Crédit Agricole SA

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

Régis CREPY
Confédération nationale
Associations familiales catholiques (CNAFC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)
Patrick MERCIER
Président
Association de défense d'éducation et d'information du consommateur (ADEIC)
Frédéric POLACSEK
Conseil national des associations familiales laïques (CNAFAL)
Maxime CHIPOY
UFC-Que Choisir

Représentants des organisations professionnelles de commerçants

Philippe JOGUET
Directeur Développement durable, RSE, Questions financières
Fédération des entreprises du commerce et de la distribution (FCD)
Marc LOLIVIER
Délégué général
Fédération du e-commerce et de la vente à distance (Fevad)
Jean-Jacques MELI
Chambre de commerce et d'industrie du Val d'Oise
Jean-Marc MOSCONI
Délégué général
Mercatel
Philippe SOLIGNAC
Vice-président
Chambre de commerce et d'industrie de Paris/ACFCI

Personnalités qualifiées en raison de leurs compétences

Éric BRIER
Chief Security Officer
Ingenico
David NACCACHE
Professeur
École normale supérieure
Sophie NERBONNE
Directeur adjoint à la direction des affaires juridiques, internationales et de l'expertise
Commission nationale de l'informatique et des libertés (CNIL)

Tableau 1

Le marché des cartes de paiement en France en 2014 – Émission

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

	Émetteur français, Accepteur français		Émetteur français, Accepteur étranger SEPA		Émetteur français, Accepteur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	8 148,87	344,31	163,38	10,70	46,99	4,38
Paiements à distance hors Internet	14,29	1,85	17,11	1,06	2,04	0,15
Paiements à distance sur Internet	781,70	58,58	155,17	7,50	30,76	1,99
Retraits	1 512,18	121,39	29,85	3,61	20,96	3,18
Total	**10 457,05**	**526,14**	**365,51**	**22,87**	**100,75**	**9,70**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,57	11,73	7,52	0,97	6,24	1,11
Paiements à distance hors Internet	1,13	0,07	–	–	–	–
Paiements à distance sur Internet	17,58	2,40	3,70	0,46	1,28	0,20
Retraits	3,28	0,30	–	–	–	–
Total	**125,56**	**14,49**	**11,22**	**1,43**	**7,51**	**1,31**
Total général	**10 582,61**	**540,63**	**376,73**	**24,30**	**108,27**	**11,01**

Source : Observatoire de la sécurité des cartes de paiement.

Tableau 2

Le marché des cartes de paiement en France en 2014 – Acceptation

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

	Émetteur français, Accepteur français		Émetteur étranger SEPA, Accepteur français		Émetteur étranger hors SEPA, Accepteur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	8 148,87	344,31	217,66	16,51	68,51	9,50
Paiements à distance hors Internet	14,29	1,85	5,61	1,20	1,62	0,76
Paiements à distance sur Internet	781,70	58,58	43,87	5,64	13,20	2,61
Retraits	1 512,18	121,39	26,68	4,86	8,87	2,19
Total	**10 457,05**	**526,14**	**293,82**	**28,20**	**92,20**	**15,06**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,57	11,73	4,31	1,10	7,03	4,03
Paiements à distance hors Internet	1,13	0,07	–	–	–	–
Paiements à distance sur Internet	17,58	2,40	0,88	0,16	0,53	0,19
Retraits	3,28	0,30	–	–	0,44	0,23
Total	**125,56**	**14,49**	**5,19**	**1,26**	**8,00**	**4,45**
Total général	**10 582,61**	**540,63**	**299,02**	**29,46**	**100,20**	**19,51**

Source : Observatoire de la sécurité des cartes de paiement.

Typologie de la fraude

L'Observatoire a par ailleurs défini une typologie de la fraude qui distingue les éléments suivants.

Les origines de fraude :

• carte perdue ou volée : le fraudeur utilise une carte de paiement suite à une perte ou à un vol ;

• carte non parvenue : la carte a été interceptée lors de son envoi à son titulaire légitime par l'émetteur. Ce type d'origine se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut moins facilement constater qu'un fraudeur est en possession d'une carte lui appartenant et où il met en jeu des vulnérabilités spécifiques aux procédures d'envoi des cartes ;

• carte falsifiée ou contrefaite : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation. La contrefaçon d'une carte suppose la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou une personne quant à sa qualité substantielle. Pour les paiements effectués sur automate de paiement, une telle carte, fabriquée par le fraudeur, supporte les données nécessaires à tromper le système. En commerce de proximité, une carte contrefaite est une carte fabriquée par un fraudeur, qui présente certaines sécurités (dont l'aspect visuel) d'une carte authentique, supporte les données d'une carte authentique et est destinée à tromper la vigilance d'un accepteur ;

• numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (voir le paragraphe sur les techniques de fraude ci-dessous) et utilisé en vente à distance ;

• numéro de carte non affecté : utilisation d'un PAN [3] cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance.

Les techniques de fraude :

• *skimming* : technique qui consiste en la copie, dans un commerce de proximité ou dans des distributeurs automatiques, des pistes magnétiques d'une carte de paiement à l'aide d'un lecteur à mémoire appelé *skimmer*. Éventuellement, le code confidentiel est également capturé *de visu*, à l'aide d'une caméra ou encore par détournement du clavier numérique. Ces données seront inscrites ultérieurement sur les pistes magnétiques d'une carte contrefaite ;

• hameçonnage ou *phishing* : technique utilisée par les fraudeurs visant à obtenir des données personnelles, principalement par le biais de courriels non sollicités renvoyant les utilisateurs vers des sites frauduleux ayant l'apparence de sites de confiance ;

• usurpation d'identité : actes frauduleux liés à un paiement par carte et supposant l'utilisation de l'identité d'une autre personne ;

• répudiation abusive : contestation par le porteur, de mauvaise foi, d'un ordre de paiement valide dont il est l'initiateur ;

3 Personal Account Number.

• piratage d'automates de paiement ou de retrait : technique qui consiste à placer des dispositifs de duplication de cartes sur des automates de paiement ou des distributeurs automatiques de billets ;

• piratage de systèmes automatisés de données, de serveurs ou de réseaux : intrusion frauduleuse sur de tels systèmes ;

• moulinage : technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de cartes pour générer de tels numéros et effectuer des paiements.

Les types de paiement :

• paiement de proximité, réalisé au point de vente ou sur automate ;
• paiement à distance réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen ;
• retrait (retrait DAB ou autre type de retrait).

La zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :

• l'émetteur et l'acquéreur sont, tous deux, établis en France. On dira également, dans ce cas, que la transaction est nationale. Pour autant, pour les paiements à distance, le fraudeur peut opérer depuis l'étranger ;
• l'émetteur est établi en France et l'acquéreur est établi à l'étranger dans l'espace SEPA ;
• l'émetteur est établi en France et l'acquéreur est établi à l'étranger hors espace SEPA ;
• l'émetteur est établi à l'étranger dans l'espace SEPA et l'acquéreur est établi en France ;
• l'émetteur est établi à l'étranger hors espace SEPA et l'acquéreur est établi en France.

Le secteur d'activité du commerçant pour les paiements à distance :

• alimentation : épiceries, supermarchés, hypermarchés,… ;
• approvisionnement d'un compte, vente de particulier à particulier : sites de vente en ligne entre particuliers,… ;
• assurance ;
• commerce généraliste et semi-généraliste : textile/habillement, grand magasin, généraliste vente sur catalogue, vente privée,… ;
• équipement de la maison, ameublement, bricolage ;
• jeu en ligne ;
• produits techniques et culturels : matériel et logiciel informatiques, matériel photographique, livre, CD/DVD,… ;
• santé, beauté, hygiène ;
• services aux particuliers et aux professionnels : hôtellerie, service de location, billetterie de spectacle, organisme caritatif, matériel de bureau, service de messagerie,… ;
• téléphonie et communication : matériel et service de télécommunication/téléphonie mobile ;
• voyage, transport : ferroviaire, aérien, maritime ;
• divers.