2012 | RAPPORT ANNUEL

DE L'OBSERVATOIRE DE LA SÉCURITÉ DES CARTES DE PAIEMENT

bservatoire
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 : 11-2324

Rapport annuel 2012
de l'Observatoire de la sécurité des cartes 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

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

SOMMAIRE

L'Observatoire de la sécurité des cartes de paiement, mentionné au I de l'article L. 141-4 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* [1].

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 des Finances et transmis au Parlement. Il comprend cette année :

- *un état des lieux de la sécurisation des paiements par carte sur Internet (1re partie) ;*
- *une présentation des statistiques de fraude pour 2012 (2e partie) ;*
- *une synthèse des travaux conduits en matière de veille technologique (3e partie), avec deux études : une sur la sécurité des paiements par carte sans contact et l'autre sur les techniques de fraude visant les transactions par carte ;*
- *une étude sur les évolutions réglementaires et les recommandations en Europe et à l'international sur la sécurité des cartes de paiement (4e partie).*

1 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.

Le dixième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2012, comprend quatre parties dont les principales conclusions sont reprises ci-après.

1re partie : sécurisation des paiements par cartes sur Internet

Depuis 2010, l'Observatoire mène sur ce sujet une enquête d'opinion annuelle auprès des porteurs et collecte des données statistiques en provenance des établissements bancaires et de leurs prestataires techniques. Des avancées positives sont de nouveau notées pour l'année 2012.

Ainsi, les dispositifs d'authentification bénéficient d'une notoriété encore accrue auprès des utilisateurs qui y sont désormais plus régulièrement confrontés. Neuf cyberacheteurs sur dix indiquent dorénavant connaître un dispositif de sécurisation complémentaire au numéro de la carte et au cryptogramme demandés lors d'une transaction en ligne et deux cyberacheteurs sur trois confirment avoir déjà été confrontés à une authentification renforcée. Ceci s'explique notamment par une hausse de la part des paiements sécurisés sur Internet, qui s'élève désormais à 27,5 % en montant, contre 23 % en 2011. Pour autant les efforts doivent être poursuivis afin que les e-commerçants mettent en œuvre plus largement les dispositifs de sécurisation permettant l'authentification renforcée des porteurs, tels que « 3D Secure », à chaque fois que cela est possible et pertinent. Ce constat a été partagé par l'ensemble des parties prenantes lors du colloque organisé en novembre 2012 par l'Observatoire sur ce thème. C'est dans ce contexte que la Banque de France a entrepris en 2013, conjointement avec le Groupement des Cartes Bancaires « CB » et en étroite collaboration avec les banques, une démarche auprès des e-commerçants les plus fraudés afin que la sécurité de leurs paiements en ligne soit renforcée.

*Ces actions s'inscrivent désormais dans un cadre européen, les recommandations du forum européen sur la sécurité des moyens de paiement (*SecuRe Pay*) ayant préconisé la généralisation de l'authentification renforcée du porteur pour les paiements sur Internet les plus risqués d'ici au 1er février 2015.*

2e partie : statistiques de fraude pour l'année 2012

Le taux de fraude s'établit pour l'année 2012 à 0,080 %, en légère augmentation pour la cinquième année consécutive, correspondant à un montant total de fraude de 450,7 millions d'euros (contre 0,077 % et 413,2 millions d'euros en 2011).

Cette hausse de la fraude s'explique par deux tendances principales :

- *une augmentation de la fraude au niveau national de 7,1 % liée :*

  – d'une part à la hausse très sensible des attaques de distributeurs automatiques de billets (+ 73 % par rapport à 2011) et de points de vente (2,5 fois plus de cas qu'en 2011) qui sont devenus des cibles privilégiées pour des réseaux de fraude organisés, et au nombre toujours important des cas de vols de carte avec code confidentiel. Face à la confirmation de

ces tendances déjà observées en 2011, l'Observatoire réitère ses conseils de prudence aux porteurs et rappelle les bonnes pratiques à suivre lors d'une opération de paiement chez un commerçant, sur Internet, ou encore lors d'un retrait (cf. annexe 1) ;

– d'autre part, à l'augmentation toujours soutenue du montant de la fraude sur les paiements à distance. On notera cependant que le taux de fraude sur les paiements sur Internet diminue pour la première fois depuis 2008 pour atteindre 0,290 % (contre 0,341 %, son maximum historique, en 2011). Cette évolution favorable traduit les efforts réalisés par les e-commerçants pour adopter progressivement les dispositifs, tels que « 3D-Secure », permettant l'authentification non rejouable du porteur de la carte lors d'un paiement sur Internet.

Toutefois, le montant de la fraude sur les paiements à distance augmente en raison du contexte de progression soutenue des paiements sur Internet et également du report partiel de la fraude vers les paiements à distance effectués par courrier ou par téléphone. Le taux de fraude sur les paiements à distance demeure plus de vingt fois plus élevé que le taux de fraude sur les paiements de proximité. L'ensemble des paiements à distance, qui représente 9,2 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude.

Ceci conduit l'Observatoire à insister pour que les e-commerçants, notamment les plus exposés à la fraude en montant ou en taux, poursuivent la mise en œuvre des dispositifs permettant l'authentification renforcée du porteur de la carte lors d'un paiement sur Internet chaque fois que cela est possible et pertinent.

Le taux de fraude sur les paiements de proximité reste, quant à lui, à un niveau très faible (0,015 %), stable par rapport à 2011.

- *une augmentation significative de la fraude au niveau international de 11,2 % liée :*

  – à la hausse de la fraude sur Internet (+ 37 %), qui peut notamment s'expliquer par un report partiel de la fraude nationale sur ce canal suite à l'adoption progressive des dispositifs de sécurisation des paiements sur Internet en France alors que des sites situés à l'étranger restent moins bien protégés. Le déploiement de dispositifs d'authentification renforcée, en particulier sous l'impulsion des recommandations du forum SecuRe Pay, *devrait toutefois se traduire dans un futur proche par un infléchissement de cette tendance au niveau européen ;*

  – et à la recrudescence des cas de vol de carte et/ou de compromission des données de carte à l'occasion notamment de séjours effectués en Amérique latine ou en Asie du Sud-Est, qui donnent lieu à une augmentation des fraudes en paiement de proximité et en retrait avec utilisation très rapide des données compromises et qu'il est en conséquence difficile pour les systèmes de paiement par carte de détecter un comportement inhabituel des porteurs.

Par ailleurs, l'Observatoire constate le bénéfice des efforts importants entrepris en Europe ces dernières années pour lutter contre la fraude, notamment en généralisant l'usage des cartes à puce au standard EMV aux points de vente et de retrait. En effet, les taux de fraude des transactions internationales réalisées en Europe (zone SEPA) comparées à celles réalisées hors Europe (hors zone SEPA) démontrent que les régions n'ayant pas adopté EMV sont victimes d'un report très significatif de la fraude.

C'est dans ce contexte qu'il est important de souligner que Visa, MasterCard, American Express et Discover (Diners Club International) ont annoncé en 2012 un ensemble de mesures incitatives visant à encourager l'adoption du standard EMV aux États-Unis à l'horizon 2015. Les bénéfices attendus, en particulier en matière de lutte contre la contrefaçon de piste magnétique, concerneront tant les cartes françaises pour les paiements de proximité et les retraits effectués aux États-Unis, que les cartes américaines pour les transactions de proximité effectuées en France.

3e partie : travaux de veille technologique autour des techniques de fraude et de la sécurité du paiement par cartes sans contact

Sécurité du paiement par cartes sans contact : *suite à l'accroissement sensible du nombre de cartes et de terminaux de paiement sans contact et à la publication d'études récentes sur leur sécurité, l'Observatoire a souhaité actualiser ses analyses de 2007 et 2009. Il en ressort que les risques liés à l'écoute passive de transactions sans contact et à l'activation à distance non légitime de la carte demeurent faibles en raison de modalités techniques de mise en œuvre particulièrement difficiles en pratique. L'intérêt financier pour un fraudeur reste également très limité compte tenu des montants peu élevés des paiements sans contact pouvant être réalisés sans la saisie du code confidentiel.*

Fort de ces constats, l'Observatoire considère que le principal risque lié aux paiements sans contact par carte est le risque d'image. La nécessité de maintenir la confiance des utilisateurs dans ce moyen de paiement conduit toutefois l'Observatoire à réitérer ses recommandations précédentes. Dans ce cadre, les émetteurs se sont engagés à mettre à la disposition de leurs porteurs des dispositifs visant à empêcher l'utilisation du mode sans contact à l'aide d'étuis de protection ou à désactiver le mode sans contact par l'envoi de scripts de désactivation à distance, voire à émettre des cartes dépourvues de cette fonction à la demande des porteurs. En outre, l'Observatoire confirme l'intérêt d'étudier la mise en œuvre d'un numéro de carte (PAN) dédié aux seuls paiements sans contact afin de rendre inopérante la réutilisation de données compromises sur d'autres canaux, notamment sur Internet. Pour ce dernier canal, l'Observatoire recommande la poursuite du déploiement de mesures visant à sécuriser les transactions à distance par de l'authentification renforcée.

Techniques de fraude : *les cartes de paiement et dispositifs d'acceptation bénéficient d'un niveau de sécurité élevé en France. La fraude sur les transactions par carte demeure ainsi bien maîtrisée et se situe à un niveau particulièrement faible pour les retraits et les paiements de proximité. L'Observatoire a néanmoins souhaité dresser un état des lieux des différentes techniques de fraude existantes et présenter les mesures destinées à réduire les risques d'attaque et de réutilisation des données compromises.*

Il ressort notamment de cette étude qu'en raison d'un volume de données conséquent présent dans les bases des commerçants et des prestataires de services de paiement, des mesures de protection adéquates doivent ainsi être mises en œuvre par les acteurs afin de limiter l'accès illégitime à ces données par des fraudeurs et leur réutilisation en particulier en paiement à distance.

En ce qui concerne le paiement de proximité, la vigilance doit être maintenue sur les terminaux et automates de paiement, les processus de certification et d'agrément de ces matériels devant constamment s'adapter afin de prendre en compte les techniques de développement à l'état de l'art.

L'Observatoire recommande par ailleurs aux commerçants et aux acteurs de la filière d'acquisition d'être attentifs aux équipements d'acceptation et de tracer rigoureusement le matériel déployé en proximité afin de prévenir toute tentative de manipulation ou de substitution. Les porteurs sont également invités à rester vigilants lorsqu'ils effectuent un paiement de proximité ou un retrait (cf. annexe 1).

Enfin, afin de limiter la réutilisation des données compromises sur le canal Internet, particulièrement exposé à la fraude, l'Observatoire recommande l'authentification renforcée du porteur en complément de l'usage du cryptogramme visuel (CVx2).

4e partie : les évolutions règlementaires et les recommandations internationales dans le paiement par carte en Europe et dans le monde

L'Observatoire a souhaité, cette année, réaliser un état des lieux des évolutions réglementaires et des recommandations en matière de paiement par carte en Europe et dans le monde.

Compte tenu de la nécessité d'assurer le maintien d'un haut niveau de sécurité pour cet instrument tout en favorisant le développement de ses usages, l'enjeu pour les régulateurs et les surveillants réside dans une adaptation permanente des cadres opérationnel et juridique déployés autour de la carte de paiement. Par ailleurs, le caractère intégré des échanges économiques et des paiements nécessite une coordination des pratiques réglementaires afin de ne pas générer de distorsions concurrentielles entre les acteurs et de limiter les opportunités de fraude.

Dès 2007, le législateur européen a entrepris d'harmoniser le cadre réglementaire du droit des paiements afin de faciliter la mise en place du marché européen unique des paiements scripturaux et d'accroître la concurrence. La réflexion lancée en 2012 par la Commission européenne en vue d'identifier et de lever les obstacles limitant l'intégration du marché devrait conduire à l'évolution prochaine du cadre juridique des paiements au niveau européen, dans le but de disposer de moyens de paiement plus efficaces, plus modernes et plus sûrs. Avec la croissance de la fraude sur les paiements par carte lors des achats sur Internet, les superviseurs et surveillants nationaux européens ont en outre créé en 2011 le forum SecuRe Pay, *dont le premier rapport publié en janvier 2013 contient des recommandations destinées à renforcer la sécurité du paiement par carte sur Internet.*

*Au niveau international, des travaux sont conduits dans le cadre de la Banque des règlements internationaux. Un rapport du comité sur les systèmes de paiement et de règlement (*Committee on Payment and Settlement Systems – *CPSS) s'est également penché en 2012 sur le sujet des paiements innovants (y compris la carte) et de leur sécurité.*

État des lieux de la sécurisation des paiements par carte sur Internet

La fraude sur les paiements à distance en France, qui représente en 2012 138,8 millions d'euros (pour un taux de fraude de 0,299 %), et les moyens mis en œuvre par les acteurs de la chaîne de paiement afin de s'en prémunir, font l'objet d'un suivi régulier par l'Observatoire. Parmi les mesures recommandées par ce dernier, la généralisation progressive de l'authentification renforcée du porteur par l'envoi d'un code de validation non rejouable pour les paiements sur Internet, à chaque fois que cela est possible et pertinent, occupe une place prépondérante.

À l'instar du rapport 2011, ce chapitre présente l'état d'avancement de la mise en œuvre de cette recommandation (1|) ainsi que les actions menées par l'Observatoire et la Banque de France pour sensibiliser les e-commerçants au renforcement de la sécurité des paiements sur Internet (2|).

1| État des lieux de la sécurisation des paiements par carte sur Internet

1|1 État d'avancement du déploiement de « 3D-Secure »

Afin de suivre le déploiement de solutions d'authentification renforcée par les émetteurs et d'identifier les éventuelles difficultés ou axes d'amélioration, l'Observatoire réalise depuis 2011 des campagnes semestrielles de collecte de données statistiques auprès des établissements bancaires et de leurs prestataires techniques, qui permettent de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification renforcée. Les données collectées par l'Observatoire montrent ainsi une nette amélioration du taux de déploiement de tels dispositifs, tant par les émetteurs que par les commerçants, au cours de l'année 2012.

1|1|1 88 % des porteurs de cartes sont désormais équipés d'un dispositif d'authentification opérationnel

La quasi-totalité des porteurs est désormais équipée d'au moins un dispositif d'authentification renforcée, conformément aux recommandations émises par l'Observatoire. Parmi ceux-ci, le dispositif d'authentification par SMS reste largement majoritaire [1].

Le taux d'activation [2] de ces dispositifs par les porteurs a progressé de 84 % à 88 % de la population totale des acheteurs en ligne en un an.

1|1|2 Le taux d'échec sur les transactions sécurisées est en recul, aux alentours de 18 %

Le taux d'échec sur les transactions s'améliore, à 18 %, contre 20 % en 2011. Ce taux, qui peut encore paraître élevé de prime abord, ne tient toutefois pas compte des échecs suivis d'une nouvelle tentative réussie ainsi que des tentatives de fraude. Le déploiement des dispositifs de sécurisation aux transactions de paiement les plus risquées peut par ailleurs expliquer un taux d'échec élevé sur ces transactions. Ce taux d'échec doit par ailleurs être comparé à celui observé sur les paiements par carte non authentifiés et non collecté à ce jour mais qui devrait faire l'objet d'un suivi à compter de l'année prochaine.

Il est à noter que la forte hétérogénéité des taux d'échec entre les établissements de la Place se réduit, dans le sillage d'échanges bilatéraux sur les bonnes pratiques entre la Banque de France et les établissements.

L'Observatoire restera dans ces conditions attentif à l'évolution et à la diminution progressive de ce taux d'échec.

1 Certains établissements ont mis en place des solutions reposant sur un « *token* », un lecteur de cartes ou un courriel adossé à la saisie d'un code unique disponible sur une carte matricielle. On se reportera au rapport 2009 de l'Observatoire, chapitre 4 (p. 51-52), pour une description plus complète de ces dispositifs d'authentification.

2 L'activation du dispositif, par exemple dans le cadre du SMS, nécessite que le porteur communique à sa banque le numéro de téléphone portable sur lequel il souhaite recevoir les codes à usage unique.

1|1|3 La part des transactions authentifiées *via* « 3D-Secure » continue de progresser grâce à la migration progressive des acteurs du e-commerce

Si la proportion de commerçants permettant l'authentification forte des cyberacheteurs reste stable à environ 50 %, la part des transactions authentifiées *via* « 3D-Secure » progresse en valeur (de 23 % à 27,5 % en montant sur un an) notamment sous l'impulsion des actions de sensibilisation menées par l'Observatoire et la Banque de France auprès des e-commerçants (cf. ci-dessous). Cette progression s'inscrit dans la continuité du passage à l'authentification renforcée de grands acteurs du commerce en ligne, à l'instar de Voyages-SNCF, Air France, Orange, ou plus récemment Mistergooddeal.

1|2 Les dispositifs d'authentification bénéficient d'une notoriété accrue auprès des utilisateurs qui y sont désormais plus régulièrement confrontés

Dans la continuité des sondages précédents visant à mesurer le ressenti des cyberacheteurs ayant été confrontés aux dispositifs d'authentification renforcée lors d'un paiement par carte sur Internet, l'Observatoire a souhaité cette année évaluer l'évolution du taux de connaissance et d'utilisation des dispositifs d'authentification renforcée auprès de la population des cyberacheteurs.

Cette étude a été menée par l'institut Harris Interactive auprès d'un échantillon de 993 individus représentatifs de la population française âgés de 16 ans et plus.

1|2|1 Les dispositifs d'authentification des paiements par carte en ligne sont désormais très largement connus par les cyberacheteurs…

Neuf cyberacheteurs sur dix indiquent désormais connaître un dispositif de sécurisation complémentaire au numéro de la carte et au cryptogramme demandés lors d'une transaction en ligne et plus de huit cyberacheteurs sur dix ont connaissance d'au moins un dispositif d'authentification renforcée, dont notamment le code unique transmis par SMS. Il est à noter que la proportion de cyberacheteurs ayant connaissance d'au moins un dispositif d'authentification renforcée a progressé de 37 % cette année, grâce notamment à une utilisation accrue.

1|2|2 … et sont de plus en plus utilisés

La proportion des cyberacheteurs qui indique avoir utilisé un dispositif d'authentification renforcée, principalement le code unique transmis par SMS, a progressé de 40 % par rapport au sondage mené l'année précédente. Ainsi, deux cyberacheteurs sur trois indiquent désormais avoir déjà été confrontés à une authentification renforcée.

L'utilisation accrue de ces dispositifs est bien entendu à mettre en lien avec la généralisation progressive des dispositifs d'authentification par les e-commerçants, auprès desquels l'Observatoire et la Banque de France ont mené des actions de sensibilisation aux risques de fraude au cours de cet exercice.

2| Les actions menées par l'Observatoire et la Banque de France pour sensibiliser les e-commerçants au renforcement de la sécurité des paiements sur Internet

2|1 Organisation en 2012 d'un colloque sur la sécurisation des paiements par carte sur Internet et publication d'une brochure de sensibilisation à destination des e-commerçants

Dans un contexte où le canal Internet est particulièrement touché par la fraude, comme le soulignent les statistiques publiées par l'Observatoire depuis plusieurs années, ce dernier a organisé le 12 novembre 2012 un colloque sur la sécurisation des paiements par carte sur Internet.

Cette manifestation placée sous la présidence du gouverneur de la Banque de France, Christian Noyer, également président de l'Observatoire, a rassemblé plus de 180 participants dont les représentants de plus de 70 enseignes de e-commerce.

Elle a permis aux acteurs concernés de partager leur expérience sur les moyens permettant de lutter efficacement contre la fraude à la carte de paiement sur Internet. Les échanges lors de ce colloque ont montré que cette lutte nécessite la mise en œuvre d'outils complémentaires, permettant notamment de détecter les paiements risqués afin de les sécuriser au moyen d'une authentification renforcée.

Il a été conclu que ces moyens d'authentification renforcée doivent dorénavant être généralisés pour faire reculer la fraude sur les paiements par carte sur Internet. Ils doivent également être adaptés aux évolutions technologiques et aux modes de consommation, notamment en ce qui concerne le recours croissant au téléphone mobile pour commander et payer sur Internet.

À ce titre, les portefeuilles électroniques peuvent faire partie des réponses adaptées pour sécuriser les paiements sur ce canal. Pour autant, les professionnels ont été invités par l'Observatoire à poursuivre leurs efforts afin de proposer des dispositifs assurant l'authentification renforcée sur l'ensemble des canaux de distribution.

Pour faire suite à ce colloque, l'Observatoire a publié à l'attention des e-commerçants une brochure sur la sécurité des paiements sur Internet, laquelle peut être consultée sur son site internet (*www.observatoire-cartes.fr* – rubrique : *Commerçants, comment renforcer la sécurité des paiements sur Internet ?*).

Cette brochure rappelle les bonnes pratiques en matière de lutte contre la fraude sur les paiements par carte sur Internet, notamment les conditions pour un déploiement réussi de l'authentification renforcée.

Cette brochure a été complétée par la mise en ligne d'une foire aux questions visant à répondre aux interrogations générales, techniques et juridiques qui permettent aux commerçants de mieux comprendre le mécanisme de l'authentification renforcée.

2|2 Parallèlement, organisation de réunions bilatérales avec les e-commerçants particulièrement exposés aux risques de fraude

La Banque de France a initié début 2013, conjointement avec le Groupement des Cartes Bancaires, des rencontres avec les e-commerçants qui font l'objet d'un montant et/ou d'un taux de fraude particulièrement élevé.

Cette démarche vise à sensibiliser les commerçants et leurs prestataires de services de paiement à la question de la fraude en vente à distance et à définir des plans d'action visant à diminuer le taux de fraude, notamment en déployant l'authentification renforcée des paiements les plus risqués.

Il ressort des premières rencontres organisées les conclusions suivantes :

• les e-commerçants rencontrés se sont engagés dans une démarche de déploiement, pour la plupart en 2013, des dispositifs d'authentification renforcée des porteurs pour les transactions les plus risquées ;

• de nombreux e-commerçants soulignent qu'ils font bien souvent l'objet de schémas de fraude qui dépassent la simple fraude au moyen de paiement et qui entrent dans une catégorie plus large de la cybercriminalité (détournement d'identité, etc.). Dans ce contexte, ils soulignent le besoin de disposer d'interlocuteurs au niveau des forces de l'ordre et de la justice en mesure d'appréhender le caractère transversal de la cybercriminalité ;

• certains e-commerçants sont confrontés à des schémas de fraudes liées à l'utilisation de cartes prépayées anonymes. Dans ce contexte, ils ont fait part de leur intérêt à ce que les e-commerçants puissent plus facilement identifier les cartes prépayées afin de renforcer la vigilance sur ces cartes et être en mesure de les bloquer lorsqu'un cas de fraude est détecté. Il est à noter que l'Observatoire a poursuivi en 2012 son analyse relative à l'utilisation des cartes prépayées anonymes et que son président a saisi par lettre le ministre de l'Économie et des Finances pour souligner les risques que représentent ces produits en termes de fraude et de financement du terrorisme et suggérer une évolution du cadre normatif en conséquence.

Ces points feront l'objet d'un suivi au sein des groupes de travail de l'Observatoire.

3| Conclusion : une progression constante du niveau de sécurité sur Internet, sous l'action de l'ensemble des acteurs

L'enquête d'opinion menée pour la troisième année consécutive par l'Observatoire et les statistiques transmises par les établissements bancaires et leurs prestataires techniques montrent de réelles avancées en termes de sécurisation des opérations de paiement par carte sur Internet en 2012. La progression de la notoriété des solutions déployées à cette fin traduit leur utilisation par les e-commerçants et devrait avoir un impact positif à moyen terme sur les chiffres de la fraude.

L'Observatoire recommande aux banques et aux commerçants de poursuivre les actions engagées afin de lutter contre la fraude sur les opérations à distance, dont le niveau reste élevé (cf. chapitre 2, paragraphe 4|) :

- les banques ayant désormais quasiment achevé le déploiement des solutions d'authentification renforcée, l'enjeu réside pour certaines dans l'amélioration du taux de réussite des transactions sécurisées ;

- la généralisation de l'authentification non rejouable et donc de « 3D-Secure » auprès des commerçants, avec un déclenchement reposant sur une analyse de risques, reste une priorité pour l'Observatoire. L'adoption de « 3D-Secure » par quelques grands e-commerçants en 2012, tel que Mistergooddeal, devrait constituer un élément déterminant pour une diffusion plus large de ce protocole auprès des e-commerçants de taille significative.

Ces actions s'inscrivent en outre désormais dans un cadre européen, les recommandations du forum européen sur la sécurité des moyens de paiement *SecuRe Pay* ayant préconisé la généralisation de l'authentification renforcée du porteur pour les paiements sur Internet les plus risqués d'ici au 1er février 2015.

Statistiques de fraude pour 2012

Depuis 2003, l'Observatoire établit des statistiques de fraude sur les cartes de paiement de type « interbancaire » et de type « privatif », sur la base de données recueillies auprès des émetteurs et des accepteurs. Ce recensement statistique suit une définition et une typologie harmonisées, établies dès la première année de fonctionnement de l'Observatoire et reprises en annexe 6 du présent rapport. Une synthèse des statistiques pour 2012 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou de retrait) et l'origine de la fraude (carte perdue ou volée, carte non parvenue, carte altérée ou contrefaite, numéro de carte usurpé). En complément, une série d'indicateurs détaillés est présentée dans l'annexe 5 de ce rapport.

1| Vue d'ensemble

En 2012, le montant total des paiements par carte s'élève à 561,5 milliards d'euros, en croissance de 5,2 % par rapport à 2011. Le rythme de croissance annuelle de l'activité est plus faible qu'en 2011 (+ 7,1 %) et légèrement inférieur à la moyenne des cinq dernières années (+ 6,2 %), mais il demeure supérieur à ceux observés en 2009 (+ 2,9 %) et 2010 (+ 4,4 %).

Encadré 1

Statistiques de fraude : 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 ».

Les statistiques calculées par l'Observatoire portent ainsi sur :

- *511 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 67,3 millions de cartes de type « interbancaire » émises en France (dont 1,97 million de porte-monnaie électroniques et 3,42 millions de cartes sans contact) ;*

- *17,4 milliards d'euros de transactions réalisées (principalement en France) avec 18,4 millions de cartes de type « privatif » émises en France ;*

- *32,1 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.*

Les données recueillies proviennent :

- *de neuf émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club et Franfinance ;*

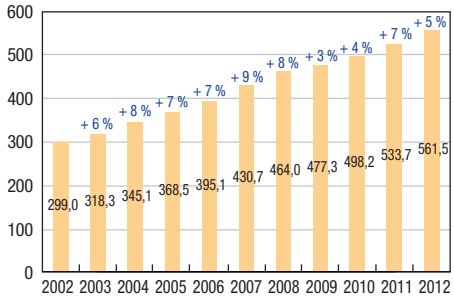
- *des 130 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et de Visa Europe France ;*

- *des émetteurs du porte-monnaie électronique Moneo.*

Graphique 1

Évolution du montant des transactions

(en milliards d'euros)

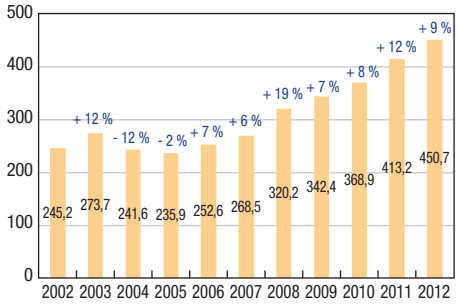


Source : Observatoire de la sécurité des cartes de paiement

Graphique 2

Évolution du montant de la fraude

(en millions d'euros)



Source : Observatoire de la sécurité des cartes de paiement

Le montant total de la fraude est quant à lui en plus forte augmentation (+ 9,1 % par rapport à 2011) pour s'élever à 450,7 millions d'euros en 2012. Cette hausse s'explique par deux tendances principales :

• une augmentation de nouveau importante de la fraude sur les transactions internationales (+ 11,2 % par rapport à 2011) après une année exceptionnelle de baisse en 2011. Les transactions internationales, qui représentent 10,3 % de la valeur totale des transactions, comptent pour 49,8 % du montant total de la fraude ;

• une augmentation de la fraude sur les transactions nationales (+ 7,1 % par rapport à 2011) qui, comme chaque année, concerne principalement les paiements à distance. L'ensemble des paiements à distance, qui représentent 9,2 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude nationale.

Compte tenu de ces évolutions, le taux de fraude sur les paiements et les retraits par carte enregistré en 2012 dans les systèmes français s'élève à 0,080 %, en légère augmentation pour la cinquième année consécutive.

Le taux de la fraude émetteur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France, s'établit en 2012 à 0,065 %, pour un montant de fraude de 345,2 millions d'euros (contre 0,061 % et 306,8 millions d'euros en 2011).

Le taux de la fraude acquéreur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France quelle que soit l'origine géographique de la carte, est en légère diminution. Il s'établit en 2012 à 0,062 %, pour un montant de fraude de 331,9 millions d'euros (contre 0,063 % en 2011, pour un montant de fraude de 317,8 millions d'euros).

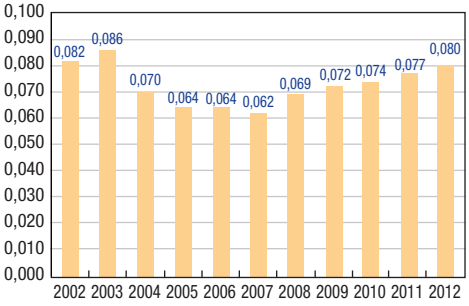
Le nombre de cartes mises en opposition en 2012 et pour lesquelles au moins une transaction frauduleuse a été enregistrée, s'élève à 767 000 (+ 3 % par rapport à 2011), soit à un niveau toujours très élevé après la forte augmentation observée en 2011 (+ 16 % par rapport à 2010).

Le montant moyen d'une transaction frauduleuse est en diminution, pour s'établir à 125 euros contre 130 euros en 2011.

Graphique 3

Évolution du taux de fraude pour tous types de cartes et transactions

(en %)



Source : Observatoire de la sécurité des cartes de paiement

2| Répartition de la fraude par type de carte

Tableau 1

Répartition de la fraude par type de carte

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

	2008	2009	2010	2011	2012
Cartes de type « interbancaire »	0,070 (304,3)	0,072 (324,3)	0,074 (351,5)	0,077 (394,9)	**0,080 (434,4)**
Cartes de type « privatif »	0,054 (16,0)	0,068 (18,2)	0,080 (17,4)	0,083 (18,3)	**0,076 (16,3)**
Total	0,069 (320,2)	0,072 (342,4)	0,074 (368,9)	0,077 (413,2)	**0,080 (450,7)**

Source : Observatoire de la sécurité des cartes de paiement

Le taux de fraude pour les cartes de type « interbancaire » s'établit à 0,080 % en 2012 (contre 0,077 % en 2011), en augmentation pour la cinquième année consécutive. Le taux de fraude pour les cartes de type « privatif » s'établit à 0,076 % en 2012 (contre 0,083 % en 2011), en diminution après quatre années consécutives d'augmentation.

Pour les cartes de type « interbancaire », les taux de fraude émetteur et acquéreur sont respectivement de 0,066 % et de 0,062 % (contre 0,061 % et 0,062 % en 2011). La valeur moyenne d'une transaction frauduleuse est de 122 euros, contre 127 euros en 2011.

Pour les cartes de type « privatif », les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,051 % et à 0,071 % (contre 0,059 % et 0,071 % en 2011). La valeur moyenne d'une transaction frauduleuse s'élève à 345 euros en 2012, contre 321 euros en 2011.

3| Répartition de la fraude par zone géographique

La diminution, observée en 2011, de la fraude sur les transactions internationales n'a pas été confirmée en 2012, et son montant atteint 224,3 millions d'euros (+ 11,2 % par rapport à 2011).

Le montant de la fraude sur les transactions internationales demeure légèrement inférieur à celui de la fraude sur les transactions nationales, qui est également en augmentation à 226,4 millions d'euros (+ 7,1 % par rapport à 2011).

Au regard du montant des opérations en jeu, le taux de fraude sur les transactions internationales (0,387 %) reste toutefois toujours près de huit fois plus élevé que le taux de fraude sur les transactions nationales (0,045 %).

Les transactions internationales représentent ainsi un peu plus de 10,3 % de la valeur totale des transactions par carte mais comptent pour 49,8 % du montant total de la fraude.

Tableau 2

Répartition de la fraude par zone géographique

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

	2008	2009	2010	2011	2012
Transactions nationales	**0,031 (130,9)**	**0,033 (144,0)**	**0,036 (163,8)**	**0,044 (211,5)**	**0,045 (226,4)**
Transactions internationales	**0,427 (189,4)**	**0,449 (198,4)**	**0,423 (205,0)**	**0,367 (201,7)**	**0,387 (224,3)**
- dont émetteur français et acquéreur étranger [a]	0,594 (118,3)	0,594 (121,6)	0,728 (54,9)	0,638 (51,0)	0,759 (62,5)
- dont émetteur français et acquéreur SEPA	–	–	0,331 (50,6)	0,255 (44,3)	0,316 (56,3)
- dont émetteur étranger [b] et acquéreur français	0,291 (71,0)	0,324 (76,8)	0,831 (64,5)	0,892 (81,3)	0,699 (78,2)
- dont émetteur SEPA et acquéreur français	–	–	0,195 (35,0)	0,122 (25,1)	0,132 (27,3)
Total	**0,069 (320,2)**	**0,072 (342,4)**	**0,074 (368,9)**	**0,077 (413,2)**	**0,080 (450,7)**

a) À partir de 2010 : acquéreur hors SEPA uniquement
b) À partir de 2010 : émetteur hors SEPA uniquement
Source : Observatoire de la sécurité des cartes de paiement

L'augmentation de la fraude sur les transactions internationales réalisées avec des cartes émises en France s'explique notamment par le renforcement des dispositifs de protection en France (standards EMV pour les paiements de proximité et authentification non rejouable du porteur de la carte pour les paiements les plus risqués sur Internet), qui a conduit les fraudeurs à reporter leurs attaques vers les transactions internationales.

On observe, parmi ces transactions internationales, une meilleure maîtrise de la fraude sur les transactions réalisées au sein de la zone SEPA que sur celles réalisées au sein des pays situés hors de la zone SEPA :

- le taux de fraude sur les transactions effectuées en France avec des cartes étrangères émises hors de la zone SEPA (0,699 %) est plus de cinq fois supérieur à celui des transactions effectuées avec des cartes étrangères émises dans la zone SEPA (0,132 %) ;

- le taux de fraude sur les transactions effectuées hors zone SEPA avec des cartes émises en France (0,759 %), est près de deux fois et demie supérieur à celui des transactions effectuées au sein de la zone SEPA avec ces mêmes cartes (0,316 %).

Ces meilleurs résultats récompensent les efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et des terminaux de paiements vers le standard EMV.

Dans ce contexte, on notera que Visa, MasterCard, American Express et Discover (Diners Club International) ont annoncé en 2012 un ensemble de mesures incitatives visant à encourager l'adoption du standard EMV aux États-Unis.

En particulier, la mise en œuvre prévue à partir d'octobre 2015, pour les points de vente qui n'auront pas encore migré vers EMV, d'un transfert de responsabilité de l'émetteur de la carte vers le commerçant en cas de fraude, devrait fortement inciter d'une part les émetteurs américains à adopter dès à présent le standard EMV pour toutes les nouvelles cartes émises et d'autre part les commerçants américains à programmer la migration de leurs terminaux vers EMV au plus tard en octobre 2015.

Les bénéfices attendus, en particulier en matière de lutte contre la contrefaçon de piste magnétique, concerneront tant les cartes françaises pour les paiements de proximité et les retraits effectués aux États-Unis, que les cartes américaines pour les transactions de proximité effectuées en France.

4| Répartition de la fraude par type de transaction

La typologie de transaction de paiement par carte adoptée par l'Observatoire distingue les paiements de proximité et sur automate (réalisés au point de

Tableau 3

Répartition du taux de fraude nationale par type de transaction

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

	2008	2009	2010	2011	2012
Paiements	0,036 (111,7)	0,038 (123,2)	0,041 (137,3)	0,049 (177,8)	0,049 (190,0)
dont paiements de proximité et sur automate	0,015 (44,5)	0,014 (41,0)	0,012 (36,2)	0,015 (48,1)	0,015 (51,2)
dont paiements à distance	0,252 (67,2)	0,263 (82,2)	0,262 (101,1)	0,321 (129,6)	0,299 (138,8)
dont par courrier/téléphone	*0,280* *(28,5)*	*0,263* *(30,3)*	*0,231* *(27,3)*	*0,259* *(25,4)*	*0,338* *(29,4)*
dont sur Internet	*0,235* *(38,8)*	*0,263* *(51,9)*	*0,276* *(73,9)*	*0,341* *(104,2)*	*0,290* *(109,4)*
Retraits	0,018 (19,1)	0,019 (20,8)	0,024 (26,5)	0,029 (33,7)	0,031 (36,4)
Total	**0,031** **(130,9)**	**0,033** **(144,0)**	**0,036** **(163,8)**	**0,044** **(211,5)**	**0,045** **(226,4)**

Source : Observatoire de la sécurité des cartes de paiement

vente ou sur distributeurs de carburant, de billets de transport…) des paiements à distance (réalisés sur Internet, par courrier, par téléphone/fax, etc.) et des retraits. Pour une meilleure lisibilité, les développements qui suivent distinguent les données des transactions nationales des données des transactions internationales.

En ce qui concerne les transactions nationales (cf. tableau 3), on observe que :

• le taux de fraude sur les paiements de proximité et sur automate est stable à 0,015 %. Ces paiements représentent plus de 67 % du montant des transactions nationales, et seulement 23 % du montant de la fraude.

Le taux de fraude sur les retraits est en augmentation de 6 % par rapport à 2011 pour s'établir à 0,031 %. Cette augmentation s'explique principalement par la hausse très sensible des attaques de distributeurs automatiques de billets (environ 1 100 en 2012, soit + 73 % par rapport à 2011) et de points de vente (environ 110 en 2012, soit 2,5 fois plus de cas qu'en 2011) qui sont devenus des cibles privilégiées pour des réseaux de fraude organisés, ainsi que par un nombre toujours important des cas de vols de carte avec code confidentiel.

Face à la confirmation de ces tendances déjà observées en 2011, l'Observatoire réitère 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).

• le taux de fraude sur les paiements à distance est quant à lui en diminution à 0,299 %, tout en demeurant vingt fois plus élevé que le taux de fraude sur les paiements de proximité. On notera en particulier que le taux de fraude sur les paiements sur Internet diminue pour s'établir à 0,290 % (contre 0,341 % en 2011), alors qu'il continue d'augmenter pour les paiements à distance effectués par courrier ou par téléphone, pour s'établir à 0,338 % (contre 0,259 % en 2011). Ces premiers résultats obtenus pour les paiements sur Internet témoignent des efforts réalisés par les émetteurs et par les e-commerçants pour déployer des dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte pour les paiements les plus risqués. On note toutefois le report d'une partie de la fraude sur les paiements sur Internet vers les autres types de paiements à distance. Dans un contexte de croissance toujours soutenue du commerce électronique, les paiements à distance, qui ne représentent que 9,2 % de la valeur des transactions nationales, comptent pour 61 % du montant de la fraude (ratio stable par rapport à 2011).

Le niveau de la fraude sur ce canal de paiement conduit l'Observatoire à renouveler ses recommandations visant au déploiement, par les e-commerçants, notamment les plus grands d'entre eux, de dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte pour les paiements les plus risqués (cf. chapitre 1 du présent rapport).

En ce qui concerne les transactions internationales (cf. tableau 4), l'Observatoire ne dispose d'une répartition de la fraude par type de transaction que pour les transactions réalisées par des cartes françaises à l'étranger.

On remarque que la fraude sur les paiements à distance auprès de e-commerçants étrangers réalisés avec des cartes françaises a très fortement augmenté (61,6 millions d'euros en 2011 contre 45,0 millions d'euros en 2011), ce qui peut notamment s'expliquer par un report partiel de la fraude nationale sur ce canal suite à l'adoption progressive par les sites de commerce en ligne situés en France de dispositifs de sécurisation des paiements sur Internet, alors que les sites situés à l'étranger restent moins bien protégés.

On constate toujours un taux de fraude sur les paiements à distance particulièrement élevé hors zone SEPA (1,551 %) et une augmentation sensible du taux de fraude sur les paiements à distance réalisés avec des cartes françaises dans la zone SEPA (0,735 % en 2012 contre 0,571 % en 2011). Le déploiement de dispositifs d'authentification renforcée, sous l'impulsion notamment des recommandations du forum européen sur la sécurité des moyens de paiement (*SecuRe Pay* – cf. chapitre 1) devrait toutefois se traduire dans un futur proche par un infléchissement de cette tendance au niveau européen.

On remarque également que la fraude a augmenté sur les paiements de proximité et sur automate réalisés avec des cartes françaises à l'étranger hors zone SEPA (44,5 millions d'euros en 2012 contre 36,5 millions

Tableau 4

Répartition du taux de fraude internationale par type de transaction

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

Émetteur français – Acquéreur étranger [a]	**2009**	**2010**	**2011**	**2012**
Paiements	0,679	0,795	0,561	0,687
	(105,2)	(39,8)	(30,5)	(37,8)
dont paiements de proximité et sur automate	0,406	0,655	0,369	0,456
	(44,7)	(25,8)	(16,0)	(19,8)
dont paiements à distance	1,350	1,310	1,320	1,551
	(60,5)	(14,0)	(14,5)	(18,0)
dont par courrier/téléphone	*1,016*	*1,193*	*1,011*	*1,150*
	(9,7)	*(3,8)*	*(3,1)*	*(4,0)*
dont sur Internet	*1,440*	*1,360*	*1,440*	*1,720*
	(50,8)	*(10,2)*	*(11,4)*	*(14,1)*
Retraits	0,331	0,596	0,800	0,904
	(16,5)	(15,1)	(20,5)	(24,7)
Total	**0,594**	**0,728**	**0,638**	**0,759**
	(121,6)	**(54,9)**	**(51)**	**(62,5)**
Émetteur français – Acquéreur SEPA				
Paiements	–	0,396	0,300	0,372
		(49,1)	(43,1)	(55,3)
dont paiements de proximité et sur automate	–	0,112	0,140	0,131
		(9,2)	(12,6)	(11,7)
dont paiements à distance	–	0,944	0,571	0,735
		(40,0)	(30,5)	(43,6)
dont par courrier/téléphone	–	*0,566*	*0,643*	*0,532*
		(4,0)	*(5,6)*	*(6,5)*
dont sur Internet	–	*1,021*	*0,557*	*0,788*
		(36,0)	*(24,9)*	*(37,1)*
Retraits	–	0,052	0,040	0,036
		(1,5)	(1,2)	(1,1)
Total	**–**	**0,331**	**0,255**	**0,316**
		(50,6)	**(44,3)**	**(56,3)**
Émetteur étranger [b] **– Acquéreur français**				
Paiements	0,397	0,982	1,056	0,739
	(74,1)	(63,2)	(80,7)	(77,7)
Retraits	0,055	0,103	0,042	0,033
	(2,8)	(1,4)	(0,6)	(0,6)
Total	**0,324**	**0,831**	**0,892**	**0,699**
	(76,8)	**(64,5)**	**(81,3)**	**(78,2)**
Émetteur SEPA – Acquéreur français				
Paiements	–	0,239	0,155	0,158
		(33,8)	(24,3)	(26,6)
Retraits	–	0,032	0,017	0,017
		(1,2)	(0,8)	(0,7)
Total	**–**	**0,195**	**0,122**	**0,132**
		(35)	**(25,1)**	**(27,3)**

a) À partir de 2010 : acquéreur hors SEPA uniquement
b) À partir de 2010 : émetteur hors SEPA uniquement
Source : Observatoire de la sécurité des cartes de paiement

Encadré 2

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

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

Tableau

Ventilation de la fraude nationale 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
Commerce généraliste et semi-généraliste	28,8	21,0
Voyage, transport	25,7	18,8
Services aux particuliers	24,6	17,9
Téléphonie et communication	15,8	11,5
Équipement de la maison, ameublement, bricolage	10,6	7,8
Produits techniques et culturels	8,3	6,0
Approvisionnement d'un compte, vente de particulier à particulier	7,6	5,5
Services aux professionnels	6,6	4,8
Alimentation	3,1	2,3
Divers	2,8	2,0
Jeu en ligne	2,4	1,8
Assurance	0,5	0,4
Santé, Beauté, Hygiène	0,2	0,1
Total	**137,0**	**100,0**

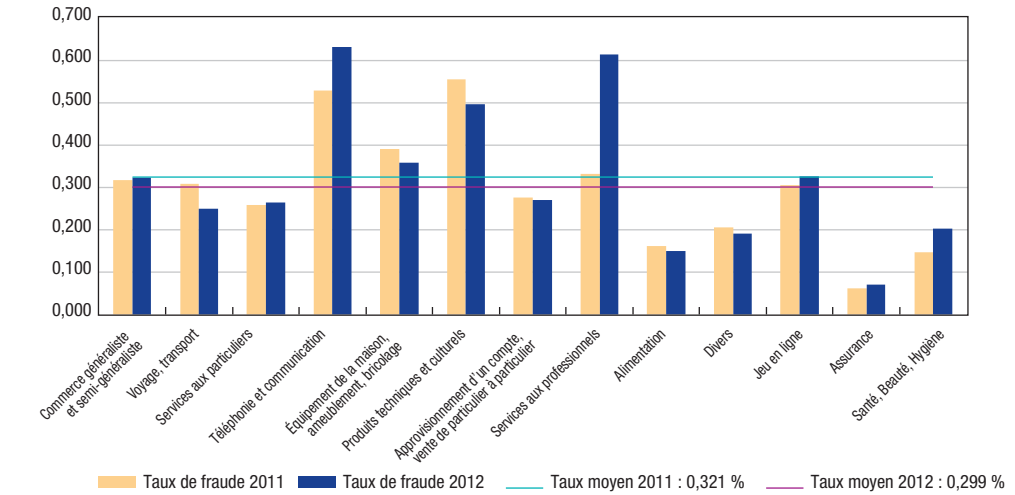
Les secteurs Commerce généraliste et semi-généraliste, Voyage/transport, Services aux particuliers et Téléphonie et communication représentent 69 % du montant de la fraude sur Internet, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Produits techniques et culturels, Services aux professionnels).

On note que le secteur Voyage/Transport n'occupe plus la première place du classement et que la fraude le concernant a diminué en 2012 à 25,7 millions d'euros contre 31,9 millions d'euros en 2011. Ce résultat s'explique par le déploiement de dispositifs d'authentification renforcée du porteur par les plus grands acteurs du secteur (en particulier Voyages-SNCF et Air France).

Graphique

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

(en %)



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

d'euros en 2011). Ceci s'explique par l'augmentation des cas de vol et de compromission des données de cartes émises en France lors, notamment, de séjours en Amérique latine ou en Asie du Sud-Est, avec une utilisation très rapide des données compromises. Il est en conséquence difficile pour les systèmes de paiement par carte de détecter un comportement inhabituel des porteurs.

Enfin, on remarquera à l'inverse une 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.

5| Répartition de la fraude selon son origine

La typologie définie par l'Observatoire distingue les origines de fraude suivantes :

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

• carte non parvenue : la carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;

• carte falsifiée ou contrefaite : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation ; une carte entièrement fausse est réalisée à partir de données recueillies par le fraudeur ;

• numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé ensuite en vente à distance ;

• une catégorie « autres », qui regroupe, en particulier pour les cartes de type « privatif », la fraude liée à l'ouverture frauduleuse de compte par usurpation d'identité.

L'histogramme suivant (cf. graphique 4) indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements).

L'origine de fraude la plus importante (61,2 %) est celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance. Elle est en légère augmentation (59,9 % en 2011). La fraude liée aux pertes et vols de cartes représente encore 34,9 % des paiements nationaux frauduleux, mais elle est de nouveau en diminution (36,1 % en 2011) après la hausse constatée en 2011. La contrefaçon de cartes n'est à l'origine que de 2,6 % des paiements nationaux frauduleux, en légère augmentation (2,3 % en 2011).

Enfin, on observe une diminution de la rubrique « autres », qui est généralement utilisée par les systèmes de carte de type « privatif » pour indiquer les fraudes par ouverture frauduleuse d'un compte ou d'un dossier de crédit (fausse identité) et qui est très significative pour ce type de carte (près de 35 %).

Tableau 5

Répartition de la fraude nationale selon son origine et par type de carte en 2012

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

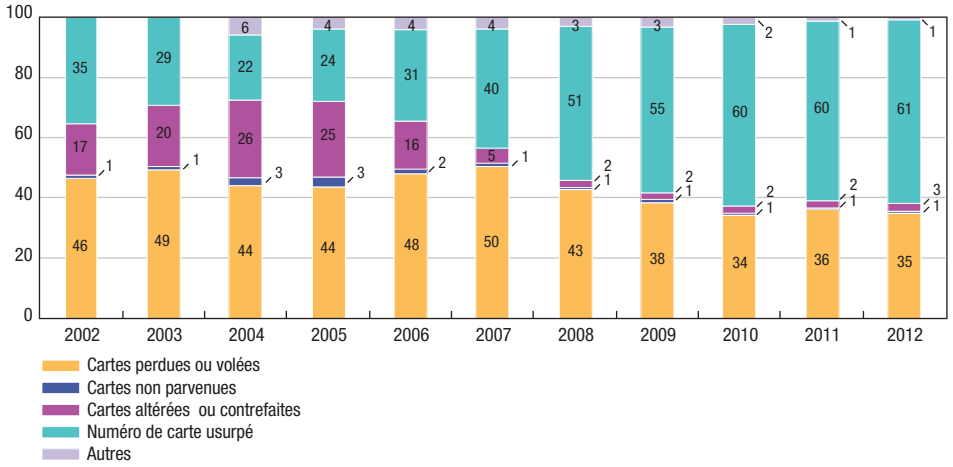
	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	78,9	34,9	78,1	35,4	0,8	14,7
Carte non parvenue	1,1	0,5	0,6	0,3	0,5	9,8
Carte altérée ou contrefaite	6,0	2,6	5,3	2,4	0,6	11,7
Numéro usurpé	138,5	61,2	136,8	61,9	1,6	30,1
Autres	1,9	0,8	0,1	0,0	1,8	33,7
Total	226,4	100,0	221,0	100,0	5,4	100,0

Source : Observatoire de la sécurité des cartes de paiement

Graphique 4

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement

Encadré 3

Indicateurs des services de police et de gendarmerie

Pour l'année 2012, les services de police et de gendarmerie enregistrent une baisse importante des interpellations pour fraude à la carte bancaire, faisant état de 122 personnes interpellées contre 234 en 2011, 235 en 2010, 190 en 2009 et 154 en 2008. Cette diminution s'explique par la prononciation de peines d'emprisonnement plus sévères par la Justice ayant entraîné dès fin 2011 une chute très nette de l'activité liée aux officines de contrefaçon de cartes bancaires étrangères.

Les attaques de distributeurs automatiques de billets (DAB) sont par contre en forte hausse avec environ 1 100 piratages de DAB en 2012 (contre 634 en 2011, 527 en 2010, 526 en 2009, 427 en 2008, 411 en 2007, 526 en 2006, 200 en 2005 et 80 en 2004). À celles-ci s'ajoutent 100 piratages liés aux points de vente (contre 33 en 2011) dont 26 attaques de terminaux de paiement (contre 32 en 2010) et 28 de distributeurs automatiques de carburant (contre 0 en 2011). Ces chiffres en nette augmentation confirment dans les faits la tendance haussière des statistiques relevées par l'Observatoire concernant la fraude en retrait ou en paiement.

Veille technologique

1| La sécurité des paiements par carte sans contact au regard des évolutions récentes

L'OSCP a publié dans ses rapports de 2007 et 2009 un état des lieux de la sécurité des cartes sans contact et a émis un certain nombre de recommandations afin d'en assurer le développement de manière maîtrisée.

Si en 2007, le déploiement des cartes sans contact restait limité, l'étude de 2009 avait pour objectif de réévaluer ces recommandations en prenant en compte le déploiement plus important envisagé de ces cartes et la mise en place de pilotes pour les paiements sans contact par téléphone mobile.

La progression du nombre de cartes sans contact désormais sur le marché, la présence à plus grande échelle de terminaux compatibles et la publication de travaux récents sur les problématiques liées à cette technologie ont amené l'Observatoire à actualiser son analyse dans le cadre de son programme de travail 2012-2013. Au regard d'évolutions moins notables sur la période pour les paiements sans contact déclenchés à partir de téléphones mobiles compatibles, la présente étude se concentre avant tout sur la sécurité des paiements par carte sans contact.

1|1 Suivi des recommandations de l'Observatoire (2007/2009)

L'Observatoire s'est très tôt saisi du sujet des paiements sans contact. Ainsi, dans ses rapports 2007 et 2009, l'Observatoire a publié ses analyses de sécurité accompagnées de recommandations couvrant l'ensemble des risques alors identifiés. Un état des lieux de ces recommandations est donné ci-après.

1|1|1 Lutter contre la collecte frauduleuse des données de carte

Les supports sans contact peuvent être soumis à un risque de capture des données échangées par ondes radio avec le terminal de paiement, ou pourraient être sollicités pour générer des opérations de paiement à l'insu du porteur. Ces risques, par ailleurs limités par la mise en œuvre de seuils de transaction unitaires ou cumulés dont l'atteinte impose de repasser en mode contact, ont conduit l'Observatoire à recommander dès 2009 aux émetteurs de poursuivre l'étude de solutions simples permettant d'activer et désactiver le mode de paiement sans contact.

Une première solution, évoquée en 2009, est celle reposant sur des étuis protecteurs permettant de bloquer les ondes radio pouvant être reçues par les antennes présentes dans les cartes sans contact.

D'autres solutions de désactivation sont également envisageables. Pour les cartes, la mise en œuvre de scripts EMV (*Europay MasterCard Visa*) lors d'opérations en mode contact (par exemple lors d'un retrait à un distributeur) permet en effet de désactiver la fonction sans contact suite à une demande du porteur ou de l'émetteur.

L'Observatoire constate qu'à ce jour, les émetteurs de cartes sans contact sont en mesure de suivre ses recommandations, soit en disposant d'étuis de protection, aisément distribuables le cas échéant, soit en implémentant dans leurs systèmes une fonction de désactivation du mode sans contact reposant sur des scripts EMV. Certains établissements se disent enfin prêts à proposer à leurs porteurs des cartes dépourvues de la fonctionnalité sans contact si ces derniers en font la demande.

1|1|2 Limiter les possibilités de réutilisation des données compromises

Afin de limiter les possibilités de réutilisation des données compromises, l'Observatoire a recommandé en 2009 d'étudier la mise en place d'un numéro de carte (PAN – *Primary Account Number*) dédié au paiement de proximité en mode sans contact, différent de celui utilisé en mode contact, également inscrit sur le support. Cette mesure permet en effet de se prémunir contre une réutilisation du numéro de carte compromis pour réaliser des transactions dans un contexte autre qu'un paiement sans contact, le système d'autorisation de l'émetteur bloquant alors tout autre usage.

Les cartes sans contact ne disposent pas aujourd'hui de cette fonctionnalité, toujours à l'étude. Les risques liés à la réutilisation de données compromises apparaissent toutefois limités, pour les raisons suivantes :

• dans un contexte de vente de proximité, les données de la puce sans contact transmises par la carte au terminal diffèrent de celles présentes sur la piste magnétique. Il est donc impossible de cloner une carte à piste valide avec des données qui auraient été capturées lors d'une transaction sans contact ;

• dans un contexte de vente à distance, la réutilisation de données compromises *via* l'interface sans contact demeure elle théoriquement possible car certaines transactions peuvent être acceptées sans cryptogramme visuel (également appelé CVx2). L'Observatoire a recommandé dès 2008 une utilisation systématique du cryptogramme visuel en vente à distance, cette donnée étant imprimée au dos de la carte mais non transmise lors des échanges entre la carte et les terminaux de paiement.

En ce qui concerne les transactions auprès de commerçants français, le Groupement des Cartes Bancaires « CB » impose l'utilisation du cryptogramme visuel depuis 2008 pour les transactions « CB » initiées par Internet (les émetteurs de cartes « CB » doivent refuser une transaction sans CVx2). Des actions sont actuellement menées par le Groupement des Cartes Bancaires « CB » afin de réduire fortement le nombre de transactions sans CVx2, notamment pour les transactions par mail ou téléphone.

Pour les transactions réalisées auprès de commerçants étrangers, les systèmes de paiement par carte internationaux Visa et MasterCard préconisent eux aussi la généralisation de l'usage du CVx2, notamment sous l'impulsion de l'EPC (*European Payment Council*) en Europe.

Enfin, en vente à distance sur Internet, l'authentification non rejouable du porteur au moment de l'achat sur un site commerçant permet de lutter plus efficacement contre la fraude sur ce canal. L'Observatoire promeut cette mesure depuis plusieurs années en France, rejoint début 2013 par le forum *SecuRe Pay* réunissant superviseurs et banquiers centraux européens [1].

1|2 Évolutions récentes (2009-2013)

Des études [2] et interventions publiques ont fait état, au cours du premier semestre 2012, de travaux portant sur la sécurité des cartes de paiement sans contact et de la technologie de communication NFC (*Near Field Communication*) utilisée. Plusieurs failles potentielles ont ainsi été identifiées. L'Observatoire a examiné ces éléments afin de déterminer s'ils pouvaient faire évoluer ses recommandations auprès des émetteurs.

Les études publiées se rapportent principalement à l'écoute passive des communications entre la carte sans contact et un terminal de paiement, afin de récupérer les données échangées et de les utiliser pour effectuer des transactions frauduleuses. Elles ont également porté sur l'activation du support sans contact au-delà de la faible distance requise lors d'un paiement légitime, cette fois-ci pour solliciter la carte de paiement et lui faire exécuter une transaction à l'insu de son porteur. De possibles évolutions sont de plus exposées dans les deux cas, afin d'augmenter les distances d'écoute ou d'activation des supports sans contact (de l'ordre de plusieurs mètres contre quelques centimètres lors d'un fonctionnement normal). L'Observatoire a étudié si les modalités techniques décrites remettaient en cause ses analyses de 2007 et 2009 qui déjà exposaient ces risques.

De nouvelles failles présentées dans ces études consisteraient à rechercher un blocage de la carte de paiement au travers de son interface sans contact. Ainsi, la carte pourrait être sollicitée sur cette interface pour procéder à des essais du code confidentiel (PIN – *Personal Identification Number*) utilisé en mode contact.

1 Recommandations accessibles en ligne à l'adresse suivante : *http://www.ecb.int/press/pr/date/2013/html/pr130131_1.en.html*.
2 Présentées notamment lors de la conférence « *Hackito Ergo Sum* » en avril 2012.

1|2|1 Écoute des transactions sans contact et activation à distance non légitime du support

Les données concernées

Les études publiées détaillaient la nature des informations susceptibles d'être compromises lors de l'écoute des communications entre la carte sans contact et un terminal de paiement ou tout autre dispositif de lecture compatible NFC : le nom du porteur, le numéro de la carte (PAN), sa date d'expiration, une copie partielle des données de la piste magnétique de la carte et un historique [3] des dernières transactions effectuées avec ou sans contact (jusqu'à une centaine de transactions en fonction des paramètres de personnalisation de l'émetteur).

Les modalités de personnalisation des cartes sans contact par les émetteurs ont toutefois évolué depuis ces publications sous l'impulsion des systèmes de paiement par carte : le nom du porteur n'est en effet plus accessible lors des échanges en mode sans contact pour la très grande majorité des cartes émises en France. En ce qui concerne l'accès à l'historique des transactions sur les supports sans contact, le système « CB » a pris la décision d'interdire, pour tous les produits désormais présentés à l'agrément, la lecture de ces données par l'interface sans contact.

Écoute passive des communications

L'écoute passive consiste principalement à intercepter et récupérer au moyen d'un dispositif spécifique les informations échangées entre une carte sans contact et un terminal de paiement compatible. Le dispositif attaquant n'a pas besoin d'alimenter en énergie la carte sans contact, puisque c'est le terminal légitime qui s'en charge. Le positionnement à respecter et les distances imposées rendent la mise en œuvre d'un tel scénario d'attaque particulièrement complexe, comme a pu le constater l'Observatoire par le passé. À ce jour, seuls du matériel spécifique et un environnement contrôlé de type laboratoire permettent de reproduire de tels scénarios. L'ajout de dispositifs intermédiaires par l'attaquant dans le but d'augmenter les distances d'écoute est, pour sa part, source de difficultés de réalisation supplémentaires.

Activation à distance non légitime – sollicitation de la carte

Les attaques par sollicitation consistent à activer la carte sans contact en lieu et place d'un dispositif légitime, tel un terminal de paiement lors d'une transaction effectuée par le porteur auprès d'un commerçant. Pour ce faire, un lecteur NFC associé à une antenne active sont nécessaires afin d'alimenter la carte. La distance d'activation du support variera non linéairement en fonction du profil de l'antenne utilisée et de la puissance électrique fournie par le dispositif. Il a été démontré à cet égard que cette distance ne peut être portée au-delà de quelques dizaines de centimètres, avec ici aussi des conditions difficiles à reproduire dans un environnement autre qu'en laboratoire. Enfin, l'intensité du champ magnétique nécessaire pour permettre l'activation directe de la carte à plus grande distance présente une dangerosité pour l'attaquant et son environnement et rend ce scénario irréaliste en pratique.

Pour pallier ces limites physiques, un système d'attaque en relais permettant de réduire les distances d'activation et donc l'intensité du champ magnétique nécessaire pourrait être envisagé. Il consisterait à utiliser des dispositifs intermédiaires relayant les signaux entre un lecteur attaquant et un terminal de paiement légitime. L'Observatoire avait d'ailleurs déjà examiné cette possibilité en 2007 et conclu à un niveau de risque faible, principalement dû à des contraintes techniques liées à la mise en œuvre effective du dispositif et au respect des temps de transaction. De plus, le bénéfice espéré de l'attaquant et de ses éventuels complices reste lui aussi particulièrement faible, les transactions sans contact étant de petits montants et plafonnées par la présence de seuils [4]. L'Observatoire restera toutefois vigilant à toute évolution de ce type d'attaque.

3 Date, pays, montant, devise principalement.
4 À la fois en nombre de transactions, mais aussi en montant total cumulé, avant de devoir passer en mode contact avec frappe du code confidentiel.

Encadré 1

Protection des données personnelles

La loi Informatique et libertés [1] *vise à protéger les citoyens contre toute atteinte découlant de l'utilisation de moyens informatiques. Elle s'applique à tout traitement de données à caractère personnel, que la personne soit directement ou indirectement identifiable, au moyen d'un numéro d'identification par exemple.*

Les cartes de paiement sans contact sont donc soumises à cette loi. Dès lors, les établissements émetteurs sont tenus de respecter différentes règles, notamment de s'assurer de la pertinence et de la proportionnalité des données par rapport à l'usage que veut en faire le responsable de traitement et d'en assurer la sécurité.

Ainsi, la Commission nationale de l'informatique et des libertés (CNIL) considère que rendre le nom du porteur accessible via *l'interface sans contact alors que cette donnée n'est pas utilisée pour réaliser une opération de paiement n'apparaît pas pertinent. En outre, une telle divulgation d'information présente un risque pour la vie privée des porteurs qui peuvent être identifiés par ce biais. La CNIL note que cette donnée n'est dorénavant plus accessible en mode sans contact pour les cartes « CB ».*

De façon analogue, la CNIL considère que l'accessibilité, via *cette même interface, de l'historique des transactions réalisées en mode contact et sans contact pose également un problème d'atteinte à la vie privée, en permettant d'obtenir des informations sur les habitudes de vie et les éventuels voyages du porteur. La CNIL prend acte des décisions d'ores et déjà prises sur ce point et étudiera les propositions d'évolution au regard des principes posés par la loi.*

Enfin, la CNIL considère que la possibilité d'obtenir le PAN en interrogeant la carte ou en interceptant des transactions légitimes demeure un point de vigilance, cette donnée personnelle étant protégée par la loi.

Une synthèse de ces points a été rendue publique par la CNIL sous le lien suivant : http://www.cnil.fr/cb-sans-contact/

1 *Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, qui rappelle que* « L'informatique doit être au service de chaque citoyen. Son développement […] ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

1|2|2 Blocage de la carte de paiement sans contact

Les études publiées ont mis en avant la possibilité d'un blocage intentionnel de la carte de paiement en sollicitant son interface sans contact pour effectuer une vérification du code confidentiel. La possibilité de deviner le véritable code confidentiel de la carte reste extrêmement faible, puisque le nombre d'essais est limité à trois. Par contre, une telle attaque pourrait, toujours selon ces études, bloquer la carte après justement trois tentatives infructueuses.

Toutefois, les travaux menés par l'Observatoire ont mis en évidence le fait que les cartes émises sur le territoire français ne sont pas vulnérables à cette attaque, puisqu'elles ne permettent pas d'être sollicitées à des fins de vérification du PIN au moyen de leur interface sans contact.

Une autre attaque consisterait à tenter d'atteindre la limite du nombre de transactions pouvant être réalisées par une carte de paiement en la sollicitant pour de nombreuses transactions sur son interface sans contact. En effet, un compteur spécifique est utilisé à cette fin sur la carte.

Cependant, atteindre cette limite prendrait plusieurs heures compte tenu des délais nécessaires à l'accomplissement de chaque transaction, ce qui n'apparaît pas réaliste.

1|3 Conclusions des travaux de l'Observatoire

L'Observatoire s'est attaché cette année à examiner les études publiées début 2012 portant sur la sécurité des cartes de paiement sans contact, afin

de déterminer si ses analyses et recommandations émises en 2007 et 2009 restent valides. Dans un contexte d'augmentation sensible de terminaux compatibles et surtout d'émission en masse de cartes de paiement sans contact, l'Observatoire reste particulièrement vigilant à ce que ces déploiements se produisent dans des conditions de sécurité maîtrisées par les différents acteurs.

Il ressort de ces analyses que les risques liés à l'écoute passive de transactions sans contact et à l'activation à distance non légitime de la carte demeurent faibles en raison de modalités techniques difficiles à mettre en œuvre et requérant un matériel et des environnements de type laboratoire. De plus, la présence de seuils pour les transactions sans contact, cantonnées à des paiements de faible montant, réduit grandement l'intérêt financier de fraudes en cas de perte ou de vol. L'Observatoire reste toutefois attentif à toute évolution dans ce domaine.

Par ailleurs, l'Observatoire note que plusieurs vulnérabilités exposées sont, dans une certaine mesure, dépendantes des options de personnalisation des cartes choisies par les émetteurs, certaines permettant de limiter voire d'éliminer les risques liés à la divulgation d'informations récupérables au travers de l'interface sans contact. En France, les cartes sans contact désormais émises ne permettent plus de capturer le nom du porteur. En ce qui concerne l'historique des transactions, les nouveaux produits carte agréés par le Groupement des Cartes Bancaires « CB » ne permettent plus d'y accéder. Ces données ne peuvent de toute façon être utilisées pour réaliser une transaction de paiement frauduleuse.

Enfin, le risque de blocage des cartes par tentatives successives de vérification du code confidentiel sur l'interface sans contact ou par la réalisation de nombreuses transactions sans contact afin d'atteindre la limite du compteur de transactions de la carte est quant à lui jugé inexistant à ce jour : les cartes émises en France ne permettent pas d'effectuer de telles vérifications dans le premier cas et les modalités de mise en œuvre rendent le second cas irréaliste en pratique.

Fort de ces constats, l'Observatoire considère que le principal risque lié aux paiements sans contact par carte est un risque d'image, mais qu'aucune conséquence notable en termes de fraude n'est à souligner. Toutefois, au regard de l'état d'avancement des projets en cours sur le territoire et afin de garantir la confiance des porteurs dans ce moyen de paiement, l'Observatoire réitère ses recommandations formulées en 2009.

En ce qui concerne la possibilité de désactiver la fonction sans contact des cartes, les émetteurs se sont engagés, soit à mettre à disposition des utilisateurs des étuis de protection, soit à mettre en œuvre la désactivation à distance de la fonction sans contact des supports, soit à substituer aux cartes sans contact des supports dépourvus de cette fonctionnalité à la demande des porteurs. L'utilisation d'un numéro de carte (PAN) dédié aux paiements sans contact, dont l'étude avait été recommandée en 2009, est par ailleurs de nature à rendre vaine toute tentative de capture des données de carte à des fins de réutilisation frauduleuse sur d'autres canaux, notamment en vente à distance sur Internet. Pour ce dernier canal, l'Observatoire recommande la poursuite du déploiement de mesures visant à sécuriser les transactions à distance par de l'authentification non rejouable.

L'Observatoire recommande en outre aux émetteurs et systèmes de paiement par carte de poursuivre la mise en œuvre des mesures visant à limiter les échanges d'informations sensibles lors de transactions en mode sans contact. L'écoute des communications et les possibilités de réutilisation ultérieure des données compromises pourraient notamment être rendues inopérantes par un chiffrement des communications entre la carte sans contact et le terminal de paiement. Une étude coûts/bénéfices de ce type de mesure pourrait être menée afin d'en évaluer la faisabilité technique et la portée en termes de lutte contre la fraude.

L'Observatoire souligne enfin que la mise en œuvre de ces dernières mesures doit désormais s'inscrire dans un contexte international. Il invite donc l'ensemble des acteurs de la chaîne de paiement à s'engager dans des actions concertées avec leurs homologues en Europe et au-delà, afin d'en accroître l'efficacité et la portée. À ce titre et dans la continuité des travaux de l'Observatoire, le forum européen *SecuRe Pay* s'est saisi du sujet des paiements sans contact, par téléphone mobile dans un premier temps, en vue d'émettre des recommandations en la matière.

2| Les techniques de fraude

La fraude sur les transactions par carte est bien maîtrisée en France et se situe même à un niveau particulièrement faible pour les retraits et pour les paiements nationaux de proximité. Elle constitue cependant un enjeu pour l'Observatoire qui, depuis sa création, assure une veille sur les techniques de fraude et recommande des mesures destinées à les circonscrire et à les réduire.

Sous l'effet des évolutions technologiques et de la multiplication des paiements internationaux, les techniques de fraude ont considérablement évolué ces dernières années. Par conséquent, même si certaines d'entre elles ont déjà reçu un éclairage spécifique dans les précédents rapports, l'Observatoire a souhaité en actualiser l'état des lieux.

Que le fraudeur cherche à s'enrichir personnellement ou à mettre en évidence les éventuelles failles des systèmes de protection, il capte des données de carte soit en volant des supports authentiques, soit en déployant des moyens d'usurpation [5] ou de création de données de carte pour les réutiliser dans la chaîne de paiement. Si déterminer l'origine de la fraude selon ces différents cas est actuellement complexe, les constats montrent que les fraudes peuvent affecter l'ensemble de la chaîne de paiement : la carte en elle-même, mais aussi les systèmes d'acceptation ou d'information. En matière de réutilisation, en revanche, la vente à distance (VAD) sur Internet constitue le canal privilégié de la réutilisation des données de carte (cf. chapitre 2 de ce rapport : *Statistiques de fraude pour l'année 2012*). À cet égard, l'Observatoire insiste depuis 2008 sur la nécessité de généraliser l'authentification non rejouable pour les transactions sur Internet, laquelle constitue l'un des moyens réellement efficaces pour réduire les opportunités de réutilisation des données de carte.

Après avoir listé les techniques de « compromission » (captation) actuellement constatées, cette partie expose les mesures de lutte contre la captation des données de carte avant de présenter les outils destinés à réduire les possibilités de réutilisation des données usurpées.

2|1 Les techniques de compromission des données de carte

Les attaques internes ou externes visant les systèmes d'information sont les plus fructueuses car elles permettent d'obtenir des quantités de données importantes. Les attaques portées aux cartes, téléphones mobiles, terminaux de paiement et automates de retrait sont difficiles à mettre en œuvre et à industrialiser au regard des caractéristiques intrinsèques des matériels. Cependant, quelles qu'en soient les modalités, le retentissement de ces attaques est important car la carte de paiement est devenue un instrument de la vie courante.

2|1|1 *Via* les systèmes d'information

Les données de carte étant véhiculées tout au long de la chaîne de paiement, elles peuvent être sujettes à une capture par des personnes malveillantes. Les points de la chaîne nécessitent donc une protection adéquate. Il s'agit notamment des ordinateurs personnels des utilisateurs (consommateurs ou commerçants), des bases de données des commerçants pour les transactions à distance, des concentrateurs monétiques pour les transactions de proximité et des systèmes gérés par les processeurs dans tous les cas. Enfin, les téléphones mobiles, apparus plus récemment dans l'écosystème carte, représentent dorénavant une cible potentielle au même titre que le matériel informatique.

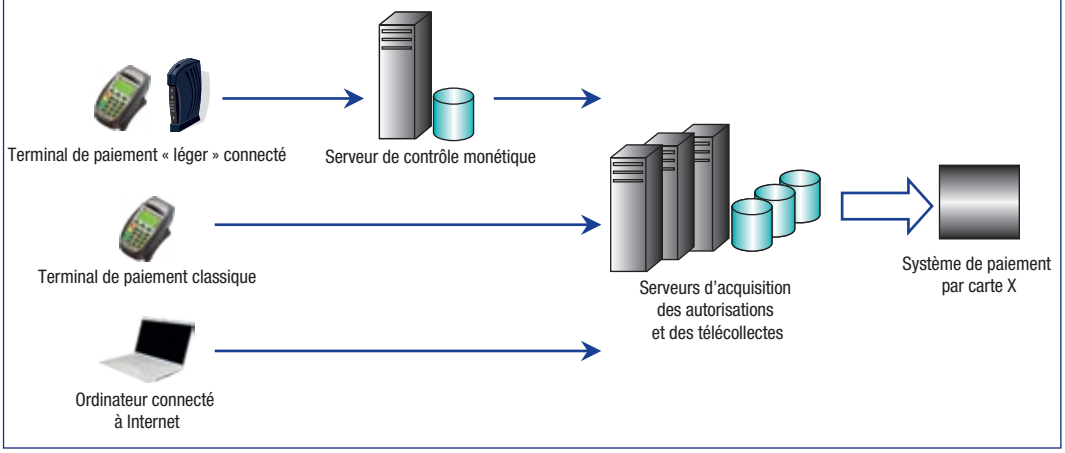
Les ordinateurs personnels peuvent être victimes d'attaques visant à capturer les données insuffisamment sécurisées. Ce type d'attaque nécessite l'installation préalable de logiciels malveillants (*malwares* ou maliciels [6]) par l'utilisateur à son insu, ces derniers étant contenus dans des sources apparemment de confiance. Les données de carte saisies sur l'ordinateur peuvent, par exemple, être captées à l'aide d'un logiciel malveillant qui enregistre les touches frappées au clavier (*malware* de type *keylogger*).

Les téléphones mobiles, de plus en plus utilisés dans le cadre de transactions de paiement par carte [7],

5 L'usurpation de données de carte implique la compromission d'une partie d'entre elles à l'insu du porteur légitime.
6 Un *malware* est tout ou partie d'un logiciel qui vise à nuire à un système d'information.
7 Que ce soit en tant que moyen de paiement ou d'authentification.

Encadré 2

La chaîne de paiement par carte



peuvent également être atteints par des *malwares* qui infectent l'appareil dans l'objectif de compromettre les données personnelles de son utilisateur, dont les données de carte. Ils peuvent également détourner les codes non rejouables transmis par l'émetteur de la carte à son titulaire légitime, afin de permettre à un fraudeur de finaliser une transaction sur un site sécurisé. Par exemple, le *malware* ZitMo (« *Zeus in the Mobile* ») agit de la sorte.

Au-delà des attaques individuelles, les bases de données constituées aux différents stades de la transaction sont devenues très attractives pour les fraudeurs du fait du volume des données exploitables. Ces dernières années, des détournements de données bancaires détenues par des commerçants ou processeurs de données de cartes (Wal-Mart, Sony, Heartland Payment Systems, RBS Worldpay, etc.) ont en effet été cités dans les médias, suite à des compromissions en ligne ou à des *malwares* introduits dans les systèmes à l'aide de supports physiques (clés USB, disques durs, etc.).

2|1|2 *Via* Internet

Un fraudeur peut inciter les porteurs à communiquer leurs données personnelles telles que les données de carte (PAN, PIN, date de validité, CVx2) ou d'authentification (comme le numéro de téléphone mobile sur lequel sont envoyés les codes non rejouables). On parle alors d'hameçonnage ou de *phishing*. Cette typologie d'attaque repose généralement sur l'envoi de courriels usurpant notamment des logos et des chartes visuelles bien connus de leurs destinataires (par exemple des établissements de crédit ou des commerçants) et invitant les victimes à se connecter à un site frauduleux dont l'unique objet est de collecter des informations sensibles. Des variantes sur d'autres canaux, comme le téléphone, sont également mises en œuvre. On parlera alors de *vishing*.

Le dévoiement ou *pharming* consiste, quant à lui, à manipuler les serveurs DNS [8] afin de rediriger l'internaute vers un site frauduleux, en apparence semblable au site légitime. Les fraudeurs peuvent enfin créer de faux sites de e-commerce de toutes pièces, dans le but de collecter frauduleusement des fonds et/ou des données de carte.

2|1|3 *Via* les courriels ou le téléphone

Dans le cadre de transactions MOTO [9] qui comportent une part de traitement manuel, des personnes mal intentionnées peuvent enregistrer des données de carte lors d'un paiement ou d'une réservation.

8 Les serveurs DNS associent les noms des sites Internet (facilement mémorisables) à leurs adresses IP (suite de nombres).
9 *Mail Order Telephone Order*, transactions initiées par courrier ou téléphone (voix).

2|1|4 *Via* les systèmes d'acceptation ou les réseaux

Les matériels d'acceptation (automates de paiement ou de retrait et terminaux de paiement) peuvent faire l'objet d'attaques physiques ou logiques dans le but d'usurper des données de carte. Seront donc abordées dans cette partie les fraudes liées directement à l'utilisation d'une carte de paiement ou de retrait.

Les attaques physiques sur le matériel d'acceptation

Le matériel d'acceptation ainsi que les réseaux véhiculant les données entre celui-ci et les serveurs d'acquisition peuvent être la cible d'attaques visant à s'approprier des données de carte.

S'agissant des automates de retrait ou de paiement, la technique majoritairement utilisée consiste à capturer, à l'insu des porteurs [10], les données écrites sur les pistes magnétiques des cartes (*skimming*). Le moyen de captation est en général suffisamment discret pour ne pas attirer l'attention. À cet effet, l'ensemble de la façade de l'automate ou sa seule fente d'insertion peuvent être factices afin de dissimuler le matériel illégitime. Le dispositif est en outre généralement associé à une caméra vidéo et/ou à un faux clavier permettant la capture du code confidentiel. Il peut également contenir des systèmes de stockage ou de transmission des données compromises.

Une seconde technique consiste à retenir la carte dans l'automate afin de la réutiliser ultérieurement. À cette fin, le fraudeur insère un dispositif, parfois rudimentaire [11], dans l'automate, observe la frappe du code confidentiel au clavier, puis revient récupérer la carte après le départ du porteur. Cette technique s'apparente au vol physique de cartes.

S'agissant des terminaux de paiement utilisés dans des points de vente, des dispositifs de *skimming* du même ordre peuvent être utilisés dans le but de capturer les données de la piste, voire le code PIN du porteur.

Les attaques logiques sur le matériel d'acceptation

Outre les dispositifs d'attaque physique décrits ci-dessus, une deuxième catégorie d'attaques vise à exploiter des failles de sécurité sur les éléments logiques des automates ou terminaux. L'objectif est ici d'injecter un code malveillant dans les systèmes de ces matériels afin d'en modifier le comportement, voire de prendre le contrôle de leurs différents composants (clavier, écran et imprimante). Les attaques peuvent être le fait de personnes disposant d'un accès privilégié à ces appareils (mainteneurs, exploitants…).

Les attaques sur les réseaux

Les réseaux eux-mêmes peuvent être la cible d'attaques lors de l'échange des données entre les matériels d'acceptation, les concentrateurs monétiques le cas échéant et les serveurs acquéreurs. Ces données sont transmises sur des réseaux répondant à deux types de techniques distinctes : sans fil (tels que Bluetooth, Wifi ou GPRS) ou filaires (câbles ou fibre optique). Dans les deux cas, le protocole de communication dominant est désormais IP, sur lequel est basé Internet.

Dans ce contexte, les réseaux IP peuvent être la cible de fraudeurs cherchant à exploiter leurs vulnérabilités pour accéder à un équipement ou capturer les données échangées.

2|1|5 *Via* la carte proprement dite

Outre le vol de cartes, tenter de mettre à mal les systèmes de protection de la carte reste une activité très prisée des fraudeurs et des *hackers*, en raison de la publicité potentielle qui peut en résulter. Différents scénarios d'attaques portant sur la sécurité des paiements par carte, tant en mode contact que sans contact, ont ainsi fait l'objet de publications au cours des derniers mois.

La mise en œuvre de mesures de protection efficaces, dont une synthèse est fournie dans le tableau 1 à

10 Pour de plus amples développements sur ce thème, se reporter au rapport 2010 de l'Observatoire.
11 L'ensemble des variantes est regroupé sous le nom de « collet marseillais ».

la fin de cette partie, a limité la portée de telles attaques, dont la faisabilité et l'efficacité nécessitent des conditions de réalisation de laboratoire.

Les vols de supports légitimes et les contrefaçons

Le vol physique du moyen de paiement pour l'utiliser en lieu et place de son porteur légitime constitue un type d'attaque. Afin d'optimiser la valeur potentielle de chaque support volé, le fraudeur tente en outre généralement de récupérer le code confidentiel de la carte et de différer au maximum le moment où le porteur déclarera le vol de son moyen de paiement. Ceci permet, à la fois, l'utilisation de la carte dans les distributeurs automatiques de billets, dans les terminaux de paiement et sur Internet, pour tous types de transactions.

L'attaque de type *man in the middle*, apparue en 2012, consiste à leurrer les contrôles automatiques effectués à la fois par le terminal de paiement et par une carte perdue ou volée, en manipulant la liaison entre ces deux équipements. Cette technique se révèle toutefois d'une mise en œuvre extrêmement complexe, et les transactions autorisées en ligne, comme les retraits d'espèces, ne permettent pas d'y recourir actuellement, ce qui en limite fortement l'intérêt pour les fraudeurs, motivés prioritairement par les possibilités de retraits.

Les fraudeurs utilisent également, dans certains cas, des logiciels qui génèrent des données de carte [12] afin de les réutiliser dans le cadre de transactions à distance.

Les attaques sur les cartes en mode sans contact

L'Observatoire s'est très tôt saisi du sujet des paiements sans contact par carte et téléphone mobile. Cette préoccupation s'est traduite par la publication d'analyses de sécurité accompagnées de recommandations couvrant les risques alors identifiés dans les rapports 2007 et 2009 et actualisés dans le présent rapport (cf. chapitre 3 : *Point sur la sécurité du paiement par cartes sans contact*).

2|2 Les mesures de lutte contre la captation des données de carte

Si la lutte contre les attaques d'ingénierie sociale repose en grande partie sur la sensibilisation préalable des victimes potentielles, les systèmes d'information doivent répondre à des standards de sécurité qui permettent de limiter les risques identifiés.

2|2|1 Contre les attaques sur les systèmes d'information

Les systèmes d'information doivent, d'une manière générale, être protégés contre les menaces internes ou externes et faire l'objet, à ce titre, d'analyses de sécurité visant à mettre en place des mesures de protection adaptées au contexte dans lequel ils évoluent.

Les systèmes d'information utilisés afin de réaliser des opérations de paiement par carte entrent dans ce cadre. Leurs gestionnaires doivent ainsi définir une politique de sécurité et réévaluer régulièrement les risques auxquels ils sont exposés. Différentes méthodes leur sont proposées. On citera par exemple Ebios (élaborée et maintenue à jour par l'Agence nationale de la sécurité des systèmes d'information – ANSSI) ou la série de normes ISO 27000.

Au regard du caractère particulièrement sensible des données transitant ou étant stockées sur ces systèmes, ceux-ci sont soumis à des mesures additionnelles établies par la profession, dites PCI [13] développées par le consortium « PCI SSC » [14]. Ces mesures additionnelles s'appliquent mondialement à l'ensemble des acteurs de la filière d'acceptation et d'acquisition (banques acquéreurs, commerçants, prestataires de service exploitant des plates-formes de paiement, etc.). Plusieurs séries de mesures de sécurité édictées par « PCI DSS » (*PCI Data Security Standard*) visent ainsi à protéger les données, qu'elles soient transmises à travers les systèmes d'information de la chaîne d'acquisition du paiement par carte, ou stockées dans ces systèmes. Plus récemment, PCI SSC a publié un guide de mise en œuvre de ces

12 Ces logiciels génèrent, par itérations successives, des numéros de carte, des dates d'expiration et parfois des cryptogrammes visuels.
13 Pour plus de développements sur les mesures PCI, se reporter au rapport 2010 de l'Observatoire.
14 Le *Payment Card Industry Security Standard Council* a été créé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. International.

mesures dans le cadre de l'informatique en nuage (*cloud computing* [15]), afin notamment d'identifier les responsabilités de chacun des acteurs dans cette architecture.

Par ailleurs, en matière d'attaque contre les bases de données, un projet de directive européenne concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et d'information dans l'Union [16] est actuellement en discussion. Il pourrait imposer aux banques, mais également aux e-commerçants, de mettre en place des systèmes de protection de leurs données adaptés aux risques évalués et de déclarer aux autorités les violations de leurs bases de données contenant des informations sur la clientèle et notamment des informations sur les moyens de paiement.

2|2|2 Contre les attaques sur Internet

Si le déploiement progressif de l'authentification non rejouable lors des achats sur Internet limite les risques de réutilisation des données de carte captées à l'insu du porteur, la sensibilisation des utilisateurs aux questions de sécurité reste seule de nature à lutter contre les attaques d'ingénierie sociale. Une communication efficace, utilisant l'ensemble des canaux disponibles : courriers, courriels, sites Internet, etc., à l'initiative de l'ensemble des acteurs de la chaîne de paiement doit donc être instaurée. Les porteurs doivent en outre être incités à n'utiliser que des sites de confiance, dont le niveau de sécurité apparaît conforme aux termes de référence cités dans ces communications.

Enfin, la sécurité des données au moment de leur enregistrement dans les systèmes doit faire partie intégrante de la politique de sécurité décrite *supra*. Celle-ci doit en effet prévoir une traçabilité de l'ensemble des accès au système d'information ayant pour objet la saisie ou la modification de données nécessaires à la réalisation de la transaction, afin de constituer une piste d'audit fiable.

2|2|3 Contre la captation des données de carte par courriel ou par téléphone

Les compromissions généralement constatées dans ce contexte relèvent de malversations initiées par du personnel indélicat. Des dispositifs d'acceptation limitant l'interaction entre les commerçants et les moyens de paiement doivent donc être privilégiés. Il est en outre important de limiter l'accès aux données de carte au seul personnel réellement habilité et de ne pas conserver de données sensibles dès lors que celles-ci ne sont plus utiles.

2|2|4 Contre les attaques sur les systèmes d'acceptation ou les réseaux

La protection de la filière d'acceptation passe par une sécurisation de l'ensemble de ses composants ainsi que des dispositifs les reliant entre eux.

Les mesures de lutte contre les attaques physiques sur le matériel d'acceptation

Les gestionnaires d'automates de paiement et de retrait disposent de moyens techniques destinés à limiter le risque de *skimming*. Les *anti-skimmers* consistent en des extensions apposées sur les automates empêchant l'ajout de matériel par les fraudeurs.

Pour les banques, il s'agit de protéger leurs propres matériels contre la mise en place de dispositifs permettant de copier les données des cartes. Quant aux porteurs, ils doivent demeurer vigilants à toute modification ayant pu intervenir sur l'automate.

Par ailleurs, l'Observatoire recommande aux établissements gestionnaires de ces automates de sensibiliser leur personnel aux risques pesant sur les appareils afin de leur permettre de détecter toute modification dans les plus brefs délais et de préserver les éléments de nature à faciliter une enquête des forces de l'ordre.

15 Consiste en la mise à disposition de ressources informatiques partagées, accessibles *via* un réseau de télécommunications.
16 Projet de directive 2013/C0027 (COD) – Procédure législative ordinaire – en attente de la première lecture du Parlement.

De façon similaire, les mesures permettant aux établissements acquéreurs de se prémunir contre le risque de *skimming* sur les terminaux de paiement sont de deux ordres :

• la sensibilisation des commerçants à la nécessité de rester à tout moment vigilants quant au comportement suspect de leur personnel ou de leur clientèle à l'égard de ces matériels est essentielle ;

• les systèmes de paiement par carte et les établissements acquéreurs devraient, quant à eux, être en mesure de détecter, lors de la transaction, toute tentative d'intrusion sur les réseaux d'autorisation par des dispositifs illégitimes. À cette fin, l'Observatoire recommande aux acteurs concernés d'assurer une traçabilité rigoureuse du matériel d'acceptation déployé en point de vente, en exploitant les informations transmises par ce matériel.

Les mesures de lutte contre l'injection de code malveillant

L'Observatoire recommandait en 2008 de durcir la sécurité des systèmes d'exploitation des automates, notamment en désactivant ou en supprimant les composants logiciels et les fonctionnalités inutilisés, et en mettant en place des restrictions d'accès à certaines données.

Compte tenu des risques relevés, ces recommandations peuvent désormais être étendues aux terminaux de paiement dont les évolutions devraient désormais être développées dans le respect de techniques à l'état de l'art. Ceci implique également la réalisation de tests réguliers incluant le système d'exploitation et les applications embarquées de ces matériels, afin d'évaluer de façon continue le niveau de sécurité de l'ensemble et sa capacité de résistance à des attaques [17].

L'Observatoire recommande enfin aux acteurs concernés de prendre en compte ces techniques de développement dans les processus de certification et d'agrément de ces matériels.

Les mesures de protection des réseaux

Les liaisons entre le matériel d'acceptation et les serveurs acquéreurs reposent sur l'utilisation de réseaux ouverts. Elles sont sécurisées par les acteurs de la chaîne de paiement à travers la mise en œuvre des mesures préconisées par les systèmes de paiement par carte, soit directement, soit par l'intermédiaire de PCI SSC [18].

Les mesures PCI DSS exigent notamment le chiffrement des données de paiement par carte transmis sur des réseaux ouverts afin d'en assurer la protection. En France, le Groupement des Cartes Bancaires « CB » impose en outre le chiffrement des données de transaction, même lorsque ces données transitent sur des réseaux privés virtuels. Il exige enfin l'utilisation d'un protocole de sécurisation TLS [19] ou équivalent, qui inclut l'authentification des concentrateurs monétiques et serveurs d'acquisition à l'aide de certificats.

Lorsque les automates et terminaux communiquent grâce à des technologies sans fil, il est également recommandé d'utiliser des mesures de chiffrement et d'authentification entre ces derniers et les bornes sans fil reliées aux réseaux filaires, comme les techniques Wifi et GPRS le permettent.

2|2|5 Contre les attaques sur les cartes de paiement

La fraude de type *man in the middle*, décrite en 2|1|5, ne peut être mise en œuvre que lors de transactions de proximité au cours desquelles le code PIN du porteur est vérifié localement.

Une première mesure serait donc de rendre systématique l'autorisation en ligne des transactions, ce qui suppose toutefois d'assurer un dimensionnement adéquat du réseau et d'accepter un allongement des temps de transaction.

Ces contraintes ont conduit le Groupement des Cartes Bancaires « CB » à s'orienter vers une seconde

17 Une des méthodes pouvant être employée est le test aléatoire (*fuzzing*), qui consiste à injecter des données aléatoires en entrée d'un programme et à en évaluer les conséquences.
18 Ces mesures sont détaillées dans le rapport 2008 de l'Observatoire.
19 « *Transport Layer Security* » a succédé à « *Secure Socket Layer* » version 3 (SSL V3). Il s'agit d'un protocole de sécurisation assurant l'intégrité et la confidentialité des données échangées ainsi que l'authentification des appareils communicants.

solution visant à anticiper la transition programmée vers un nouveau mode d'authentification de la carte lors de ses échanges avec le terminal, le CDA [20]. L'Observatoire recommande aux acteurs concernés de poursuivre la migration des cartes et terminaux vers ce nouveau mode d'authentification dans des délais compatibles avec le risque sous-jacent.

S'agissant des mesures de protection des transactions réalisées en mode sans contact, l'Observatoire réitère (cf. chapitre 3 : *Point sur la sécurité du paiement par cartes sans contact*) les mesures préconisées en 2007 et 2009, lesquelles doivent désormais s'apprécier au niveau international. Il encourage ainsi les émetteurs à mettre des étuis de protection à la disposition des porteurs ou à déployer la désactivation à distance de la fonction sans contact des supports. Il réaffirme l'intérêt de mettre en place un PAN dédié aux paiements sans contact afin de rendre vaine toute tentative de capture de cette donnée à des fins de réutilisation sur d'autres canaux. Enfin, l'Observatoire prône une étude coûts/bénéfices d'une évolution du protocole de communication sans contact, afin de permettre un chiffrement par défaut des données transitant par ce canal.

2|3 Les mesures de lutte contre la réutilisation des données usurpées

Quel que soit le canal de compromission des données de carte, celles-ci sont en grande majorité réutilisées dans des environnements de vente à distance (cf. chapitre 2 : *Statistiques de fraude pour l'année 2012*). En effet, les paiements sur Internet apparaissent moins sécurisés à ce jour que les paiements de proximité pour lesquels les mesures de sécurité montrent leur efficacité.

2|3|1 En environnement de vente à distance

Afin de lutter contre la progression constante de la fraude sur les paiements à distance, l'Observatoire a recommandé, dès 2008, deux types de mesures :

• tout d'abord, l'utilisation systématique du cryptogramme visuel (CVx2), donnée inscrite sur la carte mais non transmise lors des échanges entre la carte et le terminal de paiement, permet de s'assurer que les données de carte n'ont pas été compromises par un dispositif de *skimming*, tel que décrit en 2|1|4. Cette mesure est également préconisée par les systèmes de paiement par carte, qui mènent actuellement des actions afin de la généraliser au niveau international ;

• de plus, l'Observatoire recommande aux acteurs de la chaîne de paiement (émetteurs, acquéreurs et commerçants) de mettre en œuvre l'authentification renforcée du porteur de la carte pour les transactions considérées comme risquées. Il convient à présent que l'analyse des transactions susceptibles de déclencher une authentification non rejouable soit généralisée auprès des e-commerçants, dans le cadre d'une démarche désormais européenne sous l'impulsion du forum *SecuRe Pay*.

2|3|2 En environnement de proximité

L'utilisation de la norme EMV, développée par le consortium EMVCo [21], permet aujourd'hui de garantir un haut niveau de sécurité pour les transactions par carte dans un environnement de proximité.

L'Observatoire a recommandé dès 2003 une généralisation de la norme EMV pour les transactions de proximité. L'état d'avancement de la migration vers cette norme en Europe, aujourd'hui quasiment achevée, a fait l'objet d'un suivi régulier qui a donné lieu à une publication dans chacun de ses rapports annuels.

À plus long terme et au regard de la généralisation de l'utilisation de la puce au niveau international, l'Observatoire recommande aux émetteurs de supprimer des pistes magnétiques les données sensibles permettant de réaliser des paiements de proximité.

Par ailleurs, afin de lutter contre les malversations initiées par du personnel indélicat, les dispositifs d'acceptation limitant l'interaction entre les commerçants et les moyens de paiement lors des transactions de proximité doivent être privilégiés, afin de permettre aux porteurs de garder à tout

20 « *Combined Data Authentication* » : cette méthode d'authentification existant dans le standard EMV utilise la clé d'authentification de la carte pour signer les données de transactions qu'elle réalise.

21 EMVCo regroupe American Express, JCB Cards, MasterCard et Visa.

moment le contrôle de leurs moyens de paiement. Il est également important que les commerçants restent à tout moment vigilants quant aux modalités d'utilisation des terminaux de paiement par leur clientèle.

Enfin, outre les dispositifs de sécurité portant sur la carte, les acquéreurs disposent d'autres moyens techniques permettant de limiter la réutilisation de numéros de cartes compromis en proximité, tel le téléchargement de listes de numéros de cartes en opposition dans les terminaux.

2|4 Conclusion et conseils aux acteurs concernés

Malgré un niveau de sécurité élevé, les données de carte font l'objet d'attaques lors de leur passage dans la chaîne de paiement. Les points de compromission potentiels se situent dans les mondes physique et virtuel, ce qui nécessite une vigilance constante de l'ensemble des acteurs sur tous les environnements.

Sont ainsi désormais visés en priorité les systèmes d'information et les réseaux en raison du volume de données stockées ou transitant par ces infrastructures, pour lesquelles des mesures de protection adéquates, telle PCI DSS, doivent être mises en œuvre. Mais des techniques plus classiques visant les automates restent d'actualité. Ainsi, la protection des automates et terminaux de paiement doit demeurer une priorité des fabricants et développeurs dès la phase de conception, durant laquelle il est important de suivre des méthodes à l'état de l'art. L'Observatoire recommande ainsi aux organismes de certification ou délivrant des agréments d'inclure ces requis dans leurs propres procédures.

L'Observatoire renouvelle en outre ses conseils de prudence aux porteurs et recommande aux commerçants d'exercer la plus grande vigilance à l'égard du risque de substitution du matériel utilisé en proximité. L'Observatoire recommande par ailleurs aux acteurs de la filière d'acquisition de tracer rigoureusement le matériel déployé en proximité afin de prévenir toute tentative de manipulation ou de substitution. Le même niveau de traçabilité s'applique aux données saisies dans le cadre de transactions à distance.

Les membres de l'Observatoire (notamment les établissements bancaires, les systèmes de paiement par carte, les associations de commerçants et de consommateurs ou encore les organismes publics tel l'ANSSI) ont déposé sur leur(s) site(s) Internet [22] des documents reprenant certaines de ces bonnes pratiques.

L'Observatoire renouvelle enfin ses précédentes recommandations visant à limiter la réutilisation de données compromises dans le cadre de transactions à distance. La généralisation de l'usage du cryptogramme visuel et de l'authentification renforcée du porteur (pour les transactions les plus risquées dans ce dernier cas) doit ainsi toujours faire l'objet d'efforts soutenus de la part de l'ensemble des acteurs de la chaîne de paiement au regard du taux de fraude constaté sur ce canal [23].

Les techniques de fraude étant en constante évolution, l'Observatoire restera attentif d'une part au développement rapide de nouveaux modes de paiement utilisant la carte comme le portefeuille électronique et le mobile, d'autre part au déploiement de mesures de sécurité adaptées par l'ensemble des acteurs, dans le cadre de travaux qui s'inscrivent désormais dans un contexte européen et international.

22 Cf. tableau 2 à la fin de cette partie.
23 Cf. chapitre 2 de ce rapport : *Statistiques de fraude pour l'année 2012*.

Tableau 1

Mesures de sécurité recommandées par l'Observatoire dans ses précédents rapports

Type de risque	Mesures préconisées	Références
Contrefaçon	Insertion d'un hologramme	Rapport 2003
	Utilisation de procédés cryptographiques pour l'identification des composants	Rapport 2003
	Certification des composants (carte, terminal)	Rapports 2005, 2007, 2009
Vol de la carte	Généralisation de la norme EMV	Rapports 2003, 2005, 2007
	Authentification du porteur par code PIN	Rapports 2007, 2009
	Application de seuils pour les transactions sans contact ou en mode prépayé	Rapports 2007, 2009
	Utilisation de systèmes de détection de la fraude	Rapports 2003, 2009
Compromission des données de carte	Lutte contre le *phishing*, campagnes de communication	Rapports 2004, 2006
	Protection des données de bout en bout (chiffrement), utilisation de réseaux privés	Rapports 2003, 2004, 2005, 2006, 2008, 2009
	Utilisation du CVx2 pour les transactions à distance	Rapports 2004, 2008, 2009
	Utilisation de cartes virtuelles dynamiques	Rapports 2005, 2008
	Protection des données sensibles par l'application de normes internationales	Rapports 2005, 2006, 2007, 2008, 2009
	Renforcement de la sécurité physique des automates et dispositifs d'émission immédiate	Rapports 2006, 2008
	Limitation de l'utilisation des lecteurs de piste dans les automates	Rapport 2006
	Utilisation de PAN dédiés à certains modes d'utilisation (sans contact, mobile)	Rapport 2007
	Fonction de désactivation des transmissions radio en mode sans contact	Rapports 2007, 2009
	Utilisation d'étuis imperméables aux ondes radio	Rapports 2007, 2009
Usurpation d'identité sur Internet	Authentification renforcée du porteur (dite également « authentification non rejouable »)	Rapport 2008

Tableau 2

Exemples de bonnes pratiques - liens vers des sites Internet d'organismes représentés au sein de l'Observatoire

GIE Cartes Bancaires	*http://www.cartes-bancaires.com/spip.php?article73* *http://www.cartes-bancaires.com/spip.php?article72*
CRCAM de Paris et d'Île-de-France	*https://www.ca-paris.fr/site-securite.html*
LCL	*https://informations.lcl.fr/securite/*
BPCE	*http://www.banquepopulaire.fr/Institutionnel/a-savoir/securite-internet/Pages/securite-internet.aspx* *https://www.caisse-epargne.fr/particuliers/ile-de-france/securite_accueil.aspx*
Association Leo Lagrange pour la défense des consommateurs	*http://www.leolagrange-conso.org/03_ress_01.php?idrub=OU&rub=3*
FEVAD	*http://www.fevad.com/espace-consommateurs*
ANSSI	*http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/*
Banque de France	*http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/La_Banque_de_France/pdf/La_Banque_de_France/BDF-IDENTITES_BANCAIRES-PDFELEC_VF_1_.pdf*
Fédération bancaire française	*http://www.lesclesdelabanque.com*

Les évolutions réglementaires et recommandations en Europe et à l'international sur la sécurité des cartes de paiement

La carte est l'instrument de paiement le plus utilisé en France et en Europe en termes de nombre de transactions ; elle a vu ses usages évoluer au gré des innovations technologiques (paiement par carte sans contact, sur Internet, etc.). L'enjeu pour les acteurs en charge de sa régulation et de sa surveillance réside donc dans une adaptation permanente des dispositifs de surveillance, de façon à assurer le maintien d'un haut niveau de sécurité pour cet instrument tout en favorisant le développement de ses usages.

L'Observatoire a souhaité, dans ce cadre, réaliser un état des lieux de la réglementation et des recommandations des autorités applicables en matière de sécurité, dans un contexte tant européen qu'international. Seront donc abordés ci-après les principaux facteurs ayant contribué à faire évoluer le cadre opérationnel et le cadre juridique des paiements par carte au cours des dernières années, puis les initiatives réglementaires réalisées ou attendues au regard de ces évolutions. Les considérations ayant un caractère économique ou concurrentiel ne seront pas traitées dans le présent chapitre, conformément au périmètre des missions confiées à l'Observatoire.

1| Le moyen de paiement par carte évolue vers de nouveaux usages

La carte de paiement, conçue à l'origine pour être utilisée dans un environnement de proximité, s'est imposée dans de nombreux pays comme le moyen de paiement privilégié pour réaliser également des transactions à distance. Or, le développement du commerce par Internet ainsi que le recours aux nouvelles technologies ont modifié sensiblement la manière d'utiliser la carte comme moyen de paiement ainsi que ses méthodes d'acceptation.

1|1 Internet et les nouvelles technologies sont des facteurs d'évolution du paiement par carte

1|1|1 La sécurité des transactions sur Internet

La démocratisation du paiement par carte sur Internet s'est accompagnée d'une augmentation régulière de la fraude sur ce canal, comme le montrent les statistiques publiées par l'Observatoire depuis plusieurs années. Ceci a conduit les systèmes de paiement par carte internationaux à développer le protocole « 3D-Secure », lequel permet aux émetteurs d'authentifier de manière renforcée le porteur sur Internet. Afin d'inciter les commerçants et leurs banques acquéreurs à adopter ce dispositif, sa mise en œuvre s'accompagne d'un transfert de responsabilité en cas de fraude, de l'acquéreur des transactions vers l'émetteur de la carte utilisée.

En l'absence de systématisation de ce type de dispositif de sécurité, la fraude sur Internet demeure à un niveau élevé, représentant 57,6 % de la fraude pour seulement 9,8 % de l'ensemble des paiements par carte en France [1], ce qui justifie la poursuite des actions menées par les acteurs de la chaîne de paiement visant à augmenter, de façon continue, le niveau de sécurité de ces transactions.

1 Cf. le chapitre 2 du présent rapport.

1|1|2 Les paiements de proximité intègrent désormais la fonctionnalité sans contact

Les transactions réalisées dans un environnement de proximité ont également fortement évolué, puisqu'il est désormais possible d'initier des paiements sans contact, à l'aide d'une carte ou d'un téléphone mobile. Ces instruments utilisent à cette fin la technologie NFC [2] comme solution de communication à distance avec le terminal de paiement.

L'Observatoire considère que le principal risque lié aux paiements sans contact par carte est un risque d'image. Ceux-ci génèrent toutefois de nouveaux risques nécessitant la mise en œuvre de mesures de sécurité spécifiques, telles que décrites par l'Observatoire dans le cadre du présent rapport (cf. chapitre 3). Ces mesures s'ajoutent à celles visant à sécuriser les transactions de proximité afin de ne pas dégrader le niveau élevé de sécurité atteint à ce jour sur ce canal.

En ce qui concerne les paiements de proximité traditionnels, il est important que les acteurs concernés poursuivent le déploiement des spécifications EMV au plan international. L'Observatoire a en outre renouvelé dans le cadre du présent rapport [3] ses conseils de vigilance à l'égard des porteurs et des commerçants, de façon à prévenir toute tentative de modification ou substitution du matériel d'acceptation à des fins frauduleuses.

1|1|3 L'émergence des paiements mobiles

De nombreuses initiatives et innovations voient le jour autour du paiement par mobile (aussi appelé « *m-payment* »). Les applications pour le mobile permettent ainsi de développer des services de portefeuille électronique (*e-wallet*) afin de régler ses achats sur Internet, ou encore d'utiliser ce dernier pour payer dans les commerces de proximité en initiant un paiement par carte à distance.

Du point de vue des terminaux de paiement, l'une des principales innovations réside dans la transformation du téléphone mobile en terminal de paiement électronique. Le succès commercial de ces solutions, développées à l'origine pour le marché nord-américain qui repose sur l'utilisation de la carte à piste magnétique, suscite de nombreuses vocations en Europe. Il convient à ce titre d'être vigilant et de s'assurer en conséquence que ces solutions soient adaptées afin d'être compatibles avec le maintien de l'utilisation de la carte à puce et de la technologie EMV.

1|1|4 Le développement des cartes prépayées

L'usage de la carte de paiement dans son format initial a poursuivi sa croissance avec l'arrivée sur le marché des cartes prépayées, lesquelles permettent de réaliser des paiements par carte sans détenir un compte bancaire, participant ainsi notamment à l'inclusion financière. Lorsque ces cartes sont anonymes, elles soulèvent toutefois des risques d'utilisation à des fins de blanchiment d'argent ou de financement du terrorisme, ce qui a conduit le président de l'Observatoire à alerter les autorités publiques sur les risques attachés à ces cartes.

L'identification de transactions réalisées au moyen de cartes prépayées anonymes et la limitation de leur usage, sur un plan national, européen voire international, devraient être envisagées dans une perspective d'atténuation de ces risques.

1|2 Un cadre juridique désormais européen qui a introduit de nouveaux acteurs non bancaires

Le législateur européen a entrepris dès 2001 d'harmoniser le cadre réglementaire du droit des paiements afin de faciliter la mise en place du marché européen unique des paiements et d'accroître la concurrence.

Ainsi, la directive sur les services de paiement (ci-après DSP), adoptée en 2007 et transposée en France en 2009 notamment par l'ordonnance n° 2009-866 du 15 juillet 2009, régit l'ensemble des relations entre les prestataires de services de paiement et leur clientèle dans le cadre de transactions de paiement utilisant le virement, le prélèvement ou la carte de paiement.

2 *Near Field Communication*. Pour de plus amples développements sur les paiements sans contact, se reporter au chapitre 3 du présent rapport, paragraphe 1|2.
3 Cf. chapitre 3, 2|2|4.

Elle définit notamment le contenu des contrats cadres, les modalités d'exécution et de contestation des transactions, ainsi que le rôle et les responsabilités de chacun des acteurs dans ces processus. Les paiements par carte sont concernés par la DSP au titre de deux services de paiement que sont les « opérations de paiement effectuées avec une carte de paiement ou dispositif similaire » et l'« émission d'instruments de paiement et acquisition d'ordres de paiement ».

La directive européenne 2009/110/CE sur la monnaie électronique (« DME2 ») vient, quant à elle, parachever l'encadrement réglementaire des services de paiement. Cette directive a été transposée en France par la loi n° 2013-100 du 28 janvier 2013 et définit le cadre réglementaire de l'émission, la gestion et la distribution de la monnaie électronique dans la Communauté européenne, lequel n'avait pas été réformé depuis 2000. En France, la législation a de surcroît prévu [4] que l'ensemble des dispositions liées aux services de paiement s'appliquent aux émetteurs de monnaie électronique et aux services de paiement associés. C'est le cas, en particulier, des obligations d'information à l'attention des utilisateurs et des modalités de contestation d'une opération de paiement, clauses essentielles du contrat cadre de service de paiement qui ont été précisées dans l'arrêté du 29 juillet 2009 relatif aux relations entre les prestataires de services de paiement et leurs clients.

Les paiements par carte sont concernés par la DME2 dans la mesure où la carte – quand il s'agit de cartes prépayées – peut être un support pour réaliser des opérations de paiement en monnaie électronique. Dans ce contexte, la carte prépayée doit être soumise aux mêmes règles sécuritaires qu'une carte de paiement classique (émise par un établissement de paiement ou un établissement de crédit), comme souligné dans le rapport 2010 de l'Observatoire.

Ces deux directives ont, de surcroît, créé deux nouveaux statuts d'acteurs non bancaires pouvant offrir des moyens de paiement : les établissements de paiement et les établissements de monnaie électronique. En mai 2013, seize établissements de paiement et trois établissements de monnaie électronique étaient agréés en France.

2| Les nécessaires adaptations en réponse aux évolutions sécuritaires des paiements par carte

En France, le législateur a confié à la Banque de France la surveillance de la sécurité et du bon fonctionnement des systèmes et des moyens de paiement. Au titre de ses missions, la Banque de France agit auprès des acteurs du paiement par carte afin de sécuriser l'ensemble de la chaîne allant de l'émission à l'acceptation et au traitement des flux de carte (pour une revue détaillée des actions menées par la Banque de France, voir son rapport de surveillance 2012).

L'Observatoire de la sécurité des cartes de paiement, réunissant les acteurs publics, ceux du paiement par carte ainsi que des représentants d'associations de consommateurs, complète ce dispositif.

Face aux évolutions des usages de la carte de paiement présentées dans le précédent chapitre, l'ensemble des autorités (nationales ou européennes) adaptent les requis sécuritaires ainsi que le cadre réglementaire applicables afin de maintenir un niveau élevé de sécurité des paiements par carte. Il est à noter que ce sujet est désormais également suivi au niveau international, comme le montrent les récents travaux du comité sur les systèmes de paiement et de règlement (*Committee on Payment and Settlement Systems* – CPSS) de la Banque des règlements internationaux.

2|1 Les préconisations sécuritaires de l'OSCP et du forum *SecuRe Pay*

2|1|1 La sécurité des transactions sur Internet

La croissance continue de la fraude sur les paiements par carte lors des achats sur Internet a notamment conduit la Banque de France et l'Observatoire de la sécurité des cartes de paiement à recommander le déploiement de l'authentification renforcée des paiements par carte à distance à chaque fois que cela est possible et pertinent (cf. chapitre 1 du présent rapport).

4 Art. L. 315-5 du *Code monétaire et financier*.

Par ailleurs, sous l'impulsion de la BCE, le forum *SecuRe Pay* (*European Forum on the Security of Retail Payments*), créé en 2011, qui regroupe les banques centrales et les autorités de supervision bancaire des pays membres de l'Union européenne, a également publié en janvier 2013 un rapport consacré à la protection des services bancaires en ligne et à la sécurité des paiements par carte sur Internet.

Il a, à cette occasion, formalisé plusieurs recommandations adressées aux banques et prestataires de services de paiement et préconisé un recours à l'authentification renforcée pour les transactions de paiement les plus risquées.

2|1|2 La sécurité des paiements sans contact et par mobile

En France, l'Observatoire de la sécurité des cartes de paiement s'est très tôt intéressé à la sécurité des paiements par cartes sans contact, y compris par mobile (cf. les études publiées dans les rapports 2007, 2009 et le présent rapport). À cette occasion, il a émis un certain nombre de recommandations afin d'en assurer le développement de manière maîtrisée.

Dans le cadre de son programme 2013, le forum *SecuRe Pay* a également orienté ses travaux sur les problématiques des paiements par carte par mobile. Les recommandations y afférentes devraient être mises en consultation publique au cours du dernier trimestre 2013.

2|2 L'évolution du cadre européen de surveillance

2|2|1 Le cadre de surveillance des paiements par carte de l'Eurosystème

Les textes fondateurs de l'Eurosystème ont placé la surveillance des systèmes de paiement au cœur de ses missions essentielles [5] afin d'assurer la confiance des utilisateurs dans les instruments de paiement.

Dans ce contexte, l'Eurosystème a soutenu la décision prise par les principaux systèmes de paiement par carte européens de remplacer progressivement le parc de cartes basées sur la piste par des cartes à puce avec saisie d'un code PIN. Cette migration aux standards EMV, accompagnée d'une mise à jour du parc de terminaux d'acceptation, a fortement contribué à renforcer la sécurité des paiements par carte en proximité et à lutter contre la fraude.

En 2008 [6], un cadre de surveillance a été élaboré par l'Eurosystème afin d'évaluer la sécurité et l'efficacité des systèmes de paiement par carte. Le cadre européen a permis aux banques centrales de l'Eurosystème de mettre en œuvre une surveillance harmonisée et d'obtenir une vision cohérente et standardisée des systèmes de paiement par carte. Parmi les cinq standards, l'un d'entre eux est consacré à la sécurité, la fiabilité et la continuité des systèmes de paiement.

Ce cadre de surveillance sera prochainement adapté afin de prendre en compte les évolutions sécuritaires mentionnées précédemment, notamment les recommandations récentes émises par le forum *SecuRe Pay*.

2|2|2 Vers un nouveau cadre réglementaire européen des paiements par carte

La Commission européenne est soucieuse d'accompagner les évolutions dans le paiement en favorisant le développement de nouveaux services innovants et sûrs, rappelant que la sécurité des paiements et la confiance des utilisateurs font partie des facteurs essentiels au développement des services de paiement. En outre, avec la mise en place du SEPA [7], l'espace unique de paiement en euros, l'Europe a souhaité réunir les conditions favorables au développement d'un véritable marché européen des paiements par carte.

La forte augmentation des paiements en ligne et le recours de plus en plus fréquent au téléphone

5 « *Role of Eurosystem in the field of payment systems oversight* », June 2000.
6 « *Oversight framework for card payment schemes – standards* », January 2008.
7 *Single Euro Payment Area*, dont l'ambition est de créer une gamme unique de moyens de paiement en euros (virements, prélèvements et cartes) commune à l'ensemble des pays européens.

mobile ont conduit la Commission à lancer une consultation publique en janvier 2012 portant sur le « marché intégré des paiements par carte, par Internet et par téléphone mobile ». La synthèse des réponses a été rendue publique [8] en juin 2012 et témoigne d'une grande hétérogénéité des réponses et des attentes selon le type d'acteur concerné.

La Commission devrait, à la suite de cette consultation, annoncer de nouvelles mesures dans le cadre de la révision de la directive sur les services de paiement, prévue en juillet 2013.

Dans sa réponse à la consultation de la Commission européenne sur l'évolution de la DSP, la France avait souligné que « *la sécurité des transactions conditionne la confiance dans les moyens de paiement mis à leur disposition. [….] Un cadre harmonisé européen garantissant un haut niveau de sécurité est de ce point de vue crucial* ».

Au-delà des aspects sécuritaires, une évolution des modalités d'encadrement des acteurs actuellement non régulés, jouant un rôle d'intermédiaire entre l'utilisateur et le fournisseur de services de paiement, doit être également envisagée.

2|3 Le suivi des innovations dans les moyens de paiement au niveau international

Le CPSS de la Banque des règlements internationaux est dédié aux systèmes de paiement et de règlement, dont l'un des champs d'action concerne les systèmes de paiement de détail.

Le CPSS s'est ainsi récemment intéressé à l'innovation dans les moyens de paiement et notamment au positionnement des banques centrales dans ce cadre. Il a publié un rapport en mai 2012 à ce sujet [9]. Le rapport souligne l'importance qu'attachent les banques centrales à promouvoir l'utilisation de moyens de paiement efficients et sécurisés tout en favorisant l'innovation. Il dresse également un inventaire des freins et problématiques générales liés à l'innovation dans les paiements, comme le rôle de la standardisation, l'influence des usages dans les instruments de paiement pouvant varier d'un pays à l'autre ainsi que le rôle du régulateur.

En matière de sécurité, le rapport du CPSS souligne l'importance de maintenir la confiance des utilisateurs dans les services de paiement. La technologie doit être au service de l'efficience de l'instrument de paiement, améliorer la fluidité de l'acte de paiement sans pour autant introduire de brèche dans le processus, en particulier au niveau du consentement de l'opération de paiement. Dans cet esprit, le rapport reconnaît l'intérêt de la technologie EMV permettant l'authentification de la carte et du terminal.

Concernant les transactions à distance, des points d'attention sont identifiés concernant :

- les conditions de sécurité dans lesquelles sont conservées les données de la carte par le marchand et/ou son prestataire de services de paiement ;

- la mise en place de mécanismes d'authentification forte afin de lutter efficacement contre la fraude. Le CPSS constate, à cet égard, l'efficacité des mécanismes basés sur au moins deux facteurs d'authentification.

3| Conclusion

Le cadre réglementaire applicable aux paiements par carte a subi de profondes modifications depuis 2008, visant à construire un marché harmonisé des paiements scripturaux en Europe. Cette nécessaire évolution est à mettre en perspective avec le caractère innovant de ce moyen de paiement, lequel rend nécessaire une révision permanente du cadre réglementaire et de surveillance lui étant applicable afin d'en maîtriser les risques et de maintenir un niveau élevé de sécurité assurant la confiance des utilisateurs dans ce moyen de paiement.

Face aux importants changements des modes d'achat et de paiement, la Commission européenne a lancé, en 2012, une consultation sollicitant l'avis des parties intéressées sur les obstacles qui limitent l'intégration du marché et la manière dont ceux-ci

8 *http://ec.europa.eu/internal_market/payments/docs/cim/gp_feedback_statement_en.pdf*
9 *http://www.bis.org/publ/cpss102.htm*

pourraient être levés afin de disposer au niveau européen de moyens de paiement plus efficaces, plus modernes et plus sûrs. Cette réflexion devrait conduire à l'évolution prochaine du cadre juridique des paiements au niveau européen.

La composante sécuritaire apparaît dans ce cadre de première importance. Les régulateurs et surveillants, au niveau national ou agissant selon un mode collaboratif au plan européen se sont déjà emparés de ces problématiques au cours des dernières années, en publiant des recommandations et bonnes pratiques adressées à l'ensemble des acteurs de la chaîne de paiement. La mise en œuvre harmonisée de ces recommandations est au centre des préoccupations des autorités et des acteurs de marché, et pourrait de ce fait être prise en compte dans l'évolution du cadre juridique européen.

Au niveau international, des travaux sont conduits dans le cadre de la Banque des règlements internationaux. Un rapport du CPSS s'est également penché en 2012 sur le sujet des paiements innovants (y compris la carte) et de leur sécurité.

Annexes

Conseils de prudence à l'usage des porteurs

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

Soyez responsables

- Votre carte est strictement personnelle : ne la prêtez à personne, même pas à vos proches.
- Vérifiez régulièrement qu'elle est en votre possession.
- Si votre carte comporte un code confidentiel, gardez-le secret. Ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter et surtout ne le rangez jamais avec votre carte.
- Lorsque vous composez votre code confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal ou du distributeur de votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.

Soyez attentifs

Lors des paiements chez un commerçant

- Vérifiez l'utilisation qui est faite de votre carte par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider la transaction.

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

- Protégez votre numéro de carte : ne le stockez pas sur votre ordinateur, ne l'envoyez pas par simple courriel et vérifiez la sécurisation du site du commerçant (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 conditions générales de vente.
- 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.

Lors de vos déplacements à l'étranger

- Renseignez-vous sur les précautions à prendre et contactez l'établissement émetteur de votre carte avant votre départ, 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 votre carte.

A2

Sachez réagir

Vous avez perdu ou on vous a volé votre carte

• Faites immédiatement opposition en appelant le numéro que vous a communiqué l'établissement émetteur de la carte. Pensez à le faire pour toutes vos cartes perdues ou volées.
• 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 anomalies sur votre relevé de compte, alors que votre carte est 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 carte.

Sauf 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 carte 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 proche le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir), il faut déposer une réclamation auprès de l'établissement émetteur de la carte, dès que possible et dans un délai fixé par la loi, de 13 mois à compter de la date de débit de l'opération contestée. Dans ces conditions, votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être immédiatement remboursées sans frais. 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 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).

Protection du titulaire d'une carte en cas de paiement non autorisé

L'ordonnance de transposition de la directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 1er novembre 2009, a modifié les règles relatives à la responsabilité du titulaire d'une carte de paiement.

La charge de la preuve incombe au prestataire de services de paiement. Ainsi, lorsqu'un client nie avoir autorisé une opération, il incombe à son prestataire de services de paiement de prouver que l'opération 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 telle qu'enregistrée par le prestataire de services de paiement 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.

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 afin de déterminer l'étendue de la responsabilité du titulaire de la carte.

Opérations nationales ou intracommunautaires

Les opérations de paiement visées sont les opérations effectuées en euros ou en francs CFP sur le territoire de la République française [1]. Sont également concernées les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer, à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un autre État partie à l'accord sur l'EEE (Union européenne + Liechtenstein, Norvège et Islande), en euros ou dans la devise nationale de l'un de ces États.

Concernant les opérations non autorisées, c'est-à-dire en pratique les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, le titulaire de la carte devra contester, auprès de son prestataire dans un délai de 13 mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son prestataire devra alors rembourser immédiatement l'opération non autorisée au titulaire de la carte et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Une indemnisation complémentaire pourra aussi éventuellement être versée. Nonobstant l'extension du délai maximal de contestation à 13 mois, le porteur 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 prestataire de services de paiement.

Une dérogation à ces règles de remboursement est cependant prévue pour les opérations de paiement réalisées en utilisant un dispositif de sécurité personnalisé, par exemple la frappe d'un code secret.

1 L'ordonnance d'extension à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna des dispositions de l'ordonnance de transposition est entrée en vigueur le 8 juillet 2010.

Avant information aux fins de blocage de la carte

Avant « opposition » [2], le payeur pourra supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de la carte si l'opération est effectuée avec l'utilisation du dispositif personnalisé de sécurité. En revanche, si l'opération est effectuée sans l'utilisation du dispositif personnalisé de sécurité, le titulaire de la carte ne voit pas sa responsabilité engagée.

La responsabilité du titulaire de la carte 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 la carte si elle était en possession de son titulaire au moment où l'opération non autorisée a été réalisée.

En revanche, le titulaire de la carte 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 sa carte, convenues avec son prestataire de services de paiement.

Enfin, si le prestataire de services de paiement émetteur de la carte ne fournit pas de moyens appropriés permettant la mise en opposition de la carte, le client ne supporte aucune conséquence financière, sauf à avoir agi de manière frauduleuse.

Après information aux fins de blocage de la carte

Après mise en opposition de la carte, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de la carte ou de l'utilisation détournée des données qui lui sont liées.

Là encore, les agissements frauduleux du titulaire de la carte le privent de toute protection et il demeure responsable des pertes liées à l'utilisation de sa carte.

L'information aux fins de blocage peut être effectuée auprès du prestataire de services de paiement 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 le titulaire de la carte a informé son prestataire de services de paiement de la perte, du vol, du détournement ou de la contrefaçon de sa carte, ce dernier lui fournit sur demande et pendant 18 mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

Opérations extra-européennes

La directive sur les services de paiement n'est applicable qu'aux opérations intracommunautaires. Cependant la législation française existant avant l'adoption de cette directive protégeait les titulaires de cartes sans distinction de la localisation du bénéficiaire de l'opération non autorisée. Il a été décidé de maintenir une protection équivalente à celle à laquelle le client avait droit auparavant. À cette fin, les règles applicables aux opérations nationales ou intracommunautaires sont applicables avec des adaptations.

2 La loi utilise désormais le terme « information aux fins de blocage de l'instrument de paiement ».

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).

Missions et organisation de l'Observatoire

Les missions, la composition et les modalités de fonctionnement de l'Observatoire de la sécurité des cartes 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*.

Cartes concernées

L'ancien article L. 132-1 du *Code monétaire et financier,* dans sa rédaction antérieure au 1er novembre 2009 [1], définissait une carte de paiement comme toute carte émise par un établissement de crédit permettant à son titulaire de retirer ou de transférer des fonds. L'ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, ayant maintenu le périmètre de compétence de l'Observatoire, il a été décidé de continuer de s'appuyer sur cette définition en l'étendant aux prestataires de services de paiement qui sont, aux termes du I de l'article L. 521-1 du *Code monétaire et financier*, les établissements de crédit et les établissements de paiement.

En conséquence, les compétences de l'Observatoire concernent les cartes émises par les prestataires de services de paiement ou par les institutions assimilées [2] et dont les fonctions sont le retrait ou le transfert de fonds. Elles ne couvrent pas les cartes parfois appelées « cartes purement privatives » qui peuvent être émises par une entreprise sans avoir à obtenir un agrément délivré par l'Autorité de contrôle prudentiel. Il s'agit, d'une part, des cartes monoprestataires émises par une seule entreprise et acceptées en paiement d'un bien ou d'un service déterminé par elle-même ou par des accepteurs ayant noué avec elle un accord de franchise commerciale [3] et, d'autre part, des cartes multiprestataires, qui ne sont acceptées, pour l'acquisition de biens ou de services, que dans les locaux de l'émetteur de la carte ou, dans le cadre d'un accord commercial avec ce dernier, dans un réseau limité de personnes ou pour un éventail limité de biens ou de services [4].

Le marché français compte de nombreuses offres en matière de cartes de paiement qui relèvent des compétences de l'Observatoire. Parmi celles-ci, on distingue généralement les cartes dont le schéma d'acceptation des paiements et des retraits repose sur :

- un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs (cartes généralement qualifiées de « privatives ») ;

- un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs (cartes généralement qualifiées d'« interbancaires »).

1 Cet article a été supprimé par l'ordonnance de transposition de la directive européenne sur les services de paiement. En effet, il n'était pas compatible avec la directive qui fixe les règles applicables aux opérations de paiement en fonction de la cinématique du paiement, ceci afin d'assurer une neutralité technologique entre les différents instruments de paiement utilisés.

2 Les institutions assimilées sont, aux termes du II de l'article L. 521-1 du *Code monétaire et financier*, la Banque de France, l'Institut d'émission des départements d'outre-mer, le Trésor public et la Caisse des dépôts et consignations.

3 Ces cartes sont dispensées d'agrément par le 5° du I de l'article L. 511-7 et le II *in fine* de l'article L. 521-3 du *Code monétaire et financier*.

4 Ces cartes sont dispensées d'agrément par le II de l'article L. 511-7 et le I de l'article L. 521-3 du *Code monétaire et financier*.

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 1 du règlement CRBF n° 2002-13, « une unité de monnaie électronique constitue un titre de créance incorporé dans un instrument électronique et accepté comme moyen de paiement, au sens de l'article L. 311-3 du *Code monétaire et financier*, par des tiers autres que l'émetteur. La monnaie électronique est émise contre la remise de fonds. Elle ne peut être émise pour une valeur supérieure à celle des fonds reçus en contrepartie ».

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

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.

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 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 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.

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.

Liste nominative des membres de l'Observatoire

En application de l'article R. 142-22 du *Code monétaire et financier*, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel sont nommés pour trois ans par arrêté du ministre chargé de l'Économie et des Finances. Les derniers arrêtés de nomination datent des 29 octobre 2012 et 8 mars 2013.

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Philippe GOUJON
Député
Michèle ANDRÉ
Sénatrice

Représentant du secrétaire général de l'Autorité de contrôle prudentiel

Emmanuel CARRERE
Philippe RICHARD
Secrétariat général

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  Patrick PAILLOUX
  Pascal CHOUR
  Loïc DUFLOT

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

- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Claude MAUDELONDE

- Le directeur général du Trésor ou son représentant :
  Magali CESANA
  Fabrice WENGER

- Le directeur général de la Compétitivité, de l'Industrie et des Services ou son représentant :
  Mireille CAMPANA

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

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Charles MOYNOT
  Sixtine DU CREST
  Régis PIERRE

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 :
  Adeline CHAMPAGNAT
  Philippe DEVRED

Sur proposition du ministre de la Défense :

- Le directeur général de la gendarmerie nationale ou son représentant :
  Éric FREYSSINET

Représentants des émetteurs de cartes de paiement

Yves BLAVET (jusqu'au 7 mars 2013)
Directeur des Instruments de paiement
Société Générale
remplacé par **Jean-Marie DRAGON**
(arrêté du 8 mars 2013)
Directeur Marketing – Argent au quotidien
La Banque Postale
Jean-Marc BORNET
Administrateur
Groupement des Cartes Bancaires
Jean-François DUMAS
Vice-président
American Express France
Willy DUBOST
Directeur Systèmes et Moyens de paiement
Fédération bancaire française
Bernard GOURAUD
Directeur des technologies
Banque Populaire – Caisse d'Épargne
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
Emmanuel PETIT (jusqu'au 7 mars 2013)
remplacé par **Régis FOLBAUM**
(arrêté du 8 mars 2013)
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)
Valérie GERVAIS
Secrétaire général
Association FO Consommateurs (AFOC)
Patrick MERCIER
Président
Association de défense d'éducation et d'information du consommateur (ADEIC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)
Frédéric POLACSEK
Conseil national des associations familiales laïques (CNAFAL)

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

Eric 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)

Dossier statistique

Le dossier statistique qui suit a été réalisé à partir des données fournies à l'Observatoire de la sécurité des cartes de paiement par :

- les 130 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, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club et Franfinance ;
- les émetteurs du porte-monnaie électronique Moneo.

Total des cartes en circulation en 2012 : 85,8 millions
- dont 67,3 millions de cartes de type « interbancaire » (« CB », MasterCard et Moneo) ;
- et 18,4 millions de cartes de type « privatif ».

Cartes mises en opposition [1] en 2012 : environ 767 000

Les transactions nationales sont celles qui mettent en jeu un émetteur français et un commerçant accepteur français.

Jusqu'en 2009, les transactions internationales étaient de deux types :
- émetteur français/accepteur étranger et
- émetteur étranger/accepteur français.

À partir de 2010, l'Observatoire distinguant les transactions internationales avec la zone SEPA de celles avec le reste du monde, les transactions internationales sont donc désormais de quatre types :
- émetteur français/accepteur étranger hors SEPA ;
- émetteur étranger hors SEPA/accepteur français ;
- émetteur français/accepteur étranger SEPA ;
- émetteur étranger SEPA/accepteur français.

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

Tableau 1

Le marché des cartes de paiement en France en 2012 – 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	7 354,49	325,41	127,23	8,10	31,55	3,23
Paiements à distance hors Internet	100,78	8,56	20,15	1,22	3,11	0,34
Paiements à distance sur Internet	481,75	36,60	96,78	4,45	9,85	0,73
Retraits	1510,21	116,89	27,00	2,99	18,50	2,73
Total	**9 447,23**	**487,47**	**271,15**	**16,76**	**63,00**	**7,03**
Cartes de type « privatif »						
Paiements de proximité et sur automate	127,20	13,53	5,17	0,82	6,64	1,12
Paiements à distance hors Internet	2,13	0,15	nd	nd	nd	nd
Paiements à distance sur Internet	8,02	1,11	3,39	0,25	0,51	0,08
Retraits	3,68	0,33	nd	nd	nd	nd
Total	**141,04**	**15,12**	**8,56**	**1,07**	**7,15**	**1,20**
Total général	**9 588,27**	**502,59**	**279,72**	**17,83**	**70,15**	**8,23**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 2

Le marché des cartes de paiement en France en 2012 – Acquisition

(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	7 354,49	325,41	160,93	11,34	43,75	5,73
Paiements à distance hors Internet	100,78	8,56	6,79	1,74	3,00	1,19
Paiements à distance sur Internet	481,75	36,60	21,53	2,66	4,27	0,70
Retraits	1510,21	116,89	23,65	3,89	7,28	1,61
Total	**9 447,23**	**487,47**	**212,91**	**19,63**	**58,30**	**9,23**
Cartes de type « privatif »						
Paiements de proximité et sur automate	127,20	13,53	4,55	0,95	5,05	1,86
Paiements à distance hors Internet	2,13	0,15	nd	nd	nd	nd
Paiements à distance sur Internet	8,02	1,11	0,44	0,07	0,42	0,09
Retraits	3,68	0,33	nd	nd	nd	nd
Total	**141,04**	**15,12**	**4,99**	**1,03**	**5,47**	**1,95**
Total général	**9 588,27**	**502,59**	**217,90**	**20,66**	**63,77**	**11,18**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 3

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » en 2012 – 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	630,1	48 147,4	105,6	10 889,7	96,1	18 769,8
Cartes perdues ou volées	542,6	43 484,5	42,5	4 245,0	18,4	4 263,8
Cartes non parvenues	12,9	465,2	0,5	19,5	0,1	11,5
Cartes altérées ou contrefaites	64,4	3 686,2	14,5	2 108,3	56,0	10 758,1
Numéro de carte usurpé	5,3	455,6	46,2	4 200,0	19,6	3 300,5
Autres	4,9	55,9	2,0	317,0	1,9	435,9
Paiements à distance hors Internet	422,5	29 248,2	79,9	6 496,4	27,0	3 957,9
Cartes perdues ou volées	0,0	2,3	8,6	802,4	4,4	711,2
Cartes non parvenues	0,0	0,0	0,1	3,4	0,1	2,8
Cartes altérées ou contrefaites	0,2	7,5	13,9	1 215,1	5,2	796,1
Numéro de carte usurpé	422,3	29 237,8	56,8	4 418,9	16,9	2 412,4
Autres	0,0	0,5	0,4	56,7	0,5	35,4
Paiements à distance sur Internet	824,1	107 368,2	498,7	36 139,8	113,2	13 459,3
Cartes perdues ou volées	1,2	156,5	60,8	4 511,1	13,4	1 785,0
Cartes non parvenues	0,0	0,0	0,3	13,5	0,0	2,2
Cartes altérées ou contrefaites	0,3	48,3	93,3	7 390,5	28,1	3 287,3
Numéro de carte usurpé	822,6	107 146,3	342,6	24 054,0	71,0	8 312,3
Autres	0,1	17,2	1,7	170,7	0,7	72,5
Retraits	132,0	36 223,3	5,5	1 083,1	148,8	24 651,4
Cartes perdues ou volées	122,8	34 500,8	3,8	806,5	5,9	1 003,1
Cartes non parvenues	0,6	143,2	0,0	0,3	0,0	3,4
Cartes altérées ou contrefaites	8,6	1 577,3	1,4	220,2	135,5	22 464,7
Numéro de carte usurpé	0,0	2,0	0,1	9,7	1,3	214,1
Autres	0,0	0,0	0,2	46,3	6,1	966,2
Total	**2 008,7**	**220 987,2**	**689,7**	**54 609,0**	**385,1**	**60 838,5**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 4

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » en 2012 – Acquisition

(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	630,1	48 147,4	138,3	24 435,7	321,4	72 298,2
Cartes perdues ou volées	542,6	43 484,5	33,6	2 058,1	39,3	10 757,1
Cartes non parvenues	12,9	465,2	2,3	449,5	0,5	135,2
Cartes altérées ou contrefaites	64,4	3 686,2	12,6	2 166,3	95,6	22 700,3
Numéro de carte usurpé	5,3	455,6	87,5	19 187,9	184,0	38 164,7
Autres	4,9	55,9	2,2	574,0	2,1	540,8
Paiements à distance hors Internet	422,5	29 248,2	nd	nd	nd	nd
Cartes perdues ou volées	0,0	2,3	nd	nd	nd	nd
Cartes non parvenues	0,0	0,0	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,2	7,5	nd	nd	nd	nd
Numéro de carte usurpé	422,3	29 237,8	nd	nd	nd	nd
Autres	0,0	0,5	nd	nd	nd	nd
Paiements à distance sur Internet	824,1	107 368,2	nd	nd	nd	nd
Cartes perdues ou volées	1,2	156,5	nd	nd	nd	nd
Cartes non parvenues	0,0	0,0	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,3	48,3	nd	nd	nd	nd
Numéro de carte usurpé	822,6	107 146,3	nd	nd	nd	nd
Autres	0,1	17,2	nd	nd	nd	nd
Retraits	132,0	36 223,3	2,6	673,5	1,8	552,6
Cartes perdues ou volées	122,8	34 500,8	2,2	543,4	1,0	324,3
Cartes non parvenues	0,6	143,2	0,0	19,7	0,0	1,1
Cartes altérées ou contrefaites	8,6	1 577,3	0,3	92,2	0,7	210,3
Numéro de carte usurpé	0,0	2,0	0,1	13,1	0,1	13,8
Autres	0,0	0,0	0,0	5,2	0,0	3,1
Total	**2 008,7**	**220 987,2**	**140,9**	**25 109,2**	**323,2**	**72 850,8**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 5

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2012 – 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	5,87	3 043,36	2,41	821,13	4,32	1 034,25
Cartes perdues ou volées	1,20	458,92	0,15	44,33	0,24	87,35
Cartes non parvenues	0,77	367,34	0,40	152,39	0,12	11,20
Cartes altérées ou contrefaites	2,00	438,57	0,81	262,12	3,29	684,95
Numéro de carte usurpé	0,30	221,42	1,02	358,35	0,66	249,52
Autres	1,60	1 557,11	0,03	3,96	0,00	1,24
Paiements à distance hors Internet	0,15	156,47	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	6,03	nd	nd	nd	nd
Autres	0,13	150,44	nd	nd	nd	nd
Paiements à distance sur Internet	6,1	2 009,70	4,18	918,97	2,88	591,64
Cartes perdues ou volées	0,66	166,65	0,06	4,37	0,18	29,91
Cartes non parvenues	0,27	124,95	0,02	19,40	0,00	2,12
Cartes altérées ou contrefaites	0,60	195,70	0,18	8,19	1,03	130,90
Numéro de carte usurpé	4,35	1 400,69	3,91	886,41	1,66	428,70
Autres	0,23	121,71	0,01	0,60	0,00	0,00
Retraits	1,31	214,32	nd	nd	nd	nd
Cartes perdues ou volées	1,11	167,15	nd	nd	nd	nd
Cartes non parvenues	0,17	39,78	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	4,89	nd	nd	nd	nd
Autres	0,09	2,50	nd	nd	nd	nd
Total	**13,45**	**5 423,85**	**6,58**	**1 740,10**	**7,19**	**1 625,88**

Source : Observatoire de la sécurité des cartes de paiement

A18

Tableau 6

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2012 – Acquisition

(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	5,87	3 043,36	0,79	423,43	3,70	2 081,05
Cartes perdues ou volées	1,20	458,92	0,04	14,98	0,30	173,32
Cartes non parvenues	0,77	367,34	0,02	1,68	0,01	0,32
Cartes altérées ou contrefaites	2,00	438,57	0,59	342,02	2,97	1 643,78
Numéro de carte usurpé	0,30	221,42	0,10	53,93	0,35	228,65
Autres	1,60	1 557,11	0,03	10,82	0,08	34,98
Paiements à distance hors Internet	0,15	156,47	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	6,03	nd	nd	nd	nd
Autres	0,13	150,44	nd	nd	nd	nd
Paiements à distance sur Internet	6,1	2 009,70	4,83	1 718,51	10,85	3 283,87
Cartes perdues ou volées	0,66	166,65	0,05	24,96	0,58	162,73
Cartes non parvenues	0,27	124,95	0,08	52,80	0,06	13,48
Cartes altérées ou contrefaites	0,60	195,70	0,72	428,87	3,32	1 194,52
Numéro de carte usurpé	4,35	1 400,69	3,89	1 185,44	6,74	1 849,30
Autres	0,23	121,71	0,09	26,44	0,14	63,84
Retraits	1,31	214,32	nd	nd	nd	nd
Cartes perdues ou volées	1,11	167,15	nd	nd	nd	nd
Cartes non parvenues	0,17	39,78	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	4,89	nd	nd	nd	nd
Autres	0,09	2,50	nd	nd	Nd	nd
Total	**13,45**	**5 423,85**	**5,61**	**2 141,94**	**14,54**	**5 364,92**

Source : Observatoire de la sécurité des cartes de paiement

Définition et typologie de la fraude relative aux cartes de paiement

Définition de la fraude

À des fins de recensement statistique, l'Observatoire estime qu'il convient de considérer comme constitutif de fraude toute utilisation illégitime d'une carte de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation :

• ayant pour conséquence un préjudice pour le banquier teneur de compte qu'il s'agisse du banquier du porteur de la carte ou de celui de l'accepteur (commerçant, administration… pour son propre compte ou au sein d'un système de paiement [1]), le porteur, l'accepteur, l'émetteur, 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 ;

• quels que soient :
  – les moyens employés pour récupérer, sans motif légitime, les données ou le support de la carte (vol, détournement du support de la carte, des données physiques ou logiques, des données de personnalisation et/ou récupération du code secret, et/ou du cryptogramme, piratage de la piste magnétique et/ou de la puce…),

  – les modalités d'utilisation de la carte ou des données qui lui sont attachées (paiement ou retrait, en paiement de proximité ou à distance, par utilisation physique de la carte ou du numéro de carte, sur automate…),

  – la zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :
    - émetteur français et carte utilisée en France,
    - émetteur étranger dans l'espace SEPA et carte utilisée en France,
    - émetteur étranger hors de l'espace SEPA et carte utilisée en France,
    - émetteur français et carte utilisée à l'étranger dans l'espace SEPA,
    - émetteur français et carte utilisée à l'étranger hors de l'espace SEPA ;

  – le type de carte de paiement [2], y compris les porte-monnaie électroniques ;

• que le fraudeur soit un tiers, le banquier teneur de compte, le porteur de la carte lui-même (dans le cas par exemple d'une utilisation après déclaration de vol ou de perte, ou d'une dénonciation abusive de transactions), l'accepteur, l'émetteur, un assureur, un tiers de confiance…

1 Dans le cas d'Internet, l'accepteur peut être différent du fournisseur de service, ou d'un tiers de confiance (paiements, dons effectués par des internautes en soutien d'un site, d'une idéologie…).
2 Tel que défini à l'article L. 132-1 du *Code monétaire et financier* dans sa version antérieure au 1er novembre 2009.

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 ;

• fractionnement du paiement : action qui consiste à scinder le paiement en vue de passer en dessous des plafonds fixés par l'émetteur.

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 ;

• ouverture frauduleuse de compte : ouverture d'un compte de référence en fournissant de fausses données personnelles ;

3 Personal Account Number.

• 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 ;

• 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 répartition du préjudice entre :

• la banque du commerçant, acquéreur de la transaction ;
• la banque du porteur, émettrice de la carte ;
• le commerçant ;
• le porteur ;
• les éventuelles assurances ;
• et les autres types d'acteurs.

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 : hôtellerie, service de location, billetterie de spectacle, organisme caritatif, … ;
- services aux professionnels : matériel de bureau, service de messagerie, … ;
- téléphonie et communication : matériel et service de télécommunication/téléphonie mobile ;
- voyage, transport : ferroviaire, aérien, maritime ;
- divers.

Le *rapport de l'Observatoire de la sécurité des cartes de paiement* est en libre téléchargement sur le site internet de l'Observatoire (*www.observatoire-cartes.fr*).

Une version imprimée peut être obtenue gratuitement, jusqu'à épuisement du stock, sur simple demande (cf. adresse ci-contre).

L'Observatoire de la sécurité des cartes de paiement se réserve le droit de suspendre le service de la diffusion et de restreindre le nombre de copies attribuées par personne.

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

Directeur de la publication
Denis Beau,
Directeur général des Opérations
Banque de France

Rédacteur en chef
Frédéric Hervo,
Directeur des Systèmes de paiement et Infrastructures de marché
Banque de France

Secrétariat de rédaction
Marcia Toma

Réalisation
Direction de la Communication
de la Banque de France

Opérateurs PAO
Nicolas Besson, Pierre Bordenave, Angélique Brunelle, Alexandrine Dimouchy, Christian Heurtaux, François Lécuyer, Aurélien Lefèvre, Carine Otto, Isabelle Pasquier

Version papier
Observatoire de la sécurité des cartes de paiement
011-2324
Téléphone : +1 42 92 96 13
Télécopie : +1 42 92 31 74

Impression
Banque de France

Dépôt légal
Dès parution

Internet
www.observatoire-cartes.fr