Le neuvième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2011, comprend cette année quatre parties dont les principales conclusions sont reprises ci-après.

1re partie : sécurisation des paiements par carte sur Internet

L'enquête d'opinion menée pour la deuxième 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 2011.

Pour autant, à ce jour, seulement 23 % des transactions de paiement sur Internet sont sécurisées par des dispositifs d'authentification non rejouable, alors même que ces dispositifs ont prouvé leur efficacité auprès de certains e-commerçants et que ces derniers sont bien accueillis par les consommateurs. Ainsi, la généralisation progressive de l'authentification non rejouable et donc de « 3D-Secure » auprès des e-commerçants, notamment les sites les plus fréquentés, avec un déclenchement reposant sur une analyse de risques, reste une priorité pour l'Observatoire.

*Il est à noter que ces recommandations sont en ligne avec les conclusions du rapport Pauget-Constans sur l'avenir des moyens de paiement en France et avec celles du projet de rapport du Forum européen sur la sécurité des moyens de paiement (*SecuRe Pay*), lesquelles préconisent au niveau européen la généralisation de l'authentification non rejouable du porteur en fonction du risque de la transaction lors d'un paiement sur Internet.*

2e partie : statistiques de fraude pour l'année 2011

Le taux de fraude s'établit pour l'année 2011 à 0,077 %, en légère augmentation pour la quatrième année consécutive, correspondant à un montant total de fraude de 413,2 millions d'euros (contre 0,074 % et 368,9 millions d'euros en 2010).

Alors que la fraude à l'international est en léger recul, cette hausse de la fraude s'explique au niveau national par deux tendances principales :

- *une augmentation de la fraude sur les paiements à distance, et notamment sur le canal Internet. Ainsi, le taux de fraude sur les paiements à distance atteint 0,321 %. On notera en particulier que le taux de fraude sur les paiements sur Internet continue d'augmenter pour s'établir à 0,341 %. L'augmentation est plus modérée pour les paiements à distance effectués par courrier ou par téléphone. L'ensemble des paiements à distance, qui représente 8,4 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude. L'évolution défavorable de la fraude sur ce canal de paiement conduit l'Observatoire à insister pour que ses recommandations relatives à l'adoption de dispositifs permettant l'authentification non rejouable du porteur de la carte, tels que « 3D-Secure », soient mises en œuvre par les e-commerçants, notamment les plus grands d'entre eux, pour les paiements les plus risqués ;*

- *une hausse du taux de fraude sur les paiements de proximité qui s'établit désormais à 0,015 % (contre 0,012 % en 2010). Cette tendance s'accompagne d'une poursuite de l'augmentation du taux de fraude sur les retraits qui atteint désormais 0,029 %. L'augmentation de la fraude sur*

ces transactions, qui reste néanmoins à un niveau très faible, intervient après plusieurs années de baisse. Elle s'explique en particulier par une augmentation des vols de carte avec code confidentiel. Face à ces tendances, 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).

Par ailleurs et pour la deuxième année consécutive, l'Observatoire est en mesure de distinguer les taux de fraude des transactions internationales réalisées en Europe (zone SEPA) de celles réalisées hors Europe (hors zone SEPA). Les résultats constatés (des taux de fraude hors Europe près de deux fois et demie supérieurs au taux relevé en Europe pour des cartes émises en France, et des cartes étrangères émises hors Europe fraudées sept fois plus que celles émises en Europe) démontrent 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.

3e partie : travaux de veille technologique autour de la sécurité du téléphone mobile en tant que terminal de paiement et des nouvelles solutions de paiement sur Internet (portefeuilles électroniques)

Le mobile comme terminal de paiement. *Le marché des terminaux de paiement connaît de nombreuses évolutions depuis quelques mois, avec l'apparition d'offres reposant sur l'utilisation d'appareils mobiles évolués, notamment les* smartphones*. Les* smartphones *étant par essence multi-applicatifs, multi-tâches et dépourvus à ce jour d'éléments de sécurité, ils apparaissent de prime abord peu adaptés aux requis habituellement exigés sur les terminaux de paiement traditionnels, dédiés à cette fonction. L'utilisation d'un terminal de paiement mobile dans la chaîne d'acceptation ne peut donc être actuellement envisagée que concomitamment à l'adoption de mesures permettant de garantir un niveau de sécurité équivalent à celui prévalant pour les terminaux de paiement traditionnels.*

Portefeuille électronique et paiement par carte. *Dans un contexte de fort développement du commerce électronique, des solutions de paiement qualifiées d'alternatives sont apparues revêtant notamment la forme d'un portefeuille électronique. L'émergence des portefeuilles électroniques contribue à la diversification des offres de paiement en apportant aux utilisateurs des moyens adaptés à leurs usages. La multiplication de ces offres ne doit cependant pas se faire au détriment de la sécurité des moyens de paiement, au risque de compromettre d'une part la confiance dans les instruments de paiement actuels, et d'autre part de voir la fraude se déporter vers des solutions qui seraient moins sécurisées. Dans ces conditions, l'Observatoire recommande la protection des données sensibles (dont celles liées aux cartes de paiement) par l'ensemble des acteurs impliqués, le recours par le gestionnaire du portefeuille électronique à un mécanisme d'authentification non rejouable du porteur par l'émetteur au moment de l'enregistrement de la carte dans le portefeuille, une analyse de risque par le gestionnaire de portefeuilles électroniques conduisant au déclenchement d'une authentification non rejouable pour les paiements considérés comme risqués et la mise en place de règles claires quant à la gestion des instruments et opérations de paiement, notamment la définition et le partage des responsabilités entre les utilisateurs, les marchands et les gestionnaires de telles solutions.*

4e partie : la coopération internationale en matière de lutte contre la fraude

L'Observatoire a souhaité cette année réaliser un état des lieux des acteurs prenant part à la lutte contre la fraude sur le territoire et présenter les circuits de coopération existants à l'international. Il ressort de cette étude que si les acteurs se sont organisés dans leurs domaines respectifs avec des résultats tangibles et que des structures de coopération existent, à la fois au niveau national, européen ou international, des axes d'amélioration sont possibles. Il conviendrait notamment de garantir l'échange opérationnel de données de fraude aidant à la détection de points de compromission, de finaliser une approche commune, notamment en termes de gouvernance, en ce qui concerne la certification des terminaux d'acceptation et d'assurer une harmonisation des exigences sécuritaires par les autorités de régulation bancaire au niveau international.