



ASSEMBLÉE NATIONALE

14ème législature

commerce électronique

Question écrite n° 12199

Texte de la question

M. Dominique Dord attire l'attention de Mme la ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, sur l'augmentation préoccupante des fraudes à la carte bancaire. Chaque minute plus d'un achat frauduleux est effectué sur internet et ce type d'escroquerie en ligne représente un total de 120 millions d'euros par an. Le nombre de fraudes à la carte bancaire sur internet a été multiplié par quatre en cinq ans. Si bien qu'aujourd'hui, si 5 % des transactions par carte bancaire sont réalisées en ligne, elles représentent 33 % du coût total de la fraude. Cette augmentation sensible de la fraude en matière de paiement électronique montre que les systèmes de sécurisation des paiements déployés par les banques ont une efficacité insuffisante. Les établissements financiers ont en effet principalement sécurisé les transactions par la saisie de données statiques (numéro de carte, cryptogramme, date d'expiration). Mais à présent les progrès informatiques permettent de dérober ces données à l'aide de logiciels espions présents sur les ordinateurs ou obtenues grâce à un générateur de numéro de carte bancaire. Afin de lutter contre la fraude en ligne, les banques ont déployé une dizaine de solutions différentes, sans concertation suffisante. Certains établissements envoient un SMS unique à saisir lors de l'achat, d'autres donnent un code sur une carte ou fournissent un lecteur à brancher sur l'ordinateur. Compte tenu de cette situation et des préjudices qu'elle entraîne pour les consommateurs, il lui demande de bien vouloir lui préciser quelles sont les mesures qu'il envisage pour renforcer et harmoniser les mesures de prévention et de lutte contre ce type de fraudes.

Texte de la réponse

Les opérations frauduleuses sur les cartes bancaires font l'objet d'un encadrement juridique très strict qui permet au porteur de la carte de ne pas voir sa responsabilité engagée. Le code monétaire et financier prévoit en effet qu'en cas d'opération non autorisée (perte, vol, détournement, y compris utilisation frauduleuse à distance et contrefaçon) et avant opposition, la responsabilité du porteur n'est pas engagée. Par conséquent, lorsqu'un client n'a pas autorisé une opération, il incombe à son prestataire de services de paiement (PSP) de prouver que l'opération en question a été authentifiée. En effet, le PSP distinguera les utilisations frauduleuses effectuées sans usage du code (susceptibles d'engager la responsabilité du titulaire de la carte à hauteur de 150 euros) des utilisations frauduleuses effectuées avec usage du code (engageant alors la responsabilité du titulaire à hauteur du plafond des opérations précisé dans le contrat qui lie les deux parties). En tout état de cause, l'utilisation même de la carte, telle qu'enregistrée par le PSP, ne suffit pas en tant que telle à prouver que l'opération a été autorisée par le payeur, ni même que celui-ci a fait preuve de négligence. Quand la fraude est constatée, le prestataire de service de paiement doit rembourser les sommes débitées et, le cas échéant, rétablir le compte dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu, dès que le titulaire de la carte lui a signalé cette opération. Ces dispositions cessent toutefois de s'appliquer s'il s'avère que le porteur de la carte a agi de manière frauduleuse ou s'il n'a pas satisfait de manière intentionnelle ou par négligence grave à ses obligations de sécurité. Outre le régime juridique évoqué qui protège les utilisateurs de cartes, la sécurisation des transactions par carte bancaire est une préoccupation continue des

pouvoirs publics qui souhaitent promouvoir des moyens de paiements rapides, efficaces et surtout sûrs. Ainsi, en France, plusieurs articles de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ont introduit dans le code monétaire et financier de nouvelles dispositions destinées à garantir la sécurité des paiements effectués par carte. Cette loi charge expressément la Banque de France « d'assurer la sécurité des moyens de paiement » et institue l'observatoire de la sécurité des cartes de paiement. Cet observatoire adresse chaque année un bilan annuel sur les taux de fraude constatés sur les transactions par carte, tant à distance qu'en face à face, au niveau national comme au niveau international. En effet, le rapport pour l'année 2011 met en évidence une légère augmentation (0,077 %) pour la quatrième année consécutive du taux de fraude global qui représente un montant total de 413,2 millions d'euros (contre 0,074 % et 368,9 millions d'euros en 2010). Bien que la fraude à l'international soit en léger recul, cette hausse s'exprime au niveau national d'une part, sur les paiements de proximité (0,015 % contre 0,012 % en 2010) principalement liés aux vols de carte avec code confidentiel et, d'autre part, sur les paiements à distance, notamment sur le canal internet. Ces paiements à distance représentent un taux de fraude de 0,321 % soit 129,6 millions d'euros tout confondu et comptent pour 8,4 % de la valeur des transactions nationales, soit pour 61 % du montant de la fraude. Parmi ces paiements à distance, l'analyse des chiffres pour 2011 démontre une augmentation plus modérée pour les paiements réalisés par courrier ou téléphone, alors que le taux de fraude sur les paiements via internet continue effectivement d'augmenter (0,341 %). Le rapport fait néanmoins état de réelles avancées en matière de sécurisation des opérations de paiement par carte bancaire via internet mais constate que seulement 23 % des transactions de paiement par ce vecteur sont sécurisées par des dispositifs d'authentification « non rejouable » et partant, de la technologie « 3D-Secure » mise en place depuis le 1er octobre 2008 et qui constitue un contrôle supplémentaire lors d'un achat en ligne en complément des données bancaires. Cette sécurisation du paiement pour le titulaire de la carte garantit en outre la responsabilisation de la banque émettrice qui, si elle a admis l'authenticité du paiement, devient seule responsable en cas d'impayé. Ainsi, le déploiement croissant de ce procédé auprès des e-commerçants des sites les plus fréquentés reste une priorité pour l'observatoire de la sécurité des cartes de paiement qui recommande fortement l'adoption la plus large possible de ces dispositifs d'authentification par ces acteurs afin de sécuriser les paiements les plus risqués. Au demeurant, ces recommandations rejoignent totalement les conclusions du rapport « Pauget-Constans » sur l'avenir des moyens de paiement en France ainsi que celles du projet de rapport du forum européen sur la sécurité des moyens de paiement (SecuRe Pay) lesquelles préconisent toutes la généralisation de l'authentification « non rejouable » du porteur en fonction du risque de la transaction lors d'un paiement sur internet, au niveau européen. Par ailleurs et plus largement, pour la deuxième année consécutive, l'observatoire est en mesure de distinguer les taux de fraude des transactions internationales réalisées en Europe en zone SEPA de celles effectuées hors Europe. Les résultats pour 2011 confortent ceux déjà constatés en 2010 en évaluant les taux de fraude hors zone SEPA à un niveau près de deux fois et demie supérieur 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. Ce constat prouve 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 (EUROPAY Mastercard Visa) aux points de vente et de retrait. A cet égard, la progression de la notoriété des solutions déployées pour pallier ce fléau que constitue la fraude à la carte bancaire sur internet confère aux dispositifs qu'elles recouvrent une hausse de maturité par rapport à 2010 sous l'impulsion des différents acteurs. Ainsi, les bénéfices liés à la mise en place de moyens d'authentification renforcée et de « 3D-Secure » apparaissent de plus en plus clairement évidents pour les protagonistes concernés. Cependant, une sécurisation croissante ne peut que passer par une poursuite des actions engagées en sensibilisant, en informant encore davantage le porteur de carte, les banques, les e-commerçants et commerçants afin d'accroître le niveau de coopération entre ces acteurs et de le porter à un niveau international. Les axes d'amélioration possibles identifiés reposent en effet sur une harmonisation des exigences sécuritaires par les autorités de régulation bancaire aux niveaux européen et international. Dans le cadre de ce postulat, la question de la sécurité des paiements par carte bancaire, tant sur le volet traitement de la transaction que sur le volet protection du stock de données, fait actuellement l'objet d'études et de discussions au sein du Conseil de l'Union européenne, la Commission ayant commencé à interroger les parties prenantes sur l'opportunité d'harmoniser ces mesures au niveau européen.

Données clés

Auteur : [M. Dominique Dord](#)

Circonscription : Savoie (1^{re} circonscription) - Les Républicains

Type de question : Question écrite

Numéro de la question : 12199

Rubrique : Ventes et échanges

Ministère interrogé : PME, innovation et économie numérique

Ministère attributaire : Économie et finances

Date(s) clé(s)

Question publiée au JO le : [27 novembre 2012](#), page 6933

Réponse publiée au JO le : [19 février 2013](#), page 1875