ASSEMBLÉE NATIONALE

13ème législature

cartes bancaires

Question écrite n° 95987

Texte de la question

M. Jean-Claude Fruteau attire l'attention de M. le secrétaire d'État auprès de la ministre de l'économie, des finances et de l'industrie, chargé du commerce, de l'artisanat, des petites et moyennes entreprises, du tourisme, des services, des professions libérales et de la consommation, sur le piratage des données des cartes bancaires sur Internet. Selon l'Association française des usagers des banques (AFUB) les statistiques de la police concernant l'utilisation frauduleuse des cartes bancaires sur Internet - le code secret n'est alors pas nécessaire pour valider la transaction - ont explosé en 2009. L'association a relevé une augmentation de 20 % des plaintes liées à cette pratique. Si la vigilance et la surveillance régulière des mouvements enregistrés sur le compte bancaire constituent le moyen le plus sûr pour éviter les déconvenues, force est de constater que, dans bien des cas, les consommateurs sont très démunis pour prévenir ce genre de délits. Il souhaite donc connaître les actions entreprises pour lutter contre ce phénomène.

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. Ainsi, depuis l'entrée en vigueur de la directive 2007/64/CE concernant les services de paiement, le code monétaire et financier prévoit 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. 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. Par conséquent, l'utilisation même de la carte, telle qu'enregistrée par le prestataire de service de paiement, 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. La sécurisation des transactions par carte bancaire est une préoccupation continue des pouvoirs publics qui souhaitent promouvoir des moyens de paiement 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 faits 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. Pour l'année 2009, les taux de fraudes enregistrés sur les paiements nationaux par carte, réalisés sur les points de vente ou sur automate, sont en baisse constante et se situent à un niveau très faible. Les cartes privatives confirment cette tendance en présentant des taux de fraude inférieurs aux autres types de carte. Ainsi, alors que les cartes interbancaires enregistrent un taux de

fraude de 0,072 % (pour un montant total de 324,3 MEUR), le taux de fraude sur les cartes privatives est de 0,068 % (pour un montant total de 18 MEUR). Ces bons résultats sont le fruit des progrès technologiques accomplis pour une sécurisation toujours plus grande des transactions par carte : abandon de la piste magnétique au profit de la généralisation de la puce, développement du cryptage des informations utilisées pour les paiements en ligne, programmes de recoupement dans les centres d'autorisation de transaction. Sujet principal de préoccupation des autorités et des organes de surveillance des moyens de paiement, le paiement à distance est une modalité pour laquelle il est observé des taux de fraude relativement plus élevés que la moyenne. C'est pourquoi le paiement à distance fait l'objet de nouvelles mesures visant à renforcer la protection des données bancaires. Ainsi, depuis le 1er octobre 2008, la technologie 3D Secure ou procédure d'authentification renforcée permet de mettre en place un contrôle supplémentaire lors d'un achat en ligne en complément des données bancaires. Outre une sécurisation du paiement pour le titulaire de la carte, ce système a pour conséquence de responsabiliser la banque émettrice qui, si elle a admis l'authenticité du paiement, devient seule responsable en cas d'impayé. Le système PCI-DSS, quant à lui, est un programme qui vise à lutter contre le détournement des données de cartes afin d'éviter leur utilisation frauduleuse. Il est en cours d'expérimentation en France.

Données clés

Auteur : M. Jean-Claude Fruteau
Circonscription : Réunion (5e circonscription) - Socialiste, radical, citoyen et divers gauche
Type de question : Question écrite
Numéro de la question : 95987
Rubrique : Moyens de paiement
Ministère interrogé : Commerce, artisanat, PME, tourisme, services et consommation
Ministère attributaire : Économie, finances et industrie

Date(s) clée(s)

Question publiée le : 14 décembre 2010, page 13427
Réponse publiée le : 8 février 2011, page 1267