ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 31658	De **Mme Valérie Beauvais** (Les Républicains - Marne)	**Question écrite**

Ministère interrogé > Économie, finances et relance	**Ministère attributaire** > Économie, finances et relance

Rubrique >moyens de paiement	**Tête d'analyse** >Sécurité des transactions bancaires	**Analyse** > Sécurité des transactions bancaires.

Question publiée au JO le : **04/08/2020**
Réponse publiée au JO le : **06/10/2020** page : **6866**

Texte de la question

Mme Valérie Beauvais attire l'attention de M. le ministre de l'économie, des finances et de la relance, sur la problématique des fraudes à la carte bancaire sur internet. En effet, les fraudes sur les cartes bancaires ont atteint un montant de 439 millions d'euros en France en 2018. Le e-commerce est un mode de consommation en pleine expansion, ce phénomène a d'ailleurs été accentué avec la crise sanitaire. Même si effectuer des achats en ligne comprend toujours une part de risque, il existe des moyens de sécuriser le plus possible ces transactions. En ce sens, la directive européenne révisée sur les services de paiement (DSP2) vise à garantir une plus grande sécurité des paiements et une meilleure protection des consommateurs. Elle est partiellement entrée en vigueur le 13 janvier 2018, certaines mesures ont été transposées en droit national et l'Autorité bancaire européenne a accordé un délai additionnel qui fixe au 31 décembre 2020 la date butoir pour disposer de la pleine mise en conformité des solutions d'authentification pour les paiements en ligne. La DSP2 réitère l'obligation faite aux banques de rembourser leurs clients victimes de fraude et renforce les règles de gestion des risques et d'authentification des clients. À cet égard, elle instaure la mise en œuvre d'une procédure d'authentification forte, nécessitant une vérification renforcée de l'identité par le biais de deux ou trois éléments : - un élément que seul le client connaît (mot de passe, code) ; un élément que seul le client possède (téléphone, carte) ; une caractéristique personnelle du client (empreinte digitale, iris ou reconnaissance vocale). L'article L. 133-44 du code monétaire et financier transpose partiellement cette directive. Il dispose que le prestataire de services de paiement applique l'authentification forte du client lorsque le payeur : - accède à son compte ; - initie une opération de paiement électronique ; - exécute une opération par le biais de moyens de communication à distance constituant un risque de fraude en matière de paiement. Il pose également une obligation du prestataire de service de paiement de mettre en place des mesures de sécurité adéquates afin de protéger la confidentialité et l'intégrité des données de sécurité personnelle des utilisateurs de paiement. Néanmoins, aujourd'hui, force est de constater que cette procédure d'authentification forte n'est pas assez appliquée, voire pas appliquée du tout. Pourquoi les banques ne sont-elles pas obligées d'appliquer strictement cette DSP2 afin d'apporter de meilleures garanties en matière de sécurité aux consommateurs ? En conséquence, elle lui demande de bien vouloir lui indiquer, d'une part quelles mesures il entend mettre en œuvre pour assurer une application stricte de la DSP2, et d'autre part de lui préciser s'il entend imposer une obligation d'information des titulaires de carte bancaire, à la charge des établissements bancaires, sur les risques et les moyens de sécurisation des paiements en ligne.

Texte de la réponse

Les dispositions sécuritaires de la seconde directive sur les services de paiement (DPS2), complétées par des

normes techniques règlementaires (RTS) introduites dans le cadre d'un règlement délégué – entrées en application le 14 septembre 2019 – renforcent substantiellement la sécurité des services et des données de paiement, au bénéfice de l'ensemble des acteurs (clients, commerçants, prestataires de services de paiement). En matière d'authentification forte des paiements (« strong customer authentication » - SCA) par carte sur internet, ces nouvelles exigences de sécurité nécessitent des évolutions structurelles sur deux volets : 1. Le remplacement de la solution d'authentification, considérée jusqu'alors comme forte et mise en œuvre par les principaux établissements français dans le cadre des paiements par carte sur internet, à savoir la saisie des données de la carte et d'un code temporaire reçu par SMS, dont l'Autorité Bancaire Européenne a jugé dans un avis de juin 2018 qu'il ne pouvait constituer une solution d'authentification forte (strong customer authentication – SCA en anglais) conforme à la nouvelle réglementation, par des techniques d'authentification forte pour les paiements par carte sur internet. 2. L'évolution du protocole informatique « 3-D Secure », qui régit les échanges relatifs à l'authentification des paiements par carte sur internet ente les e-commerçants, les prestataires d'acceptation technique, la banque acquéreur et la banque émetteur. La version préexistante de ce protocole (« v.1 ») ne permet pas d'assurer les règles de responsabilité de la DSP2 (le choix de ne pas recourir à l'authentification forte doit désormais être validé par l'émetteur) et la gestion des exemptions d'authentification forte (notamment bénéficiaire de confiance, paiement de moins de 30 euros, paiement récurrent ou transaction à faible niveau risque), contrairement à la nouvelle version « 3-D Secure v.2 » en cours de déploiement. Afin de favoriser un déploiement rapide et coordonné sur ces deux volets, l'Observatoire de la sécurité des moyens de paiement (OSMP) a élaboré un plan de migration cohérent avec l'échéance du 31 décembre 2020 fixée par l'Autorité bancaire européenne. Ce plan fait l'objet d'un pilotage par un groupe de travail institué au sein de l'OSMP, auquel participent de nombreux acteurs de place (banques, prestataires techniques et commerçants), la Banque de France, l'ACPR et la DG Trésor. Cette enceinte, qui se réunit à un rythme mensuel, assure un suivi périodique à la fois qualitatif et quantitatif de la migration de manière à pouvoir évaluer au plus près les progrès réalisés et à identifier les points de blocage éventuels. Les travaux évoluent de manière satisfaisante et laissent augurer une mise en œuvre de ces nouvelles obligations d'authentification permettant de respecter le cadre européen. Dans ces conditions, il n'est pas prévu de mettre à la charge des établissements bancaires ni des commerçants une obligation spécifique supplémentaire sur les paiements en ligne.