ASSEMBLÉE NATIONALE

17ème legislature

Question N° : 167	De **Mme Félicie Gérard** (Horizons & Indépendants - Nord)	**Question écrite**
Ministère interrogé > Consommation	**Ministère attributaire** > Économie, finances et industrie	
Rubrique >banques et établissements financiers	**Tête d'analyse** >Arnaque au faux conseiller bancaire	**Analyse** > Arnaque au faux conseiller bancaire.
Question publiée au JO le : **08/10/2024** Réponse publiée au JO le : **03/12/2024** page : **6450** Date de changement d'attribution : **29/10/2024**		

Texte de la question

Mme Félicie Gérard attire l'attention de Mme la secrétaire d'État auprès du ministre de l'économie, des finances et de l'industrie, chargée de la consommation sur la multiplication des arnaques au faux conseiller bancaire, aussi appelées *« spoofing »* qui permettent aux escrocs de récupérer des données bancaires et d'ainsi effectuer des opérations sur les comptes. De plus, ils incitent les victimes à effectuer eux-mêmes les transactions, limitant ainsi les possibilités de remboursement une fois l'arnaque découverte. Chaque année, plusieurs milliers de Français sont victimes de ces arnaques qui débutent par du *« phishing »* par SMS ou courriel, ou directement par un appel téléphonique frauduleux. En effet, une hausse de 78 % est recensée en 2023 par rapport à 2022. Au-delà d'un véritable préjudice financier que subissent les victimes, elles font également face à un réel préjudice moral causé par la capacité des escrocs à se faire passer pour des personnes de confiance. Malgré la sensibilisation déjà existante, toute personne peut être concernée par ces arnaques qui ne limitent donc plus à un public vulnérable. C'est pourquoi elle lui demande si le Gouvernement prévoit des mesures visant à renforcer la lutte contre ce type d'arnaque, ainsi que l'accompagnement des personnes qui en sont victimes.

Texte de la réponse

La pratique du « spoofing » ou fraude au faux conseiller bancaire, qui consiste pour des fraudeurs à appeler une personne en usurpant le numéro de téléphone d'un conseiller bancaire afin de rassurer la victime dans le but qu'elle authentifie une opération de paiement, est une préoccupation importante du Gouvernement en ce qu'elle peut toucher l'ensemble des citoyens et en particulier les plus vulnérables. Cette fraude en fort essor ces dernières années et, plus largement, les escroqueries exploitant les vulnérabilités du secteur des communications électroniques, sont autant de pratiques malveillantes contre lesquelles le Gouvernement lutte afin de protéger les citoyens et les entreprises. Comme l'indique le dernier rapport annuel de l'Observatoire de la sécurité des moyens de paiement (OSMP) publié le 11 septembre dernier, les techniques de fraude par manipulation de l'utilisateur, dont la fraude au faux conseiller bancaire, progressent pour représenter en 2023 un montant de 379 millions d'euros. Face à l'ampleur de cette menace, le ministère de l'économie, des finances et de l'industrie, la Banque de France, la Fédération bancaire française et l'OSMP ont décidé d'appeler l'attention des Français face aux tentatives de fraude aux moyens de paiement en leur rappelant les bonnes pratiques à cet égard (ne jamais authentifier des opérations dont un utilisateur n'est pas à l'initiative, ne pas communiquer de mots de passe ou de codes confidentiels à des tiers, même leur banquier, etc.). Une grande campagne de sensibilisation en presse écrite, radio et sur internet a ainsi été lancée depuis le 8 juin dernier. Des messages de sensibilisation à destination des utilisateurs apparaissent également dans

les applications bancaires. Le Gouvernement continue d'œuvrer pour garantir aux utilisateurs une sécurité optimale en cherchant d'une part à renforcer la lutte contre la fraude, et d'autre part à faciliter les démarches de remboursement, même lorsqu'une authentification forte a été réalisée, en application du droit existant qui généralise depuis 2018 l'authentification forte du payeur en application de la deuxième directive européenne sur les services de paiement du 25 novembre 2015 (dite DSP2). Toutefois, si l'authentification forte a largement permis de réduire les taux de fraude, les fraudeurs contournent la robustesse de cette authentification en manipulant les victimes pour les amener à valider elles-mêmes des opérations ou en leur soutirant des données personnelles, notamment par des SMS frauduleux, en vue de réaliser à la place des utilisateurs des opérations de paiement. Le renforcement de la lutte contre la fraude repose en amont sur la prévention à destination de l'ensemble des publics, avec des moyens de sensibilisation variés. Lutter contre la fraude requiert également la vigilance de tous. Le Gouvernement a appelé l'ensemble des acteurs à s'approprier les recommandations de l'OSMP publiées le 16 mai 2023 et à adopter les meilleurs pratiques et comportements à cet égard : - les consommateurs et les entreprises, en étant toujours vigilants dans l'utilisation des instruments de paiement, doivent veiller à la sécurité des données, en privilégiant dans la mesure du possible la solution d'authentification forte la plus sûre et en faisant preuve de réactivité et de transparence en cas de fraude subie en vue de rapporter l'ensemble des éléments de contexte associés et de faciliter ainsi l'action des services de police et de gendarmerie ; - les prestataires de services de paiement doivent améliorer la clarté des notifications relatives aux opérations réalisées par leurs clients, renforcer les contrôles effectués au moment de la validation d'opérations sensibles et déployer des procédures de blocage facilement accessibles et gratuites pour l'ensemble des instruments de paiement ; - pour les autres acteurs de l‘écosystème des paiements notamment pour les acteurs du secteur de la téléphone : en déployant des mécanismes de protection des attaques frauduleuses, en particulier au moment de l'émission de nouvelles cartes SIM, en sécurisant davantage les SMS et les appels téléphoniques, et ce pour minimiser les pratiques de « spoofing ». Lors du traitement des contestations, les recommandations de l'OSMP éclairent les démarches de remboursement des victimes de fraude auprès de leurs prestataires de services de paiement tout en rappelant la responsabilité des utilisateurs dans la sécurité de leurs moyens de paiement. L'article L. 133-6 du code monétaire et financier prévoit que le consentement du payeur est nécessaire pour qu'une opération de paiement soit autorisée. Dans le cas où un consommateur nie avoir autorisé une opération de paiement qui a été exécutée, les articles L. 133-18 et suivants s'appliquent s'agissant des modalités de traitement de la contestation et du potentiel remboursement. En pratique, si une transaction contestée par l'utilisateur a fait l'objet d'une authentification forte, alors il revient à l'établissement teneur de compte de déterminer si cette transaction peut être considérée comme autorisée par l'utilisateur. Cette analyse doit s'appuyer sur les différents paramètres associés à la transaction (origine de la transaction, paramètres de l'authentification forte, interactions avec le payeur, etc.), l'existence d'une authentification forte n'étant pas suffisante en soi pour considérer que la transaction a été autorisée. Après analyse du dossier et à défaut d'éléments suffisants pour justifier le caractère autorisé de la transaction ou démontrer une négligence grave de l'utilisateur, l'établissement est tenu de rembourser sans délai l'opération en cause. Par ailleurs, dès lors qu'une transaction contestée par le titulaire du compte n'a pas fait l'objet d'une authentification forte, l'établissement teneur de compte est tenu de la lui rembourser sans délai, c'est-à-dire au plus tard à la fin du premier jour ouvré après réception de cette contestation. Par ailleurs, le Gouvernement rappelle l'entrée en application, depuis le 24 juillet 2023, de la loi n° 2020-901 du 24 juillet 2020 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux dite Naegelen. Cette loi oblige les opérateurs de communications électroniques à mettre en place un dispositif d'authentification à destination des opérateurs afin d'empêcher la réutilisation illicite d'un numéro légitime dans le but de l'afficher à l'utilisateur et de mettre ce dernier en confiance, notamment dans le cadre d'une fraude au faux conseiller bancaire. Les opérateurs ont mis en place un mécanisme d'authentification des numéros (MAN), sous l'égide de l'association des plateformes de normalisation des flux interopérateurs (APNF), afin de déployer une infrastructure technique commune permettant aux opérateurs d'authentifier les appels téléphoniques et d'interrompre l'acheminement des appels non authentifiés à compter du 1er octobre 2024. Le déploiement du programme MAN réduira les possibilités pour les fraudeurs d'effectuer du spoofing. Enfin, la révision en cours de la DSP2 comprendra une série de mesures visant à combattre plus efficacement la fraude aux paiements. L'article 59 du projet de règlement sur les services de paiement (RSP) publié en juin 2023 par la Commission européenne prévoit en particulier une obligation de coopération entre les prestataires de services de paiement et les prestataires de services de communications

électroniques en cas de fraude à l'usurpation d'identité. Le règlement permettra également aux prestataires de services de paiement de partager entre eux des informations relatives à la fraude, les obligera à sensibiliser davantage leurs clients aux risques de fraudes, tout en renforçant l'authentification forte des clients et en étendant les droits au remboursement des consommateurs victimes de fraude.