Les nouvelles normes commencent à réduire la fraude

Après d'énormes efforts de sécurisation de la part de tous les acteurs, la deuxième directive sur les services de paiement montre des effets positifs.

PAR **ALEXANDRA OUBRIER**

@AlexOubrier
+ **EMAIL** *aoubrier@agefi.fr*

Après plus de deux années de mobilisation, la migration est terminée. La deuxième directive sur les services de paiement (DSP2), qui devait entrer officiellement en application le 14 septembre 2019, est désormais en vigueur. L'authentification forte des consommateurs lors des achats sur internet est généralisée. La Banque de France indique que 97 % des porteurs de cartes sont équipés par leur banque d'une solution dédiée : le plus souvent, ils reçoivent une notification dans leur application mobile bancaire et, pour valider la transaction, ils doivent s'authentifier avec leur code d'accès ou leur biométrie (empreinte digitale, reconnaissance faciale…). De plus, 97 % des paiements par carte sur internet sont conformes à la DSP2, c'est-à-dire authentifiés fortement ou relevant d'une exemption prévue par la réglementation : montant inférieur à 30 euros, paiement récurrent, niveau de fraude en dessous d'un seuil variable selon le montant, transaction avec un bénéficiaire de confiance… Il ne reste donc que 4 % des consommateurs


ADOBE STOCK

pour lesquels des dispositifs alternatifs devront être mis en œuvre.

La route a été difficile pour les marchands, pour leurs partenaires prestataires de paiement et pour les banques, mais la Banque de France a mené le projet en s'appuyant sur le *soft decline*, le rejet des transactions non conformes permettant de présenter à nouveau la transaction avec demande d'authentification. Et le résultat est là : « *La fraude a baissé depuis six mois et ça va continuer* », indiquait Julien Lasalle, directeur de la surveillance des moyens de paiement à la Banque de France, lors d'une conférence sur le sujet en décembre. « *L'authentification forte a permis des gains de sécurité considérables et demain, l'identité numérique devrait permettre d'atteindre un niveau de sécurité encore plus élevé* », complétait-il lors d'une autre intervention.

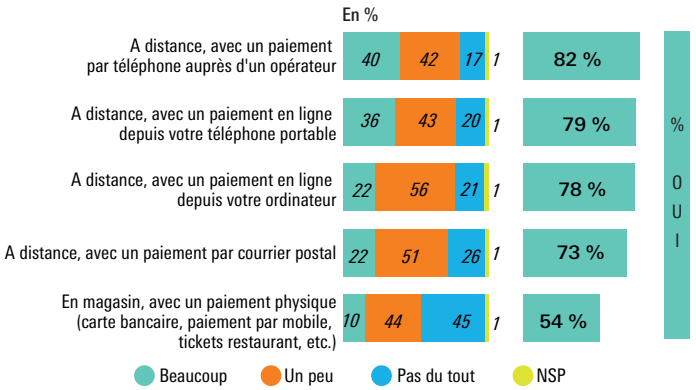
PROTECTION

Certains prestataires de services de paiement ont même constaté entre 20 % à 30 % de fraude en moins ! C'est positif mais encore faut-il que l'activité e-commerce puisse continuer à se développer. Après des taux d'échec parfois très importants, qui reflétaient l'impossibilité des consommateurs à valider leurs achats en raison de difficultés techniques liées à l'authentification forte, l'ordre semble être revenu. Une étude réalisée par Adyen auprès des acheteurs en ligne montre qu'ils se sont habitués à ces nouvelles procédures de sécurité. Ainsi, 27 % achètent au moins une fois par semaine, 64 % au moins une fois par mois et 69 % règlent leurs achats en ligne avec leur carte bancaire. La sécurité du paiement est le premier critère de choix d'un site d'e-commerce (cité à 56 %). 86 % des acheteurs se sentent mieux protégés par le système 3DS lors d'un achat en ligne, même si 20 % ont déjà abandonné leur panier pour cause d'incapacité à valider la transaction par authentification forte.

Les commerçants peuvent être soulagés. « *C'est incroyable que tout cela fonctionne*, s'est étonné Jean-Michel Chanavas, délégué général de Mercatel, une association de grands commerçants en ligne. *Il faut maintenant relever le défi de la permanence et que tout fonctionne 24h sur 24 !* » La haute disponibilité d'un dispositif aussi complexe et concernant autant d'acteurs est l'un des sujets à traiter. Ce n'est pas le seul. La Banque de France aussi a identifié des cas où les règles d'authentification et d'exemption ne sont pas correctement appliquées, comme le recours à des transactions initiées par le marchand (MIT, demande de paiement adressée au client) pour contourner l'authentification forte à chaque paiement, que pratiquent certaines plateformes de livraison de repas, de location de trottinettes ou de VTC… Divers cas spécifiques feront l'objet d'une clarification. Le superviseur se soucie également de la montée des escroqueries par manipulation des consommateurs au téléphone pour leur faire valider des transactions frauduleuses. Et le secteur du voyage, qui bénéficiait d'une dérogation en raison de la crise sanitaire, va également devoir rentrer dans le rang.

MÉFIANCE SUR LE PAIEMENT À DISTANCE

Craignez-vous d'être victime de fraude dans les situations suivantes ?



89 % craignent d'être victimes de fraude dans au moins une de ces situations

55 % craignent beaucoup d'être victimes de fraude dans au moins une de ces situations

SOURCE : « ETUDE OPINIONWAY-ACI WORLDWIDE : LES FRANÇAIS ET LE PAIEMENT »

Etude réalisée les 20 et 21 octobre 2021, auprès d'un échantillon de 1.121 personnes représentatif de la population française âgée de 18 ans et plus.

LA SÉCURITÉ DU PAIEMENT EST LE PREMIER CRITÈRE DE CHOIX D'UN SITE D'E-COMMERCE

En réalité, l'impact de cette réglementation se verra à long terme. « *Il y a encore beaucoup à faire pour améliorer la réussite des transactions*, selon Arnaud Crouzet, vice-président *consulting, payment and smart mobility* chez FIME, prestataire technique. *L'exemption d'authentification forte grâce à l'analyse de risque de la transaction n'est pas bien utilisée, elle pourrait concerner 70 % des transactions mais n'en touche que 30 % ! Les exemptions liées aux paiements fractionnés, paiements récurrents, transactions initiées par les marchands, paiements à des bénéficiaires de confiance… ne sont pas correctement activées. Le déploiement technique n'a pas été bien fait, il faut aider les émetteurs* (banques des consommateurs, NDLR) *à mieux gérer leur risque.* » En outre, les marchands ne peuvent plus relancer une transaction après un premier échec d'authentification, certaines transactions sur mobile sont perdues, les marchands qui pratiquent l'authentification forte par délégation voudraient être reconnus par les banques des porteurs. De multiples ajustements restent à faire.

FLUIDITÉ

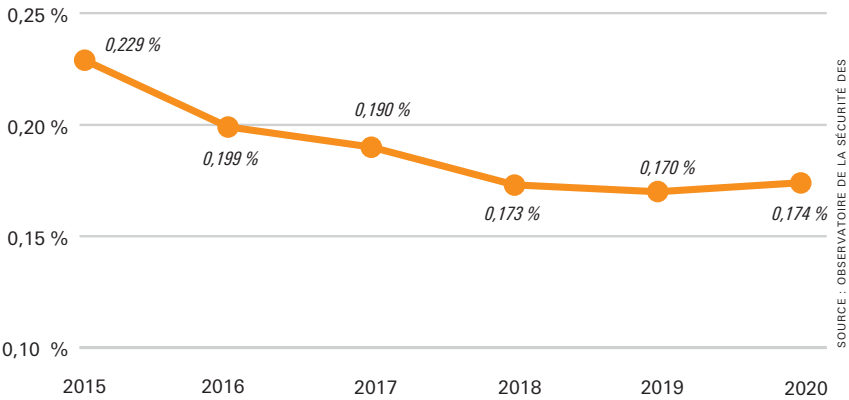
Le grand sujet est la fluidité des transactions qui pourra être obtenue par une plus grande maîtrise du risque et par un plus grand recours aux exemptions. Le régulateur l'a prévu pour ceux qui parviendront à maintenir le taux de fraude en dessous de certains seuils variables selon le montant. « *Le système est en place, il faut maintenant faire tourner la machine pour que*

L'exemption d'authentification amorcée

les outils donnent la pleine mesure de leur efficacité et apportent des scorings plus performants qui feront baisser la fraude », estime Jean-Michel Chanavas. Les prestataires de services de paiement sont à pied d'œuvre. Ils gèrent également la migration vers 3DS V2 qui doit permettre aux marchands de transmettre davantage de données sur les transactions afin d'obtenir des exemptions. « *La majorité de nos commerçants clients a basculé en 3DS V2, la performance est meilleure qu'avec 3DS V1*, annonce Ludovic Houri, président de Dalenys. *Les banques disent aux commerçants que c'est à eux d'estimer le 'frictionless'* (pas de déclenchement de l'authentification forte, NDLR) *par rapport à leurs niveaux de fraude, mais elles doivent aussi être capables de traiter les informations transmises par les commerçants et d'avaliser les transactions en quelques secondes pour donner plus de performance.* » Et le fait que Dalenys appartienne au groupe BPCE facilite la communication avec les banques grâce à Fast Pass, une solution technique qui permet de garantir un traitement sans authentification forte pour les paiements initiés par les consommateurs clients de BPCE, ce qui a une influence claire sur le taux de conversion.

GARDER LA MAÎTRISE

Taux de fraude sur les paiements à distance



SOURCE : OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT – BANQUE DE FRANCE

A l'échelle nationale, Fast'R, le « *directory server* » du Groupement Cartes Bancaires, traite les données envoyées par les commerçants, calcule son propre score de risque et transmet aux banques une recommandation d'exemption. Les résultats sont très encourageants : 57 % des transactions passent en *frictionless* et les taux de fraude atteignent des niveaux les plus bas observés. Tous ces efforts n'auront pas été vains. A

LA PAROLE À... **ANGELO CACI**, directeur général de Syrtals Cards

« *In fine, ces mesures n'auront pas d'incidence sur l'essor de l'e-commerce* »

La fraude a-t-elle reculé depuis l'entrée en vigueur des dernières mesures liées à la seconde directive sur les services de paiement (DSP2) ?

Le prochain rapport de l'Observatoire de la sécurité des moyens de paiement publié par la Banque de France chaque année en juillet donnera une vision définitive de l'année 2021. Mais je pense que la fraude a effectivement baissé grâce au recours plus fréquent à l'authentification forte et à de nouvelles mesures plus performantes que l'envoi d'un code par SMS, comme la validation des transactions dans l'application mobile de la banque par exemple. L'inconnue est l'impact de ces mesures sur le taux de conversion et sur le chiffre d'affaires des marchands, car on sait que chaque étape supplémentaire dans le processus de paiement réduit le taux de succès des achats en e-commerce. Comment les consommateurs ont-ils réagi face à cette nouvelle méthode d'authentification : ont-ils abandonné leurs achats suite à une incompréhension ou un dysfonctionnement ? Ont-ils recommencé ou changé d'enseigne ?

La croissance de l'e-commerce est-elle la preuve que les consommateurs se sont habitués ?

Les gens se sont accoutumés à acheter sur internet et, in fine, ces mécanismes n'auront pas de réelle incidence sur l'essor de l'e-commerce. L'authentification renforcée est une décision réglementaire pour lutter contre la fraude mais elle comporte des exemptions pour tenir compte de la réalité de l'e-commerce. Ce n'est pas le seul outil de lutte contre la fraude, d'autres dispositifs sont mis en œuvre en parallèle à tous les niveaux : commerçant, prestataire d'acceptation technique (PAT), acquéreur, émetteur pour surveiller les comportements suspects et les transactions à risque.

Où en est le dialogue technique entre les e-commerçants et les banques émettrices ?

C'est le rôle des prestataires de paiement d'optimiser progressivement ces échanges de données afin de fluidifier les transactions tout en assurant leur sécurité. Chacun a un rôle à jouer pour réduire la fraude sans nuire au business, ce qui sera bénéfique à terme. L'optimisation des échanges de données sera au cœur des préoccupations en 2022.