

Authentification forte des paiements : un délai supplémentaire à mettre à profit !

Par Julien Soulard, Directeur Retail Banking, chez
Chappuis Halder & Co.

Authentification forte des paiements : un délai supplémentaire à mettre à profit !

Initialement prévue le 14 septembre dernier, l'entrée en vigueur de l'obligation « d'authentification forte » a finalement été repoussée de 36 mois en France. Les acteurs concernés, à commencer par les banques, ont tout intérêt à tirer profit de ce délai supplémentaire.

S'inscrivant dans le cadre de la Directive sur les Services de Paiement 2 (DSP2), l'entrée en vigueur de l'obligation « d'authentification forte » (SCA) était initialement prévue le 14 septembre. Pour mémoire, cette directive crée trois facteurs d'authentification : la connaissance (quelque chose que seul l'utilisateur connaît), la possession (quelque chose que seul l'utilisateur possède) et l'inhérence (quelque chose que l'utilisateur est). Ces facteurs doivent être "indépendants" de sorte que "la compromission de l'un ne remet pas en question la fiabilité des autres".

En France, l'entrée en vigueur de cette obligation est désormais repoussée de 36 mois. Une annonce qui a résonné comme un soulagement pour bon nombre d'acteurs - banques, Fintech et e-commerçants en tête. L'objectif est de donner plus de temps aux acteurs de la chaîne du paiement pour respecter les nouvelles règles de sécurisation des transactions en ligne : 18 mois qui doivent permettre aux acteurs d'être en règle sur 80 % des paiements et 18 autres mois pour le passage à 100% des paiements conformes. D'autres pays, à l'image du Royaume-Uni ou de l'Allemagne ont eux aussi accordé un délai supplémentaire. Cependant, les calendriers de mise en conformité semblent pour le moment encore bien hétérogènes alors que l'ambition

originelle des textes européens était de créer un cadre commun. Toujours est-il que dans l'Hexagone, les acteurs se mettent en ordre de bataille pour tirer parti de cette prochaine obligation.

Une redistribution des cartes autour de l'expérience client et de la sécurisation

Car au cœur de l'authentification forte se joue la bataille de l'expérience client. Sur ce point, la France présente des spécificités bien différentes de ses voisins. Ainsi, parmi les critères de satisfaction dans l'expérience client, 60 % des Français préfèrent la sécurité à la simplicité du paiement¹, le taux le plus fort constaté en Europe occidentale. Seulement 33 % des sondés en France déclarent avoir déjà abandonné un processus de paiement complexe, alors qu'ils sont 44 % au Royaume-Uni et 48 % en Allemagne. Dans le cas français, il s'agit pour les acteurs de faire de la sécurisation une priorité fondamentale, au-delà de l'amélioration de l'expérience client.

Les Fintech déjà présentes sur le marché, et qui se construisent par définition à partir de la « *user experience* », disposent avec cette nouvelle évolution d'une corde supplémentaire à leur arc pour faire la différence avec les acteurs traditionnels. En outre, elles n'auront pas la crainte de « celui qui tire le premier », à laquelle s'exposent les acteurs traditionnels, et pourrait donc prendre un coup d'avance pendant ce délai de 3 ans. Les GAFAs, eux, pourraient ne pas hésiter à se saisir de l'occasion pour se positionner sur le créneau de l'authentification. La société de Mark Zuckerberg s'appuiera sur son bouton « Je me connecte avec Facebook » tandis qu'Apple

¹ Etude GoCardless, réalisée auprès de 4000 personnes en France, Allemagne, Espagne et Royaume Uni de mai à Juin 2019

Authentification forte des paiements : un délai supplémentaire à mettre à profit !

maîtrise d'ores et déjà a minima deux facteurs d'authentification forte grâce à son système de paiement sur mobile et va même lancer sa propre solution d'authentification « Se connecter via Apple » dès cet automne. Le cas échéant, il sera intéressant d'observer la réaction du régulateur chargé de garantir l'équité entre acteurs, a fortiori avec l'émergence des nouvelles de formes de monnaie...

De plus, nous pouvons anticiper à terme une consolidation du marché et l'émergence de certains PISP (« *payment initiation service providers*») en champions du paiement e-commerce. Et ce, pour continuer à démocratiser leur utilisation auprès des commerçants, et donc des clients finaux, ainsi que pour faciliter la prévention, la détection et le suivi des fraudes. Les fournisseurs de cartes bénéficient eux aussi d'un délai supplémentaire pour affirmer leur positionnement vis-à-vis de cette évolution structurante.

Quelles marges de manœuvre pour les banques ?

Les actions concernées par l'obligation d'authentification forte sont quotidiennement au cœur des parcours clients : le paiement en ligne, les opérations mobiles ou internet, la visualisation de comptes en ligne. Les banques ont donc l'occasion de repenser certains parcours client. L'objectif serait double : faciliter la vie des clients particuliers et e-commerçants, mais également faire évoluer leurs organisations pour demain, « piloter la banque par les parcours clients ». A ce titre, il serait intéressant de mettre à profit cette période supplémentaire en vue de solliciter les clients dans une logique de « *test & learn* » collaborative.

Cette évolution laisse également aux banques une opportunité d'adresser sous un angle nouveau la clientèle des Entreprises qui représente une part significative de leur cœur de cible. Dans le modèle émergent de « Banque Plateforme », les banques pourraient ainsi se positionner en partenaire de choix pour leur faire bénéficier de services comme :

- Des offres clé en main avec une solution de paiement PISP intégrée (choix d'un fournisseur, assistance à la mise en place technique, conseil sur les aspects réglementaires, ...)
- Une exploitation des données des paiements pour les aider à mieux connaître leurs propres clients, à évaluer les typologies de consommation, à mettre en place des campagnes marketing ciblées, voire même à proposer des dispositifs de paiement et de gestion de la fraude adaptés en fonction du niveau de risque représenté par le client ;
- Une fonction de tiers de confiance vis-à-vis du régulateur. En effet, les e-commerçants devront prouver à terme qu'ils sont bien conformes avec la réglementation : toutes les données, tous les paiements vont devoir être conservés, et des synchronisations avec la CNIL seront nécessaires. Ce serait une façon pour la banque de prendre en charge une partie du coût de la gestion de la fraude pour le compte de leurs clients préférentiels.

Tactiquement, il est probable que l'ensemble de ces acteurs traditionnels patientent jusqu'au dernier moment. Cependant, certains d'entre eux auraient tout à gagner à « sortir du bois » les premiers, pour bénéficier d'une longueur d'avance en termes d'image mais aussi de business.

Authentification forte des paiements : un délai supplémentaire à mettre à profit !

Cette évolution structurante qui impacte la vie quotidienne des consommateurs de services financiers sera intéressante à observer. Elle est particulièrement symbolique des mouvements de fond en cours dans l'ensemble de l'écosystème...

Julien Soulard
Directeur Retail Banking, chez Chappuis
Halder & Co