

Open Finance : les prémices d'une révolution financière

L'année 2024 s'annonce comme une période décisive pour l'Open Finance. Dans le prolongement de la directive DSP2 qui vise à renforcer la sécurité des paiements en Europe, la Commission européenne a adopté en avril dernier le règlement Fida (Financial Data Access), base législative de la mise en œuvre de l'Open Finance à l'échelle de l'UE. Une initiative qui, comme d'autres, ambitionne de favoriser l'innovation axée sur les données et de créer un écosystème numérique concurrentiel qui profiterait aux consommateurs et aux entreprises de tous secteurs, dont les services financiers. En permettant un accès plus large aux données financières, il est impératif dans ce contexte de répondre aux défis majeurs que sont la protection des données personnelles et la sécurité des systèmes face aux tentatives de fraude financière.



LAURENT SARRAT,
CEO et fondateur de Sis ID

Dans le paysage financier mondial en constante évolution, le concept de l'Open Finance s'impose de plus en plus comme un facteur de changement et de transformation. Bien plus qu'une simple évolution des services financiers, l'Open Finance représente les prémices d'une révolution majeure dans la manière dont nous concevons, accédons et utilisons les produits et services financiers. Incarnant le principe fondamental de libération des données jusqu'à présent cloisonnées, il ouvre un vaste écosystème défini par l'innovation, la concurrence et l'inclusion. Inspiré par les principes de l'open source et de l'open data, l'Open Finance transcende les frontières institutionnelles et redéfinit les interactions entre les acteurs du marché financier.

Un cadre sécurisé et transparent pour accéder aux données financières

Au cœur des enjeux de l'Open Finance se trouve la question sensible de la

confidentialité des données personnelles. Alors que les consommateurs recherchent un contrôle accru sur leurs informations financières, les entreprises doivent naviguer avec prudence pour assurer leur sécurité et leur protection. Les risques de violation de la vie privée et de fraude financière restent des préoccupations majeures qui nécessitent





une attention constante. Pour cela, le collectif est capital. Aujourd'hui, c'est en équipe que la sécurité est de mise face à la fraude. Pour faciliter la collaboration entre les entreprises, un échange de données plus étendu est nécessaire. Cependant, cette expansion s'accompagne d'un défi crucial : garantir la sécurité de ces échanges. Des systèmes de données partagées plus vastes augmentent nécessairement les tentatives de fraude financière, soulignant ainsi la nécessité de mettre en place des mesures de sécurité robustes et des protocoles renforcés de protection des données. Des techniques de chiffrement peuvent, par exemple, être utilisées, permettant grâce à une clé numérique unique de déchiffrer les données ou encore les techniques de hachage, surtout utilisées pour vérifier la non altération des données.

De nouvelles techniques d'authentification font également leur apparition, sécurisant l'accès à différentes applications et données sensibles. L'authentification forte vérifie ainsi deux preuves d'identité, envoyant un code par email, par sms ou encore via des applications

d'authentification à deux facteurs générant des mots de passe.

Si la confidentialité est un enjeu crucial pour les institutions de paiement, elle n'en est pas moins importante pour l'ensemble des acteurs de la chaîne de paiement, du payeur au payé. Le monde de la collaboration n'exclut pas la confidentialité des données. D'une part, il s'agit pour la plupart des usages de vérifier des informations et non d'en fournir. Dans ce cas, les données à comparer, source et cible peuvent être chiffrées et avec les mêmes mécaniques. La vérification de la véracité de l'information se fait alors par comparaison de données chiffrées, rendant leur exploitation impossible pour un fraudeur en cas de fuite d'information.

Des techniques et outils de vérification voient régulièrement le jour afin de pallier les potentielles failles de sécurité. Ainsi les entreprises peuvent avoir recours à des plateformes de vérification des données, telles qu'Infogreffe ou Infolegale pour les informations légales ou encore Sis ID pour la vérification des coordonnées bancaires. Les schémas CoP (Confirmation of

Payee) sont également de bons premiers remparts dans ce dernier cas. Le penny drop s'avère être une autre technique de plus en plus couramment utilisée pour vérifier l'authenticité d'un compte bancaire. Une somme d'argent (souvent quelques centimes) est déposée sur le compte bancaire à vérifier. Les informations (coordonnées bancaires, nom de son propriétaire ainsi que le statut du compte) remontent alors auprès de l'organisme, lui confirmant ou non sa légitimité.

Par ailleurs des mécanismes tels que la blockchain, agissant en tant que registre peuvent être utilisés pour distribuer la donnée, rendant sa modification à des fins malveillantes quasi impossible. Cette dernière technologie nécessite néanmoins un nombre de participants suffisant pour en assurer le bon fonctionnement. Si de tels mécanismes ont pu être mis en place entre institutions financières, ils n'incluent cependant pas l'ensemble des participants de la chaîne de paiement, provoquant une rupture dans le traitement de la donnée et sa sécurisation. La gouvernance d'un tel mécanisme est certes complexe, mais doit être encouragée afin que l'ensemble des acteurs soit impliqué dans la collaboration et la sécurisation des données.

Réguler et harmoniser : les deux piliers de l'Open Finance

Les réglementations jouent également un rôle essentiel dans la promotion d'une collaboration efficace, offrant un cadre pour guider les interactions entre les acteurs de la finance. Applicable depuis le 13 janvier 2018, la directive DSP2, qui instaure notamment des normes de sécurité plus strictes pour les paiements en ligne afin de renforcer la confiance des consommateurs dans les achats sur internet, illustre parfaitement cette tendance. Dans son prolongement, l'UE a proposé et adopté en avril dernier le règlement Fida, pour créer un nouveau cadre d'accès aux données financières. Toutes ces politiques ont le même objectif : consolider l'écosystème de l'Open Finance pour créer des nouveaux services plus personnalisés, et garantir plus de transparence aux consommateurs et aux organisations sur leur situation



financière. Cependant, il est essentiel que ces réglementations soient sans cesse révisées et adaptées pour refléter l'évolution constante du marché.

Un autre défi majeur réside dans la diversité des processus et des pratiques entre les entreprises. Cette hétérogénéité rend souvent difficile la mise en place de collaborations fluides et efficaces. Pour surmonter ce défi, des initiatives favorisant la centralisation des informations et encourageant l'entraide entre les utilisateurs, peuvent jouer un rôle majeur. En favorisant un échange transparent et harmonieux d'informations, de telles initiatives contribuent à renforcer la collaboration au sein du secteur financier.

L'Open Finance offre ainsi de multiples possibilités pour transformer la manière dont les services financiers fonctionnent et sont utilisés par les consommateurs et les entreprises. Cependant, pour démocratiser son usage, il est impératif que les entreprises du secteur abordent de front les défis de confidentialité, de sécurité et de collaboration. Seules une réglementation efficace, des technologies avancées et une culture commune de la collaboration pourront garantir un déploiement à grande échelle de l'Open Finance, pour les consommateurs et les entreprises. ■