



Le rôle des CDP dans les secteurs les plus réglementés : la banque



Sommaire

Avant-propos	3
Le nœud du problème : l'anonymisation et la pseudonymisation	4
Le rôle des CDP dans le secteur bancaire	6
La gouvernance et ses conséquences	10
Dernières observations	12



Avant-propos



Personne ne nous connaît aussi bien que notre banque. On pourrait même dire qu'elle nous connaît mieux que nous-mêmes (ou, du moins, plus que nous voulons bien le reconnaître).

Au quotidien, les banques savent où vous dépensez votre salaire durement gagné, à quel moment, avec quelles marques et comment. Elles connaissent votre café préféré et les plats à emporter que vous aimez tant. En outre, elles connaissent votre destination de vacances. Elles savent quand vous vous mariez et certainement aussi quand vous fondez une famille.

Sachant qu'il n'y a aucun moment de notre vie où nous ne sommes pas tributaires de notre situation financière, la relation que nous entretenons avec les banques qui gèrent notre argent revêt une importance capitale. Cependant, la façon dont nous interagissons avec elles a suivi l'évolution de la technologie (et dans la plupart des cas, de façon positive). Je suis d'un âge suffisamment avancé pour me souvenir des fois où j'ai fait la queue à la banque, muni de mon livret de compte pour retirer des espèces. Si la banque n'était pas ouverte, alors tant pis pour vous : vous repartiez sans argent liquide.

D'un autre côté, il y avait toujours ce directeur de banque qui vous connaissait et qui avait le pouvoir de prendre des décisions. À l'époque, avant que « l'ordinateur refuse » une opération, un simple regard au guichet numérique suffisait.

Mais l'ère du « tout technologique » a mis la pression sur les banques pour qu'elles évoluent rapidement et qu'elles s'adaptent aux demandes et attentes des consommateurs. Désormais, elles doivent représenter davantage qu'une simple alternative à la possibilité de glisser vos économies sous le matelas.

Toutefois, face à la multitude de plateformes, de nouveaux défis sont apparus en matière de réglementation et de responsabilité. De fait, la plus grande simplicité d'utilisation sur les mobiles, les ordinateurs de bureau et les tablettes multiplie les points de fuite potentiels et chaque nouvelle application ou interface représente également un nouveau risque.

Cela ne saurait cependant constituer un obstacle à l'innovation : le secteur doit se montrer plus ingénieux dans sa façon de traiter les données de ses clients pour les fidéliser et leur offrir une meilleure expérience bancaire.

Tout cela est compliqué. Mais heureusement, ce n'est pas non plus insurmontable.

Lindsay McEwan

Senior Vice President, EMEA GM, Tealium

Le nœud du problème : l'anonymisation et la pseudonymisation

Avant d'aborder le rôle potentiel d'une CDP dans un secteur extrêmement réglementé, il est essentiel de s'intéresser aux deux aspects fondamentaux qui définissent l'efficacité de la gestion des données : l'anonymisation et la pseudonymisation.

Il est particulièrement important de bien les connaître lorsqu'il s'agit de trouver un équilibre entre la conformité au RGPD et la possibilité d'exploiter les données à des fins d'analyse.

L'anonymisation

C'est la suppression de toute possibilité d'identifier un client précis en le rendant anonyme. Les données concernées sont totalement dissociées de leur sujet et, par conséquent, ne peuvent être appréhendées que dans leur globalité. Par exemple, les données rendues anonymes montreront combien de clients de banques ont élargi leur portefeuille de comptes pour passer de la trésorerie courante à l'épargne et aux comptes d'épargne individuels (ISA).

À cet égard, ces données peuvent révéler des macro-tendances dans l'ensemble des données relatives aux clients. Mais cela ne permettra pas à une banque de savoir qui a ajouté un ISA à son compte courant et donc quels autres produits ou services pourraient l'intéresser. L'anonymisation peut renseigner sur la stratégie commerciale et déterminer les domaines dans lesquels le marketing peut être efficace, mais uniquement dans une perspective pyramidale.



La pseudonymisation

Si l'utilisation exclusive de données anonymisées permet de supprimer complètement le risque lié à la manipulation des données clients, elle génère comme nous l'avons vu une certaine opacité et ne permet pas vraiment de prendre des mesures ciblées en fonction des informations recueillies.

Cependant, l'introduction d'une étape de pseudonymisation dans la gestion des données permet aux entreprises de personnaliser leurs résultats marketing, tout en restant conformes au RGPD et en protégeant les informations sur les clients.

Dans ce cadre, les points de données clients individuels sont marqués par des identifiants avant d'être analysés (« Michel Dupont » deviendra par exemple « ClientBanque001 »). Néanmoins, dans le champ d'application de la CDP, les pseudonymes peuvent être décryptés en toute sécurité pour révéler l'identité et les coordonnées de la personne concernée, afin que la banque puisse la contacter.

Le marketing des identifiants

En d'autres termes, la banque peut comprendre le comportement de ce « ClientBanque001 » : ce qu'il aime et ce qu'il n'aime pas, la fréquence de ses opérations bancaires, ainsi que ses magasins, ses cafés et ses lieux de vacances préférés.

Mais surtout, la banque sait uniquement ce que fait cet identifiant. Elle ne sait pas directement qu'il s'agit en fait de Michel Dupont : grâce à la pseudonymisation des données, la banque est en conformité avec le RGPD tout en pouvant exploiter le potentiel des données qu'elle détient.

Cette approche permet d'ajouter le « ClientBanque001 » à un lot de commercialisation pour l'envoi de promotions et d'offres ciblées pertinentes, sans pour autant compromettre le respect de la vie privée. Grâce à cette stratégie, les banques peuvent partager une information connue avec des tiers et des marques sans risquer une violation des données.



Le rôle des CDP dans le secteur bancaire

Les CDP et le scénario « gagnant-gagnant »

Lorsque nous examinons la façon dont une CDP peut stimuler la croissance et la fidélisation de la clientèle dans le secteur de la banque de détail, nous devons considérer deux fonctions interdépendantes.

Tout d'abord, comme tout secteur en contact direct avec les consommateurs, il est bien sûr nécessaire de répondre à un besoin commercial. Elle doit augmenter les montants que les clients déposent sur leurs comptes ou investissent, et réaliser des ventes croisées avec des produits d'assurance ou autres. Cette stratégie peut être étendue aux partenaires de la marque ou du commerce de détail, pour lesquels les données détenues par la banque peuvent servir à cibler les promotions.

Ensuite, cette démarche doit être associée à l'accompagnement du client tout au long de son parcours de vie. Le consommateur ne restant pas la même personne tout au long de sa relation avec sa banque, on peut le fidéliser en comprenant son parcours et en y apportant des réponses adaptées.

La combinaison de ces éléments permet d'accroître la valeur du client tout au long de sa vie : plus le client sera un partenaire essentiel tout au long de sa vie, plus il rapportera d'argent à sa banque.

Des données au service de la fidélisation

Les consommateurs attendent (ou exigent) des marques qu'elles proposent des promotions et des offres spéciales : ils veulent se sentir compris, valorisés et importants. C'est la contrepartie sine qua non du partage de données.

Toutefois, on peut légitimement dire que les banques de détail (notamment les banques traditionnelles bien établies) n'accordent pas toujours un tel traitement VIP. Compte tenu des données qu'elles détiennent sur les comportements d'achat et les dépenses, on pourrait considérer que les banques qui ne saisissent pas cette occasion font preuve d'une certaine naïveté commerciale.

Sachant que les données financières d'un client doivent être traitées avec la plus grande précaution, on pourrait facilement imaginer que les banques sont freinées par une aversion à voir ces données être exploitées à des fins promotionnelles.

Et pourtant, l'étude que nous avons menée en 2021 a au contraire révélé une forte demande de promotions et d'offres spéciales de la part des partenaires bancaires à partir des données clients.



Des opportunités manquées

Malgré une audience très réceptive, il est évident que les banques de détail ne saisissent pas l'occasion qui leur est donnée de proposer des promotions et des offres spéciales. Selon notre étude, trois banques de détail britanniques sur dix proposent actuellement des offres et des promotions, alors que les deux tiers des clients feraient confiance à leur banque pour leur proposer des promotions personnalisées.

En effet, les consommateurs britanniques sont plus susceptibles de faire confiance à leur banque (67 % des personnes interrogées) pour leur proposer des promotions personnalisées qu'à leur supermarché local (57 %), au site de vente en ligne qu'ils utilisent le plus fréquemment (54 %) ou à leur opérateur de téléphonie mobile (52 %).

Ne pas profiter de cette confiance revient à passer à côté d'une énorme opportunité commerciale. Les marques doivent saisir les possibilités qu'offre cette ouverture d'esprit à propos des banques en tant que canal de consommation, même s'il appartient au secteur financier de mener ce processus de sensibilisation.

Une analyse sécurisée

Ce cas démontre clairement comment une CDP peut conférer aux banques les moyens de se rendre indispensables auprès des clients et de remédier à un éventuel désabonnement.

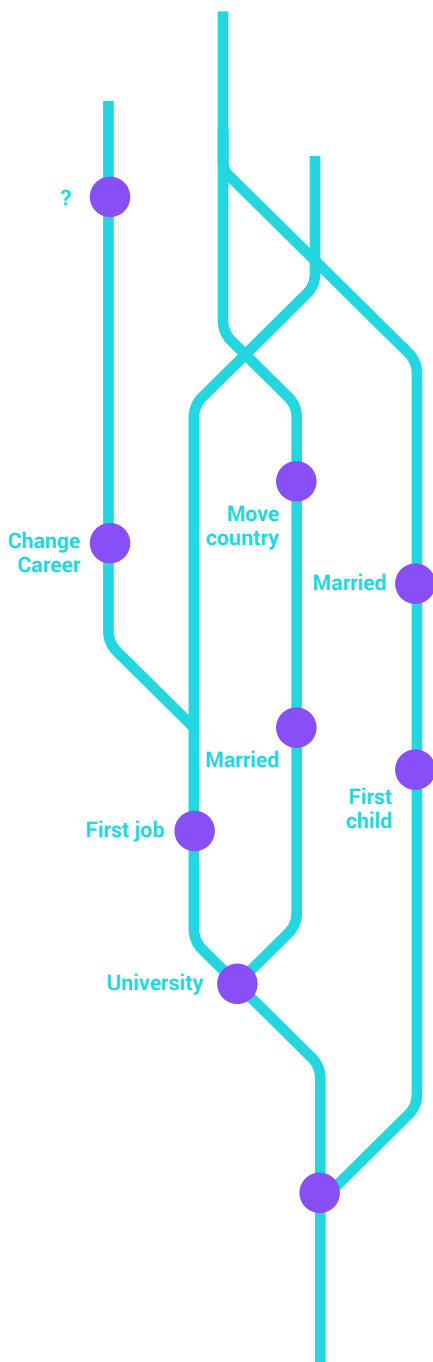
La sécurité renforcée des CDP permet aux banques d'analyser les données d'achat et de solliciter les marques selon leurs besoins, en sachant exactement quels clients (pseudonymisés) achètent régulièrement leurs produits. En proposant directement un partenariat aux acheteurs connus, les banques s'imposent à leur tour en tant qu'acteurs essentiels de l'écosystème marketing et comme l'un des moyens les plus efficaces et les mieux ciblés de promotion directe auprès des consommateurs.

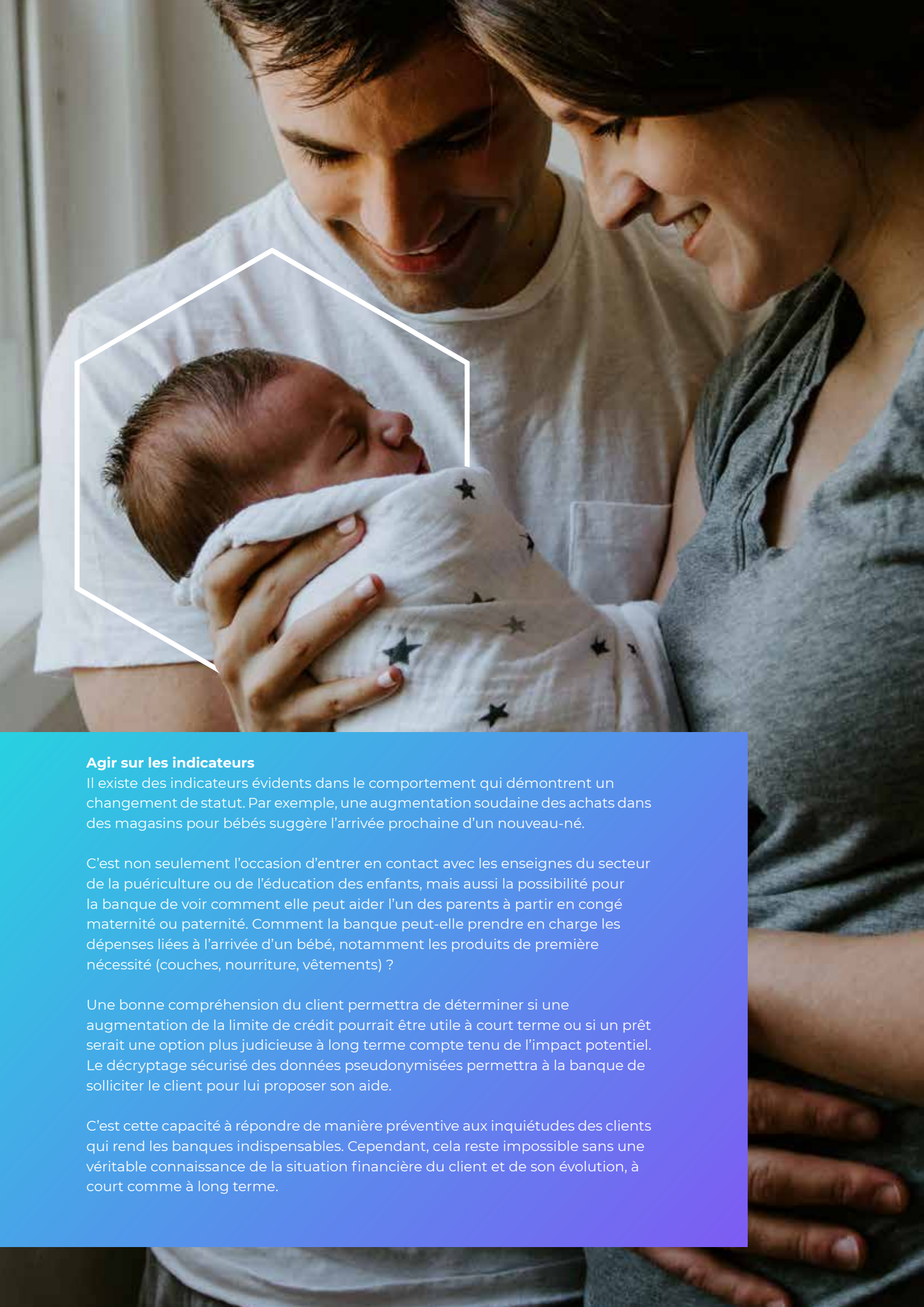
Les aspects réglementaires peuvent toutefois être source de préoccupation. Le recours à l'analyse des données pour orienter les promotions et le partage systématique d'opportunités avec les marques et les partenaires impliquent de nouvelles exigences en matière de conformité. Mais la capacité à gérer les risques grâce à une CDP fait de cette conformité un facteur d'hygiène dans le cadre de l'analyse.

Le « parcours de vie » du client

En soi, chaque client du secteur bancaire est bien plus qu'un simple numéro de compte. Il représente un ensemble de personnes qui suivent toutes leur propre parcours de vie. Aucun individu ne mène la même vie qu'un autre et, à ce titre, une banque se doit de reconnaître que chaque client a son propre parcours de vie et pas uniquement un parcours client. Par conséquent, un « programme de développement » de la marque traditionnel ne saurait constituer l'unique solution.

Les banques doivent comprendre à quel niveau se situent les clients dans leur parcours et, en conséquence, quels sont leurs besoins. Si chaque cheminement est différent, les étapes sont souvent les mêmes : terminer l'école, trouver un(e) partenaire, acheter ou louer un bien immobilier, avoir des enfants, prendre sa retraite (bien que ce ne soit pas toujours dans cet ordre).





Agir sur les indicateurs

Il existe des indicateurs évidents dans le comportement qui démontrent un changement de statut. Par exemple, une augmentation soudaine des achats dans des magasins pour bébés suggère l'arrivée prochaine d'un nouveau-né.

C'est non seulement l'occasion d'entrer en contact avec les enseignes du secteur de la puériculture ou de l'éducation des enfants, mais aussi la possibilité pour la banque de voir comment elle peut aider l'un des parents à partir en congé maternité ou paternité. Comment la banque peut-elle prendre en charge les dépenses liées à l'arrivée d'un bébé, notamment les produits de première nécessité (couches, nourriture, vêtements) ?

Une bonne compréhension du client permettra de déterminer si une augmentation de la limite de crédit pourrait être utile à court terme ou si un prêt serait une option plus judicieuse à long terme compte tenu de l'impact potentiel. Le décryptage sécurisé des données pseudonymisées permettra à la banque de solliciter le client pour lui proposer son aide.

C'est cette capacité à répondre de manière préventive aux inquiétudes des clients qui rend les banques indispensables. Cependant, cela reste impossible sans une véritable connaissance de la situation financière du client et de son évolution, à court comme à long terme.



L'évolution de la numérisation

L'occasion de devenir un véritable partenaire tout au long du « parcours de vie » du client repose avant tout sur l'augmentation du volume de données collectées par les banques, qui est le résultat direct de la numérisation rapide du secteur au cours des dernières années, ainsi que des attentes des clients en matière d'interaction avec leur banque sur diverses plateformes.

Cette évolution est en partie due à l'explosion des banques « challenger » (dont la plupart sont des banques numériques) par rapport aux établissements commerciaux traditionnels. Ces derniers ont dû évoluer rapidement pour suivre le rythme imposé par ces banques numériques qui, dès le départ, ont l'avantage de proposer des services très intuitifs.

Ainsi, les clients s'attendent à une expérience en ligne intuitive aussi bien sur les ordinateurs de bureau que sur les applications, les mobiles et les tablettes. Dans la mesure où la situation financière constitue un élément déterminant de notre vie, toute fragmentation ou absence de synchronisation peut devenir source d'inquiétude. Paradoxalement, au lieu de devenir un facteur de différenciation positif, les plateformes numériques sont devenues source de mécontentement et de désabonnement potentiel.

Outre le changement de comportement, les banques doivent faire face à de nouveaux défis sur le plan de la réglementation. Elles ont le devoir de contacter les clients pour évaluer l'impact des changements de situation sur leurs finances et de les aider si nécessaire.

Cependant, les établissements qui ne disposaient pas de systèmes numériques pleinement fonctionnels ont découvert dans quelle mesure les données (non financières) des clients étaient détenues par des tiers. Comme toutes les données détenues par les banques étaient anonymisées, ces dernières ont dû s'appuyer sur des informations provenant de sources externes qui détenaient les données de leurs clients pour pouvoir les contacter directement.

Dans ce cas, en vertu de leur « mission d'intérêt », les banques étaient en mesure de s'approprier ces données et de les exploiter comme leurs propres actifs faussement first-party. Si une telle prise de conscience peut représenter une lueur d'espoir, il ne devrait pas pour autant être nécessaire d'opérer un changement profond pour souligner les défaillances opérationnelles.

« La pandémie a mis en évidence le niveau d'avancement des banques dans leur propre parcours de transformation numérique. Selon les estimations, le précédent ratio de 80 % de clients en ligne contre 20 % de clients mobiles s'est inversé en l'espace de quelques mois. Le service mobile s'est quasiment standardisé. »

La gouvernance et ses conséquences

Pour des raisons évidentes, le secteur bancaire est l'un des plus réglementés au monde. Les organismes de réglementation veillent non seulement à ce que les données et les informations relatives aux clients soient conservées en toute sécurité (avec des amendes importantes et des retraits de licence en cas de violation), mais aussi à ce que les clients soient protégés des conséquences d'une transgression bancaire.

Voici les principaux acteurs au Royaume-Uni :

La Financial Conduct Authority (FCA), l'autorité de « bonne conduite » financière, est l'organisme le plus important du secteur bancaire et financier. Par son rôle fondamental de protection des consommateurs et de leurs finances, elle intervient en cas d'infraction et de défaillance institutionnelle.

La FCA a le pouvoir d'interdire des produits financiers, de publier des renseignements sur les promotions financières trompeuses, de divulguer les manquements au devoir de précaution et de publier des informations sur toute mesure disciplinaire adoptée, notamment des amendes et même des retraits de licences.

Parmi les autres instances, citons le Payment Services Regulator (PSR), responsable de la surveillance de tous les systèmes de paiement de masse, et le Financial Ombudsman Service (FOS), légalement chargé de traiter les plaintes et les demandes d'indemnisation.

Le FOS a la compétence pour régler les litiges et établir des règlements. Malgré son indépendance, cet organisme a conclu un protocole d'accord avec la FCA et il exerce une influence considérable sur les banques de détail.

Enfin, le Trésor de Sa Majesté (HM Treasury) a l'entière responsabilité de la structure institutionnelle du secteur bancaire et de la réglementation, et il rend compte au Parlement britannique des dysfonctionnements graves du système financier, ainsi que des mesures requises pour les résoudre. Il convient de souligner que le Trésor surveille la résilience du secteur bancaire et qu'il est chargé de gérer les perturbations opérationnelles, comme cela a été mis en évidence pendant la pandémie.



Les erreurs commises

L'adoption de réglementations de plus en plus strictes réduit considérablement le nombre d'incidents dans le secteur, qu'il s'agisse de l'utilisation abusive de données pour protéger le client ou pour faciliter les opérations bancaires. La majorité des amendes sont infligées pour des manquements en matière de lutte contre le blanchiment d'argent.

Cependant, un rapport de Which? datant de janvier 2022 a fait état d'une mauvaise gouvernance des applications et des services en ligne. La négligence dans la mise en œuvre de mots de passe et de cryptage suffisamment sécurisés y figurait en bonne place parmi les principaux facteurs, de même que les sites Web non sécurisés, laissant ainsi supposer une mauvaise mise en place de l'infrastructure. Cette situation pourrait être la conséquence immédiate de l'accélération ou de la précipitation des processus de transformation numérique de la part des opérateurs qui sont à la traîne dans le domaine.

Fait inquiétant, la protection insuffisante de la connexion, la navigation dans les applications et la facilité de gestion des comptes sur les différentes plateformes constituaient un problème parmi les quinze grandes banques évaluées. Dans le cadre de ce test, il a également été constaté qu'une banque « challenger » ne demandait pas à ses utilisateurs de se connecter chaque fois qu'ils accédaient à leur compte, ce qui peut être considéré comme un manquement au devoir de diligence d'une banque.

Même si certaines banques ont évidemment obtenu d'excellents scores, l'ampleur de ces problèmes reste préoccupante. Les résultats de cette étude n'ont pas encore donné lieu à des amendes ; on ne sait pas encore comment la FCA va les interpréter pour agir en conséquence.

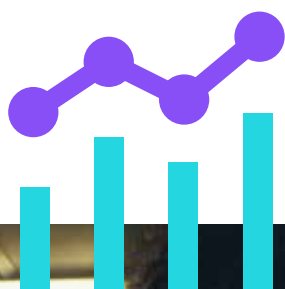


Dernières observations

Il convient de souligner que les bonnes nouvelles font rarement la une des journaux. Une mauvaise infrastructure qui engendre des fractures et des défaillances ne devrait pas être autorisée à déterminer le comportement d'une banque. Après tout, les inquiétudes légitimes concernant l'effet de certaines difficultés opérationnelles doivent être levées en s'attaquant à leurs causes, qui relèvent des compétences des services techniques et de la gouvernance.

En interne, les discussions devraient plutôt porter sur la manière dont les banques peuvent devenir plus flexibles avec les données clients, tout en se conformant aux réglementations strictes en vigueur. Une protection de niveau militaire laisse libre cours à l'analyse de données complexes et permet aux banques de comprendre chaque client, comme jamais auparavant.

Une fois établie, cette bonne compréhension fera de la banque un partenaire sur le long terme, ce qui se traduira par une croissance des investissements. La banque pourra également se poser en plaque tournante de la stratégie marketing de n'importe quelle marque, car, au final, les consommateurs ont montré qu'ils souhaitent être les premiers à bénéficier de l'exploitation de leurs données.



Les outils étant conçus pour une meilleure compréhension du client, les banques doivent se montrer plus audacieuses dans leur approche pour rester compétitives, aussi bien en 2022 qu'à plus long terme. Les craintes d'une transgression ne doivent pas les empêcher de saisir les innombrables opportunités qui se présentent à elles.





Collecter, enrichir et agir sur les données client

Tag Management | API Hub | Customer Data Platform and Machine Learning | Data Management

Tealium connecte vos données client web, mobile, offline et objets connectés pour que vous puissiez vous connecter à vos clients. L'écosystème d'intégration clé en main de Tealium supporte plus de 1300 fournisseurs et technologies client-side et server-side permettant aux marques de créer une infrastructure de données client unifiée et en temps réel. Collecter, enrichir et activer vos données clients. L'Universal Data Hub de Tealium comprend la gestion de tags, un API hub, une Customer Data Platform avec machine learning ainsi que des solutions de data management. Les données client ont alors une plus forte valeur, sont plus facilement disponibles et mieux sécurisées. Cela permet en temps-réel aux entreprises de tirer partie des données pour créer des expériences digitales riches et mieux personnalisées avec les différentes équipes, technologies et les multiples points d'interactions client. Plus de 1000 entreprises dans le monde entier font confiance à Tealium pour piloter leur stratégie de données clients.

Pour en savoir plus, veuillez consulter :

tealium.com/fr