Livre Blanc

Les enjeux de la fraude dans le secteur de la Banque Assurance Finance

Sponsorisé par : IBM

Stéphane Krawczyk
février 2017

DANS CE LIVRE BLANC

Le secteur de la Banque Assurance Finance est aujourd'hui confronté à un double enjeu : la nécessaire évolution de ses modèles pour faire face aux nouvelles attentes de ses clients, usagers et affronter un nouveau paysage concurrentiel, et en même temps de se conformer à de nouvelles réglementations qui se sont durcies depuis la crise de 2008. Ces deux enjeux amènent les acteurs de ce secteur à revoir leur gouvernance, à modifier leurs modèles opérationnels mais aussi à redéfinir le rôle qu'ils donnent à la sécurité, notamment dans le cadre de la lutte contre la fraude qu'il s'agisse d'usurpation d'identité, de vol de données personnelles ou encore de fraude aux transactions de paiement. Car en effet, si en France, la fraude sur les transactions par cartes se stabilise à un niveau relativement bas, les interrogations se portent aujourd'hui sur la problématique des transactions hors cartes.

Ce livre blanc abordera en particulier :

- Les priorités en matière d'initiatives de sécurité de ces acteurs en France
- Les principales évolutions réglementaires touchant le secteur
- L'état des lieux des moyens de paiement en Europe et en France
- La présentation des principales évolutions technologiques avec la généralisation des services bancaires en ligne, les paiements mobiles ou encore le développement des API ouvertes
- Les typologies de fraudes auxquelles doivent faire face les acteurs
- Ce que font ces entreprises face à la fraude

Ce livre blanc est basé sur la recherche réalisée en continu par IDC Financial Insights et sur les résultats de l'observatoire Digital Banking 2017 d'IDC France

février 2017, IDC #FR448

INTRODUCTION : LA SECURITE UN ENJEU MAJEUR POUR LE SECTEUR DE LA BANQUE, FINANCE ASSURANCE

Depuis des années, les acteurs de ce secteur réalisent d'importants investissements pour maintenir un degré de sécurité élevé et respecter les évolutions réglementaires.

Le socle de la relation entre les acteurs du secteur de la banque / assurance et leurs clients est la confiance, et il est essentiel de la préserver en mettant en œuvre tous les moyens nécessaires et ce notamment pour la sécurité des transactions de paiement ainsi que la protection des données personnelles.

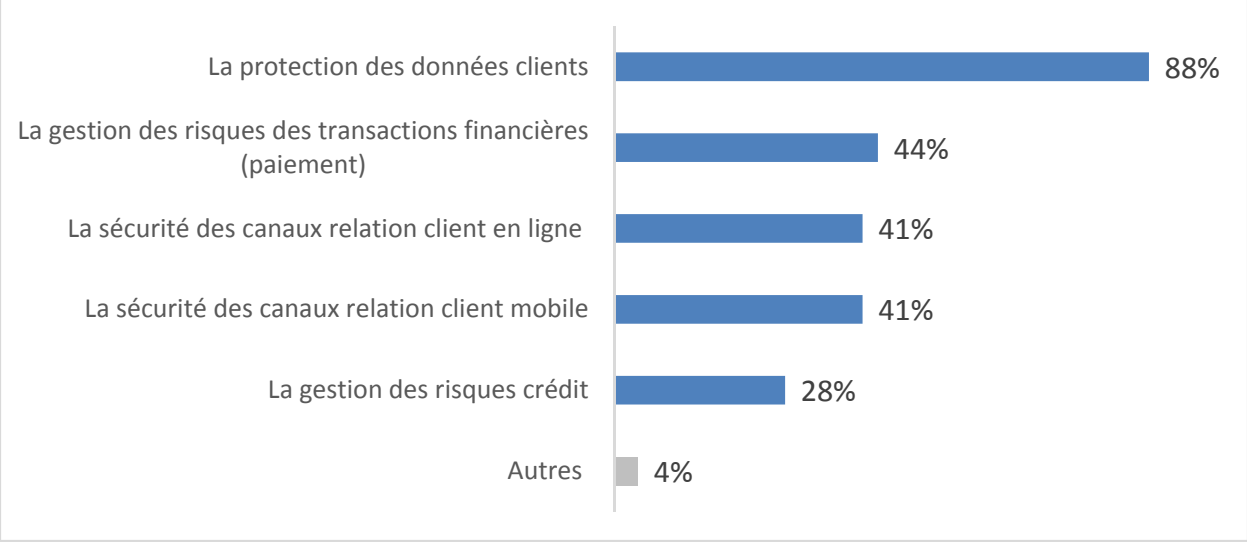
En effet, le développement du commerce en ligne et l'arrivée de nouveaux acteurs sur les services de paiement ne doit pas entamer cette sécurité. Ainsi les banques, avec la digitalisation de leurs services ont développé des systèmes d'authentification à distance de plus en plus sophistiqués tel que 3D Secure (réception d'un code d'authentification par SMS), ou de nouvelles solutions de sécurisation innovantes comme la carte à cryptogramme visuel dynamique.

Lorsque l'on interroge les acteurs sur leurs priorités en matière de sécurité, les résultats de l'observatoire IDC sur le Digital Banking (Cf. Graphique 1) montrent que les initiatives de sécurité prioritaires avant tout sur la **protection des données clients** (88%) suivi par **la gestion des risques de fraude sur les transactions de paiements** (44%) et la sécurisation des canaux de relation client en ligne ou mobile.

GRAPHIQUE 1

Initiatives sécurité : les priorités

Q. Parmi les initiatives de sécurité, lesquelles sont prioritaires pour votre organisation ?



Source : IDC France, Observatoire Digital Banking 2017

METHODOLOGIE

Pour réaliser ce document IDC s'est appuyé sur plusieurs sources parmi lesquelles : Une recherche documentaire auprès d'organismes comme la BCE, la Banque de France, l'ONDRP, l'ACPR, ERPB, l'EPC, l'EBA… Des données publiées par les centre d'expertise d'IDC Financial Insight "IT Spending Guide H2-2016" et "Risk IT Spending Guide H2-2016" (Nov 2016). Les résultats de l'enquête IDC France – Observatoire Digital Banking 2017 (Janvier 2017) menée auprès de 100 Banques et Assurances présentes en France. Des entretiens qualitatifs auprès de quelques grandes Banques et Assurances.

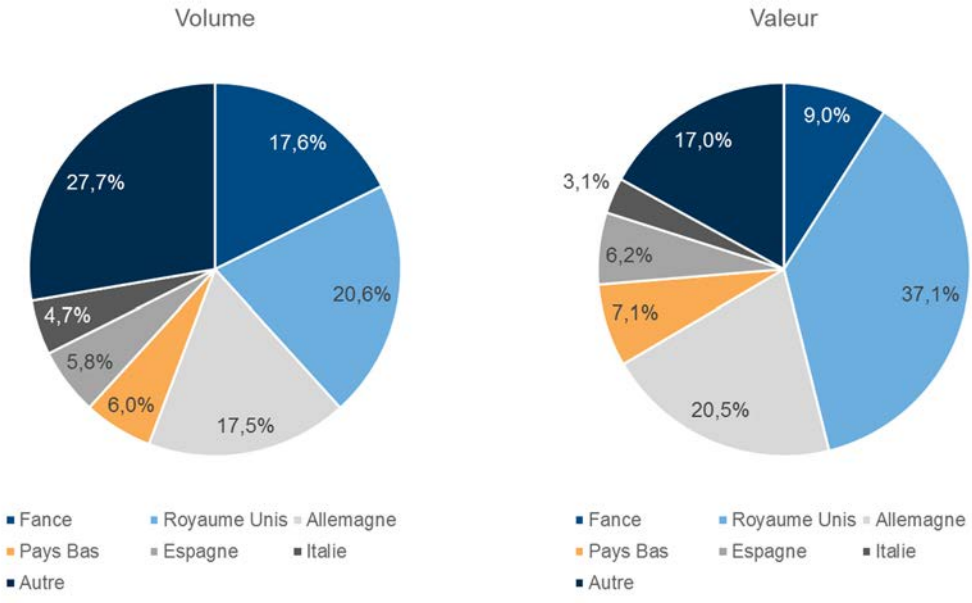
UN ENJEUX DE TAILLE: SE PREMUNIR CONTRE LA FRAUDE AUX TRANSACTIONS DE PAIEMENTS

Les entreprises et les consommateurs bénéficient aujourd'hui en France d'une palette de moyens de paiements diversifiés caractérisés par un niveau de sécurité et continuité opérationnelle élevée, à des coûts relativement limités. La France se caractérise par une utilisation large et croissante des moyens de paiement scripturaux (virements, prélèvements…) +4.4% de croissance en volume en 2015 y compris pour les petits montants.

En 2015, **19,7 milliards de paiements scripturaux** ont été réalisés par les clients des prestataires de services de paiement français pour un montant total de 25 026 milliards d'euros. Ce volume de transactions représente 17,6% des paiements scripturaux réalisés en Europe. Le marché des paiements français est le second marché le plus important en Europe derrière le Royaume Uni (20.6%) et devant l'Allemagne (17.5%). (Cf. Graphique 2)

GRAPHIQUE 2

Transactions de paiement en Europe -Poids des principaux pays



Source : BCE, 2017

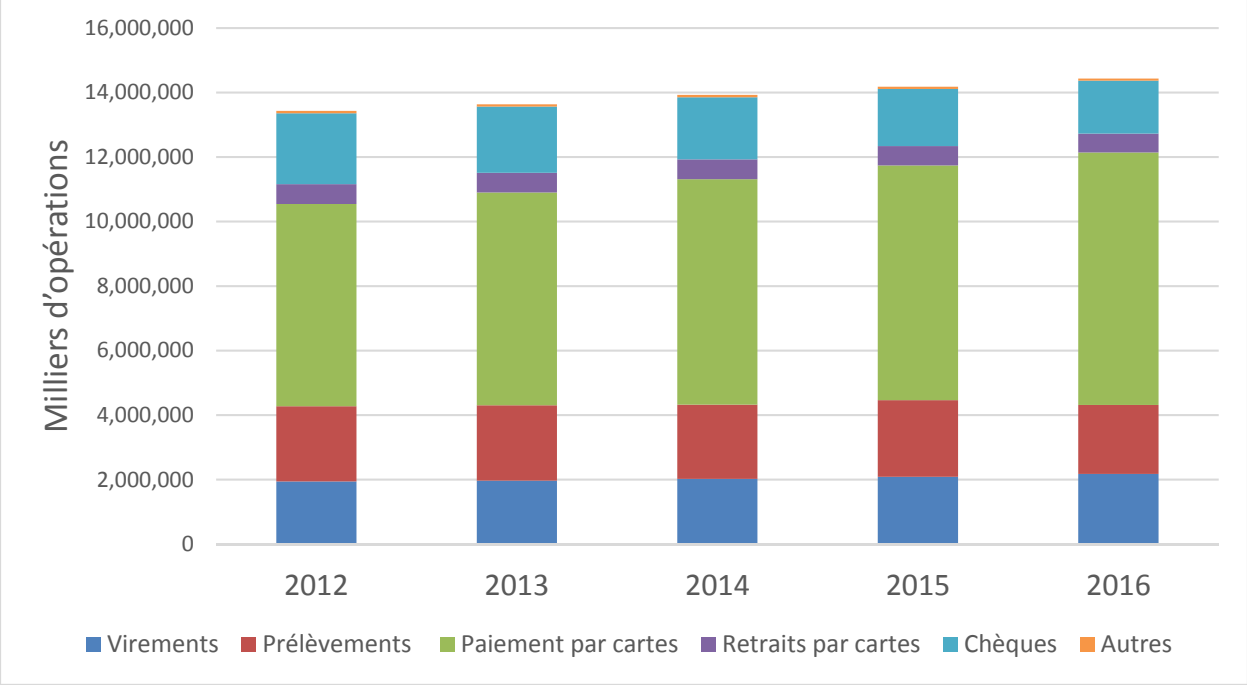
Pour l'année 2015, les transactions du système de paiement de masse (CORE) représentaient 71,7% de l'ensemble des transactions de paiement scripturaux en France.

Les virements et prélèvements représentent 75% de la valeur

Comme le montre le graphique 3, le volume de transactions de paiement de détail en France a atteint en 2016 selon la banque de France, **14.4 milliards de transactions** en croissance de +1.8% par rapport à 2015.

GRAPHIQUE 3

Evolution de la répartition des moyens de paiement système de masse en volume 2012-2016



Source : Banque de France, 2017

Ces données montrent que si les paiements et retraits par cartes concentrent la plus grande part du volume de transactions pour l'année 2016 (58%), les virements et les prélèvements regroupent 30% de ce volume.

Cependant lorsque l'on s'intéresse à la fraude sur les transactions de paiement il est particulièrement important de regarder la répartition de ces transactions en valeur.

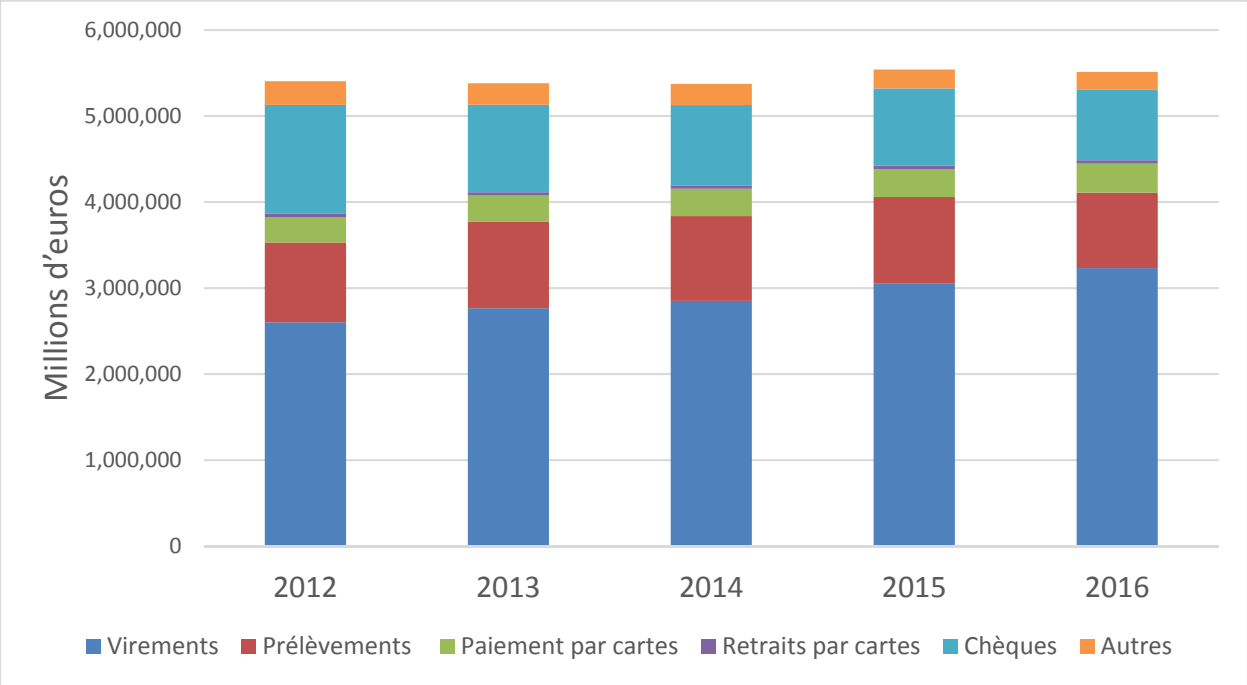
En effet, comme le montre le graphique 4, le volume de transactions de paiement de détail en France a atteint en 2016, une valeur de **5 506 milliards d'euros** en progressions de +0.5% sur la période 2012-2016.

Au-delà de cette valeur et de cette tendance, c'est avant tout le poids que représentent ces divers moyens de paiement sur la totalité de la valeur de ces transactions sur lequel il convient de se focaliser. En effet, les **virements et prélèvements regroupent 75% de la valeur des transactions** pour l'année 2016

alors que les paiements et retraits par cartes ne représentent que 7% de cette valeur. D'ailleurs, les données publiées dans le rapport annuel 2015 de l'observatoire de la sécurité des cartes de paiement, confirment la poursuite du repli de la fraude domestique sur les paiements par carte, amorcé l'année précédente, y compris sur les paiements à distance qui restent toutefois significativement plus exposés à la fraude. En revanche, la fraude transfrontière, qu'il s'agisse de paiements de proximité ou à distance, est en hausse. Le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2015 s'élève à 868 400, en baisse de 4,1 % par rapport à 2014. En incluant également les transactions réalisées en France avec des cartes émises dans d'autres pays, **le montant total de la fraude s'élève à 522,7 millions d'euros en 2015,** en augmentation de 4,4 % par rapport à 2014, pour un montant total des transactions qui atteint 636,1 milliards d'euros, en augmentation de 1,8 %. Compte tenu de ces éléments, le taux de fraude global sur les transactions traitées dans les systèmes français, comprenant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises et les paiements et les retraits réalisés en France avec des cartes étrangères, augmente légèrement à 0,082 %. L**e montant moyen d'une transaction frauduleuse est resté stable, à 113 euros,** contre 112 euros en 2014. On comprend alors facilement l'enjeu financier que représente la fraude potentielle associée aux transactions de paiements (hors cartes) en France.

GRAPHIQUE 4

Evolution de la répartition des moyens de paiement système de masse en valeur 2012-2016



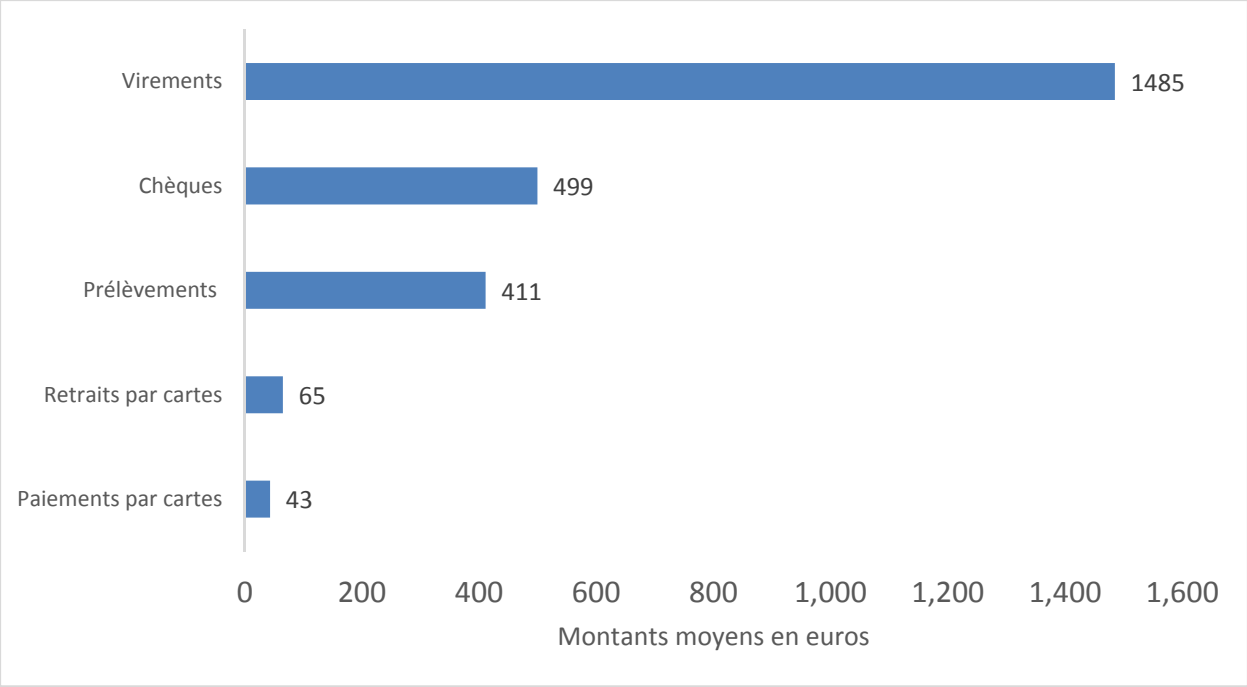
Source : Banque de France, 2017

L'intérêt des fraudeurs pour les transactions de paiement hors cartes est encore plus flagrant si l'on regarde la valeur des montants moyens par typologie de transactions pour l'année 2016 (Cf. Graphique 5). Les virements arrivent largement en tête avec un montant moyen de 1 485 euros en moyenne par

transactions suivi des chèques avec 499 euros et des prélèvements 411 euros. Les montants moyens des retraits et paiements par cartes sont largement inférieurs avec respectivement des montants moyens de 65 et 43 euros en moyenne par transactions.

GRAPHIQUE 5

Montants moyens par types de transaction en 2016



Source : Banque de France, 2017

Instant Payment : Quel impact pour les banques en matière de fraude ?

L'instant payment ou paiement instantané est défini par l'Euro Retail Payments Board (ERPB) comme « solution de paiement électronique disponible 24/7/365, résultant d'une compensation interbancaire immédiate ou quasi immédiate de l'opération et du crédit du compte du bénéficiaire avec une demande de confirmation au payeur », et devrait être mise en place en France d'ici fin 2017.

Certains acteurs européens ont déjà adopté ce nouvel instrument de paiement. Les exemples les plus courant en matière d'Instant payment sont :

- Le Faster Payment Services du Royaume-Uni, mise en place en 2008,
- L'application Swish en Suède (2012.) Grâce à son smartphone, les consommateurs peuvent effectuer de manière instantanée un virement ou bien un achat. Cette dématérialisation représente, bien évidemment une réelle menace pour les banques traditionnelles.

L'instant payment a été mis en place dans le but de réduire les contraintes liées à la monnaie physique (dépôt de la monnaie à la banque par le commerçant, développement d'économies souterraines, et circulation de chèques et d'espèces couteux pour les banques…). L'instant payment permet d'effectuer des virements de compte à compte en 10 secondes, alors qu'actuellement, en France, un virement prend 2 jours pour être pris en compte.

Dans un contexte de forte croissance des paiements en ligne, les fraudes commencent à s'installer sur ce canal et l'instant payment soulève des problématiques liées à la gestion des données des utilisateurs. De plus, la notion d'instantanéité devrait avoir un effet sur la non récupération des montants de la fraude touchant ce type de transactions.

ENVIRONNEMENT REGLEMENTAIRE, PAIEMENT MOBILE, SERVICES BANCAIRES EN LIGNE: DE NOUVEAUX RISQUES DE FRAUDE POUR LE SECTEUR BANQUE, ASSURANCE, FINANCE

Digitalisation et décentralisation un vecteur de risque pour les banques

Il y a encore quelques années les services bancaires étaient fortement centralisés et opérés par le conseiller en agence. Aujourd'hui chaque utilisateur devient son propre agent.

Ce phénomène de digitalisation des services bancaires élargit considérablement le champ des possibles des cybercriminels et au regard des montants moyens par type de transactions présentés dans la section précédente de ce document on comprend pourquoi l'ensemble de l'écosystème de la chaîne des paiements se mobilise pour lutter contre la fraude.

Au regard des multiples annonces, la fermeture d'agences bancaires semble aujourd'hui être un phénomène inéluctable qui concerne la plupart des banques françaises.

Les raisons de ce mouvement sont multiples. Tout d'abord l'évolution du comportement des clients : la digitalisation des services bancaires provoque une baisse de la fréquentation des agences physiques, alors même que le nombre de contacts augmente, via les mails, les applis, etc. Selon l'Observatoire de l'image des banques 2015, 21 % des personnes interrogées fréquentent leurs agences plusieurs fois par mois, contre 52 % en 2010.

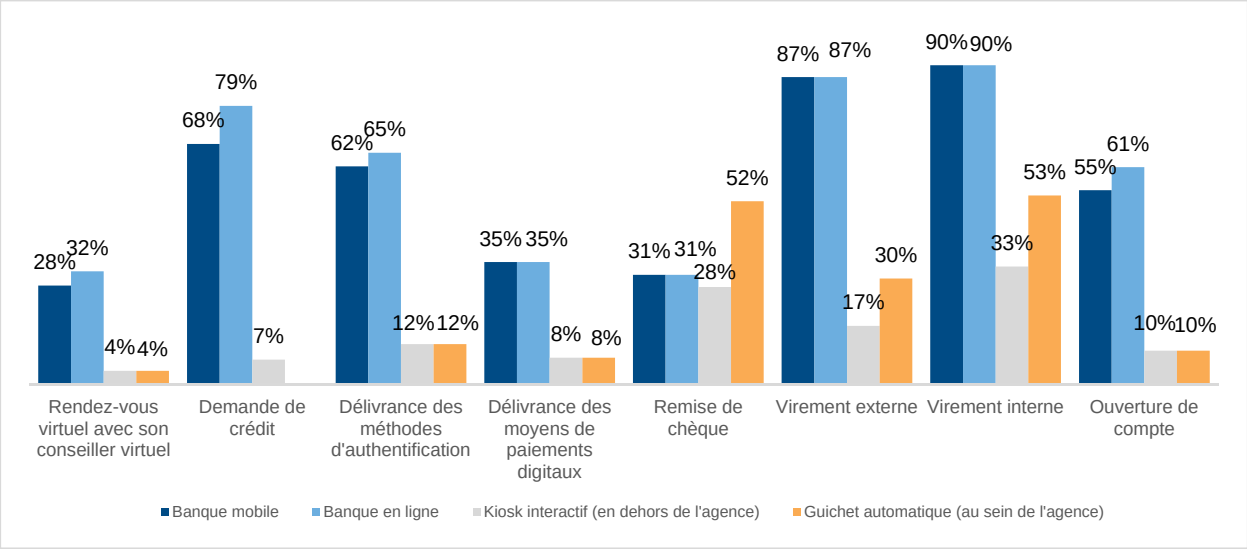
Ensuite, la pression sur les marges des banques, liée aux taux bas et au contexte déflationniste, oblige les établissements à s'appliquer ce qu'ils suggèrent à leurs clients entreprises : à savoir la baisse de leur structure de charge. Ainsi, ces fermetures, un temps déniées, sont désormais, pour les banques cotées, un levier de communication positif en direction des marchés boursiers.

Dans le cadre de son observatoire Digital Banking 2017, IDC a notamment interrogé les établissements bancaires et financiers pour identifier ce qu'ils prévoyaient à court terme comme alternatives aux agences bancaires pour diverses opérations (cf. Graphique 6)

GRAPHIQUE 6

Quelles alternatives aux agences bancaires?

Q . Prévoyez-vous à court terme des alternatives aux agences bancaires pour les opérations suivantes



Source : IDC France, Observatoire Digital Banking, 2017

Sans surprise, les résultats montrent que 90% des établissements interrogés prévoient de proposer à leurs clients la possibilité d'effectuer des virements internes via des services de banque en ligne ou de banque mobile, et tout de même **87% pour ce qui concerne les virements externes.** Plus surprenant, la banque mobile pour 62% ou banque en ligne pour 65% sont une alternative pour la délivrance de méthodes d'authentification. Enfin, pour 35% des établissements interrogés, la banque mobile ou la banque en ligne constitue une alternative pour la délivrance des moyens de paiement digitaux.

Sécuriser les paiements mobiles pour éviter le piratage de données personnelles

L'adoption de paiements mobiles a quelque peu sous-performé les attentes ces dernières années, mais commence à prendre considérablement de la vitesse, soutenu en grande partie par l'entrée d'Apple avec son Apple Pay en Juillet 2016. Pour rappel, l'Apple Pay est un service intégré à iOS8 qui combine technologie NFC (Near Field Communication) et biométrie pour permettre aux porteurs de certains produits Apple (les smartphones depuis l'iPhone 6 et iPhone 6 plus, et la montre connectée Apple Watch, ainsi que les iPads à partir de l'iPad Air 2 pour les achats en ligne) de payer d'un seul geste aussi bien en ligne qu'en magasin.

Porté par les technologies Near Field Communication (NFC), Host Card Emulation (HCE), ou encore puce microSD, le mobile payment entre significativement dans le paysage des nouveaux moyens de paiement.

De nombreux acteurs se positionnent sur ce marché : Samsung a annoncé son Samsung Pay et Google son Android Pay. En France, certaines banques proposent déjà une offre compatible NFC (comme Kix chez BNP Paribas) ou d'autres acteurs, comme Orange Cash, SMoney ou Lydia. Cela, sans compter l'arrivée des autres GAFA qui représente une réelle menace pour les banques, de par leurs solides

capacités financières mais aussi pour ses ressources en données consolidées par leur interface respective.

Toutefois, malgré l'aspect innovant de ce moyen de paiement, le principal frein souligné est celui du risque élevé de piratage de données personnelles susceptible de générer des transactions de paiement frauduleuses.

DSP2 - Une véritable opportunité pour les banques

La DSP2, ou Révision de la Directive sur les Services de Paiement suit la directive initiale des services de paiement adopté fin 2007. Depuis DSP1, le marché des paiements de détail a connu une innovation technique significative : le nombre de paiements électroniques et mobiles a augmenté rapidement, et de nouveaux types de services de paiement ont vu le jour, entrainant de nouvelles habitudes d'achat chez les consommateurs. En conséquence, le marché a développé des moyens qui se sont avérés difficiles à intégrer d'un point de vue réglementaire.

La DSP2 a ainsi pour objectif majeur d'harmoniser les services de paiements de l'Union Européenne et de stimuler la concurrence. Un nouveau statut d'Établissement de Paiement (EP) a été créé. Il permet à de nouveaux acteurs autres que les banques et les établissements de crédit de fournir des services de paiement.

L'entrée en vigueur en janvier 2018 de la directive européenne va, sans aucun doute, provoquer une transformation en profondeur des relations des banques de détail avec leurs clients.

Les apports de la DSP 2 sont également importants pour la sécurité : elle crée des obligations en matière de gestion des risques opérationnels et de sécurité, elle met en place une procédure de **notification des incidents** et elle systématise **l'authentification forte du client**.

La réglementation DSP2 contient en effet des règles strictes sur l'authentification des utilisateurs de services de paiement pour veiller à ce que les prestataires de services de paiement soient certains que les gens qui utilisent leurs services sont bien ceux qu'ils prétendent être.

Les prestataires de services de paiement tiers qui initient les opérations de paiement sont également tenus de veiller à ce qu'ils appliquent l'authentification client forte. Les PSP tiers fournissant des services d'initiation de paiement ou informations de compte sont tenus de s'authentifier auprès du PSP du propriétaire du compte.

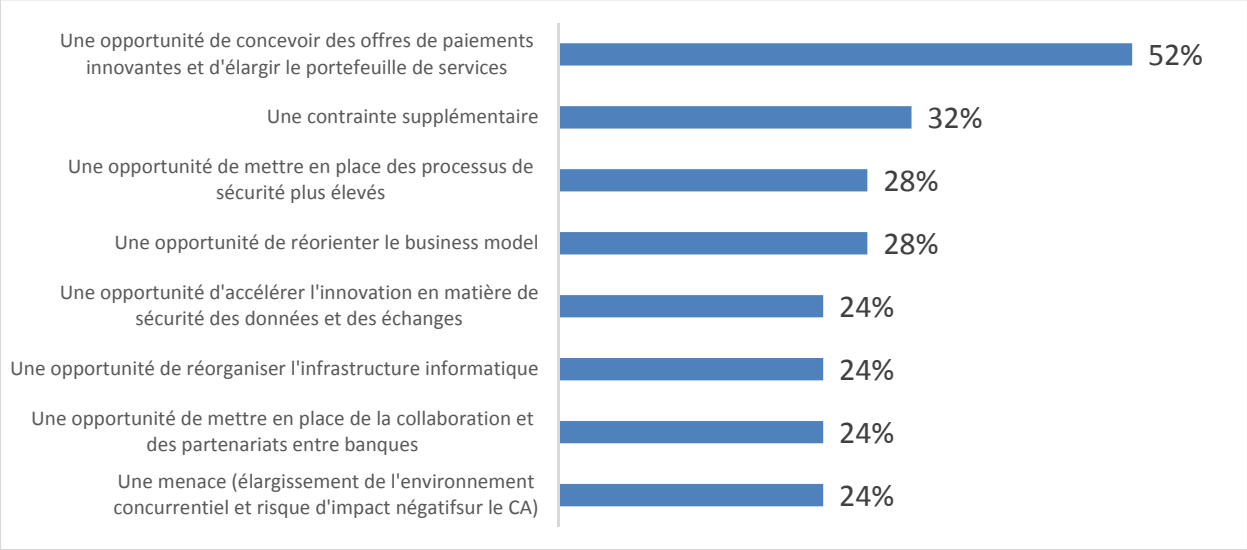
Le PSP devrait appliquer l'authentification client forte lorsque les payeurs accèdent à leurs comptes de paiement en ligne, lancent une transaction de paiement électronique à distance, ou d'effectuent une action à travers un canal à distance, ce qui peut impliquer un risque de fraude de paiement voir d'autres abus. Le PSP devra également veiller à ce que l'authentification comprenne des éléments reliant dynamiquement la transaction à un montant spécifique et à un bénéficiaire spécifique Ces exigences supplémentaires sont également applicables aux cas où les paiements sont initiés par les prestataires de services d'initiation de paiement (PISP).

Lorsque l'on interroge les banques sur la manière dont elles perçoivent cette nouvelle directive (cf graphique 7), pour plus de la moitié d'entre elles (52%) il s'agit d'une **opportunité pour concevoir des offres de paiement innovantes et d'élargir leurs offres de services**.

GRAPHIQUE 7

Perception de DSP2

Q. Comment percevez-vous la DSP2 (Directive sur les Services de Paiement 2) qui facilite l'utilisation des services de paiement électronique sur internet et qui impose d'ouvrir le SI des banques à des tiers ?



Source : IDC France, Observatoire Digital Banking 2017

Bien que près d'un tiers considèrent cette directive comme une contrainte supplémentaire, pour 28% c'est également **une opportunité pour renforcer la sécurité** par la mise en place de processus de sécurité plus élevés et pour 24% il s'agit d'une **opportunité pour accélérer l'innovation en matière de sécurité des données et des échanges**. Enfin, seul 24% perçoivent cette directive comme une menace du à l'élargissement de l'environnement concurrentiel avec le risque d'avoir un impact négatif sur leur activité.

La révision de la directive sur les services de paiement (DSP 2) de la Commission européenne, marque ainsi une première étape importante dans le renforcement de la sécurisation des paiements au niveau des établissements financiers. Avec la DSP 2, les établissements financiers n'auront d'autre choix que de mettre en place une stratégie de sécurité à la fois évolutive et rentable, mais suffisamment robuste pour assurer une transmission parfaitement sûre des données.

Vers le déploiement d'API ouvertes

La notion d'API (Application Programming Interface) a déjà largement fait son apparition avant même la mise en œuvre de la DSP2. Même si le texte de la directive ne mentionne pas la notion d'API en tant que telle et que l'EBA se contente de lister des exigences techniques, les APIs apparaissent comme la solution la plus adéquate pour prendre en compte l'ensemble des exigences mentionnées par la DSP2.

Les API Ouvertes (Open API) exigent de la part du fournisseur de services de paiement Tiers (PSP Tiers) d'accepter les termes et conditions d'utilisation et nécessitent un processus de garantie et de sécurité via un enrôlement d'authentification. L'inscription est nécessaire pour utiliser ce service. Dans le cadre fourni par la DSP2, les Open API sont celles qui correspondent le mieux aux attentes concernant le recours à des interfaces dédiées, car elles permettent au prestataire de services "services de paiement gestionnaire de compte" (ASPSP) de contrôler les utilisateurs qui se connecteront afin de

venir récupérer des données Par analogie, on peut comparer une API ouverte à un objet dans une boite en verre trempé : on peut voir l'objet, on peut secouer cette boite, mais on ne peut pas le toucher. L'API apparait comme le point critique en termes de sécurité dans la mesure où le PSP tiers, au travers de celle-ci, va directement interroger le SI des ASPSPs. De plus, avec l'Open API, l'enrôlement d'authentification est obligatoire, ce qui limite encore davantage le risque. L'enrôlement d'authentification n'est pas un protocole d'authentification, mais un protocole de délégation d'autorisation, ainsi il permet d'autoriser une application à utiliser une API sécurisée pour le compte d'un utilisateur. Il s'agira donc d'une couche de sécurité supplémentaire en plus de celle représentée par l'authentification forte.

Pour résumer, on constate que de la directive va entièrement bouleverser les relations entre les acteurs tant en matière juridique que technique. L'impact majeur de ces innovations concerne aujourd'hui les services bancaires proposés par les nouveaux entrants.

Evolutions concernant les données à caractère personnel : le cas de la santé et de l'assurance

Les données à caractère personnel dites sensibles recouvrent, selon l'article 8 de la loi « Informatique et Libertés », cinq catégories distinctes auxquelles appartiennent les données de santé.

- Art. 2 de la loi Informatique et Libertés : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».
- Art. L.1111-8 du Code de la santé publique : « Données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins » inséré par la loi n° 2002-303 du 4 mars 2002, dite loi « Kouchner ».

Toutefois, la définition proposée dans le cadre du règlement européen sur la protection des données personnelles apporte certaines précisions : « Toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ». D'un périmètre plus large dans son champ d'application, cette définition englobe les informations relatives à l'existence d'interactions entre les acteurs de santé et les individus, indépendamment des données effectivement recueillies et/ou produites lors de ces mêmes interactions.

Parallèlement tout candidat à l'agrément hébergeur de donnée santé doit apporter des garanties quant à sa capacité à respecter les obligations du décret (décret n° 2006-6 du 4 janvier 2006). A cette fin, il lui est demandé de couvrir chacun des articles par au moins une règle, engagement et/ou disposition de sécurité. A savoir :

- Le traitement doit être réalisé conformément à la loi « Informatique et libertés » et en adéquation avec l'agrément ministériel délivré ;
- L'hébergeur doit (sans se substituer au responsable du traitement des données hébergées) :
  - Apporter des garanties en matière de sécurité, d'archivage, de protection, de conservation et de restitution des données,
  - Définir une politique de confidentialité et de sécurité,
  - S'assurer de l'information des personnes à l'origine du dépôt.
- L'hébergeur est soumis au secret professionnel ;

- La présence d'un médecin régulièrement inscrit au Tableau de l'Ordre des Médecins est obligatoire dans l'organisation candidate à l'agrément.
- Les données ne peuvent être utilisées à d'autres fins que celles définies dans le contrat d'hébergement ;
- Lorsqu'il est mis fin à l'hébergement (notamment lorsque l'agrément arrive à expiration),
- L'hébergeur restitue les données qui lui ont été confiées sans en garder de copie.

Jusqu'ici, les données de santé n'étaient pas disponibles pour les assureurs. Mais un nouvel arrêté ministériel change la donne.

Un arrêté du ministère de la Santé empêchait jusqu'à aujourd'hui l'accès aux informations personnelles des patients pour les organismes à but lucratif. Ces données, enregistrées dans le Système national d'information inter-régimes de l'Assurance maladie, le SNIIRAM, étaient accessibles uniquement aux organismes de recherche publiques. Il s'agit en effet d'un nombre conséquent de données puisque l'on parle de 1,2 milliard de feuilles de soins et de 500 millions d'actes médicaux mais aussi de 11 millions de séjours hospitaliers. Toutes ces informations permettent d'aider la recherche à réaliser des analyses plus poussées basées sur des faits et non des conjectures.

Suite à l'annulation de l'arrêté ministériel par le Conseil d'Etat, qui l'a jugé illégal, ces données à caractère personnel peuvent aujourd'hui être consultées par les assureurs, sous certaines conditions. En effet, l'accès à ces données sera possible pour toute structure souhaitant conduire une étude d'intérêt général validée au préalable par l'Institut national des données de santé et d'autres acteurs du secteur (représentants de l'Etat, d'usagers de l'Assurance Maladie, etc). La CNIL sera également concertée pour s'assurer du respect de la vie privée, une fois que le protocole scientifique de l'étude aura été approuvé par un comité scientifique supplémentaire. Cependant, la loi Santé interdit d'utiliser ces données pour promouvoir des produits. De même, les compagnies de mutuelle santé ne pourront pas réaliser des modifications de contrat en fonction des informations recueillies.

Bien que l'analyse des données personnelles de santé par les assureurs, pourrait permettre d'améliorer la surveillance de la sécurité sanitaire, de proposer une meilleure offre de soins, une meilleure évaluation des politiques de santé ou encore une étude plus efficace des maladies et de leurs traitements, pour IDC, l'accès à ce type de données sensibles amènera nécessairement les acteurs à renforcer leurs solutions de d'authentification et de traçabilité pour être en parfaite légalité.

LUTTER CONTRE LA FRAUDE ET L'USURPATION DES DONNEES PERSONNEL : UNE PRIORITE

La fraude en entreprise a plusieurs visages. C'est un phénomène dont les préjudices financiers, juridiques ou d'image ne sont plus à démontrer. Cybercriminalité, ingénierie sociale, piratage informatique, blanchiment d'argent, fraude aux moyens de paiement, fraude à la carte bancaire, détournement d'actifs, corruption sont les principaux types de fraudes auxquels les entreprises doivent faire face. Avec le développement des nouvelles technologies et la révolution numérique, la cybercriminalité ne cesse d'augmenter. La lutte contre la cybercriminalité constitue un enjeu considérable pour les entreprises. Elles doivent désormais être capables d'identifier précisément les risques et d'avoir une stratégie anti-cybercriminalité.

Le cybercrime est un phénomène complexe, regroupant des méthodes (virus, malware, spyware, hameçonnage, keylogger…), des cibles et des motivations variées, La cybercriminalité correspond à tout

acte criminel perpétré au moyen d'un ordinateur ou d'un système informatique, généralement connecté à un réseau. Selon sa forme et ses contenus, trois types d'infraction cybercriminelles sont identifiés :

- Les infractions qui menacent l'intégrité des données, incluant le piratage : atteintes aux systèmes de traitement automatisé de données, traitements non autorisés de données personnelles, infractions aux cartes bancaires…
- Les infractions utilisant les contenus des systèmes d'information : pédopornographie, incitation au terrorisme et à la haine raciale sur internet…
- Les infractions facilitées par les technologies de l'information et de la communication : escroqueries en ligne, blanchiment d'argent, fraude en ligne…

La fraude aux moyens de paiement

Faux ordre de virement, fraude aux coordonnées bancaires, fraude au président, fraude à la carte bancaire… la fraude aux moyens de paiement explose en France et à l'international.

Plusieurs centaines de millions d'euros sont détournées chaque année. En janvier 2016 le ministère de l'intérieur publiait un communiqué stipulant que depuis l'apparition de ce nouveau type d'escroquerie en 2010, plusieurs milliers de faits ou de tentatives ont été recensées pour un **préjudice global de 485 millions d'euros** Les montants annoncés ne représentent cependant que la partie visible de l'iceberg, les entreprises touchées ne communiquant que rarement sur les fraudes dont elles sont victimes. Beaucoup d'entreprises n'osent pas déposer plaintes par peur de mauvaise publicité.

De l'autre côté de l'Atlantique en Avril 2016, La police fédérale américaine s'inquiétait de l'accroissement spectaculaire de cette « fraude au président ", qui aurait coûté selon elle **2,3 milliards de dollars aux entreprises entre octobre 2013 et février 2016.** Le FBI se base sur des plaintes reçues aux Etats-Unis et dans au moins 79 pays du monde, déposées auprès des forces de l'ordre par 17.642 entreprises (de toutes tailles et de toutes sortes) victimes de cette escroquerie. Depuis janvier 2015, le FBI a constaté une augmentation de **270% du nombre de victimes identifiées**.

Les fraudes aux moyens de paiement les plus connues

La "**Fraude au président**" consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.

Le "**Changement de RIB**" consiste pour les fraudeurs à envoyer un mail à un salarié du service de comptabilité ou trésorerie de l'entreprise en se faisant passer pour un fournisseur, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs

Les «**faux fournisseurs**»: l'information est communiquée par téléphone ou par e-mail: le faux fournisseur indique avoir changé de coordonnées bancaires et communique sur quel compte il faudra désormais régler les factures.

Typologie des fraudes les plus récurrentes

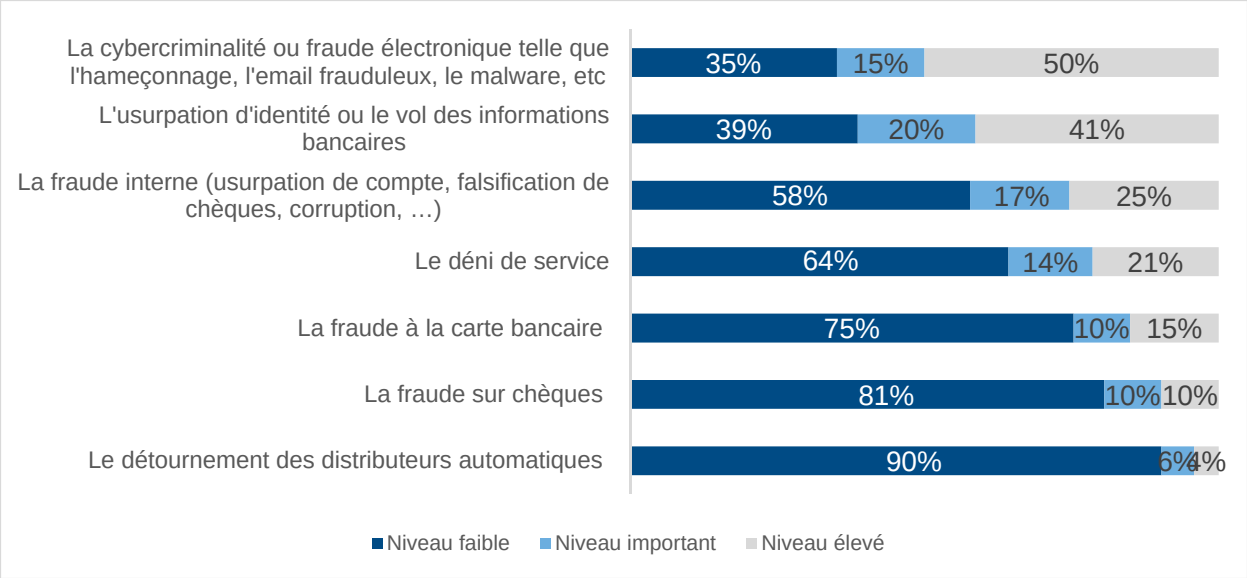
Dans le cadre de l'observatoire Digital Banking 2017, IDC a interrogé les institutions bancaires et financières sur le type de fraude auxquelles les clients ou elles-mêmes étaient le plus confrontés. Les résultats présentés graphique 8 montrent que les trois principaux types de fraudes étaient : **la cybercriminalité**, **l'usurpation d'identité ou le vol d'information bancaires** et **la fraude interne**.

En effet près de 65% des institutions interrogées considèrent que la fraude issue de la **cybercriminalité ou de la fraude électronique** (hameçonnage, emails frauduleux, malware…) est aujourd'hui en France à un niveau important ou élevé.

GRAPHIQUE 8

Typologie des fraudes les plus récurrentes

Q. Quelles sont les fraudes auxquelles votre entreprise / vos clients sont le plus confrontés ?



Source : IDC France Observatoire Digital Banking 2017

L'usurpation d'identité ou le vol d'informations bancaires arrive en seconde position avec 61% des institutions interrogées considérant être confronté à un niveau important ou élevé vis-à-vis de ce type de fraudes. En effet, le vol de données personnelles permet non seulement aux cybercriminels de frauder sur les divers canaux par lesquels sont proposés les services (call center, cartes bancaires…) mais également de revendre ces informations sur le "Dark Web". Enfin, **la fraude interne** (falsification de chèques, corruption…) représente le troisième type de fraude auxquelles les différentes institutions interrogées sont le plus confrontées.

Au regard de ces résultats et de l'évolution de l'écosystème d'acteurs du secteur de la Banque, Finance, Assurance, dans les années à venir les efforts porteront avant tout sur la lutte contre ces trois principaux types de fraude.

QUE FONT LES ENTREPRISES FACE A LA FRAUDE ?

La fraude est généralement incluse dans le domaine plus large des risques opérationnel. Pour pouvoir identifier et maîtriser ces risques, il est nécessaire de définir ce qu'est un risque opérationnel. Il est généralement défini comme « le risque de perte résultant d'erreurs humaines, de systèmes ou processus internes défaillants, ou des évènements externes ». Le risque opérationnel est donc un risque subi par l'entreprise. Il est parfois diffus et difficile à appréhender de par la multitude de formes qu'il peut prendre.

Dépenses des banques assurances et autres acteurs du secteur de la finance dans les technologies de lutte contre la fraude en Europe

IDC dispose d'une expertise sectorielle aux seins des Insights. Selon les dernières évaluations de marché publiées par IDC Financial Insights, les banques assurances et autres institutions du marché des capitaux en Europe ont dépensé **16,1 milliards d'euros en 2016 pour gérer les risques opérationnels**. Ce montant représente 86% des dépenses IT dans la gestion des risques chez ces acteurs. Cette dépense devrait progresser de +6,6% en moyenne par an sur la période 2016-2020 pour atteindre 20,9 milliards d'euros à cette échéance. Cependant la part des dépenses attribuée aux risques opérationnels dans la dépense IT varie en fonction de la typologie des acteurs. Si les Banques et les institutions du marché des capitaux dépensent respectivement 15% et 14%, le poids dédié pour gérer les risques opérationnels des assurances est largement inférieur et ne représente que 5% de la dépense IT.

Au sein de la dépense IT pour faire face aux risques, **la gestion de la fraude représente en 2016, 7,2%** soit **1,4 milliards d'euros.** Sur ce segment IDC prévoit une croissance annuelle moyenne de +6,9% sur la période 2016-2020. A titre de comparaison, les dépenses associées au contrôle et à la conformité représentent 20% de la dépense IT pour faire face aux risques. Soit près de trois fois plus.

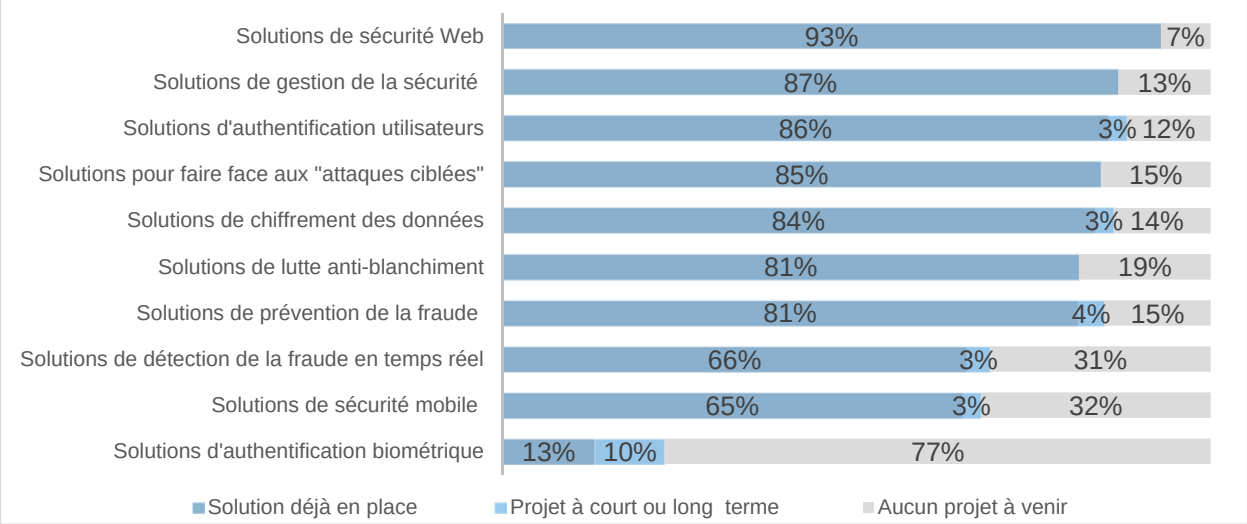
Solutions de sécurité misent en place pour lutter contre les fraudes

Lorsque l'on interroge les banques et les assurances sur le type de solutions mises en place pour lutter contre la fraude (Cf. graphique 9), le premier constat est qu'il ne semble pas y avoir de solution miracle unique.

GRAPHIQUE 9

Les Solutions de sécurité misent en place contre les fraudes

Q. Parmi les solutions suivantes de sécurité et de lutte contre la Fraude, quelles sont celles que vous avez vous mises en place ou que vous prévoyez de mettre en place ?



Source : IDC France, Observatoire Digital Banking 2017

En effet, les résultats de l'observatoire Digital Banking montrent des taux d'équipement élevés que ce soit les solutions de sécurité web, solutions d'authentification des utilisateurs, solutions de chiffrement, solutions de lutte anti-blanchiment ou encore de solutions de prévention de la fraude.

Les solutions de détection de la fraude en temps réel ou les solutions de sécurité mobile sont légèrement en retrait.

Enfin les projets à court ou long terme portent principalement sur les **solutions d'authentification biométriques.**

Apport des technologies analytiques et du Big Data

En interrogeant les banques et assurances françaises sur l'usage qu'elles ont des technologies Big data/ analytiques, il ressort des résultats de l'observatoire que les principaux usages portent sur des éléments qui touche avant tout les clients. En effet, optimiser la qualité de la relation client, améliorer la compréhension des clients ou mener des campagnes de marketing ciblés sont les principaux cas d'usages qui ressortent en priorité.

Cependant, au-delà de ces résultats, il est particulièrement intéressant de remarquer que **34% des institutions interrogées envisagent d'utiliser l'analytique pour détecter la fraude et limiter les risques.** Ceci laisse déjà présager de l'évolution des solutions de lutte contre la fraude qui corrèleront des solutions d'analyse comportementale avec des solutions d'analyse de l'historique des transactions.

CONCLUSION

Face à la généralisation des services en ligne, au développement des services mobiles et aux évolutions réglementaires, les acteurs de la banque et de l'assurance doivent sans cesse évoluer afin de s'adapter à ces changements ainsi qu'à l'évolution de la fraude qui en découle usurpation d'identité, fraude aux transactions de paiement, vol de données personnelles…

En effet, si le vol de données personnelles ou la fraude aux transactions de paiement par cartes ont fréquemment fait partie de l'actualité de ces dernières années en matière de fraude, l'activité des cybercriminels se déplace aujourd'hui vers la fraude aux transactions de paiements hors cartes (faux ordre de virement, fraude au président, changement de RIB…), le vol d'information bancaire ou de données personnelles pour être revendues sur le "Dark Web".

En ce qui concerne les transactions de paiement, la valeur des virements pour l'année 2016 représente 9,6 fois la valeur des paiements par cartes alors que le volume de transactions de ces derniers est 3,6 fois supérieur. Attiré par la possibilité de décupler leurs gains, on comprend alors aisément les raisons qui amènent les cybercriminels à déplacer leur attention sur ce type de transactions de paiement. Parallèlement, les évolutions technologiques comme le paiement mobile ou la notion d'open API, élargissent toujours plus les possibilités d'attaques.

Dans ce contexte, la technologie Blockchain actuellement testée par certaines banques pour par exemple réaliser de manière quasi-instantanée des virements internationaux multi-devises devrait prendre de l'ampleur dans les années à venir. Cette technologie garantit une traçabilité complète et une visibilité totale de l'opération dès l'origine. Il n'y a donc plus recours aux banques correspondantes de façon séquentielle mais envoi direct entre donneur d'ordre et bénéficiaire tout en synchronisant le transfert de liquidité interbancaire. Cependant, les premiers démonstrateurs ont volontairement évacué certains sujets réglementaires, sécuritaires ou liés au données personnelles. La technologie étant

encore relativement jeune nous sommes encore loin d'une industrialisation qui devrait néanmoins se faire à moyen terme.

Enfin, au regard des principales évolutions réglementaires (DSP2, protection des données personnelles), et de l'émergence de nouveaux acteurs sur le marché des paiements, **les solutions d'identification des utilisateurs,** s'appuyant sur des technologies big data, cognitives ou d'analyses comportementales **seront le point d'entrée pour garantir la sécurité de toutes les activités financières des différents acteurs en améliorant la détection la fraude et limiter les risques**. C'est en tout cas ce que pensent 75% des organisations interrogées dans le cadre de l'observatoire Digital Banking 2017 d'IDC France.

LEXIQUE

EBA (European Banking Authority ou Autorité Bancaire Européenne) : autorité indépendante de l'Union Européenne qui oeuvre afin de garantir un niveau de règlementation et de surveillance prudentielle efficace et cohérent dans l'ensemble du secteur bancaire européen.

RTS (Regulatory Technical Standards ou Standards Techniques) : ensemble des standards techniques préparés par l'Autorité Bancaire Européenne en collaboration avec la BCE (Banque Centrale Européenne) et les banques centrales nationales. Ces standards techniques sont discutés avec l'ensemble des parties prenantes au travers des « discussions papers ». Ils portent essentiellement sur l'authentification forte et les moyens de communication sécurisés, afin de permettre la mise en oeuvre opérationnelle de la directive. Ces standards seront soumis à la Commission Européenne en 2017 pour application règlementaire.

Open-Banking : concept actuellement en cours d'élaboration autour de l'évolution de la banque. L'Open-Banking est fondé sur le principe de la transparence bancaire ; il prône le recours aux Open APIs afin de permettre à des tiers d'accéder aux informations dans le but de développer leurs propres applications.

PSU (Payment Service User ou Utilisateur d'un service de paiement) : utilisateur particulier ou professionnel possédant un ou plusieurs comptes bancaires et/ou utilisateur d'un service de paiement.

ASPSP (Account Servicing Payment Service Provider ou Prestataire de services services de paiement gestionnaires de comptes) : prestataire au sein duquel un client (PSU), détient un ou plusieurs comptes et/ou au sein duquel le PSU initie des paiements. Chaque ASPSP doit posséder le statut d'Établissement de Paiement (EP), avec si nécessaire un passeport lui permettant d'exercer dans différents pays ; les établissements de crédit, de monnaie électronique et les établissements de paiement déjà agréés sont considérés comme étant ASPSP.

Etablissement de Paiement (EP) : ils ont été créés suite à la Directive sur les Services de Paiement (DSP) de 2009. Auparavant, seuls les banques et les établissements de crédit avaient l'autorisation de fournir des services de paiement. Avec le développement du paiement en ligne, de nouveaux acteurs, de tailles plus petites se sont vu accorder le droit d'obtenir ce statut afin de rendre le paysage plus concurrentiel. Ce statut est délivré par les autorités financières du pays dans lequel la demande est effectuée ; en France il s'agit de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), liée à la Banque de France. L'obtention et la conservation d'un agrément relèvent de procédures rigoureuses afin d'apporter des garanties fortes aux utilisateurs des services de paiements.

TPP (Third Party Provider ou PSP Tiers) : prestataire pouvant initier des paiements à la demande du payeur, sans détenir les fonds et à partir de comptes qu'il ne gère pas, et offrir des informations consolidées sur ces comptes. Il comprend les deux catégories de prestataires suivants :

> **PISP (Payment Initiation Service Provider ou Prestataire de Services d'Initiation de Paiement)** : prestataire proposant un service qui consiste à initier un ordre de paiement à la demande d'un PSU à partir d'un compte bancaire détenu par un ASPSP.
>
> **AISP (Account Information Service Provider ou Prestataire de Services d'Information sur les Comptes)** : prestataire fournissant un service de consolidation des informations relatives à un ou plusieurs comptes détenus par un PSU auprès d'un ou plusieurs ASPSPs.

ONDRP : L'Observatoire national de la délinquance et des réponses pénales est un département de l'Institut national des hautes études de la sécurité et de la Justice.. Il a comme activité principale la production et la diffusion de statistiques sur la criminalité et la délinquance. L'ONDRP inscrit ses travaux dans le cadre de la statistique publique et du code des bonnes pratiques de la statistique européenne.

ACPR : L'Autorité de contrôle prudentiel et de résolution est l'organe de supervision français de la banque et de l'assurance.

ERPB : La BCE a annoncé le19 décembre 2013 le lancement de l'Euro Retail Payments Board (ERPB). Cette nouvelle entité, qui remplace le conseil SEPA, contribuera au développement d'un marché intégré, innovant et compétitif pour les paiements de détail en euros dans l'Union européenne.

EPC : Le Conseil européen des paiements (ou European Payments Council : EPC) est né en juin 2002, à l'initiative des banques européennes et leurs fédérations européennes, avec l'objectif de mettre en place le Single Euro Payments Area (SEPA). Ses travaux portent sur les flux en euro en Europe, avec une approche prioritaire sur la zone euro.

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

IDC France

13 Rue Paul Valéry
75116 Paris, France
+33.1 56.26.26.66
Twitter: @IDCfrance
idc-community.com
www.idc.com / www.idc.fr
