livre blanc

fédération e-commerce et vente à distance
octobre 2013

Les moyens de sécurisation des paiements sur internet

LA LUTTE CONTRE LA FRAUDE VUE PAR LES E-MARCHANDS

fevad
www.fevad.com

PREFACE

Marc Lolivier
Délégué Général
de la Fevad

Pour la première fois depuis 2008, l'Observatoire de la Sécurité des Cartes de Paiement (OSCP) constate qu'en 2012 le taux de fraude sur les paiements sur Internet a diminué pour atteindre 0,290 % (contre 0,341 %, son maximum historique en 2011).

C'est incontestablement un signe encourageant pour l'ensemble des acteurs, et particulièrement pour les E-Commerçants, qui se mobilisent au quotidien pour endiguer la fraude sur les moyens de paiement à distance.

Il n'en reste pas moins que la lutte contre la fraude doit plus que jamais être au centre de toutes les attentions et faire appel, plus que jamais, à la mobilisation générale !

Au-delà des différences de définitions et de calcul du taux de fraude ou bien encore des intérêts sectoriels particuliers des différents acteurs, il convient de rappeler **que l'enjeu commun essentiel est le maintien et le développement de la confiance du consommateur dans les moyens de paiement et dans le E-Commerce en général. Car la confiance est la clé même du développement du e-commerce. Et la sécurisation des paiements figure au premier rang des attentes légitimes des consommateurs à l'égard du e-commerce.**

Conscients de ces enjeux la plupart des sites travaillent activement à la sécurisation de leurs transactions. La principale difficulté pour eux réside dans la nécessité de renforcer en permanence la sécurisation des paiements, tout en perturbant le moins possible le parcours client. Car si le client souhaite, de manière légitime, que sa transaction soit sécurisée, il souhaite aussi que son parcours d'achat ne se transforme pas en parcours du combattant.

C'est dans cet état d'esprit qu'est née l'idée de ce Livre Blanc entrepris par la FEVAD avec le soutien de très nombreux adhérents de la FEVAD qui ont contribué activement à son élaboration en répondant à notre enquête et pour certains d'entre eux en participant à des interviews individuels. Les e-commerçants interviewés ont accepté de partager leur vision et leurs retours d'expérience sur la mise en place de moyens de lutte contre la fraude sur Internet. C'est à partir de cette matière qu'est construit le présent ouvrage.

Qu'on ne se méprenne pas : ce Livre Blanc n'est pas un manuel des techniques de lutte contre la fraude. Ce n'est pas non plus un inventaire des solutions de lutte contre la fraude (il existe d'excellents ouvrages sur ces sujets). Non, ce Livre Blanc est avant tout le ressenti "sur le terrain" de la lutte contre la fraude telle qu'elle est vécue au quotidien par les E-Marchands. C'est la première fois qu'une telle étude est menée, en toute indépendance, auprès des marchands.

Dans des débats parfois un peu dogmatiques sur le sujet, ce Livre Blanc apporte des illustrations concrètes tant des difficultés rencontrées par les E-Marchands que des solutions qu'ils mettent d'ores et déjà en œuvre ou qu'ils comptent développer. Même s'il a été rédigé avec un souci d'objectivité, ce document reprend sciemment des points de vue ou perceptions des E-Commerçants, sans filtre, en conservant, parfois, toute leur subjectivité.

Ce Livre Blanc constitue également pour les E-Commerçants l'occasion d'exprimer 6 messages clés sur la lutte contre la fraude, directement inspirés des réflexions menées dans le cadre de ces travaux.

Si l'on devait n'en retenir qu'un seul, cela devrait être celui-ci : **la sécurisation des moyens de paiement ne peut être traitée sans son corollaire, la fluidité du parcours clients. Ces deux objectifs sont indissociables pour les E-Commerçants. Pour les concilier, la FEVAD n'a eu de cesse (et continue encore) de préconiser une gestion de la fraude par les risques.**

C'est dans la recherche de ce point d'équilibre que se situe aujourd'hui le principal enjeu de la sécurisation des paiements. Cet équilibre ne pourra être atteint que si l'ensemble des acteurs de la chaine de paiement décide de travailler ensemble, main dans la main, afin de dégager les solutions les plus adaptées, en tenant compte des particularités et des contraintes propres à chacun d'eux.

C'est la raison pour laquelle nous avons tenu également à associer à la rédaction de ce Livre Blanc d'autres parties prenantes qui, elles aussi, travaillent quotidiennement à la sécurisation des paiements sur internet et qui ont accepté de nous livrer leur point de vue et permis ainsi d'enrichir la réflexion.

Au nom de la FEVAD, je tenais une nouvelle fois à remercier toutes celles et ceux qui ont accepté d'apporter leur concours à la réalisation de ce Livre Blanc qui n'a d'autre ambition que de contribuer à l'émergence de solutions concertées les plus efficaces et adaptées à la sécurisation des paiements sur internet, dans l'intérêt commun des consommateurs et de l'ensemble des professionnels du secteur.

Bonne lecture !

Marc Lolivier

Délégué général de la Fevad

SYNTHESE

Pour la première fois depuis 2008, l'Observatoire de la Sécurité des Cartes de Paiement (OSCP) constate qu'en 2012 le taux de fraude sur les paiements sur Internet a diminué pour atteindre 0,290 % (contre 0,341 %, son maximum historique en 2011).

C'est incontestablement un signe encourageant pour l'ensemble des acteurs, et particulièrement pour les E-Commerçants, qui se mobilisent au quotidien pour endiguer la fraude.

Il n'en reste pas moins que le montant de la fraude sur les moyens de paiement à distance n'a pas cessé de croître au cours des dernières années et que ce constat appelle, plus que jamais, à la mobilisation générale !

Au-delà des différences de définition de la fraude et des intérêts sectoriels particuliers de chacun des acteurs, il convient de rappeler que l'enjeu commun est le maintien et le développement de la confiance du consommateur dans les moyens de paiement et dans le E-Commerce en général.

C'est dans cet esprit que de très nombreux adhérents de la FEVAD ont répondu à un questionnaire quantitatif sur le sujet et que 15 E-Commerçants parmi les plus représentatifs ont participé à des interviews individuelles et ont accepté de partager leur vision et leurs retours d'expérience sur la mise en place de moyens de lutte contre la fraude sur Internet. C'est à partir de cette matière qu'est construit cet ouvrage.

A.1 MESSAGES CLES ET CONVICTIONS

Ce Livre Blanc est l'occasion pour les E-Commerçants d'exprimer 6 messages clés ou conviction sur la lutte contre la fraude sur les moyens de paiement à distance:

- **La fraude concerne tous les acteurs**. Maintenir et développer la confiance du Consommateur dans les paiements par cartes bancaires sur Internet et demain par tout autre moyen de paiement imaginable doit constituer l'objectif commun de l'ensemble des parties prenantes de la lutte contre la fraude.
- **Sécurisation des moyens de paiement ET fluidité du parcours Client sont deux objectifs indissociables pour les E-Commerçants.** Pour concilier ces deux objectifs, la FEVAD n'a eu de cesse (et continue encore) de préconiser une gestion de la fraude par les risques.
- **Face à la globalisation de la fraude, un renforcement indispensable de la coopération entre les acteurs :** les nouvelles formes de fraude imposent une coordination accrue entre toutes les parties prenantes et doivent notamment aboutir à un meilleur partage de l'information, dans le respect de règles protégeant les données personnelles qui doivent évoluer.
- **Une chaîne de paiement qui doit être sans faille:** La question de la lutte contre la fraude sur les moyens de paiement sur Internet renvoie plus globalement à la question de la sécurisation des données qui transitent dans un monde de plus en plus interconnecté!
- **L'outil universel de lutte contre la fraude n'existe pas !** Face à une fraude protéiforme et en perpétuelle mutation et qui se professionnalise, les E-Marchands considèrent comme illusoire (et mensonger) de croire (ou laisser croire) qu'une solution unique peut à elle seule endiguer le développement de la fraude sur Internet.

- **Accélérer l'adaptation de méthodes de paiement aux spécificités du E-Commerce:** L'expansion très rapide que connaît actuellement le E-Commerce rend nécessaire l'évolution des méthodes de paiement actuelles et voire même la création de nouveaux moyens de paiement notamment pour le M-Commerce en très fort développement !

A.2 RAPPEL DES ENJEUX DE LA LUTTE CONTRE LA FRAUDE POUR LES E-COMMERÇANTS

Pour bon nombre de E-Marchands, l'enjeu principal de fraude est d'abord financier. Le montant de la fraude a un impact direct sur le résultat net du E-Marchand. Or, le E-Commerce reste une activité pour laquelle les marges opérationnelles sont relativement faibles et la profitabilité souvent à venir. Le deuxième enjeu financier est que le taux de commission exigé par la Banque Acquéreur dépend étroitement du niveau de maîtrise de son taux de fraude par le E-Commerçant.

Le deuxième enjeu de la fraude pour les E-Commerçants est opérationnel.

La sécurisation des paiements par carte bancaire revêt une importance majeure pour les E-Commerçant tout simplement parce que, d'après les chiffres de la FEVAD, 80 % des paiements à distance se font par carte bancaire dans notre pays.

Le paiement est évidemment pour le E-Commerçant un moment crucial. Les E-Marchands interviewés rappellent combien la fluidité et la rapidité de paiement sont essentielles à la conclusion d'une vente : les dixièmes de secondes comptent ! Dès lors, les E-Marchands sont particulièrement attentifs à tout alourdissement du tunnel de commande, d'autant plus que, dans la plupart des cas, les processus d'authentification et de validation de la commande leur échappent.

Le troisième enjeu, et non des moindres, est un enjeu d'image. Tous les E-Commerçants savent combien il est difficile de conquérir la confiance d'un Client et combien il peut être rapide de la perdre ! Et, en matière de fraude, le E-Commerçant n'a pas le droit à l'erreur : une mauvaise évaluation du risque de la transaction peut avoir des conséquences désastreuses auprès de très bon clients.

A.3 VISION DE L'EVOLUTION DE LA FRAUDE PAR LES MARCHANDS

A.3.1 Vers une professionnalisation de la fraude sur les moyens de paiement sur Internet

La fraude s'est professionnalisée, c'est le constat unanime des E-Marchands interviewés. Elle devient de plus en plus technique et, pour partie, le fait de réseaux de fraudeurs experts en la matière. Elle est par ailleurs très "dynamique"; les fraudeurs testent en permanence, cherchant à détecter les failles des systèmes de protection en visant une fraude la plus "efficace possible" avec les meilleurs rendements.

A.3.2 Une fraude "Tout azimut"

Si, jusqu'à encore récemment, certains produits ou services pouvaient encore être considérés comme "peu ou pas attractifs" pour les fraudeurs, ce temps est bel et bien révolu ! Certains E-Marchands interviewés ont constaté de la fraude sur les achats de couche-culotte !

Les critères d'évaluations du risque doivent être revus et actualisés en permanence; le lieu géographique ou le mode de livraison, l'ancienneté du client... : ces critères à eux seuls ne suffisent plus pour identifier une fraude. Une analyse multidimensionnelle du risque est maintenant requise !

La lutte contre la fraude nécessite par conséquent une véritable expertise. Sur le terrain, lutter contre la fraude c'est trouver des réponses adaptées aux points suivants:

Difficultés	Commentaires
Faire face aux volumes	Pour certains E-Marchands, un dispositif de lutte contre la fraude efficace doit être en mesure d'évaluer le risque de plusieurs milliers de transactions par jour. Pour le E-Marchand, repérer les transactions frauduleuses, c'est comme repérer "l'aiguille dans la meule de foin".
Frapper "chirurgicalement" les fraudeurs parmi les bons clients !	Les conséquences d'une mauvaise évaluation du risque peuvent avoir des conséquences extrêmement dommageables; impact financier d'une transaction frauduleuse non détectée, impact d'image dans le cas d'un client soupçonné à tort. Mal évaluer le risque d'une transaction, c'est risquer de porter atteinte à la relation de confiance patiemment tissée avec le client et finalement de le perdre.
S'adapter en permanence aux évolutions de la fraude	Les techniques de fraude évoluent sans cesse. Pour être efficace, le dispositif de fraude doit évoluer en permanence. Il en va de même pour les équipes anti-fraude qui doivent s'astreindre à une veille constante sur toutes les nouvelles tendances en matière de fraude.
Avoir une capacité de réaction suffisante	Une faille qui ne serait pas rapidement repérée par le E-Marchand peut avoir dans les semaines qui suivent des conséquences financières catastrophiques. La fraude nécessite une vigilance 24/24, 7/7 et des outils de monitoring qui renseignent le E-Commerçant en quasi temps réel.
La fraude, un sujet complexe d'organisation interne	La fraude est un arbitrage permanent entre des objectifs qui au sein des organisations peuvent paraître antagonistes; objectifs marketing et commerciaux vs objectifs financiers de rentabilité. La fraude est un sujet transverse à l'entreprise et nécessite une coordination étroite entre différentes directions: direction générale, Ventes, direction de la Relation client, direction financière... Pour les groupes internationaux, c'est un sujet qui nécessite un juste équilibre entre la mutualisation des moyens et la prise en compte des spécificités locales de la lutte contre la fraude.

Allouer les moyens et maintenir la priorité	Dans une phase de croissance très rapide du E-Commerce, l'arbitrage sur les moyens à consacrer à la lutte contre la fraude par rapport à d'autres priorités ayant un impact plus visible sur le développement de l'activité est loin d'être simple. Elle nécessite une certaine capacité d'anticipation et de projection qui peuvent paraître comme difficilement conciliables avec des impératifs courts termes.
Agréger des données de plus en plus nombreuses et provenant de sources externes	Pour gérer efficacement son système anti-fraude, un E- marchand doit pouvoir intégrer et consolider, a minima, deux sources d'information (informations en provenance du PSP et informations en provenance de la banque acquéreur). Ces deux sources d'informations doivent être ensuite croisées avec les données internes.

A.3.3 Des moyens de lutte contre la fraude qui sont de plus en plus sophistiqués

Face à la professionnalisation de la fraude et sa sophistication, les E-Commerçants déploient de véritables "arsenaux" de lutte contre la fraude. L'outil universel qui endiguerait à lui-seul la fraude sur les moyens de paiement n'existe pas !

Le point clé reste l'accès et l'exploitation de l'information qui "nourrit" les algorithmes d'évaluation du risque de fraude. La fraude se globalisant, les E-Marchands doivent de plus en plus intégrer des données en provenance de sources multiples tant internes qu'externes, nationales comme internationales ...

A.3.4 Vers un plus grand partage de l'information entre les acteurs de la lutte contre la fraude

Les E-Marchands interviewés affirment que l'efficacité de la lutte contre la fraude passera forcement par un plus grand partage de l'information entre les parties-prenantes, dans le respect des règles de protection de la confidentialité des données qui devront être adaptées.

A.4 3D SECURE TROUVE NATURELLEMENT SA PLACE DANS LES DISPOSITIFS DE LUTTE CONTRE LA FRAUDE

Tous les E-Marchands interviewés ont déjà mis en place des mécanismes d'authentification forte comme 3D Secure (ou sont dans des phases de réflexion avancées).

Si les bénéfices de cette solution sont indéniables, des freins à son déploiement existent, notamment le "taux d'échec d'authentification" qui reste anormalement élevé.

Freins à l'adoption de 3D Secure	Bénéfices perçus à la mise en place de 3D Secure
• Niveau actuel du taux d'échec d'authentification • Une information des clients jugée encore très nettement insuffisante • La non éligibilité de certaines cartes étrangères au transfert de responsabilité • La gestion opérationnelle du transfert de responsabilité • Une uniformisation très (trop) tardive des moyens d'authentification	• Réduction de la fraude • Amélioration de la satisfaction client • Amélioration du taux de facturation • Réduction des coûts de lutte contre la fraude et gains de productivité • Amélioration du taux d'acceptation des autorisations • Baisse des commissions bancaires • Des contrôles plus qualitatifs
Limites de la solution	**Risques à ne pas mettre en place 3D Secure**
• Inadaptation de 3D Secure au M-Commerce • Durée de garantie de 3D Secure contrainte par la durée de garantie de l'autorisation • Paiements fractionnés: transfert de responsabilité limité au premier versement • Effet dissuasif limité sur les fraudeurs • Pas d'allégement des dispositifs anti fraude existants grâce à 3D Secure • Faillibilité de 3D Secure	• Risque de déport de la fraude sur les sites qui n'auront pas mis en place 3D Secure • Risques d'image

A.5 RECOMMANDATIONS DES E-MARCHANDS AUX ACTEURS PARTIE-PRENANTES DE LA LUTTE CONTRE LA FRAUDE

A.5.1 Recommandations aux E-Marchands

Mesurer l'impact de la fraude dans sa globalité

Pour les E-Marchands interviewés, considérer la fraude comme un coût financier inévitable et l'intégrer dans son calcul de marge, c'est en mésestimer totalement les conséquences à moyen et long terme.

Déposer systématiquement plainte, avec le cas échéant constitution de partie civile

Les E-Marchands ne déposent pas systématiquement plainte en cas de fraude. Bien souvent, le E-Marchand considère le dépôt de plainte uniquement sous l'aspect économique et pratique.

Là encore, ne pas déposer plainte, c'est laisser se développer un sentiment d'impunité parmi les fraudeurs et entretenir un phénomène de nature à saper inexorablement l'ensemble de l'écosystème de l'E-Commerce. Il faut ici saluer l'attitude de certains E-Marchands rencontrés pour qui le dépôt systématique de plainte relève d'une question de principe.

Dans le déploiement et l'exploitation de 3D Secure, mettre en œuvre les bonnes pratiques identifiées dans le Livre Blanc

Dans ce Livre Blanc, les E-Marchands qui ont mis en œuvre 3D Secure ont accepté de donner leur retour d'expérience et de partager un certain nombre de bonnes pratiques qu'ils en ont tirées. Ces recommandations sont totalement désintéressées. Elles n'ont d'autres finalités que de faciliter l'adoption de 3D Secure par les E-Marchands qui ne l'ont pas encore mis en place (ou s'interrogent encore), dans les meilleures conditions possibles compte tenu des limites de la solution qui ont été identifiées. Ces recommandations visent également à permettre aux E-Marchands d'exploiter pleinement les bénéfices de la solution 3D Secure, au sein de leur dispositif de lutte contre la fraude étant entendu qu'une authentification renforcée ne garantit en rien le marchand contre une fraude ; au mieux, elle le garantit contre un futur "charge back".

Mieux utiliser et exploiter les informations « de base » déjà disponibles auprès des PSPs ou des banques

Alors que certains E-Marchands interviewés considèrent ne pas disposer de suffisamment d'outils pour piloter leur lutte contre la fraude, certains prestataires de solutions de paiement rencontrés dans le cadre de ce Livre Blanc, déplorent quant à eux une sous-utilisation des outils de lutte contre la fraude qui sont pourtant librement accessibles sur les boutiques des Marchands. Mais, pour être réellement efficaces, ces PSP rappellent que ces outils doivent être mis à jour régulièrement par les E-Marchands.

La question de l'externalisation de la lutte contre la fraude peut se poser pour certains E-Marchands dont les moyens sont focalisés sur d'autres sujets et qui, même s'ils en mesurent les enjeux, considéreraient que cette compétence n'est pas "au cœur de leur métier".

Se mobiliser collectivement contre la fraude - Partager l'information

La globalisation de la fraude et du développement des réseaux de fraude rend nécessaire un renforcement de la coopération entre les professionnels du secteurs sur l'échange des bonnes pratiques (ce Livre Blanc veut en être une illustration) mais également un renforcement des échanges d'informations entre les sites, dans le respect bien évidemment des exigences de la

CNIL, dont les E-Marchands souhaiteraient qu'elles évoluent (cf. Pistes de réflexions à engager avec la CNIL plus loin dans ce document).

A.5.2 Recommandations aux Banques

Réduire le taux d'échec d'authentification pour le rendre compatible avec les exigences économiques du E-Commerce

Le niveau de taux d'échec d'authentification reste le frein majeur au développement de 3D Secure en France. Même si, beaucoup de E-Marchands en conviennent, il s'agit d'un taux d'échec "brut", 18% des authentifications qui n'aboutissent pas est un taux qui reste "incompatible avec les règles économiques du E-Commerce". Des échanges qu'a eu la FEVAD avec elle il ressort que la Banque de France souhaite maintenir la pression sur les banques afin de faire rapprocher le taux d'échecs 3D-Secure de celui constaté lors des paiements non 3D-Secure. Au-delà du taux moyen, c'est bien l'écart très important d'une banque à l'autre qui "choque" particulièrement les E-Marchands. Ces écarts tendent à prouver, si cela était encore nécessaire, qu'une réduction très importante du taux d'échec d'authentification est possible et qu'elle ne dépend que de la mobilisation des moyens appropriés par les banques.

Veiller à une meilleure transparence dans la garantie de paiement

La garantie de paiement (et le transfert de risques associé) demeure un élément très fort de l'attrait de la solution 3D Secure pour le E-Marchand. Il semble qu'il est dans l'intérêt mutuel des banques et des E-Commerçants de lever les ambiguïtés sur les limites de celle-ci, tout simplement par une communication claire et transparente sur les dites règles et, dans la pratique, par une information claire fournie aux E-Marchands sur les transactions ayant bénéficié du transfert de risque et celles qui n'en n'ont pas bénéficié.

Développer le niveau de compétence et l'expertise des responsables de compte sur la lutte contre la fraude et/ou développer des cellules dédiées à la lutte contre la fraude et plus généralement au E-Commerce

Comme évoqué dans le chapitre relatif à la perception des E-Marchands sur la collaboration avec les banques, il ressort très nettement de la part des E-Marchands d'un besoin de support plus fort des banques sur le sujet de la lutte contre la fraude. Là encore, les situations sont différentes en fonction du pouvoir de négociation du E-Marchand vis-à-vis de sa banque. Même s'il est compréhensible que les interlocuteurs commerciaux des E-Marchands au sein des banques ne puissent maîtriser tous les sujets, il serait néanmoins apprécié que les E-Marchands (et notamment de petite taille) puissent avoir accès plus facilement à des cellules d'expertises dédiées à la lutte contre la fraude au sein des banques.

A.5.3 Recommandations et pistes de réflexion avec la Banque de France

Dans leur ensemble, les E-Marchands interviewés saluent le travail réalisé par la Banque de France notamment dans le cadre de l'Observatoire de la Sécurité des Cartes de Paiement (OSCP)

On saluera à cet égard l'action de communication engagée en décembre 2012 par l'OSCP, par la publication d'une brochure « Commerçants, comment renforcer la sécurité des paiements sur Internet ? », où il est fait mention du mécanisme d'authentification renforcée et de la solution 3D Secure. Parallèlement, la Banque de France a elle-même publié en novembre 2011, à

destination des particuliers, un document sur la protection des identifiants bancaires (numéros de compte, numéros de carte bancaire, identifiants de la banque en ligne).

Poursuivre la promotion d'une approche par les risques pour impacter graduellement la fluidité du parcours client : inciter à l'usage sélectif de 3D Secure

Les E-Marchands collectivement soutiennent l'objectif de la Banque de France d'assurer la sécurisation des moyens de paiement et comptent assumer pleinement leurs responsabilités dans l'atteinte de cet objectif, qui est absolument essentiel pour eux.

Mais ils rappellent que la généralisation des moyens de sécurisation des paiements sera d'autant plus rapide et efficace que ces moyens s'inscriront de façon la plus fluide possible dans les parcours de paiements et que ces moyens de sécurisation perturberont le moins possible les habitudes d'achat des consommateurs.

La FEVAD, qui en fût très tôt l'instigatrice, recommande une approche de la sécurisation des moyens de paiement par les risques (proportionnalité des moyens de sécurisation au risque de la transaction), seule approche qui permette de concilier fluidité du parcours et maîtrise de la fraude.

Définir et contrôler les engagements d'amélioration des banques notamment sur la réduction du taux d'échec d'authentification

Les E-Marchands constatent que malgré les intentions affichées et le temps écoulé depuis le lancement de 3D Secure, le taux d'échec d'authentification moyen reste élevé. Ils subissent en parallèle une pression de plus en plus forte pour mettre en œuvre 3D Secure. Ils leur semblent que cette pression serait d'autant plus efficace si elle s'accompagnait d'engagements fermes des banques sur des délais de réduction du taux moyen d'échec, objectifs dont la réalisation pourrait être vérifiée par la Banque de France.

Poursuivre, renforcer et (le cas échéant) organiser le dialogue entre les parties prenantes (notamment via l'OSCP) particulièrement sur les points suivants:

Lors des entretiens, les E-Marchands interviewés ont réaffirmé l'importance à leurs yeux soit de poursuivre soit d'engager des réflexions avec l'ensemble des parties prenantes sur les thèmes suivants:

- La clarification des limites de la garantie de paiement en fonction des cartes de paiement
- L'extension de garantie 3D Secure à l'ensemble des transactions, dans le cas d'un paiement fractionné.
- La définition et le suivi de la qualité de service (QoS) de la demande d'authentification : définition d'un délai maximum d'affichage de la page d'authentification, adaptation de la page de saisie du code aux spécificités du terminal appelant (rendering) …
- Les moyens à mobiliser pour réduire la fausse répudiation (incluant une réflexion sur la communication à faire sur les conséquences économiques de ce type de fraude et ses conséquences pénales pour le fraudeur)
- Les modalités d'accès des E-Marchands de petite taille aux informations et aux moyens techniques leur permettant de bénéficier de dispositifs anti-fraude adaptés à leurs moyens.
- L'harmonisation des législations européennes sur l'utilisation des moyens de paiement (qui néanmoins progresse avec le projet de DSP 2).

A.5.4 Pistes de réflexion à engager avec la CNIL

Quel équilibre trouver entre "protection des données personnelles" et "lutte contre la fraude"?

Pour les E-Marchands, la protection des données personnelles est un enjeu majeur pour le développement de l'économie numérique et ils y souscrivent totalement.

Néanmoins, il leur paraît maintenant utile de revisiter les modalités de mise en œuvre des procédures de protection des données personnelles à la lumière des nouvelles exigences de lutte contre la fraude sur internet. Il leur semble qu'il en va de l'intérêt du consommateur d'être assuré de la protection de ses données personnelles comme de la sécurisation des moyens de paiement qu'il utilise.

Engager une réflexion spécifique avec la CNIL sur certains thèmes spécifiques

La plupart des E-Marchands interviewés se sont dits prêts à participer à un éventuel groupe de réflexion autour du thème du bon équilibre à trouver entre protection des données personnelles et efficacité des systèmes de lutte contre la fraude.

Au-delà du thème générique de réflexion précédemment cité, les E-Marchands souhaiteraient que puissent s'ouvrir des débats plus spécifiques notamment sur les conditions de mutualisation de certaines données (notamment entre filiales d'un même groupe et/ou entre clients d'un même prestataire), la durée de conservation de certaines données nécessaires à l'évaluation du risque de fraude, les conditions d'utilisation des méthodes de reconnaissance du terminal (Device FingerPrint). A l'heure où les terminaux mobiles s'équipent de lecteurs d'empreintes digitales stockées à l'autre bout du monde, il paraît anachronique de souhaiter interdire l'identification d'un terminal.

Engager une réflexion avec la CNIL sur les modalités d'instruction des dossiers d'autorisation

Comme évoqué lors de la description de la perception des E-Marchands de la collaboration avec la CNIL, le délai d'instruction des dossiers d'autorisation est globalement jugé très long (de l'ordre de six mois jusqu'à plus d'une année) et, peu compatible avec la réactivité que nécessite la lutte contre la fraude.

La CNIL a régulièrement affirmé que la protection de la vie privée et des données personnelles n'a pas pour objet de protéger les comportements frauduleux, mais d'éviter les exclusions illégitimes ou mutualisées parmi plusieurs secteurs professionnels et de fixer des durées de conservation proportionnées et impératives.

Il conviendrait que cette approche s'illustre dans l'instruction des demandes d'autorisation.

Repenser la responsabilité du E-Marchand en matière de traitement des paiements et de prévention des fraudes

Lorsqu'un E-Marchand recourt aux services d'un PSP, il ne décide généralement pas des modalités de sécurisation et de conservation des données traitées par le PSP, lesquelles sont essentiellement régies par les réglementations bancaire et financière et par les normes de traitement des paiements et de sécurité appliquées par le PSP. Il parait de plus en plus fictif de considérer que le E-Marchand serait « responsable du traitement » des données réalisé par le PSP.

Aussi paraît-il nécessaire que la CNIL ouvre une réflexion sur la meilleure régulation des systèmes de prévention des fraudes intégrés au traitement des paiements par des PSP. En effet, il parait peu pertinent de soumettre à la CNIL des centaines de demandes d'autorisation identiques présentées par autant de E-Marchands, alors que les traitements de données

concernés seront mis en œuvre par une poignée de PSP, représentant peu de demandes d'autorisation à examiner.

A.5.5 Attentes vis-à-vis des services de police et des pouvoirs publics en général

Les E-Commerçants rencontrés formulent quatre demandes:

1) Revoir les modalités de dépôt de plaintes pour les particuliers et pour les E-Marchands

Pour les particuliers : rendre obligatoire le dépôt d'une plainte pénale sans lequel la banque devrait s'interdire l'enregistrement et la comptabilisation d'une contestation d'un paiement réalisé à distance ou, a minima, inciter à nouveau au dépôt de plaintes pour les particuliers.

Pour les E-Marchands : faciliter le processus de dépôt de plainte.

2) Durcir les sanctions et les peines encourues dans le cadre de la fraude au E-Commerce

Activité criminelle parmi d'autres, la fraude sur les moyens de paiement à distance exige un investissement moindre que pour d'autres filières criminelles. De plus, les peines encourues sont plus faibles comparées à celles occasionnées par d'autres délits « physiques ». Il est ainsi plus facile et moins risqué de déployer des compétences dans le secteur de la cybercriminalité, que dans d'autres activités illégales. Les E-Commerçants appellent de leurs vœux un durcissement des sanctions à l'encontre des fraudeurs aux moyens de paiement.

3) Sans remettre en cause l'administration de la politique pénale de chaque procureur, obtenir une meilleure homogénéisation des décisions de l'autorité judiciaire sur l'ensemble du territoire national

4) Renforcement de la coopération fonctionnelle entre les principaux acteurs de la sécurité des moyens de paiement en VAD (CB, PSP, Prestataires) et de la coopération judiciaire internationale

Il s'agit pour les E-Commerçants d'un point essentiel, notamment dans le cadre du mouvement de globalisation de la fraude et de sa structuration en réseau. Pour faire face à ces nouveaux enjeux, le renforcement de la coopération fonctionnelle entre les principaux acteurs de la sécurité des moyens de paiement à distance (CB, PSP, Prestataires) est indispensable. Il passe notamment pour les trois points repris ci-après:

- Faciliter la coopération avec les services de police : créer un « guichet unique » permettant d'orienter le Marchand vers le service compétent ou, à défaut diffuser l'information sur « qui contacter en cas de fraude» aux E-Marchands ;
- Renforcer la coopération entre services de police et E-Marchands: organiser des échanges croisés (formations, séminaires) entre eux ;
- Veiller au maintien de moyens suffisants pour traiter les demandes d'information avec une réactivité adéquate.

Enfin, au niveau international, il apparait également souhaitable de renforcer la coopération judiciaire internationale notamment avec certains pays d'où émanent un grand nombre de fraudes et avec lesquels la France n'a pas d'accords.

SOMMAIRE

Partie A
INTRODUCTION

A.1 OBJECTIFS DU LIVRE BLANC

Le montant de la fraude sur les moyens de paiement à distance n'a pas cessé de croitre au cours des dernières années, même si en proportion du nombre total de transaction, le taux de fraude a baissé pour la première fois en 2012, selon l'Observatoire de la Sécurité des cartes de paiements (OSCP).

Cette augmentation de la fraude fait courir un risque fort pour l'ensemble du E-Commerce en France car elle est de nature à entamer profondément et durablement la confiance des consommateurs dans les moyens de paiement, crainte relayée et amplifiée par certains média.

Construit à partir du retour d'expérience des adhérents de la FEVAD, ce Livre Blanc a notamment pour objectifs de :

- Démontrer, par une approche pragmatique et constructive, que la FEVAD entend contribuer activement à la lutte contre la fraude en assurant la promotion des « meilleures pratiques » en fonction des enjeux et des différentes typologies de E-Commerçants et que la FEVAD jouera un rôle actif dans l'effort commun de déployer la solution 3D Secure dans les cas où cette solution est pertinente.
- Présenter une vision fidèle et sans parti pris du déploiement des solutions de sécurisation des moyens de paiement sur internet dont 3D Secure.
- Montrer objectivement tous les bénéfices (directs et indirects) de cette solution mais également ses limites, lors de son déploiement et en exploitation : Illustrer, au travers de cas précis, que 3D Secure n'est pas la solution unique pour lutter efficacement contre la fraude.
- Objectiver les risques d'un déploiement unilatéral de la solution 3D Secure pour tous les E-Commerçants.
- Faire des propositions aux autres parties prenantes de la lutte contre la fraude pour rendre encore plus efficaces les moyens de lutte actuels.

A.2 CONVICTIONS ET MESSAGES CLES

A.2.1 La Fraude concerne tous les acteurs

En fonction du prisme qui est retenu, la fraude peut être vue très différemment par les acteurs concernés. Comme on le verra, certains acteurs, particulièrement les E-Marchands et les banques, n'ont pas seulement une vision différente de la fraude, ils peuvent même utiliser des méthodes différentes pour la calculer !

Mais, au-delà des intérêts sectoriels particuliers de chacun, ce qu'il convient de rappeler à tous c'est l'enjeu commun que constituent le maintien et le développement de la confiance du consommateur dans les moyens de paiement et dans le E-Commerce en général.

Si la fraude sur les paiements à distance continue à se développer au rythme actuel, c'est la confiance du consommateur qui sera durablement entamée!

Maintenir et développer la confiance du consommateur dans les paiements par cartes bancaires sur Internet et demain par tout autre moyen de paiement imaginable, voilà l'objectif sur lequel l'ensemble des parties prenantes de la lutte contre la fraude doit se rassembler.

C'est bien dans cet esprit que les adhérents de la FEVAD ont accepté de participer à ce Livre Blanc.

A.2.2 Sécurité et fluidité du parcours de paiement

Ces deux objectifs sont indissociables pour les E-Marchands. Pour les concilier, la bonne approche est une approche par les risques.

Comme aime à le rappeler de façon un peu provocante la FEVAD : « il y aurait un moyen simple d'endiguer totalement la fraude sur les moyens de paiement à distance; il consisterait à arrêter le E-Commerce ! »

La FEVAD souscrit évidemment à l'objectif de sécurisation des moyens de paiements, poursuivi notamment par la Banque de France, les banques et le GIE Cartes Bancaires, mais tient à faire valoir que l'atteinte de cet objectif ne doit pas se faire au détriment de la fluidité du parcours client.

Relever le défi de l'endiguement de la fraude sur Internet, c'est mettre en place des dispositifs et des outils qui assurent la sécurisation de la transaction tout en perturbant le moins possible le consommateur dans son acte d'achat.

Pour la FEVAD, l'approche à retenir pour atteindre ce double objectif est une approche par les "risques" ; c'est à dire proportionner les mécanismes de sécurisation au risque de la transaction.

Parvenir à "manager" le risque de fraude, voilà le défi majeur qu'ont à relever les prestataires de services de paiement et les E-Marchands.

A.2.3 Face à la globalisation de la fraude, un renforcement indispensable de la coopération entre les acteurs

Il revient à chacun et en premier lieu aux E-Commerçants, quelle que soit leur taille, de mettre en place les dispositifs de lutte contre la fraude qui conviennent.

Mais, les réponses à une fraude sur Internet qui se globalise et s'organise de plus en plus en réseaux doivent également être collectives. Les nouvelles formes de fraude imposent une coordination accrue entre toutes les parties prenantes.

Elles nécessitent aussi d'avoir l'audace de revisiter un certain nombre de principes ou dogmes et de faire preuve d'imagination collective pour parvenir à concilier le principe de "protection des données personnelles" et la nécessité de "mutualisation de certaines données nécessaires à l'évaluation du risque".

Les E-Marchands et les prestataires techniques sont parfaitement conscients que ce débat ne pourra progresser que s'il s'inscrit dans le cadre d'engagements qu'ils prendront et sur la base de la confiance qu'ils auront su développer avec les pouvoirs publics.

Plus que jamais, la fraude est l'affaire de tous.

A.2.4 Une chaîne de paiement qui doit être sans faille

Les E-Marchands souhaitent rappeler que les paiements sur Internet font intervenir un nombre conséquents d'acteurs sur la chaîne et qu'ils en constituent uniquement que le dernier maillon.

La question de la lutte contre la fraude sur les moyens de paiement sur Internet renvoie plus globalement à la question de la sécurisation des données qui transitent dans un monde de plus en plus interconnecté !

A.2.5 L'outil universel de lutte contre la fraude n'existe pas.

Face à une fraude protéiforme en perpétuelle mutation et qui se professionnalise, les E-Marchands considèrent comme illusoire (et mensonger) de croire (ou laisser croire) qu'une solution unique peut à elle seule endiguer le développement de la fraude sur Internet.

Comme ce Livre Blanc le montre, c'est un ensemble de dispositifs et de mesures qui permettent de lutter efficacement contre la fraude.

Il est aussi utile de rappeler que tous les E-Commerçants ne se trouvent évidemment pas dans la même situation par rapport à l'enjeu que constitue la lutte contre la fraude. Aussi, les solutions qui doivent être mises en place doivent évidemment tenir compte des spécificités de chacun.

La FEVAD, en tant que lieu de partage privilégié entre les E-Commerçants, continuera à promouvoir l'échange de bonnes pratiques qui bénéficieront à l'ensemble des acteurs de la profession.

A.2.6 Accélérer l'adaptation de méthodes de paiement aux spécificités du E-Commerce

Toutes les parties prenantes en conviennent, le E-Commerce s'est développé grâce à des moyens de paiement préexistants qui ne lui étaient pas destinés.

L'expansion très rapide que connait actuellement le E-Commerce rend nécessaire l'évolution des méthodes de paiement actuelles et voire même la création de nouveaux moyens de paiement notamment pour le M-Commerce en très fort développement !

A.3 METHODOLOGIE

Pour rédiger son Livre Blanc, la FEVAD a mené une démarche quantitative complétée par une approche qualitative (interview en face à face avec un panel représentatif d'adhérents).

Un questionnaire a été envoyé à 280 adhérents afin de recueillir les éléments chiffrés permettant d'établir le bilan quantitatif. Une attention particulière a été portée au caractère possiblement récurrent du questionnaire : pouvoir utiliser le même questionnaire d'une année sur l'autre pour mesurer les évolutions.

Une série d'interviews, 15 au total, a ensuite été menée afin de recueillir la vision qualitative des adhérents de la FEVAD au cours des mois de mai, juin et début juillet 2013.

Chaque entretien a fait l'objet d'un compte-rendu qui a été revu par l'interviewé.

Remerciements

Les rédacteurs de ce Livre Blanc tiennent à remercier les adhérents de la FEVAD qui ont répondu au questionnaire et particulièrement les adhérents du panel qualitatif qui ont pris le temps de recevoir les rédacteurs au cours d'entretiens qui ont largement débordé l'heure prévue !

En acceptant de les recevoir et en leur livrant leur vision et le retour d'expérience sur la fraude, les E-Marchands rencontrés ont fait preuve d'une très grande transparence qui mérite d'être saluée.

Il n'est pas aisé de parler de la fraude. La fraude est loin d'être un sujet agréable à aborder. La fraude, c'est un rapport de confiance qui a été rompu !

Ensuite, la fraude est un sujet sensible qui revêt de forts enjeux d'abord économiques mais également d'image. Les acteurs entretiennent souvent des liens de dépendance étroits entre eux. Dès lors, chaque propos doit être soupesé avant d'être exprimé publiquement !

Enfin, la fraude est un sujet empreint de mystère qui touche à la fois au "secret de famille" (avec lequel on est plus ou moins à l'aise) et "à la recette de Grand-Mère" que l'on souhaite jalousement garder.

L'esprit de transparence dont ont fait preuve les interviewés n'en est que d'autant plus remarquable. Il témoigne à la fois de la prise de conscience collective par les adhérents de la FEVAD des enjeux de la lutte contre la fraude et aussi de leur engagement à trouver collectivement des solutions.

De sincères remerciements sont également adressés aux "amis" banquiers des E-Commerçants (le Groupement des Cartes Bancaires CB, ci-après « CB ») et à la Fédération Bancaire Française qui, eux aussi, ont accepté de donner leur point de vue dans le cadre de cet exercice peu commun.

A noter ! Des enrichissements juridiques importants (signalés la plupart du temps par des encadrés de couleur) ont été apportés par **Maître Etienne Drouard**, avocat associé, Partner K&L Gates LLP et **Maître Pierre Storrer**, avocat au barreau de Paris, spécialisé dans le droit des moyens et services de paiement. Nous les remercions vivement pour leur contribution.

A tous les contributeurs, les véritables rédacteurs de ce Livre Blanc, merci !

Rédacteurs

Ce Livre Blanc a été réalisé à l'initiative de la FEVAD par **Mathieu Sené,** Directeur Associé de Praxton Consulting sous la direction de **Bertrand Pineau**, responsable Veille & Innovation au sein de la FEVAD.

Praxton est un cabinet de conseil indépendant spécialisé dans la conception et la mise en oeuvre de stratégies de différenciation par les services qui exploitent notamment le potentiel du mobile et des réseaux connectés (réseaux sociaux, P2P...) – www.praxton.fr

Liste des e-commerçants interviewés

Entreprise	Nom	Fonction
CDISCOUNT.COM	Thierry SKROBALA Jacques LECHAT	Directeur Risque et Recouvrement Directeur de Projets Paiement
DELAMAISON.FR groupe ELBEE	Philippe BRUAND Salomon OUAKNINE	Directeur des Systèmes d'information Directeur Administratif et Financier
GROUPE 3 Suisses	Olivier RAES Fabrice BENIN Michel RIME	Directeur des moyens de paiement - crédit et fidélité Responsable Département Fraude Correspondant informatique et Libertés CIL
PRICEMINISTER.COM	Steven HAREL	Directeur Back Office
LA REDOUTE	Michel TAOUI Matthieu WILLEMS	Directeur Comptable et Responsable du département des fraudes DSI - Responsable pôle Etude
LASTMINUTE.COM	Laurent CURUTCHET Daphné DAGET	Directeur général France Directrice Financière France
MISTERGOODDEAL.COM	Morgan SEVENO	Responsable Relation Client
PECHEUR.COM	Olivier BERNASSON	Président
RUEDUCOMMERCE.COM	Laurent BERTIN	Secrétaire Général
VENTE-PRIVEE.COM	Eric FOREST Son NGUYEN	Directeur Comptable Directeur de projets
VOYAGES-SNCF.COM	Céline LAMBERT Nicolas BOSMANS	Responsable lutte contre la fraude et moyens de paiement Fraude Manager
ATOS WORLDLINE	Nicolas BRAND	Sips - e-Payment Product Manager
FEDERATION BANCAIRE FRANCAISE	Catherine BERTRAND	Etudes et activités bancaires et financières / Systèmes et moyens de paiement
GROUPEMENT DES CARTES BANCAIRES "CB"	Antoine SAUTEREAU Benoit CLAVEYROLAS	Responsable du département lutte contre la Fraude et Systèmes d'information Département lutte contre la Fraude et Systèmes d'information
BE2BILL, **Groupe Rentabiliweb**	Jean-Pierre SEPIETER	Head of Risk & Payment Analytics

Partie B
VISION DES E-MARCHANDS SUR LA FRAUDE ET SUR SON EVOLUTION

RETOUR D'EXPERIENCE DES E-MARCHANDS SUR LES DISPOSITIFS DE LUTTE CONTRE LA FRAUDE

B.1 LES ENJEUX DE LA FRAUDE POUR LES E-MARCHANDS

B.1.1 Les moyens de paiement au cœur de l'activité d'un E-Marchand

B.1.1.1 L'acte d'achat, là où tout se joue

Dans le commerce physique, le taux de transformation est de l'ordre de 50 % tandis que sur Internet il n'est que de 2 à 3 %. Dès lors, le E-Commerçant doit déployer des efforts très importants pour amener le client vers l'achat.

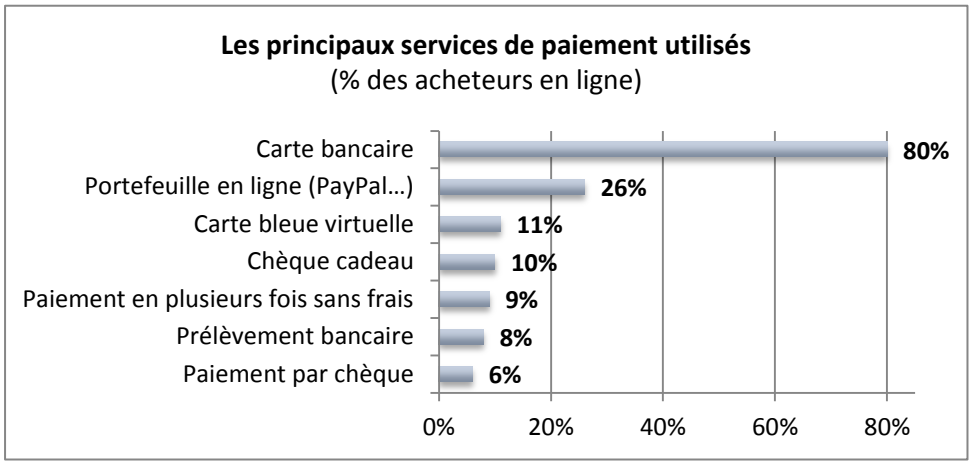
Pecheur.com rappelle ces trois points clé du paiement sur Internet :

- l'importance de la contextualisation; les pages d'achat doivent être esthétiquement belles et s'inscrire en harmonie avec les autres pages du site ;
- l'importance de la "fluidité" : les pages d'achat doivent se dérouler dans la continuité de l'acte d'achat pour ne pas créer de ruptures qui pourraient éveiller le doute ou la suspicion chez le futur acteur de l'acte d'achat ;
- l'importance de la rapidité : pecheur.com rappelle que les E-Marchands et leurs PSP "se battent pour gagner des millisecondes sur un acte de paiement qui ne doit pas excéder 30 secondes !" ;

Le paradoxe c'est qu'après avoir déployé tant d'efforts, le E-Commerçant perd le contrôle sur le déroulement de la transaction puisque la page de paiement peut ne pas être hébergée chez lui mais chez sa banque. Quant au processus d'authentification 3D Secure, le E-Marchand n'a aucun contrôle sur son déroulement.

B.1.1.2 La carte bancaire reste le moyen de paiement largement majoritaire

Il est bon de rappeler cette évidence; la sécurisation des paiements par carte bancaire est un enjeu majeur pour les E-Commerçants parce que c'est par ce moyen que s'effectue la très grande majorité des transactions !



Source : baromètre Fevad Médiametrie // NetRatings - juin 2013

La carte bancaire est le premier moyen de paiement en France depuis 2002. En 2010, on dénombrait 60 millions de cartes "CB" auquel il faut ajouter les cartes bancaires non marquées "CB" (environ 4 millions de cartes). Entre 2002 et 2010, le nombre de cartes bancaires et le nombre de paiements en France ont respectivement augmenté de 30 % et de 20,7 %.

Selon la FEVAD, 80 % des acheteurs déclarent utiliser la carte bancaire pour leurs achats en ligne.

La Fédération Bancaire Française rappelle que la France compte parmi les pays Européens les plus avancés en matière de moyens de paiement. 45% des paiements sont réalisés par carte, ce qui en fait le premier moyen de paiement utilisé en France.

Sans surprise, on retrouve cette prédominance de la carte bancaire comme moyen de paiement chez les E-Commerçants interviewés. Chez Vente-privee.com, en France, 100 % des transactions est réalisé au moyen d'une carte bancaire (Visa, MasterCard, Amex).

Sur le site Rueducommerce.com, la carte bancaire est présente dans environ 90 % des transactions effectuées, 85% chez Delamaison.fr, 70% chez Mistergooddeal.com, 55% pour Laredoute.com chez qui les cartes de paiement privatives ont un poids fort (33% des transactions).

B.1.1.3 Les autres moyens de paiements

Face à la très grande prédominance de la carte bancaire, les autres moyens de paiement apparaissent comme très marginaux. Pour autant, ils ne sont évidemment pas négligés par les E-Marchands qui ne peuvent pas se permettre de faire du moyen de paiement une barrière à l'achat!

Le rapport annuel 2011 de l'Observatoire de la sécurité des cartes de paiement établit une typologie de 4 familles de solution de paiement, en fonction des acteurs qui les proposent :

- des acteurs spécialisés dans les services de paiement sur Internet (par exemple Paypal, FiaNet avec l'offre Kwixo) ;
- des acteurs traditionnels (par exemple Crédit Mutuel avec l'offre Pay2You) ;
- des opérateurs téléphoniques (avec l'offre Buyster) ;
- des systèmes de paiement par carte tels Cartes Bancaires, Visa ou MasterCard.

PayPal

Chez les E-Marchands interviewés, la part des transactions effectuées avec PayPal peut atteindre jusqu'à 5% de l'ensemble des transactions. Un E-Commerçant interviewé résume ainsi l'appréciation généralement partagée : "Pour nous, PayPal est une très belle promesse faite au client, mais dont le coût pour le E-Marchand peut paraitre élevé".

Outre le fait que les clients de Delamaison.fr semblent le plébisciter, PayPal présente l'avantage pour Delamaison.fr d'accepter les cartes AMEX. Quel que soit le pays en Europe, Vente-privee.com constate que PayPal est un moyen de paiement significatif sur tous les marchés sur lesquels le site est présent.

La carte virtuelle dynamique (CVD)

Pour rappel, la CVD permet au client d'effectuer ses achats en ligne sur tous les sites marchands en France et à l'étranger, sans avoir à communiquer son numéro de carte réelle. L'utilisation de la CVD nécessite l'installation préalable par le Client d'une application sur son ordinateur.

Plusieurs marchands interviewés s'étonnent de la faible promotion de ce moyen de paiement par les banques. Pourtant, selon le Groupe 3 Suisses, la CVD répond à la fois aux besoins des banques de sécuriser les moyens de paiement et aux besoins du E-Marchand de lutter contre la fraude, même si le processus ne fluidifie pas le tunnel de paiement. RueduCommerce.com voit dans la CVD une réponse à la problématique de l'authentification des paiements fractionnés.

Au très faible taux de pénétration du produit, s'ajoutent selon certains E-Marchands, des difficultés de mise en œuvre. Le Crédit Mutuel, qui serait le principal distributeur de CVD n'identifie pas ses cartes dans le fichier BIN[1]. Ainsi, le E-Marchand est incapable de les repérer parmi d'autres numéros de cartes.

Au final, CB est un peu réservé sur l'avenir de ce moyen de paiement. La e-Carte Bleue est un produit lancé par Carte Bleue qui ne semble pas faire partie des produits que Visa souhaite particulièrement promouvoir.

Buyster, Kwixo … : les E-Marchands ne demandent qu'à y croire mais la démonstration se fait attendre...

Les E-Marchands interviewés sont tous attentifs à l'apparition de nouvelles solutions de paiement qui apportent une vraie plus-value notamment en ce qui concerne la prise en compte des spécificités du M-Commerce. Certains d'entre-deux ont même prêté main forte au lancement de ces solutions en les proposant très tôt à leurs clients pour contribuer à leur "massification" auprès du Grand Public.

C'est ainsi que Buyster, le moyen de paiement lancé en février 2011 conjointement par les principaux opérateurs mobiles Bouygues Telecom, Orange et SFR et par Atos Worldline est disponible chez plusieurs E-Marchands interviewés comme rueducommerce.com ou mistergooddeal.com.

[1] Voir définition en annexe

Kwixo la solution de paiement sécurisée qui permet de régler ses achats sur Internet et de transférer de l'argent entre particuliers est également citée par les E-Marchands interviewés. Pour rappel, cette solution développée par Crédit Agricole, FIA-NET Europe et LCL a été lancée en mai 2011.

Force est de constater qu'à côté des moyens de paiement "incontournables", les chances de s'imposer pour les moyens de "niche" sont très réduites.

B.1.1.4 L'Europe des moyens de paiement est loin d'être une réalité; une difficulté supplémentaire pour les E-Marchands

Même si le discours des marchands interviewés était principalement centré sur le marché français, certains d'entre eux, notamment ceux exerçant une activité à l'international, ont néanmoins fait part de leur retour d'expérience sur les différences qui pouvaient exister au niveau européen en ce qui concerne les moyens de paiement.

Le point de vue du juriste - L'Europe des paiements se réalise aujourd'hui dans le cadre du projet SEPA d'espace unique de paiement en euros ou Single Euro Payments Area, qui repose sur l'idée première qu'il ne devrait pas y avoir de distinction dans l'UE entre les paiements de détail électroniques en euros selon qu'ils sont transnationaux ou nationaux.

Concernant les moyens de paiement scripturaux (carte, virement, prélèvement), une étape importante a été marquée par l'adoption de la directive (d'harmonisation totale) 2007/64/CE du 13 novembre 2007 concernant les services de paiement (DSP), dont l'ambition fut la promotion d'un marché unique des services de paiements et la principale innovation la création d'une troisième catégorie de prestataires de services de paiements (PSP) : celle des établissements de paiement, prenant place aux côtés des traditionnels établissements de crédit et des nouveaux établissements de monnaie électronique.

À la suite d'un Livre vert intitulé « Vers un marché intégré des paiements par carte, par internet et par téléphone mobile », la Commissions a publié, le 24 juillet 2013, une proposition de DSP 2 visant à parfaire l'intégration d'un marché unique des paiements électroniques à l'heure du développement de l'économie numérique.

L'enjeu pour les E-Marchands ayant une couverture internationale est de parvenir à gérer des systèmes de lutte contre la fraude qui puissent tenir compte de la spécificité de chacun des moyens de paiement mis à la disposition de leurs clients quel que soit le pays.

Dans le débat sur l'évolution des moyens de paiement la dimension européenne est en effet très importante à prendre en compte notamment dans le cadre des différentes directives prises par la communauté européenne.

Certains acteurs du paiement sont évidemment incontournables quels que soient les pays : Visa MasterCard, Amex et PayPal notamment.

En revanche, il existe bel et bien des spécificités locales. Vente-privee.com rappelle qu'aux Pays-Bas, iDeal est le moyen de paiement incontournable. En Allemagne, Vente-privee.com considère comme nécessaire la mise en place de solutions de paiement comme ELV et Sofort.

Pour vente-privee.com, qui l'expérimente au travers de son implantation internationale, il y a de fait "deux Europe des moyens de paiement": une Europe du sud dans laquelle l'usage de la carte est prédominant, et une Europe du Nord dans laquelle l'usage de la carte est beaucoup moins fréquent (à l'exception de l'Angleterre, où comme en France, l'usage de la carte est prédominant). C'est particulièrement vrai en Allemagne, un pays très important pour le développement de vente-privee.com.

En Italie et en Espagne, les achats par carte sont prépondérants. La spécificité de l'Italie est l'importance des cartes pré payées, qui progressivement s'ouvrent à des acteurs étrangers.

B.1.2 Enjeux financiers, commerciaux et d'image

B.1.2.1 Enjeux financiers

La fraude impacte directement le résultat net du E-Marchand

Cette évidence mérite d'être rappelée : le montant de la fraude a un impact direct sur le résultat net du E-Marchand. Or, le E-Commerce reste une activité pour laquelle les marges opérationnelles sont relativement faibles et la profitabilité souvent à venir.

Une étude récente de CCM Benchmark / Webloyalty[2] montrait que sur l'ensemble du panel, seulement 50% des sites étaient rentables, avec certes de fortes disparités entre "sites leaders" et "petits sites". Et, parmi les sites ayant observé une hausse de leur rentabilité, l'amélioration du taux de conversion est mentionnée dans 56% des réponses comme raison de cette amélioration.

Dans ces conditions, des montants d'impayés de 300 000 ou 400 000 € comme ont dû en subir certains interviewés, peuvent avoir des conséquences dramatiques pour la poursuite de leur activité. D'autant plus que ces impayés surviennent brutalement en l'espace de deux ou trois mois seulement sans que le E-Marchand n'ait pu réagir.

Il faut également rappeler qu'en cas d'impayés, le marchand est doublement pénalisé: il est débité du montant des impayés par sa banque acquéreur (impact sur la trésorerie) et il doit prendre à sa charge la valeur de la marchandise expédiée (perte nette de résultat).

Pecheur.com réfute l'argument selon lequel certains E-Marchands considèreraient les impayés comme une avance de trésorerie (le E-Marchand livre un produit dont il sait qu'il fera probablement l'objet d'une contestation client). Pour Pecheur.com, entre les commissions perçues par la Banque et les frais d'impayés (50€), le taux de l'avance de trésorerie consenti par la banque serait prohibitif ! Sachant qu'en plus, le E-Commerçant ne maîtrise pas la date effectif du cash back l'intérêt de gérer sa trésorerie au moyen d'impayés est donc nul.

La fraude impacte directement le taux de commissionnement que paie le marchand à sa banque acquéreur

Outre la perte directe de revenu, la lutte contre la fraude revêt un second enjeu financier pour le E-Marchand, celui du montant des commissions qui sont prélevées par sa banque Acquéreur. Atos Wordline décrit de la façon suivante le lien entre le taux d'impayé que subit le E-Marchand et le taux de commission bancaire. Deux événements sont à distinguer: la date de demande d'autorisation (Autor) et la date de remise en banque (REB)

Le point de vue du juriste - Le contrat entre le E-marchand et sa banque acquéreur définit les conditions de la garantie des opérations et notamment la nécessité d'une authentification du porteur, d'une autorisation positive de l'opération et du respect d'un délai maximum de remise à l'encaissement. La règlementation interbancaire du paiement par carte (ou RIPC), établie par le GIE Cartes Bancaires, précise qu'une demande d'autorisation à l'émetteur (demander à l'émetteur de garantir le paiement de

[2] Etude CCM Benchmark / Webloyalty de mai 2013: enquête auprès des responsables de 65 sites d'e-commerce menée de février à mars 2013

l'opération de paiement) doit être systématiquement effectuée lors d'une opération de paiement à distance sécurisée CB. Lorsque la demande d'autorisation est délivrée par l'émetteur, le transfert de risque est accepté et l'opération de paiement est remise à l'acquéreur, ainsi garanti, qui peut présenter l'opération en compensation.

Ainsi, si ces conditions sont respectées, quel que soit le type d'incident (y compris les cas de litige commercial) qui ait pu survenir pendant la période de garantie, le E-marchand est assuré d'être crédité du montant de la transaction par sa banque acquéreur.

La période et les conditions de garantie dépendent du contrat de vente à distance entre le marchand et sa banque acquéreur (en générale la durée de la période de garantie est de six jours).

Le point de vue du juriste - Le contrat d'acceptation en paiement à distance sécurisé par cartes CB ou agréés CB (contrat VADS) prévoit (article 6.1) que toute réclamation par l'accepteur (le commerçant) doit être formulée par écrit à l'acquéreur dans un délai maximum de 6 mois à compter de la date de l'opération contestée, délai réduit à 15 jours à compter de la date de débit en compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

Ainsi, si le délai entre la remise en banque et la réalisation de l'opération de paiement (avec la demande d'autorisation) se situe dans la période prévue au contrat et qu'un incident se soit produit dans ce délai de six jours, alors le marchand est quand même garanti d'être crédité du montant de la transaction.

Si le délai est supérieur à celui prévu au contrat et qu'une transaction s'avère frauduleuse le e-marchand est exposé à un impayé sur cette transaction.

Une banque acquéreur ne devrait toutefois pas envoyer en compensation une transaction effectuée par une carte en opposition[3] sous peine d'être pénalisée. Or, ce n'est pas toujours le cas..

La recommandation à formuler au marchand pourrait donc être de :

- réduire au maximum le délai entre la demande d'autorisation et la remise en banque pour limiter son risque par rapport au délai figurant au contrat avec la banque acquéreur ;
- Veiller à ce que le PSP demande systématiquement une vérification OPOTTOTA[4] avant la mise en banque (soit au moment de la livraison si le marchand facture de cette façon) ;
- ou procéder à une demande d'autorisation au moment de la livraison (dans le cas d'une facturation à l'expédition).

B.1.3 Des enjeux sectoriels spécifiques

Aux enjeux partagés de façon générique par tous les E-Marchands, s'ajoutent des enjeux de la lutte contre la fraude spécifique par secteur, comme par exemple dans le transport/tourisme.

Lastminute.com décrit par exemple deux spécificités du secteur Transport / Tourisme.

[3] Présence de la carte dans le fichier OPOTTOTA au moment de la mise en compensation

[4] Voir définition en annexe

Débit du client uniquement sur confirmation de la disponibilité par le fournisseur

Comme on l'a vu précédemment, le risque pris par le E-Marchand est d'autant plus grand que le délai entre la demande d'autorisation et la remise en banque est long. Mais, les règles du secteur empêchent de débiter un client tant que la confirmation n'a pas été obtenue du fournisseur. Or le délai pour obtenir cette confirmation peut être long notamment dans le cas de la vente de "packages".

Remboursement impossible auprès des opérateurs low cost en cas d'annulation de la commande pour suspicion de fraude

Lastminute.com considère qu'il est doublement pénalisé par la fraude ; en subissant l'impayé d'une part et, d'autre part, en supportant le coût de la "non réservation" dans le cas de vols non remboursables. La bonne évaluation du risque de fraude a donc des impacts financiers très importants. Pour en atténuer les effets, Lastminute.com a passé des accords avec certains tour operator aux termes desquels Lastminute.com peut être remboursé en cas de suspicion de fraude, si cette dernière intervient dans les 24 heures suivant la commande.

B.2 UNE PERCEPTION DE LA FRAUDE DIFFERENTE EN FONCTION DES ACTEURS

B.2.1 Vision de la fraude par les E-Marchands

B.2.1.1 Les E-Marchands soulignent le développement de la part des répudiations abusives dans les motifs de la fraude

Une répudiation abusive peut se définir assez simplement comme la répudiation par le porteur de la carte d'une transaction dont il est bel et bien l'auteur. Elle provoque un impayé chez le E-Marchand.

Ils sont unanimes à considérer que ce type de fraude s'est développé. Pour certains, c'est même la principale raison du développement global de fraude récemment enregistré.

Ainsi, Pecheur.com est persuadé qu'en France plus de la moitié des fraudes a pour origine la répudiation abusive. Pour Pecheur.com, les fausses répudiations ou "répudiations commerciales" devraient même être sorties des statistiques de fraude !

Pour Pecheur.com, il n'est pas normal qu'un client puisse annuler une transaction pour un litige commercial. L'achat et le litige commercial doivent rester dissociés. Un chèque ne peut pas être annulé en cas de litige commercial. Pourquoi en serait-il différemment pour les paiements par cartes ?

Le point de vue du juriste - Le contrat porteur CB stipule expressément que « les réclamations qui portent sur le prix des biens ou services achetés ne sont pas recevables auprès de l'Emetteur. Seules celles qui portent sur l'absence ou la mauvaise exécution de l'ordre de paiement donné par le Titulaire de la carte "CB" à l'Emetteur sont visées par le présent article » (art. 16.2, al. 1er).

Pour Pecheur.com, il est indispensable de rappeler les risques encourus par le Client en cas de fausse répudiation qui, sinon, apparait aux yeux du grand public comme "facile". L'effort de

pédagogie doit être renforcé ! "*Il ne sert à rien de chercher à élever la hauteur de la barrière, si le fraudeur n'a pas même conscience qu'il y en a une* !"

Le constat est partagé par PriceMinister.com pour qui les répudiations abusives expliquent en grande partie le développement de la fraude constaté en fin d'année 2011 et début 2012.

Pour Laredoute.com, certains clients mal intentionnés ont parfaitement intégré le fait que la répudiation d'un achat est finalement simple et souvent sans risque. Ces clients comptent sur le fait que le marchand n'engagera pas de procédures compte tenu des faibles montants en jeu.

Pecheur.com le confirme; les petits E-Marchands, qui n'ont pas les moyens de collecter les éléments de preuve, sont démunis contre les fausses répudiations.

En cas de contestation sur une répudiation d'achat, c'est en effet au E-Marchand d'apporter la preuve de son bon droit. Le rassemblement des preuves n'est pas forcement simple; elle requière la mobilisation de ressource chez le E-Marchand.

Cela fait dire à Laredoute.com que les E-Commerçants n'ont pas toujours une vision "globale" et "objective" de la fraude. Il peut leur arriver d'exclure du calcul du taux de fraude des remboursements qu'ils concèdent aux clients sous prétexte de litiges commerciaux mais qui sont bel et bien des répudiations abusives ... donc une fraude !

Pour les E-Marchands, la crise a joué un rôle manifeste dans le développement de ce type de fraude. Mais, ils citent également un autre élément conjoncturel, la suppression de la nécessité du dépôt de plainte, depuis août 2011.

Une dépêche du ministère de la justice a en effet demandé le 12 août 2011, aux procureurs généraux, d'indiquer aux officiers de police judiciaire de ne plus effectuer d'enregistrement de plaintes liées à des fraudes à la carte bancaire, arguant que ce dépôt de plainte n'était pas nécessaire au remboursement du consommateur par la banque.

Pour un grand nombre d'interviewés, cette mesure a rendu moins impliquant, pour les clients-fraudeurs, les répudiations abusives. Priceminister.com va même jusqu'à considérer que cette directive a constitué un « permis de frauder ».

Priceminister.com recommande que la possibilité de déposer plainte soit rétablie et appelle plus globalement à un support plus actif des pouvoirs publics pour endiguer la fraude par fausses répudiations.

Les E-Marchands interviewés constatent que bien souvent les consommateurs-fraudeurs n'ont pas conscience des risques pénaux qu'ils encourent (pour Pecheur.com, le manque d'information sur le délit de répudiation abusive est patent) et que, plus grave encore, ils n'ont pas le réel sentiment de réaliser un acte répréhensible.

Dans leur esprit, il n'est même pas évident que le E-Marchand subira un préjudice. Ils pensent qu'il sera, d'une façon ou d'une autre, remboursé par sa banque. Pour Priceminister.com, la pratique de la répudiation abusive s'inscrit dans la croyance générale que "sur Internet, tout est gratuit" !

Les E-Marchands reconnaissent ce mérite à 3D Secure de rendre plus difficile pour le porteur la répudiation abusive et plus facile pour le E-Marchand ou la banque émettrice d'en apporter la preuve. CB confirme que la mise en œuvre systématique de 3D Secure protège le E-marchand de tous les risques de contestation de la part des clients, abusive ou non.

Le point de vue du juriste - Le terme de « répudiation », courant en pratique, n'est pas un terme juridique. Le Code monétaire et financier (CMF) ne connaît que les cas d'une opération de paiement autorisée par le porteur (consentement donné à l'exécution d'une opération de paiement valant ordre

de paiement et entraînant son irrévocabilité une fois reçu par le prestataire de services de paiement du payeur ; montant de l'opération crédité sur le compte du prestataire de services de paiement (PSP) du bénéficiaire au plus tard à la fin du premier jour ouvrable suivant le moment de la réception de l'ordre de paiement) ou non autorisée : lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, le porteur en informe sans tarder son PSP (ou au plus tard dans les 13 mois suivant la date de débit), aux fins de blocage ou d'opposition de l'instrument ; le PSP rembourse alors immédiatement le porteur du montant de l'opération non autorisée, sauf à ce que l'opération de paiement non autorisée soit consécutive à la perte ou au vol de l'instrument de paiement, auquel cas le payeur supporte, …

… avant blocage ou opposition, les pertes liées à l'utilisation de cet instrument dans la limite d'un plafond de 150 € (somme qui serait ramenée à 50 € dans la proposition de DSP 2).

La responsabilité du porteur n'est toutefois pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé (tout moyen technique propre à l'authentifier, tels le code confidentiel pour le paiement de proximité ou les données carte en cas de vente à distance : numéro, date de validité et cryptogramme visuel). Au contraire, le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisée si ces pertes résultent d'un agissement frauduleux de sa part. Sauf que, pratiquement, la preuve d'une opération non autorisée pèse sur le PSP et s'avèrera presqu'impossible en cas de vente à distance. Car « *lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre* », étant ajouté que « *l'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière* » (CMF, art. L. 133-23).

Du côté des contrats CB, on note que pour faciliter la preuve du paiement, le préambule du contrat d'acceptation en paiement sécurisé par cartes CB et agréées CB (contrat VADS) invite à limiter l'utilisation du seul numéro de carte pour donner un ordre de paiement, d'où la mise en place de procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de cartes tel que le protocole 3D Secure. Du côté du contrat porteur, il est prévu que « *lorsque le Titulaire de la carte "CB" nie avoir donné son consentement pour réaliser une opération de paiement et/ou de retrait, il appartient à l'Emetteur d'apporter la preuve que l'opération a été authentifiée, dûment enregistrée et comptabilisée conformément à l'état de l'art et qu'elle n'a pas été affectée par une déficience technique. Cette preuve peut être apportée par tous moyens, notamment par les enregistrements des Equipements Electroniques ou leur reproduction sur un support informatique de l'utilisation de la carte "CB" et du dispositif de sécurité personnalisé* » (art. 10.1). S'agissant du remboursement des opérations non autorisées (ou mal exécutées), l'article 17 du contrat porteur stipule :

« Le titulaire de la carte "CB" et/ou du compte sur lequel fonctionne la carte "CB", est remboursé :

- du montant des débits contestés de bonne foi par le Titulaire de la carte "CB" dans le cas de perte et/ou vol, d'utilisation frauduleuse ou de détournement de sa carte "CB" et des données qui y sont liées, pour des opérations survenues avant la demande d'opposition (ou de blocage)(…) ;

- du montant de tous les débits contestés de bonne foi par le Titulaire de la carte "CB", pour des opérations survenues après la demande d'opposition (ou de blocage) (…) de telle manière que le compte débité est rétabli dans l'état où il se serait trouvé si le débit des montants contestés n'avait pas eu lieu ;

- du montant de tous les débits correspondant à des opérations mal exécutées ».

Enfin, selon la réglementation interbancaire du paiement par carte (RIPC), le traitement des réclamations d'un titulaire de carte est sous la seule responsabilité de l'émetteur, la réclamation devant être émise dans un délai maximum, à compter de la date d'écriture en compte, fixé par le contrat porteur entre 70 et 120 jours).

B.2.2 La fraude vue du consommateur

D'après l'étude annuelle menée par l'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP)[5], en 2011, 650 000 ménages (2,3 % du total) ont déclaré avoir été victimes d'au moins un débit frauduleux sur un compte bancaire, contre 500 000 (1,8% des ménages) en 2010.

Toujours d'après cette étude, dans 70 % des cas ce sont les consommateurs qui ont détecté la fraude, les banques n'ayant prévenu les clients que dans 22 % des cas.

47 448 falsifications et usages frauduleux de cartes de crédit ont été constatés en 2011, représentant 13,6 % des escroqueries et infractions économiques et financières.

On notera que l'Acte pour le marché unique II (« Ensemble pour une nouvelle croissance », Action-clé n° 8 : « Soutenir l'offre de services en ligne, en rendant les services de paiement dans l'UE plus efficaces »), constatait, fin 2012, que « *35 % des internautes n'effectuent pas d'achats sur l'Internet du fait de leurs appréhensions quant aux méthodes de paiement* ». La confiance des consommateurs est donc une priorité.

B.2.3 Vision de la fraude par les banques

Pour CB, du point de vue des banques, les fraudes sur les moyens de paiement se segmentent en trois catégories: la fraude VAD, la fraude sur les paiements de proximité, la fraude sur les retraits (cf. dernier rapport OSCP).

Il faut également distinguer la fraude sur les porteurs français en France, la fraude sur les porteurs français à l'étranger et enfin la fraude sur les porteurs étrangers en France.

Pour CB, l'attention des banques émettrices se porte en priorité sur la fraude sur les paiements de proximité et la fraude sur les retraits. Ces deux derniers types de fraudes concentrent en effet les principaux risques de fraude nette pour les banques émettrices.

En comparaison, le risque lié aux fraudes sur des transactions authentifiées 3D Secure est marginal pour les banques émettrices. Néanmoins les banques émettrices surveillent de près la fraude brute qui génère des charges de back-office et une gêne pour leurs clients (impact d'image et coûts de gestion de la contestation Client).

Pour suivre l'évolution de la fraude, CB se fonde principalement sur les déclarations émises par les banques. CB possède une visibilité globale de la fraude car c'est une obligation, pour les banques, de déclarer les fraudes constatées.

[5] Résultats de l'enquête de victimisation « Cadre de vie et sécurité », réalisée en partenariat avec l'INSEE. Cette enquête complète les données fournies par l'ensemble des administrations ou organismes publics ou privés relatives à la délinquance, à partir des réponses collectées auprès de plus de 17 000 ménages ou personnes de 14 ans et plus.

Selon le rapport 2012 du GIE Cartes Bancaires, il a été décidé de mettre en place une procédure d'agrément pour les plateformes techniques du commerce électronique et de paiement sur Internet.

Dans le cas particulier de la VAD en France, CB analyse également les impayés. Il arrive en effet que les banques émettent des impayés[6] mais n'émettent pas de déclaration de fraude. Ces impayés sont réintégrés par CB dans les calculs du taux de fraude.

B.2.4 Vision de la fraude par la Banque de France et l'OSCP

Le rapport 2011 de la Banque de France sur la surveillance des moyens de paiement et des infrastructures de marché relève que « l''authentification de l'internaute ou du porteur de la carte étant cruciale s'agissant d'opérations effectuées à distance, la Banque de France a demandé en 2008 aux banques d'équiper leurs clients de solutions d'authentification non rejouable, pour une partie significative de la clientèle en 2009, puis de généraliser l'usage de telles solutions dès juin 2010 ».(p. 32).

Son rapport annuel 2012 évoque sa mission d'assurer la sécurité des moyens de paiement scripturaux et met en avant le fait que, « sur un plan national, la Banque de France a poursuivi ses actions visant à lutter contre la fraude sur les paiements par carte à distance qui, bien que ne représentant que 8,4 % des transactions nationales, comptent désormais pour 61 % de la fraude » (p. 56).

S'agissant du rapport annuel 2012 de l'Observatoire de la sécurité des cartes de paiement (OSCP), on note que les E-Commerçants sont invités à mettre en « œuvre plus largement les dispositifs de sécurisation permettant l'authentification renforcée des porteurs, tels que "3D Secure", **à chaque fois que cela est possible et pertinent** ».

Le taux de fraude nationale sur les paiements en ligne demeure toutefois faible en pourcentage, même si les montants (en millions d'euros) sont conséquents : 2008 : 0,235 (33,8) ; 2009 : 0,263 (51,9) ; 2010 : 0,276 (73,9) ; 2011 : 0,341 (104,2= et 2012 : 0,290 (109,4).

B.2.5 L'impayé, le dénominateur commun entre E-Marchands et banquiers

Si, comme évoqué dans les paragraphes précédents, E-Marchands et banquiers ne développent pas tout à fait la même vision de la fraude, c'est bien l'impayé qui semble néanmoins en constituer le dénominateur commun.

Le point de vue du juriste - Techniquement (mais non pas juridiquement, la notion étant absente du Code monétaire et financier), l'impayé est défini par le Règlement des impayés et opérations de remboursement (RIOR) comme « *un mouvement de compensation dont l'objet est d'inverser le sens de l'écriture d'une opération initiale de paiement ou de retrait, au motif que l'opération n'est pas recevable par l'émetteur suite au non respect des règles sécuritaires par l'accepteur* ».

[6] Un impayé est une opération financière qui doit passer en compensation pour faire l'objet d'un règlement. La déclaration de fraude se limite à une simple information.

Un impayé peut avoir trois origines possibles.

- le litige commercial (non applicable dans le cas d'un paiement CB) : le client prend contact avec sa banque et lui indique qu'il refuse de payer un produit ou un service en raison de sa non-conformité par rapport à sa commande, réelle ou supposée (cf. répudiation abusive).
- l'usurpation d'identité ;
- l'opération frauduleuse suite à usurpation d'identité ou le vol ou perte de carte (pas d'impayé dans le cas de la mise en œuvre de 3D Secure par le E-marchand et sa banque acquéreur).

Lorsqu'il se produit, l'impayé peut donner lieu à ce qui est communément appelé un "charge back" de la banque Acquéreur sur le E-Marchand. En clair, la banque débite sans préavis le compte du E-Marchand de la somme de l'impayé, dans les conditions prévues au contrat.

Le délai d'apparition du Charge Back peut varier considérablement en fonction des éléments suivants :

- Délai nécessaire au porteur de la carte pour s'apercevoir de l'utilisation frauduleuse de sa carte et du délai de mise en opposition ;
- Délai de traitement de la demande par la banque émettrice ;
- Délai de traitement au sein de la banque Acquéreur.

Selon Be2bill, le délai moyen d'instruction entre la mise en opposition d'une carte et une demande de charge back est de un à deux mois, avec une très forte variabilité.

Charge back et mise en opposition de la carte

Be2bill confirme que certaines transactions peuvent être passées en "Charge Back" sans pour autant que la carte ait été préalablement mise en opposition. Ce cas n'est évidemment pas le plus fréquent.

Les différents cas de *charge back* qui n'entrainent pas le blocage de la carte:

- (hors CB) litiges commerciaux : le client conteste la livraison du produit ou du service (par exemple produit non conforme à sa description). Ces motifs sont considérés comme valables pour VISA et MasterCard; ils ne le sont pas pour CB. Ainsi, il ne peut y avoir ce type de *charge back* sur une transaction réalisée par un marchand en France et une carte CB. En revanche un porteur français est en droit de contester un achat réalisé chez un marchand dont la banque n'est pas située en France.
- les transactions techniquement invalides ou "transactions dupliquées" : le client constate que la transaction a été débitée deux fois de son compte.
- (hors CB) « *Friendly charge back* » [7]: cas de l'utilisation non autorisée de la carte par un proche. Le client conteste la transaction mais ne souhaite pas bloquer sa carte. L'importance du « *friendly charge Back* » varie selon le secteur d'activité ; il est relativement important dans le secteur de la vente de contenus numériques.

[7] CB souligne que l'utilisation d'une carte par une personne autre que le titulaire est une fraude (y compris un proche ou membre de la famille.)

Mise en opposition des cartes « par erreur »

Il existe des cas de mise en opposition des cartes « par erreur » (relativement fréquent dans le secteur du jeu en ligne). Par exemple, un porteur met en opposition la carte du compte joint parce qu'il croit à une utilisation frauduleuse de la carte alors que finalement c'est le conjoint qui l'a utilisée. On constate à ce sujet de grandes différences de comportements en fonction des pays; un porteur allemand fera beaucoup plus systématiquement la démarche d'avertir la banque émettrice d'une mise en opposition de la carte « par erreur » qu'un porteur français.

B.2.6 La fraude sur les moyens de paiement calculée différemment par les E-Marchands et les Banques

Pour Rueducommerce.com, la Banque de France et les E-Marchands ne semblent pas calculer le taux de fraude de la même manière. Le E-Marchand exclut généralement du taux de fraude les tentatives de fraude qui sont détectées avant la livraison effective du produit et qui n'engendrent dès lors aucun préjudice. Dans ce cas, il n'y a pas de «Dol». En revanche, ces transactions sont incluses dans le taux de fraude calculé par la Banque de France, si les transactions sont remises en compensation.

Rueducommerce.com constate ainsi un nombre important de transactions clients finalement annulées puisque l'expédition n'est pas réalisée, une tentative de fraude ayant été détectée avant l'envoi de la marchandise. Pour Rueducommerce.com, la comptabilisation actuelle des fraudes génère "une pollution administrative" dans les reportings du E-Commerçant et des banques.

Cette différence ne vaut que pour la livraison de produits physiques pour lequel il y a un délai entre le paiement et la livraison ou quand la facturation a lieu à la commande et pas à l'expédition; elle ne vaut pas pour le commerce de biens immatériels ou de services rendus « dans l'instant ».

Rueducommerce.com relate un autre cas concret de différence de comptabilisation de la fraude entre E-Marchands et Banques.

Par l'intermédiaire d'une de ses banques acquéreurs, Rueducommerce.com a été averti par sa banque Acquéreur d'une brusque hausse de son taux de fraude. Après analyse par son prestataire Atos Wordline, Rueducommerce.com a constaté que les transactions incriminées correspondaient en fait à des tentatives de fraude en masse opérées par des fraudeurs qui cherchaient à tester des faux numéros de cartes. Ces transactions en provenance de sites étrangers, notamment estoniens ou lituaniens étaient systématiquement bloquées par Rueducommerce.com. Dès lors, elles n'étaient pas "vues" par Rueducommerce.com comme des impayés mais apparaissent bien dans les chaînes de traitement bancaires.

Pour CB, les E-Marchands ne mesurent pas la fraude dans son ensemble mais uniquement « la fraude qui reste à leur charge ». Du point de vue de CB, dès lors que le E-Marchand présente une opération en compensation et que cette dernière revient en impayé, il y a fraude, et cela même si la transaction frauduleuse a été détectée par le E-Marchand avant l'expédition et qu'elle ne lui a pas causé de préjudice.

Pour CB, une transaction doit être considérée comme frauduleuse quand le porteur conteste la transaction et qu'un impayé a été généré. L'impayé concrétise le fait qu'une transaction a pu être passée sur le site du E-Marchand de façon frauduleuse. Le E-Marchand sera bien crédité du montant de la transaction puis débité de l'impayé.

Pour CB, les seuls cas de fraudes qui ne sont pas comptabilisés (et qui sont donc exclus des statistiques produites par CB) sont les cas des tentatives de fraude détectées par le E-Marchand avant la remise en banque.

Ces cas peuvent notamment se produire quand le débit a lieu "à la commande" et pas "à l'expédition". C'est le cas notamment chez vente-privee.com compte tenu de la particularité du business modèle. Ainsi, Vente-privee.com confirme que si l'annulation de la transaction a lieu dans un délai de 24 à 48 heures (à la suite des résultats de l'analyse de risque), elle n'est pas comptabilisée par Visa et MasterCard comme un impayé.

B.2.7 Le calcul du taux de fraude : un exercice difficile

Le taux de fraude est le rapport entre le montant des transactions frauduleuses et le montant total des transactions réalisées par les contrats VAD. Ce taux est calculé par CB ainsi que par les autres réseaux (Visa, Mastercard, Amex...). Il est publié par l'OSCP.

Pour le GIE, la difficulté n'est pas de calculer le montant de la fraude mais de calculer le chiffre d'affaires auquel il est rapporté.

L'estimation du chiffre d'affaires total VAD ne peut pas provenir du réseau de compensation bancaire français qui ne fournit pas de statistiques détaillées par type de transaction. De plus, certaines transactions ne transitent pas par le réseau de compensation (cas d'une banque à la fois émettrice et acquéreur).

Pour estimer le chiffre d'affaires total VAD, CB se fonde donc sur le déclaratif des banques acquéreur (déclarations mensuelles par SIRET). C'est là que réside la difficulté car, il peut arriver qu'un même commerçant exerce plusieurs activités pour un même SIRET. Par exemple, un opérateur Telecom peut exercer une activité de VAD conjointement avec une activité commerciale "off line" via son réseau de distribution physique.

Or, pour CB, il est difficile de dissocier la part du chiffre d'affaires réalisé en VAD du total du chiffre d'affaires. Il ne peut être qu'estimer grâce aux "autorisations préalables". Dans la VAD en effet, toutes les transactions font l'objet d'une autorisation préalable (à la limite près que certaines autorisations ne sont pas visibles de CB, les autorisations intra banques notamment).

Il n'en reste pas moins que les tendances observées restent non seulement pertinentes mais utiles à l'analyse de l'évolution de la fraude.

B.3 L'EVOLUTION QUANTITATIVE ET QUALITATIVE DE LA FRAUDE VUE PAR LES E-MARCHANDS

B.3.1 Evolution quantitative de la fraude

Dans son rapport annuel d'activité 2012, l'OSCP constate pour la première fois depuis 2008 que le taux de fraude sur les paiements sur Internet diminue pour atteindre 0,290 % (contre 0,341 %, son maximum historique en 2011). La fraude continue de progresser mais à un rythme moins soutenu que la croissance du marché. A noter que l'OSCP attribue ce bon résultat aux efforts réalisés conjointement par les émetteurs et les E-Commerçants pour déployer des dispositifs d'authentification forte tels que 3D Secure.

L'ensemble des paiements à distance, qui représente 9,2 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude.

La fraude sur les paiements à distance en France représente 138,8 millions d'euros en 2012[8].

Toujours selon le rapport 2012 de l'OSCP, le taux de fraude sur les transactions internationales (0,387 %) reste huit fois plus élevé que le taux de fraude sur les transactions nationales (0,045 %). Les transactions internationales représentent ainsi un peu plus de 10,3 % de la valeur totale des transactions par carte (pour un montant de 224,3 millions €), mais comptent pour 49,8% du montant total la fraude.

De son côté, le GIE Cartes Bancaires a constaté dans son rapport annuel 2012 une augmentation de la fraude en paiements domestiques de 6 % (182 millions €), augmentation principalement due au poids toujours important de la fraude en vente à distance, qui représente les ¾ du total de la fraude en paiement domestique.

B.3.1.1 Distinguer "taux de fraude" et "volumes" de fraude

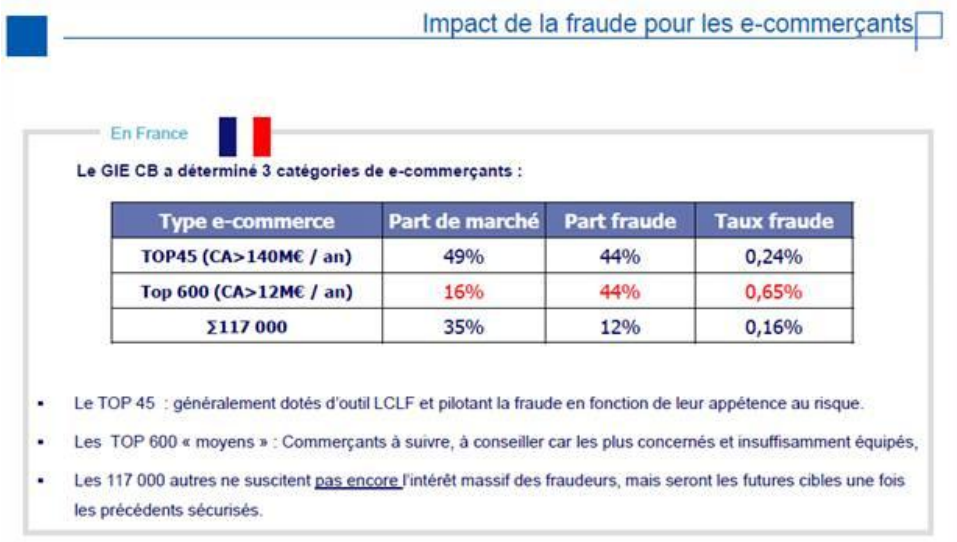
Quantitativement, la fraude concerne un nombre relativement limité de E-Commerçants

Quand on observe les chiffres fournis par CB, on constate que 50 % de la fraude sont "produits" par seulement une cinquantaine de sites. Plus impressionnant encore, un seul (qui a un taux de fraude faible) réalise à lui seul 8% du montant des transactions frauduleuses ! Ces sites réalisent également 50 % de l'activité du E-Commerce en France. Les 50% restant sont réalisés principalement par des sites de taille moyenne. Les tout petits sites pèsent très peu dans le montant global de la fraude car ils génèrent un nombre de transactions très limité et ils intéressent peu les fraudeurs !

On peut donc en tirer la conclusion (un peu hâtive) que la fraude serait finalement un phénomène assez concentré. Il suffirait d'appliquer aux sites les plus importants "le" remède miracle contre la fraude (3D Secure par exemple) et le tour serait joué ! La question est évidemment un peu plus complexe que ça !

A de très rares exceptions près, les gros E-Commerçants en France ont des taux de fraude très bas et maîtrisés.

Le graphique réalisé par le CB, repris ci-après, montre bien que les plus gros E-Marchands ont les taux de fraude les plus bas !



[8] Dont fraude par courrier et téléphone et fraude internet

Source : GIE Cartes bancaires 2011

Même si aucun "gros" sites n'est à l'abri d'une recrudescence violente de la fraude, ces sites maîtrisent bien le risque de fraude et savent réagir de façon appropriée. C'est ce que confirme CB quand il constate que la fraude "tourne" entre les gros E-Marchands.

Ainsi, un E-Marchand peut voir son taux de fraude brutalement se détériorer, faire partie des E-Marchands les plus fraudés, prendre des actions de lutte contre la fraude et disparaître de la liste ! Ce qui, d'ailleurs rend complexe le suivi réalisé par CB. Le temps de rencontrer le E-Marchand, le problème est résolu !

Sans surprise, aucun des E-Commerçants interviewés, dont plusieurs font partie des plus gros sites de E-commerce en France, n'a déclaré que son taux de fraude dépassait la moyenne nationale publiée par l'OSCP. La plupart ont même indiqué que leur taux de fraude se situait bien en deçà du chiffre de 0,29% en 2012, mais sans pour autant vouloir en donner le chiffre à l'exception de Mistergooddeal.com (0,0197 %) et Priceminister (0,1%) .

Le paradoxe de l'effet volume

Ainsi, c'est parce qu'ils génèrent le plus de transactions que les gros E-Marchands enregistrent les volumes de fraude les plus importants :

Taux de fraude bas X Volume élevé de transaction = **Volume de fraude important**

Ainsi, la question centrale pour un gros E-Marchand est de parvenir à réduire un niveau de fraude déjà très bas. Or, c'est précisément les quelques dixièmes ou centièmes de point en moins sur le taux de fraude qui sont les plus complexes à aller chercher.

B.3.1.2 Situation de la France en Europe :

Chiffres européens

Le deuxième rapport sur la fraude à la carte de paiement publié le 16 juillet 2013 par la Banque centrale européenne (BCE) constate une diminution de celle-ci depuis 2007, grâce aux avancées technologiques rendant les transactions plus sûres (standard de sécurité des cartes à puce EMV en particulier). La fraude se déplace toutefois vers les pays où la technologie demeure moins développée (l'Irlande compte par exemple plus d'une transaction frauduleuse sur 1 000, par rapport à la moyenne de la zone euro de l'ordre d'une transaction sur 4 000).

Les cartes émises au Luxembourg, en France et au Royaume-Uni ont enregistré en moyenne les pertes au titre de la fraude les plus élevées en pourcentage des transactions régulières.

Le montant total de la fraude s'est élevé à 1,16 milliards € en 2011, soit une baisse de 5,8 % par rapport à 2010. Entre 2007 et 2011, le montant total de la fraude a diminué de 7,6 %, tandis que la valeur totale des transactions s'est accrue de 10,3 %. Il n'en demeure pas moins que ce constat est accablant : "*€1 of fraud per €2,805 spent*" (Communiqué de presse de la BCE).

En 2011 toujours, 56 % environ de la valeur de la fraude résultait des paiements à distance (par courrier, par téléphone ou sur internet). Sa valeur absolue est passée de 648 millions en 2010 à 655 millions € en 2011, les paiements à distance s'étant réalisés en très grande majorité (73 %) sur internet.

En matière de fraude, l'Angleterre est-elle si exemplaire ?

CB relativise les statistiques de fraude anglaises en rappelant que, dans ce pays, le règlement des impôts et taxes s'effectue très majoritairement par Internet. Ce n'est absolument pas le cas en

France. Or, ce type de transaction est rarement fraudé ! Pour autant, elles entrent dans le décompte total des transactions et diminuent en conséquence le taux de fraude global.

Selon CB, Visa indiquerait que le taux d'utilisation de 3D Secure en l'Angleterre ne serait "que" de 50% en valeur (contre 25% en France). On est loin d'une utilisation systématique de 3D Secure comme l'indiquent certains media !

Par ailleurs, comme l'ont indiqué certains interviewés, ce qui importe réellement, ce sont les demandes d'authentification 3D Secure qui vont à leur terme. Or, il est fréquent en Angleterre de rattraper une transaction d'un client qui ne parvient pas à s'identifier; quand cela arrive, les règles d'authentification sont parfois minimalistes.

La France mal préparée à la fraude du fait de son niveau historiquement bas de fraude sur les paiements de proximité ?

En France, historiquement, le niveau de fraude sur les paiements de proximité était bas grâce à la généralisation de la carte à mémoire. Ce n'était pas le cas dans les autres pays européens (notamment en Angleterre) qui en conséquence ont vu se développer des solutions de lutte anti-fraude beaucoup plus précocement qu'en France. Ainsi, ces pays ont-ils été probablement mieux préparés au développement de la fraude sur les moyens de paiement à distance.

B.3.1.3 Le ressenti des E-Marchands interviewés sur l'évolution quantitative de la fraude

Vente-privée.com

Jusqu'à très récemment, Vente-privee.com considérait que son taux de fraude était suffisamment « acceptable» pour ne pas justifier une évolution de son dispositif anti-fraude.

L'activité de vente-privee.com était peu exposée au risque de fraude pour au moins deux raisons; d'abord des délais de livraison importants (en moyenne de 15 jours), ensuite des produits vendus moins attractifs pour les fraudeurs que ceux proposés par d'autres sites moins bien protégés.

Mais, récemment, le site a enregistré une augmentation de son taux de fraude (qui reste néanmoins inférieur au taux moyen donné par la Banque de France). Vente-privée explique cette soudaine progression de la fraude par deux éléments qui se sont cumulés; la plus forte attractivité des produits vendus pour les fraudeurs du fait de l'élargissement de l'offre et la fin du « parrainage client », il y a plus d'un an.

Groupe 3 Suisses

Le Groupe 3 Suisses considère que son taux de fraude actuel est faible et maîtrisé. Il y a deux ans, l'application de règles de filtrage « simples » a permis d'endiguer une augmentation du taux de fraude sur la carte bancaire. Le simple apport d'expertise sur les techniques de détection de fraude au niveau du front office a déjà permis d'atteindre de bons résultats.

Priceminister.com

Le taux de fraude de Priceminister.com en valeur est de 0,1 % du chiffre d'affaires. Après une période difficile fin 2011 et début 2012, le site considère que son taux de fraude est maintenant maîtrisé.

A noter, le développement du piratage des comptes au moyen de *spyware* a contraint Priceminister.com à revoir complètement sa stratégie de lutte contre la fraude qui, jusqu'à présent, était fondée sur une white list.

Laredoute.com

Pour laredoute.com, il est très peu probable que le niveau général de la fraude baisse. Il atteindra très probablement un palier puis n'évoluera plus. La question sera donc de savoir qui devra en supporter le coût!

B.3.2 Evolution qualitative

B.3.2.1 Vers une professionnalisation de la fraude

La fraude s'est professionnalisée. Ce constat est unanimement partagé par les E-Marchands interviewés.

Le service anti-fraude de Priceminister.com considère avoir en face de lui de "véritables professionnels" qui connaissent parfaitement le monde internet, ses outils et le fonctionnement des sites. Leurs techniques évoluent en permanence. Ces professionnels conçoivent de véritables stratégies d'attaque des sites. Ils savent analyser le risque : "La fraude est devenue un véritable métier !"

Le constat est partagé par la Fédération Bancaire Française pour qui la fraude devient de plus en plus technique et requière une expertise de plus en plus pointue. Elle est par ailleurs très "dynamique"; les fraudeurs cherchant en permanence à détecter les failles des systèmes de protection en visant une fraude la plus "efficace possible" avec les meilleurs rendements.

L'impression des E-Commerçants d'une professionnalisation de la fraude se fonde principalement sur les éléments décrits ci-après:

La sophistication des "schémas (patterns)" de fraude

Les E-Commerçants interviewés constatent que les «schémas de fraude» se sont complexifiés. Au bon vieux principe de la "mule" (toujours à l'oeuvre), sont apparus des schémas beaucoup sophistiqués comme par exemple celui de la triangulation: le fraudeur repère un acheteur sur un site comme "Le Bon Coin". Le fraudeur vend à l'acheteur le produit recherché et encaisse le montant de la transaction. Le fraudeur achète ensuite le produit sur un autre site, au moyen d'une carte volée. Il fournit les coordonnées du premier acheteur comme adresse de livraison. L'acheteur a acheté en toute bonne foi une marchandise achetée frauduleusement.

PriceMinister.com a été récemment victime de ce type de fraude qui impliquait (à son corps défendant évidemment) le site Darty.com (site sur lequel les marchandises étaient achetées) et le site Priceminister.com qui était utilisé pour la revente de la marchandise frauduleusement achetée.

Le développement de ce type de fraude a été facilité par la multiplication, sur les cinq ou dix dernières années, des plates-formes de mise en relation électronique d'un acheteur et d'un vendeur et ce, pour tous types de produits sur Internet.

La rapidité d'action des fraudeurs

Laredoute.com l'a constaté : dans un délai de temps très court, des transactions peuvent être passées à partir d'une même carte à partir de plusieurs pays.

La rapidité avec laquelle les fraudeurs sont capables de repérer une faille dans le système de protection et la capacité des fraudeurs à « lire » les filtres qui sont mis en place

CDiscount.com donne l'exemple de 12 fraudes en 6 heures sur des cartes non enrôlées à la suite de la mise en place de 3D Secure sur des produits sensibles. Une telle dextérité ne peut être

atteinte que par des fraudeurs aguerris, ce qui fait dire à Be2bill que s'est développée une véritable expertise technique de la fraude poussée par «des individus particulièrement habiles dans ce domaine».

La mobilisation de moyens "industriels"

CDiscount.com a pu constater que plus d'une centaine de cartes bancaires pouvaient être utilisées par des fraudeurs pour parvenir à réaliser une commande !

Les E-Marchands peuvent mesurer le niveau d'activité des fraudeurs en relevant les commandes à faible montant (généralement inférieur à 5€) qui sont autant de traces laissées par les fraudeurs de tentatives de "carding" une méthode qui consiste à trouver un numéro de carte bancaire valide et sa date d'expiration, grâce à un algorithme informatique.

La couverture nationale des fraudeurs pour récupérer les colis

Certains E-Marchands interviewés ont constaté que certains réseaux disposaient du maillage logistique suffisant pour pouvoir demander la livraison de la marchandise à n'importe quel endroit du territoire !

Finalement, la professionnalisation de la fraude aboutit au paradoxe que les activités des fraudeurs et celles des E-Marchands sont finalement régies par les mêmes objectifs de rentabilité et de retour sur investissement!

Il en résulte qu'un professionnel de la fraude privilégiera toujours les attaques les plus rentables, c'est à dire celles les plus faciles avec le bénéfice le plus élevé. Les sites mal protégés sont prévenus !

B.3.2.2 Une fraude tout azimut

Si, dans le passé, le niveau de risque de certaines transactions pouvait être considéré comme quasi nul, ce temps-là est bel et bien révolu. Les E-Marchands en conviennent : la fraude frappe tout azimut !

Evolution géographique de la fraude

Encore récemment, la fraude était cantonnée principalement aux zones périurbaines des grandes agglomérations. Certains départements de livraison appelaient la vigilance plus que d'autres. Or, les fraudeurs sont maintenant organisés pour être livrés sur l'ensemble du territoire (cf. point précédent) Dès lors, le critère « lieu géographique de livraison » n'est plus aussi pertinent qu'avant pour détecter une fraude.

Le Groupe 3 Suisses a ainsi très récemment constaté une évolution géographique de la fraude qui touche maintenant des régions dans lesquelles elle était absente jusqu'à présent. Pour Groupe 3 Suisses, cette évolution est liée aux déplacements des réseaux de « mules ».

Généralisation de la fraude quel que soit le produit

Pour Mistergooddeal.com, les produits à faible encombrement ou fortement attractifs comme les produits high-tech continuent à concentrer une forte proportion de la fraude. Par exemple, Mistergooddeal.com a constaté une augmentation récente de la fraude sur la téléphonie mobile concomitamment avec l'arrivée de Free sur le marché et ses offres sans subvention du terminal. Mais, force est de constater que les produits high Tech ne sont plus les seuls à être fraudés.

La fraude se développe quel que soit le produit, là où une faille est identifiée par les fraudeurs dans le système de protection...

Les E-Marchands interviewés ont vu se développer la fraude sur n'importe quel type de produits, du lave-linge, en passant par les couches culottes ou bien encore les lots de jeans à marque de l'enseigne ou sur les moulinets de pêche du site Pecheur.com

Les produits physiques ne sont évidemment pas les seuls à être fraudés; les contenus digitaux le sont également. La vente de produits digitaux est elle aussi exposée à un risque élevé de fraude; un code promo donnant l'accès à une heure de voyance par exemple se revend très bien sur Internet ! Un produit est d'autant plus fraudé qu'il est facilement revendable sur le marché noir ou sur l'une des nombreuses plateformes de revente de produits digitaux.

Priceminister.com a constaté une diminution du "panier moyen fraudé" ce qui tend à prouver que la fraude ne se concentre plus uniquement sur les produits chers.

S'il n'avait jamais existé, le profil type du fraudeur a bel et bien disparu ! Un bon client peut cacher un fraudeur...

Pour les E-Marchands interviewés, il n'y a pas non plus de profil type de fraudeur. Tout à chacun peut être tenté un jour ou l'autre par la fraude d'autant plus facilement que demeure l'idée, dans l'esprit de nombreuses personnes, que « tout est gratuit sur internet ».

Il est également fini le temps où les E-Marchands pouvaient se fier "les yeux fermés" à leurs bons clients; un bon client peut se transformer en fraudeurs, sciemment ou à son insu.

Laredoute.com cite le cas de clients qui ont été approchés (et abusés) par des fraudeurs qui les ont persuadés d'utiliser leurs comptes clients pour réaliser des transactions frauduleuses. Ces bons clients de Laredoute.com sont devenus du jour au lendemain des « mules ».

Il est d'ailleurs frappant de constater que les « mules » sont assez peu conscientes des risques qu'elles encourent. Et, les professionnels de la fraude savent exploiter la crédulité du public renforcée par la vulnérabilité de certaines personnes notamment en période de crise économique. Selon Priceminister.com, une prise de conscience générale sur le sujet serait nécessaire.

Les E-Commerçants se demandent dans quelle mesure il ne serait possible d'attirer l'attention des sites de publication d'annonces de recrutement et, idéalement le grand public, sur les caractéristiques d'une annonce de recrutement de mules.

Autres cas possibles, la corruption de compte client grâce à des méthodes de "*phishing*" ou bien encore le cas de la création de "faux bons comptes client" par la passation de transactions normales pour "normaliser" le compte avant la survenue d'une transaction frauduleuse.

En proportion, ce type de fraude est relativement limité. En revanche, les conséquences en termes d'image vis-à-vis des clients sont toujours très négatives. Ce phénomène peut avoir deux origines pour CDiscount; le phishing et, malheureusement aussi, de possibles complicités internes.

Aussi, CDiscount.com met-il en œuvre des procédures de sécurité strictes visant à protéger les comptes clients notamment en rendant inaccessible au Service Client les codes confidentiels des clients et en ayant recours au cryptage des données. A cet égard, la question de la fraude rejoint celle de l'identité numérique.

B.4 LA LUTTE CONTRE LA FRAUDE : SIMPLE ET COMPLIQUEE

B.4.1 Par certains aspects, la lutte contre la fraude est simple

Pour les E-Marchands interviewés, qui possèdent tous une solide expérience du sujet, une très grande partie de la fraude peut être facilement éradiquée par la mise en place de solutions ou de procédures qui relèvent parfois du simple bon sens ! Encore faut-il que le E-Commerçant puisse et veuille y consacrer le minimum de moyens nécessaires et n'attende pas le "coup dur" pour réagir ! On l'a vu, les conséquences pour lui peuvent être désastreuses !

Laredoute.com, dont le taux de fraude est pourtant parmi les plus bas des E-Marchands rencontrés indique bien que son dispositif anti-fraude n'a rien d'exceptionnel; pourtant il est très efficace.

Eradiquer une grande partie de la fraude est donc relativement simple car les principaux facteurs de risques sont bien connus.

Le rapport encombrement /prix

Rueducommerce.com rappelle cette évidence; plus les produits sont chers et petits, plus le risque de fraude est important. La tendance à la miniaturisation des produits High tech est incontestablement un facteur de risque. Un acteur comme Delamaison.fr qui vend du mobilier de jardin est naturellement moins exposé au risque de fraude.

La part des ventes réalisées à partir de cartes étrangères

La fraude dont est victime Pecheur.com est à 90% due à des transactions émises à partir de cartes étrangères.

Plus la part des ventes réalisées depuis l'étranger elle est importante, plus l'exposition du E-Marchand au risque de fraude est importante.

Le mode de livraison : le risque n'est pas le même en fonction du point relai

Unanimement, les E-Marchands interviewés citent le mode de livraison comme un bon indicateur de risque. C'est ce que confirme notamment Rueducommerce.com qui intègre ce facteur dans son évaluation du risque. Les demandes de livraison en « point relais » sont particulièrement scrutées. Il est indubitable, qu'il est plus facile pour un fraudeur de récupérer une marchandise dans un point relais qui n'effectue pas toujours la vérification de l'identité.

Delamaison.fr, comme d'autres E-Marchands, a pu observer que certains points relais présentaient des risques de fraude supérieurs à la moyenne. Delamaison.fr a intégré cet élément dans son dispositif de détection des commandes à risque.

B.4.2 Par d'autres aspects, elle requiert une véritable expertise

Difficultés	Commentaires
Faire face aux volumes	Pour les E-Marchands, un dispositif de lutte contre la fraude efficace doit être en mesure d'évaluer le risque de plusieurs milliers de transactions par jour. Pour le E-Marchand, repérer les transactions frauduleuses, c'est comme repérer "l'aiguille dans la meule de foin".
Frapper "chirurgicalement" les fraudeurs parmi les bons clients !	Les conséquences d'une mauvaise évaluation du risque peuvent avoir des conséquences extrêmement dommageables; impact financier d'une transaction frauduleuse non détectée, impact d'image dans le cas d'un client soupçonné à tort. Mal évaluer le risque d'une transaction, c'est risquer de porter atteinte à la relation de confiance patiemment tissée avec le client et finalement de le perdre.
S'adapter en permanence aux évolutions de la fraude	Les techniques de fraude évoluent sans cesse. Pour être efficace, le dispositif de fraude doit évoluer en permanence. Il en va de même pour les équipes anti-fraude qui doivent s'astreindre à une veille constante sur toutes les nouvelles tendances en matière de fraude.
Avoir une capacité de réaction suffisante	Une faille qui ne serait pas rapidement repérée par le E-Marchand peut avoir dans les semaines qui suivent des conséquences financières catastrophiques. La fraude nécessite une vigilance 24/24, 7/7 et des outils de monitoring qui renseignent le E-Commerçant en quasi temps réel.
La fraude, un sujet complexe d'organisation interne	La fraude est un arbitrage permanent entre des objectifs qui au sein des organisations peuvent paraître antagonistes; objectifs marketing et commerciaux vs objectifs financiers de rentabilité. La fraude est un sujet transverse à l'entreprise et nécessite une coordination étroite entre différentes directions: direction générale, Ventes, direction de la Relation client, direction financière... Pour les groupes internationaux, c'est un sujet qui nécessite un juste équilibre entre la mutualisation des moyens et la prise en compte des spécificités locales de la lutte contre la fraude.
Allouer les moyens et maintenir la priorité	Dans une phase de croissance très rapide du E-Commerce, l'arbitrage sur les moyens à consacrer à la lutte contre la fraude par rapport à d'autres priorités ayant un impact plus visible sur le développement de l'activité est loin d'être simple. Elle nécessite une certaine capacité d'anticipation et de projection qui peuvent paraitre comme difficilement conciliables avec des impératifs court terme.
Agréger des données de plus en plus nombreuses et provenant de sources externes	Pour gérer efficacement son système anti-fraude, un E- marchand doit pouvoir intégrer et consolider, à minima, deux sources d'information (informations en provenance du PSP et informations en provenance de la banque acquéreur). Ces deux sources d'informations doivent être ensuite croisées avec les données internes.

B.4.3 La fraude, un arbitrage permanent pour les E-Marchands

Pour le E-Marchand, le pilotage du taux de fraude est toujours un arbitrage entre le développement du chiffre d'affaires, le risque financier et le risque d'image.

B.5 MOBILISATION DES E-MARCHANDS CONTRE LA FRAUDE

B.5.1 Une mobilisation de longue date

Pour bon nombre des E-Marchands rencontrés, la lutte contre la fraude est un combat qu'ils mènent de longue date. La mise en place des organisations et des outils qui sont opérationnels aujourd'hui ne l'ont pas été du jour au lendemain; elle a nécessité du temps.

Pour certains E-Marchands, la lutte contre la fraude est même inscrite dans les gènes de leurs entreprises.

Pour Priceminister.com, la capacité à lutter contre la fraude a fait partie des fondements de l'activité. Dès sa création, priceminister.com a voulu en faire un axe différenciant et le développer. Ainsi, priceminister.com s'est doté d'outils de lutte contre la fraude qu'il a délibérément conçus de façon paramétrable pour pouvoir répondre aux évolutions de la fraude.

Pour les E-Marchands qui développent une activité de place de marché, la lutte contre la fraude a fait partie intégrante de leur "modèle économique" dès leur lancement.

Ces E-Marchands mettent à disposition et peu ou prou "vendent" aux E-Marchands de leur galerie leur expertise et leurs outils de lutte contre la fraude.

Rueducommerce.com considère qu'en matière de lutte contre la fraude, il partage exactement la même logique que ses partenaires. Rueducommerce.com rappelle qu'il assure la prestation d'encaissement pour le compte de ses partenaires et qu'en conséquence, il porte au premier chef le risque de la fraude. Ses commissions sont dues sur les transactions réellement encaissées.

Par ailleurs, un panier d'un client de rueducommerce.com peut être composé à la fois de produits distribués par rueducommerce.com et de produits distribués par l'un de ses partenaires. L'intérêt de lutter contre la fraude est bien commun.

B.5.2 Mobilisation des moyens humains et financiers

B.5.2.1 Organisation de la lutte contre la fraude chez les E-Marchands

Il est intéressant de constater que la localisation du service fraude au sein des organisations des E-Marchands rencontrés traduit les deux prismes par lesquels peut être abordée la lutte contre la fraude.

Pour certains E-Marchands, la lutte contre la fraude nécessite une grande proximité avec le client. Il s'agit avant tout de comprendre le comportement des clients pour évaluer au plus près le risque de fraude. C'est pour ces raisons que des E-Commerçants comme Voyages-sncf.com ou le Groupe 3 Suisses ont choisi d'intégrer leur département anti-fraude à la Direction de la Relation Client. Pour Voyages-sncf.com, ce choix se justifie pleinement car " le paiement est au cœur de l'acte d'achat du client".

Le département anti-fraude chez Voyages-sncf.com

C'est en 2012, que la Direction Financière de la SNCF et la Direction Générale de Voyages-sncf.com ont décidé la création du service «fraude et moyens de paiement ». Outre la lutte contre la fraude sur la vente des billets de train, ce service est également en charge d'étudier des réponses appropriées à apporter aux nouveaux comportements d'achat des clients (paiement "en un clic" par exemple) et de proposer des moyens de paiement adaptés aux habitudes de chaque pays européen.

Le département anti-fraude de vente-privee.com

Chez Vente-privée.com, la fraude est prise en charge par une équipe dédiée de quatre personnes. Comme dans le cas de laredoute.com, son périmètre couvre à la fois la prévention de la fraude et le recouvrement. Mais, à la différence de laredoute.com, l'équipe est rattachée à la direction de la Relation Client.

Une des missions du département anti-fraude au sein du Groupe 3 Suisses: fédérer les stratégies anti-fraude pour les filiales du groupe

Jusqu'à très récemment, les différentes enseignes du Groupe 3 Suisses géraient la fraude en fonction de leurs spécificités organisationnelles, de la nature de leurs activités et de leurs outils propres. L'un des chantiers dont le service fraude a la responsabilité, est de généraliser et d'uniformiser les règles de prévention de la fraude pour les enseignes du groupe.

Pour d'autres E-Marchands, le service fraude doit être sciemment « extrait » des entités directement en contact avec le client, souvent pour des raisons de respect des règles de contrôle interne; dans ce cas, le service fraude dépend généralement de la Direction Administrative et Financière mais peut être également intégré à la Direction du "Back Office Client".

Chez Priceminister.com, une équipe fraude très indépendante, capable d'agir avec une grande autonomie.

L'équipe de détection de la fraude chez Priceminister.com compte aujourd'hui cinq personnes. Elle fait partie de la Direction du Back Office Clients.

Selon son responsable, cette équipe travaille de façon très « indépendante » des autres services de l'entreprise. Elle est capable d'identifier seule un problème et possède suffisamment d'autonomie pour pouvoir prendre des décisions rapides.

Chez Cdiscount.com, un apport nécessaire de compétences techniques

Chez Cdiscount.com, le Service de lutte contre la fraude dépend de la Direction Financière.

L'équipe de lutte contre la fraude chez Cdiscount.com était jusqu'à présent très opérationnelle. Elle s'est étoffée de compétences techniques pour pouvoir faire face aux évolutions récentes de la fraude.

Pour le service anti-fraude de laredoute.com, "prévenir plutôt que guérir" !

L'équipe anti-fraude de laredoute.com compte cinq personnes. Le service dépend de la Direction Comptable. L'équipe gère la fraude et le contentieux. L'objectif est de réduire la part du contentieux au profit de la lutte contre la fraude: prévenir plutôt que guérir !

B.5.2.2 La lutte contre fraude, un processus encore très manuel

Même si la lutte contre la fraude s'appuie sur un certain nombre d'outils notamment informatiques, il n'en demeure pas moins que certains processus, notamment la récupération et la vérification des pièces justificatives, reposent sur des actions principalement humaines.

Parmi les marchands interviewés, c'est le service anti-fraude de Groupe 3 Suisses qui mobilise le plus de personnes: 17 collaborateurs pour l'activité B2C!

Après l'application automatisée de différents filtres d'analyse de risque, ce sont entre 1500 à 2000 commandes journalières, pour l'ensemble du Groupe 3 Suisses, qui font l'objet de vérifications manuelles.

Ces vérifications sont faites, pour tout ou partie, manuellement; elles consistent par exemple à vérifier la cohérence entre l'adresse e-mail et l'adresse de livraison, vérifications auprès des banques (nom et adresse du titulaire de la carte bancaire). Elles peuvent nécessiter d'appeler certains clients pour avoir confirmation. "Parfois, la fraude est très simple. Elle peut être intra familiale". Parfois, le Groupe 3 Suisses utilise les réseaux sociaux ou Google pour vérifier certaines informations. Le Groupe 3S collabore étroitement avec les banques, notamment pour vérifier que le titulaire du compte Client est bien le titulaire de la carte (processus manuel par échange de fax).

L'accroissement des commandes à vérifier dû au développement de l'activité et à l'augmentation des tentatives de fraude pose un vrai problème de gestion des ressources humaines pour les E-Marchands interviewés. Les services anti-fraude rencontrés sont tous à la recherche de gains de productivité.

Aux dires de Priceminister.com, "ce qui nous coûte cher ce n'est pas tant les impayés que les coûts du dispositif anti fraude.... ". Il y a deux ans, la lutte contre fraude n'occupait qu'une seule personne chez Priceminister.com. Aujourd'hui, le service compte cinq personnes ! Avec le développement de l'activité et de la fraude, le nombre de paniers « mis sous observation » s'est en effet considérablement accru.

C'est la nécessaire augmentation de la productivité, pour faire face à l'accroissement du volume d'activité particulièrement à l'international, qui a notamment conduit vente-privee.com à mettre en place un outil comme *Accertify*.

Dans ce contexte, un certain nombre des interviewés voit dans la mise en place de 3D Secure une opportunité intéressante à saisir car 3D Secure est une alternative très efficace au recueil des pièces justificatives.

Dans l'évaluation du risque, les outils ne peuvent pas tout ! L'expérience et l'intuition humaine jouent également un rôle prépondérant

Pour Delamaison.fr, l'analyse du risque "à priori" ne peut remplacer totalement l'analyse "à posteriori"; elles sont complémentaires. Delamaison.fr prend l'exemple d'une première commande analysée sans risque. Si elle est suivie d'une deuxième commande exactement identique dans un laps de temps court alors le Risk Manager pourrait être amené à revoir son appréciation du risque sur les deux commandes.

C'est l'expertise et l'expérience du Risk Manager qui lui permet d'arbitrer rapidement sur les risques d'une commande et, dans le cas d'une fraude suspectée, de pouvoir libérer la marchandise pour une autre vente, valide cette fois.

Profil actuel de l'analyste de risque de fraude et évolution à terme.

Pour le responsable du service anti-fraude de laredoute.com, les compétences clés de l'analyste fraude résident dans une bonne connaissance du fonctionnement de l'entreprise, une bonne connaissance du catalogue de produits et du plan commercial (notamment des promotions), une expérience du service client (connaissance du profil type) : en somme, "une bonne compréhension du business".

Pour laredoute.com, le profil type de l'analyste anti-fraude sera probablement amené à évoluer dans l'avenir pour s'adapter aux évolutions de la fraude. Les compétences à posséder seront des notions de marketing, de finance, un intérêt pour les nouvelles technos et pour les nouvelles tendances de consommation.

B.5.2.3 Coûts d'investissement et d'exploitation des arsenaux anti-fraude. Quel ROI ?

Les coûts d'OPEX (dépenses d'exploitation) et de CAPEX (dépenses d'investissement) des outils de lutte contre la fraude déployés chez les E-Marchands sont difficiles à obtenir, et parfois même, il semble que les E-Marchands n'en aient eux-mêmes qu'une vague estimation. A fortiori, le calcul du ROI d'un dispositif anti-fraude n'est quasiment jamais fait.

Rueducommerce.com estime que les coûts liés à la lutte contre la fraude représentent de l'ordre de 0,1% du chiffre d'affaires.

Pour Delamaison.fr, les coûts de son dispositif anti-fraude, qui intègre 3D Secure, est essentiellement des CAPEX et très peu d'OPEX , l'objectif de l'outil étant justement d'automatiser au maximum le processus d'évaluation du risque. Delamaison.fr évalue la charge de développement à quatre et cinq hommes-mois, soit l'équivalent de quelques pourcents du budget annuel SI. "La charge de développement d'une telle solution est cependant très variable en fonction de la situation de chaque E-Commerçant" estime Delamaison.fr

Selon Delamaison.fr, compte tenu de son coût, le développement d'une solution de détection du risque de fraude en interne peut apparaitre comme inenvisageable pour un E-Commerçant de taille modeste.

Le calcul de la rentabilité économique d'un dispositif de lutte contre la fraude n'est pas aisé pour un E-Marchand. En effet, Delamaison.fr rappelle que le E-Commerçant ne dispose que d'une vision partielle des impayés. Une grande partie d'entre eux est prise en charge par le réseau Visa ou Master Card. Le réseau répercute ensuite le coût des impayés aux banques au travers de l'augmentation des commissions.

Ce qui est certain en revanche, c'est qu'un dispositif de lutte contre la fraude aura forcément un impact direct sur le taux d'impayés. Or, ce taux d'impayé, même pour un E-Marchand de taille modeste, peut rapidement se chiffrer en centaines de milliers d'euros.

B.5.3 Les arsenaux de lutte contre la fraude

B.5.3.1 Précision de vocabulaire : "Méthode d'évaluation du risque" pas "scoring"

Pour Delamaison.fr, l'utilisation du terme "scoring", pourtant largement employé quand il est question de la lutte contre la fraude, est inappropriée. En matière de lutte contre la fraude, il ne s'agit pas d'attribuer aux clients une note de solvabilité mais de détecter un comportement ou une commande à risque.

Pour Delamaison.fr, à la différence du scoring bancaire, la détection des risques de fraude ne vise pas à empêcher un client d'acheter. Il vise à permettre au E-Commerçant d'adapter ses moyens de protection au risque de fraude.

L'analyse de risque de la transaction porte couramment sur des éléments comme:

- Typologie des articles achetés,
- heure de la commande,
- encours de commandes
- commandes passées dans les 24 heures précédentes
- pays de la banque émettrice de la carte
- ...

B.5.3.2 Un ensemble d'outils pour un objectif unique

Retour d'expérience de Delamaison.fr sur la mise en place de son outil de détection du risque

La solution a été développée en quelques mois. Pour Delamaison.fr, ce ne sont pas les développements techniques en eux-mêmes qui constituent la principale difficulté d'un tel projet mais l'analyse des données et leur corrélation qui doivent l'alimenter.

Delamaison.fr insiste sur le nécessaire "*fine tunning*" de l'outil qui doit se faire régulièrement pour que l'outil conserve son efficacité. Le délai nécessaire au "réglage" d'un outil d'évaluation du risque peut être relativement long avant que l'outil ne soit pleinement efficace. Ainsi, même si le système mis en œuvre par Delamaison.fr a été opérationnel fin 2010, les premiers résultats constatés sur le taux d'impayés n'ont été perceptibles qu'à partir d'avril ou mai 2011.

Mise en place d'un vaste programme de lutte contre la fraude chez vente-privee.com

Pour faire face à la progression de la fraude, Vente-privee.com a décidé la mise en place d'un important programme visant à renforcer la sécurisation des moyens de paiement sur l'ensemble des pays dans lesquels Vente-privee.com est présent. La mise en place de 3D Secure courant 2013 est un des éléments de cet ensemble dont la brique principale est la mise en place de l'outil *Accertify*. Le déploiement de l'outil est prévu en juillet 2013.

Le choix de la solution Accertify s'est fait à la suite d'un appel d'offre. Le principal avantage de cette solution, perçu par vente-privee.com, est qu'il propose en standard quatre modèles de détection du risque et que chacun d'eux est adaptable au contexte et spécificités de l'E-

Marchand. Vente-privee.com n'a pas retrouvé la même souplesse dans les solutions concurrentes.

L'outil *Accertify* doit permettre d'automatiser des processus qui, jusqu'à présent, étaient pris en charge manuellement. Il permet la mise en œuvre d'un certain nombre de règles plus ou moins sophistiquées de détection de la fraude en utilisant un nombre très important de sources de données différentes.

Selon vente-privee.com, un outil d'évaluation du risque de la transaction peut être mis en œuvre de deux manières. La première implantation possible est de positionner l'outil en « pré autorisation de la carte". La seconde est de faire fonctionner l'outil après la réception de l'autorisation.

Pour vente-privee.com, l'intérêt de cette deuxième méthode (finalement retenue par vente-privee.com) est de limiter l'impact du processus d'évaluation du risque sur la transaction proprement dite et ainsi de ne pas risquer de dégrader le taux de conversion.

Le paramétrage de l'outil a été initié lors d'ateliers menés conjointement entre les référents métiers de vente-privee.com et les équipes d'*Accertify*. Vente-privee.com insiste sur la nécessité que des personnes connaissant parfaitement les spécificités de l'activité participent aux travaux de paramétrage de l'outil.

A l'issue de ces travaux, Vente-privee.com a constaté que les règles standard d'*Accertify* avaient été finalement complètement adaptées aux spécificités de son activité.

Vente-privee.com souligne un point important à ne pas négliger dans la phase d'intégration d'un outil comme *Accertify* : la formalisation du processus de mises à jour des règles de paramétrage afin de garantir la bonne application des règles de contrôles internes.

Pour Vente-privee.com, l'utilisation d'un outil comme *Accertify* ne nécessite pas de compétences particulières et peut être confiée à des profils de séniorité moyenne, ayant une expérience de la Relation Client.

Chez Priceminister.com, un outil d'analyse du risque fondé sur la détection de mots clés

Après que le client a validé sa commande, la demande d'autorisation bancaire est émise. C'est après réception du résultat de la demande d'autorisation qu'est déclenchée l'analyse de risque. Le résultat de cette analyse peut être soit la validation de la commande soit la mise en observation de la transaction pour analyse manuelle.

L'outil de détection de la fraude de Priceminister.com fonctionne sur la détection de mots-clés qui permettent d'identifier des transactions à risque. Ces transactions font ensuite l'objet d'une analyse manuelle.

Chez CDiscount.com, des contrôles à plusieurs niveaux

Chez CDiscount.com, des premiers contrôles ont lieu en "Front Office" comme par exemple la consultation de l'historique de paiement et des éventuels incidents de paiement et détection des comportements anormaux.

Des contrôles de second niveau sont ensuite pris en charge par le prestataire de services de paiement ou PSP (application de filtres de pré-autorisation), notamment les cartes en opposition.

CDiscount.com a ensuite recours aux services de Fia-Net qui lui fournit des informations additionnelles telles que la fréquence d'utilisation de la carte sur les derniers jours, les derniers mois.

CDiscount.com constate que récemment encore, les seuls contrôles Fia-Net suffisaient pour avoir une bonne appréciation du risque de la transaction. Des contrôles internes supplémentaires doivent maintenant être mis en place.

L'ultime filtre mis en place par CDiscount.com est l'intervention en logistique. Le Service logistique a en effet la possibilité de suspendre une livraison qu'il considérerait à risque lors de la préparation de commande.

Chez laredoute.fr, un outil "qui n'a rien d'exceptionnel" mais qui bénéficie de 15 ans d'ancienneté

Selon les propres mots du responsable de la lutte contre la fraude, l'outil de lutte contre la fraude de laredoute.fr n'a "rien d'exceptionnel". A en juger par le niveau de fraude très bas du site, il n'en est pas moins très efficace, probablement en partie grâce à la longue expertise qu'a développée laredoute.fr dans sa mise en œuvre et son paramétrage.

Pour le rendre encore plus pertinent, Laredoute.com mène une réflexion sur la mise en place d'un outil d'analyse du comportement du Client sur le site; par exemple analyse du nombre d'aller-retour entre la page de paiement et la page de livraison.

Exemple de Groupe 3 Suisses

Le groupe s'appuie sur l'outil de Front Office "FORCE" (un outil propriétaire de prise de commandes) qui gère un certain nombre de règles de prévention de la fraude qui s'appliquent à chacune des commandes.

Une fois la demande d'autorisation réalisée par Atos, le PSP du Groupe, (vérification sur la "non mise en opposition de la carte") et sur la liste "grise", les transactions sont systématiquement filtrées en fonction de leur niveau de risque présumé.

La liste « grise » est une liste hébergée chez Atos. Elle est mise à jour par les enseignes du groupe. Cette liste répertorie l'ensemble des cartes présentant un risque de fraude avéré.

Les transactions ainsi filtrées "à risque" sont alors analysées manuellement.

Les filtres sont appliqués avant que la commande ne parte en facturation. Mais, d'autres filtres permettent de pousser encore l'analyse et de bloquer une commande après la facturation, jusqu'au moment de la préparation de la commande voire même dans le point relai.

Un certain nombre de règles de filtrage sont également déportées au niveau d'Atos (refus systématique de certaines adresses IP en fonction de leur origine géographique).

Chez Mistergooddeal.com, un "retardateur de facturation client" intégré au dispositif.

Une évaluation du risque de premier niveau sur la transaction est réalisée en interne par mistergooddeal.com.

Le moteur d'évaluation du risque développé en interne s'appuie sur une centaine de règles différentes. À l'issue de cette analyse automatisée, les différents cas de figure suivants peuvent survenir :

- Transaction acceptée
- Transaction à ne pas facturer (risque de fraude jugé trop important)
- Transaction à soumettre à Fia-Net
- Transaction à soumettre à une analyse humaine

Les transactions douteuses sont transmises à Fia-Net pour pousser l'analyse. En fonction du résultat, Mistergooddeal.com procède, le cas échéant, à un contrôle manuel interne.

Ce dispositif est complété par la mise en place de "retardateurs de facturation client". Mistergooddeal.com ne facture pas le Client tant qu'il ne s'est pas assuré de la validité de la transaction. Cette procédure s'applique particulièrement sur les paiements en trois fois qui représentent 25 % des ventes chez Mistergooddeal.com. L'authentification 3D Secure ne vaut que pour la première transaction et pas pour les deux suivantes.

Lastminute.com: avantages (et limites) d'un dispositif de lutte contre la fraude mutualisé entre les filiales locales d'un groupe multinational

Le groupe Lastminute.com dispose d'un outil développé en interne (Revenue Protection Tool). Cet outil s'appuie sur une "Black list" (qui recense les clients fraudeurs) ainsi que sur le passage d'un certain nombre de règles visant à mesurer le risque de fraude. L'analyse des transactions par l'outil permet de séparer les transactions jugées sans risque et les transactions nécessitant une analyse plus poussée. A la suite de cette analyse, l'équipe fraude propose une liste de transactions à rejeter qui est définitivement validée par le Service Client en France. 30 % des transactions françaises font ainsi l'objet d'une analyse manuelle.

Dans le cas où cette analyse est défavorable, la carte du client est recréditée. Lastminute.com demande alors le remboursement aux fournisseurs pour suspicion de transactions frauduleuses.

L'équipe fraude est centralisée en Angleterre pour l'ensemble de l'Europe. Une partie de l'activité est sous-traitée en Inde (vérification manuelle des transactions frauduleuses: contrôle de cohérence).

Selon la Directrice Administrative et Financière de Lastminute.com, un travail reste à mener pour mieux intégrer les spécificités des marchés locaux en matière de fraude.

Les règles de détection de la fraude sont ainsi établies en Angleterre. De plus, il semble malcommode que les transactions à risque soient revues par du personnel indien n'ayant jamais eu l'occasion de séjourner en France. Selon Lastminute.com, la fraude a un caractère « très local ».

La mutualisation des moyens de lutte contre la fraude pour un groupe international présente des avantages économiques évidents pour peu que cette mutualisation des moyens aille de pair avec une réactivité adéquate. Le temps moyen de détection d'une fraude chez Lastminute.com est de 2,5 mois : un délai qui peut être très certainement réduit.

Autre axe d'amélioration identifié, l'analyse des risques de fraudes "a priori" et pas seulement à posteriori quand l'impayé est survenu. Cela passe par le développement d'une expertise de risque au niveau des transactions entrantes.

B.5.3.3 Des outils principalement développés en interne...

Dans leur très grande majorité, les -E-Marchands interviewés ont choisi de développer leurs outils de lutte contre la fraude en interne.

Ce constat est confirmé par CB alors même que certaines banques acquéreurs sont aussi en mesure, selon CB, de proposer ce type de service. Mais, ces services ont un prix que certains E-Marchands (qui ne sont pas encore dotés de solutions internes) ne seraient pas forcement prêts à payer.

B.5.3.4 ... mais des réflexions pour les externaliser partiellement ou totalement

Des entretiens avec les E-Marchands interviewés, il ressort néanmoins qu'un mouvement de réflexion est en cours pour étudier la possibilité, sinon d'externaliser totalement les systèmes

anti-fraude développés en interne, tout au moins d'intégrer des modules additionnels du marché aux dispositifs déjà en place. Plusieurs raisons expliquent ce "mouvement".

La première raison est le développement rapide du E-Commerce et du nombre de transactions à traiter qui nécessite la mise en place d'outils automatisés pour gagner en productivité.

La deuxième raison est la nécessité qu'éprouvent les E-Marchands d'enrichir leur analyse du risque par des données externes dont ils ne disposent pas. Face à une fraude de plus en plus complexe à repérer, les E-Marchands ne peuvent plus se contenter de l'analyse de leurs propres données sur leurs transactions et se limiter à estimer un risque en les rapprochant des informations qu'ils possèdent sur leurs propres clients. Ils ont besoin d'accéder à des sources d'informations mutualisées de type Fia-Net. Avec sa base mutualisée de plus de 17 millions d'internautes, Certissim (l'offre dédiée de Fia Net à la lutte contre la fraude) identifie puis retraite les commandes à risque et apporte une protection du E-Commerçant contre les impayés.

La troisième raison de la réflexion sur l'externalisation des moyens de lutte contre la fraude est l'enrichissement et l'élargissement récent de l'offre de solutions anti-fraude. Des acteurs précédemment cités comme Cybersource ou Retail & Decisions sont apparus relativement récemment sur le marché français. Pour les E-Marchands les plus importants, ces nouvelles offres ouvrent des ponts intéressants vers des outils ou pratiques déjà en œuvre à l'étranger et qui ont fait leurs preuves. La question reste leur acceptabilité par la CNIL (Cf. § spécifiques dédiés à ce sujet dans le document).

Pour CB, ce foisonnement de solutions n'aura qu'un temps. Il est très probable que le marché se concentrera sur quelques gros acteurs.

Description des offres combinant des prestations d'établissement acquéreur (PSP) et des prestations de solutions de paiement.

Certains prestataires, encore peu nombreux en France[9], commercialisent des offres qui combinent des prestations de services de paiement et celles d'un établissement de paiement. A ces deux prestations peuvent s'ajouter des compétences d'agence Web[10].

- prestations d'établissement acquéreur : mise en œuvre du contrat VAD qui inclut la gestion du risque de fraude, la gestion des impayés, la gestion des transactions par un *Back Office* dédié, la fourniture de statistiques mais aussi la collecte, le traitement des transactions monétiques et le crédit du compte bancaire du marchand.
- prestations de solutions de paiement: gestion technique des flux sur une plateforme sécurisée, prévention de la fraude par la détection, le scoring et l'intervention puis, de manière collaborative avec le marchand, grâce à la mise à disposition d'un moteur de filtres fondé sur des règles métiers évolutives.

[9] L'offre Acquéreur-prestataire encore peu répandue en France l'est beaucoup plus dans d'autres pays européens comme les Pays-Bas ou l'Angleterre, pays dans lesquels le statut d'établissement de paiement (tel que défini par la directive européenne de 2007) existait déjà. Avant la mise en œuvre de cette directive en France, il était impossible pour un prestataire de solutions de paiement de gérer un contrat de vente à distance. C'était la prérogative exclusive des banques membres du GIE cartes bancaires.

[10] Personnalisation du graphisme et de la cinématique de l'étape de paiement et l'étude analytique des comportements de sorte à optimiser le nombre de ventes tout en gardant une sécurité optimale mais également un service de marketing direct

Le point de vue du juriste - Créé par la directive concernant les services de paiement de 2007 (DSP), un établissement de paiement est une personne morale qui a obtenu un agrément l'autorisant à fournir et à exécuter des services de paiement dans l'Espace économique européen. Avec les établissements de crédit (banques) et les établissements de monnaie électronique, les établissements de paiement sont qualifiés de prestataires de services de paiement (PSP). S'ajoutera bientôt la catégorie nouvelle des PSP tiers, c'est-à-dire des prestataires de services d'initiation de paiement et de services d'information sur les comptes (Proposition de DSP 2 du 24 juillet 2013). Les PSP sont à distinguer des prestataires de solutions de paiement, prestataires « techniques » (plateforme de paiement etc.) non réglementés.

B.5.3.5 ... mais une externalisation qui se heurte à certains freins

L'externalisation des dispositifs de lutte contre la fraude se heurte toujours à un certain nombre de freins dont certains sont d'ordre stratégique. Comme évoqué précédemment, la lutte contre la fraude est considérée par certains E-Marchands comme un atout concurrentiel à préserver (parfois jalousement !). Dès lors, considérant que leur savoir-faire en matière de détection de la fraude fait partie de leur "core business", ils ne sont pas prêts à l'externaliser.

L'externalisation complète nécessiterait de plus que le E-Marchands transmette en tout ou partie sa connaissance de ses clients à un tiers qui, par ailleurs, est susceptible de travailler pour l'un de ses concurrents. Là encore, cet écueil est difficilement franchissable pour bon nombre de E-Marchands rencontrés.

Troisième frein souvent évoqué, les investissements déjà consentis par les E-Commerçants pour développer leurs propres solutions en interne qui, compte tenu des coûts des solutions du marché, rendent les projets d'externalisation difficilement justifiables d'un point de vue économique; d'autant moins, que les E-Marchands les plus importants ont des taux de fraude déjà bas.

Enfin, pour être parfaitement efficace, un outil anti-fraude doit non seulement intégrer des spécificités sectorielles (le risque de fraude n'est pas le même dans la distribution de biens physiques que dans la vente de biens immatériels par exemple) mais également tenir compte de spécificités du E-Marchand comme son offre produits ou de services et la typologie de ses clients.

Dès lors, l'intérêt de complètement paramétrer une offre du marché paraît finalement encore assez limité pour une grande majorité des marchands interviewés.

Mistergooddeal.com évoque une dernière raison « pratico pratique » pour ne pas externaliser son dispositif d'évaluation du risque. Chez Mistergooddeal.com, on considère comme important de pouvoir conserver la visibilité sur le nombre de transactions effectivement entrées dans le tunnel de vente et ayant fait l'objet d'une analyse, ce que Mistergooddeal.com appelle « la base 100 du calcul du taux de facturation".

B.6 3D SECURE, UN DES OUTILS DE L'ARSENAL ANTI-FRAUDE

Que 3D Secure soit un moyen de lutte contre la fraude pour Visa, MasterCard et les banques, c'est incontestable. En revanche, il n'est pas juste de le vendre comme tel aux marchands. En aucune façon le marchand n'a la main sur cet outil et ne peut en modifier les règles ou le paramétrage. Au mieux, pour le marchand, c'est une information valable à un instant précis, dans des conditions précises, sur l'identification du porteur et son accord sur la transaction.

Le point de vue du juriste - Le Code monétaire et financier (CMF) définit un dispositif de sécurité personnalisé comme « tout moyen technique affecté par un prestataire de services de paiement à un utilisateur donné pour l'utilisation d'un instrument de paiement. Ce dispositif, propre à l'utilisateur de services de paiement et placé sous sa garde, vise à l'authentifier » (CMF, art. L. 133-4, a).

La directive sur les services de paiement (DSP) précise quant à elle que l'authentification s'entend de « la procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité personnalisés » (Dir. 2007/64/CE, 13 nov. 2007, art. 4, 19).

Nouveauté de la proposition de DSP 2 du 24 juillet 2013, l'authentification forte est définie comme « une procédure de validation de l'identification d'une personne physique ou morale reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories connaissance, possession et inhérence, qui sont indépendants, en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification » (art. 4, 22). Les PSP (y compris les PSP tiers initiateurs de paiements) sont invités à appliquer l'authentification forte du client lorsque celui-ci initie une opération de paiement électronique.

Quant à 3D-Secure, déployé sous les appellations commerciales Verified By Visa et MasterCard SecureCode, il s'agit d'un protocole d'authentification renforcée basée sur trois domaines (d'où les « 3D » que sont l' Acquirer Domain : relation entre la banque et son client E-Commerçant ; l' Issuer Domain : relation entre la banque et son client titulaire (ou porteur) de la carte, et l'Interoperability Domain : relation entre la banque du client et celle du E-Commerçant) permettant de s'assurer, lors de chaque paiement en ligne, que la carte est bien utilisée par son titulaire.

B.6.1 Les origines de 3D Secure

3D Secure a été lancé début 2000. Comme le rappelle Atos Wordline, 3D Secure est né du constat préoccupant tiré par Visa et MasterCard sur l'évolution de la fraude sur les moyens de paiement à distance qui, contrairement aux moyens de paiement de proximité, ne bénéficiaient pas de l'authentification forte EMV.

Or, la sécurisation des moyens de paiement à distance est devenue cruciale pour Visa et MasterCard, notamment en raison du développement du e-commerce et, un peu plus tard, au développement d'autres moyens de paiement à distance concurrents tels PayPal. Les deux principaux "Schemes" ont donc été contraints d'agir.

Pour que le système se mette en place, il a fallu trouver un intérêt pour chacun des acteurs à intégrer une des composantes du système, avec comme principe fondamental un transfert de responsabilité de l'acquéreur vers l'émetteur à partir du moment où le marchand est inscrit et respecte les règles de 3-D Secure, que la transaction ait été authentifiée ou non.

L'intérêt des banques émettrices était d'enrôler le plus rapidement possible leurs clients pour ne pas avoir à supporter "seules" la fraude. Il en allait d'ailleurs naturellement de l'intérêt de leurs clients et de la sécurité de leurs moyens de paiement, favorisant ainsi le développement et la pérennité des solutions de paiement bancaires.

Les motivations des banques acquéreur étaient la réduction des impayés de leur client E-Marchand et la diminution des charges de gestion de la fraude. Elles devaient trouver un intérêt évident à l'enrôlement de leurs clients E-Marchands à 3D Secure.

L'adhésion des E-Marchand au système devait être acquise par le bénéfice qu'ils tireraient du transfert de responsabilité.

Le point de vue du juriste - Précisions juridiques sur la notion de « transfert de responsabilité »

L'expression courante de « transfert de responsabilité » n'apparaît pas dans le Code monétaire et financier (CMF) ; tout au plus la Réglementation interbancaire du paiement par carte (RIPC) utilise la notion de « transfert de risque », liée à la réponse que l'émetteur donne (ou ne donne pas) à la demande d'autorisation émise par l'acquéreur, laquelle demande d'autorisation est une demande à l'émetteur de garantir le paiement de l'opération. Par transfert de responsabilité, il faut entendre en réalité deux choses : le régime de franchise de responsabilité mis en place par le CMF et la garantie du paiement prévue par le contrat d'acceptation en paiement à distance sécurisé (contrat VADS).

Tel que prévu par le CMF, voici en effet, du côté du payeur, comment se déroule en détail l'exécution juridique d'une opération de paiement :

- une opération de paiement est autorisée si le payeur a donné son consentement à son exécution (art. L. 133-6, I) et l'ordre de paiement devient par principe irrévocable une fois reçu par le prestataire de services de paiement (PSP) (art. L. 133-8, I) ;

- le PSP du payeur peut refuser l'exécution de l'ordre de paiement (art. L. 133-10, I) et même procéder au blocage de l'instrument de paiement pour des raisons objectivement motivées relatives à la sécurité de l'instrument de paiement, à la présomption d'une utilisation non autorisée ou frauduleuse de celui-ci ou au risque évident que le payeur soit dans l'incapacité de s'acquitter de son obligation de paiement (art. D. 133-1) ;

- le montant de l'opération de paiement est crédité sur le compte du PSP du bénéficiaire au plus tard à la fin du premier jour ouvrable suivant le moment de réception de l'ordre de paiement (art. L. 133-13, I) ;

- en cas d'opération de paiement non autorisée consécutive à la perte, au vol, au détournement ou à toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, le payeur en informe sans tarder son PSP aux fins de blocage de l'instrument de paiement (art. L. 133-17, I) ; le PSP rembourse alors immédiatement le payeur du montant de l'opération non autorisée (art. L. 133-18) ;

- dans le cas particulier des instruments de paiement dotés d'un dispositif de sécurité personnalisé (code confidentiel pour le paiement de proximité, données carte pour le paiement à distance), lorsque l'opération de paiement non autorisée est consécutive à la perte ou au vol de l'instrument de paiement (la carte par exemple), le payeur supporte avant opposition les pertes liées à l'utilisation de cet instrument dans la limite de 150 €, sauf à ce que l'opération de paiement frauduleuse ait été effectuée sans utilisation d'un dispositif de sécurité personnalisé (art. L. 133-19, I. À noter que la proposition de DSP 2 du 24 juillet 2013 fait obligation aux PSP d'appliquer une authentification forte du client, à défaut de quoi le payeur ne sera pas responsable des conséquences financières de l'opération de paiement frauduleuse, étant ajouté que le plafond de 150 € serait ramené à 50 €). Cette franchise de responsabilité « saute » dans quatre autres cas : lorsque l'instrument de paiement ou les données qui lui sont liées ont été détournées à l'insu du payeur ; en cas de contrefaçon de l'instrument de paiement alors que le payeur était en sa possession au moment de l'opération de paiement ; si le PSP n'a pas fourni au payeur les moyens appropriées permettant l'information de blocage de l'instrument de paiement ; enfin le payeur supporte toutes les pertes si elles résultent soit d'un agissement frauduleux de sa part, soit de sa négligence intentionnelle ou grave vis-à-vis de ses obligations de préserver la sécurité des dispositifs de sécurité personnalisés ou de celle de procéder au blocage de son instrument de paiement perdu, volé ou détourné (art. L. 133-19, II, III et IV) ;

- une fois l'instrument de paiement mis en opposition par le payeur, il ne supporte aucune conséquence financière liée à son utilisation ou à l'utilisation des données qui lui sont liées, sauf agissement frauduleux de sa part (art. L. 133-20) ;

- enfin, lorsqu'un payeur nie avoir autorisé une opération de paiement, ou conteste sa bonne exécution, c'est à sur son PSP que repose la charge de prouver que l'opération litigieuse a été authentifiée, dûment enregistrée et comptabilisée et n'a pas été affectée par une déficience technique ou autre (art. L. 133-23).

Du côté du E-Commerçant accepteur, un article spécifique (l'article 5) du contrat VADS est consacré à la garantie du paiement, qui dispose en son point 1 : « *Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées au présent article* [Option : définies par les présentes Conditions Générales] *ainsi que dans les Conditions Particulières. Toutes les mesures de sécurité sont indépendantes les unes des autres. En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestations* ».

B.6.2 Rappel de quelques principes de fonctionnement de 3D Secure

B.6.2.1 Les grands principes de fonctionnement de 3D Secure

La première étape d'une authentification 3D Secure est l'interrogation par le PSP du E-Marchand des Directory Server de Visa et MasterCard.

Grâce au BIN de la carte, les Directory Server de Visa et MasterCard sont à même d'identifier la banque émettrice de la carte et redirigent la requête vers son ACS[11].

Si la transaction doit faire l'objet d'une authentification 3D Secure, l'ACS renvoie au PSP l'URL sur laquelle le porteur devra s'authentifier. L'affichage de la fenêtre d'authentification incombe à l'ACS de la banque émettrice de la carte.

Les échanges d'information sont plus complexes quand la page de paiement est hébergée chez le marchand plutôt que chez le PSP.

B.6.2.2 La banque émettrice pilote le choix du mode d'authentification

Il revient à l'ACS de la banque émettrice de déterminer si la transaction nécessite ou pas l'authentification effective du porteur et de quelle manière cette authentification doit avoir lieu. Cette décision repose sur l'évaluation du risque par l'application d'un certain nombre de règles au niveau de l'ACS.

Ces règles s'appuient notamment sur le montant de la transaction et/ou sur le nombre de transactions effectuées par le porteur sur une période de temps déterminée.

Ainsi, pour une transaction de faible montant, la date de naissance pourra par exemple être privilégiée comme mode de certification par rapport à l'envoi d'un code non rejouable envoyé par SMS. Mais, le montant de la transaction n'est pas le seul critère pris en compte. Une transaction d'un faible montant peut déclencher une authentification forte, si cette transaction succède à plusieurs transactions de faibles montants.

De même, lors de la phase d'enrôlement de ses clients, la banque émettrice peut décider qu'un client qui ne s'est jamais été authentifié puisse ne pas avoir à le faire dans la limite de trois

[11] **A**ccess **C**ontrol **S**erver (cf. glossaire en annexe du document)

transactions maximum. Elle assume le risque lié au transfert de responsabilité en cas de transaction frauduleuse.

Il faut donc bien conserver à l'esprit que la banque émettrice reste totalement libre d'appliquer ses propres règles de déclenchement du mode d'authentification en fonction de son appréciation du risque de la transaction. Et, le E-Marchand n'a aucune prise sur ce choix.

Il convient également de rappeler que le transfert de responsabilité est acquis même si l'émetteur a fait le choix de ne pas déclencher une authentification lors d'un paiement 3D-Secure. Ce principe respecté par les banques CB pose cependant quelques problèmes d'application pour les banques émettrices étrangères (non CB, voir plus bas).

B.6.2.3 Lien entre la demande d'authentification et la demande d'autorisation

Pour bénéficier du transfert de responsabilité et de la garantie du paiement, le marchand doit systématiquement faire appel au Directory Server pour déclencher ou non l'authentification du porteur avant d'effectuer la demande autorisation.

En effet, lorsque que la banque émettrice valide l'authentification (que le porteur se soit authentifié ou qu'il n'ait pas eu à le faire), elle transmet au marchand et à son PSP un "sceau d'authentification" (la signature de confirmation). La demande d'autorisation adressée par le PSP à la banque émettrice devra obligatoirement contenir ce "sceau", sans lequel le transfert de responsabilité ne pourra s'appliquer.

B.6.2.4 Motifs de l'impayé et transfert de responsabilité

Pour les cartes françaises (cartes CB), lorsqu'une transaction a fait l'objet d'une authentification 3D Secure réussie, le transfert de responsabilité **ne peut pas être remis en cause**.

Ceci n'est pas forcément le cas pour toutes les cartes étrangères, un impayé pouvant être émis par l'émetteur pour cause de litige commercial. Ainsi, il arrive que certains émetteurs non CB exploitent de façon indue les "litiges commerciaux" pour ne pas avoir à assurer le transfert de responsabilité.

Des litiges peuvent apparaître entre ces banques émettrices non CB et le E-Marchand parce qu'elles auront « mal codifié » la nature de la contestation du porteur.

Dans ce cas, il reviendra au marchand de prouver sa bonne foi en transmettant les pièces justificatives à la banque émettrice, qui le cas échéant, pourra être amenée à requalifier le motif de l'impayé.

B.6.3 Plusieurs façons de mettre en œuvre 3D Secure

B.6.3.1 3D Secure systématique ou 3D Secure sélectif

Le contrat standard VAD prévoit le déclenchement systématique de l'authentification 3D Secure pour l'ensemble des transactions réalisées par le marchand. Pour Visa, MasterCard et les banques, 3D Secure est en effet le pendant, pour la vente à distance, de la saisie du code PIN pour les paiements de proximité.

En proposant uniquement des contrats d'acceptation VADS les banques acquéreurs répercutent une obligation de leurs conditions d'adhésion à CB. Néanmoins, la banque acquéreur reste libre

de prendre le risque d'autoriser son Client E-Marchand de n'utiliser 3D Secure que de manière sélective si elle considère que son client maîtrise le risque de fraude.

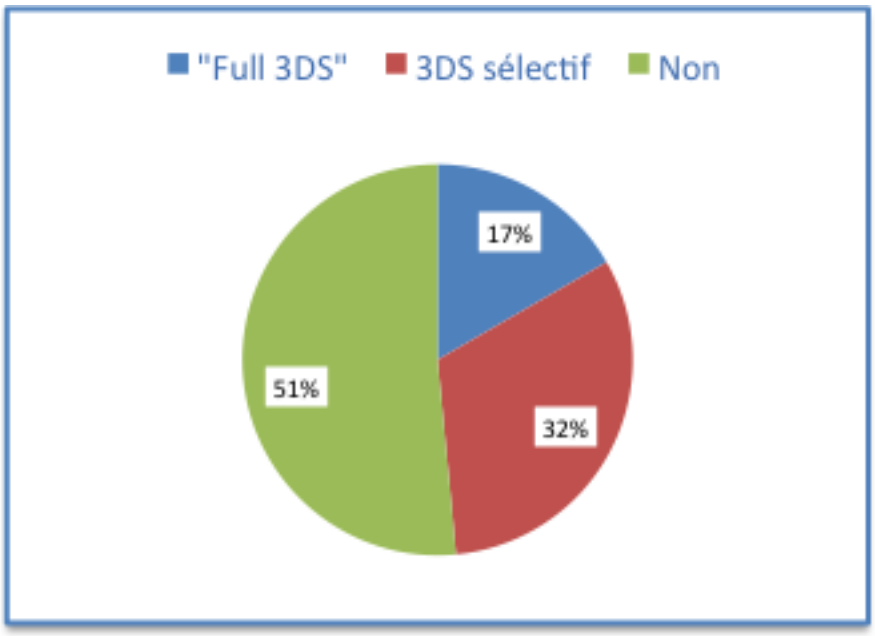
Ainsi, certains marchands (notamment les plus gros) parviennent à négocier avec leur banque la possibilité de n'appliquer 3D Secure que sur certaines transactions qu'ils estiment particulièrement risquées. Dans ce cas, la mise en œuvre de 3D Secure est dite **"sélective" ou "débrayable"** par opposition à une **utilisation systématique** de 3D Secure aussi appelée "full 3D Secure".

B.6.3.2 3D Secure déclenché dans le « tunnel de vente » ou après paiement

Une autre variante de mise en œuvre de 3D Secure, est le moment de déclenchement de 3D Secure dans le processus de paiement. Généralement, 3D Secure est déclenché directement dans le « tunnel d'achat ». C'est d'ailleurs ce qui peut rendre la mise en œuvre de 3D Secure complexe. Cependant, certains marchands, pour l'instant très minoritaires - CDiscount et PriceMinister.com parmi les marchands interviewés- ont mis en oeuvre (ou réfléchissent) à la mise en place de 3D Secure après le paiement. Pour les transactions jugées «à risque», la commande ne serait validée qu'en cas d'authentification réussie.

Ainsi CDiscount utilise quasiment autant 3DS pour authentifier les transactions en "post achat" que lors de la prise de commande. Pour CDiscount, la simplification du process de récupération des pièces justificatives et la bonne perception par les Clients de cette modalité de vérification de la validité de la commande constituent des bénéfices indéniables de 3DS.

B.6.4 Adoption de 3D Secure par les E-Marchands : résultats du questionnaire quantitatif



Source : sondage auprès des adhérents FEVAD Mai Juin 2013

Parmi les adhérents de la FEVAD ayant répondu au questionnaire, quasiment la moitié ont mis en œuvre 3D Secure. Parmi ceux qui ne l'ont pas adopté, près des 2/3 l'envisagent ou ont une réflexion sur le sujet.

Ce chiffre est en ligne avec celui de l'OSCP qui indique qu'en 2011, 50% des E-Marchands ont mis en œuvre 3D Secure.

Le dernier rapport de l'observatoire indique par ailleurs que la part des paiements sécurisés par une authentification non rejouable sur Internet s'élève à 27,5 % en valeur contre 23 % en 2011.

B.6.5 Unanimité des E-Marchands contre l'obligation de déployer 3D Secure de façon systématique

Comme nous le verrons dans les chapitres suivants, les marchands ont des avis nuancés sur les bénéfices et les inconvénients de 3D Secure. En revanche, s'il y a bien un sujet qui fait l'unanimité, c'est bien celui de l'obligation qui serait faite aux marchands de mettre en œuvre 3D Secure de manière systématique (Full 3D Secure). Même les plus fervents avocats de 3D Secure se prononcent contre l'obligation de mettre en œuvre 3D Secure de manière systématique.

Cette menace est bien réelle ; des articles de presse récents pressaient les Pouvoirs Publics de légiférer en faveur de l'imposition systématique d'une authentification forte (principalement 3D Secure). Un amendement à la proposition de loi Hamon relatif à la consommation a été déposé dans ce sens. Il a été finalement retiré par la Commission des affaires économiques de l'Assemblée nationale, le ministre Hamon jugeant que, « dans ce domaine, il ne nous semble pas opportun de légiférer, car les évolutions techniques sont si rapides que, si nous fixions un standard technique, il serait rapidement dépassé ».

Pour Delamaison.fr, la généralisation obligatoire de 3D Secure aurait un impact très préjudiciable pour l'ensemble du marché. Pour Delamaison.fr, un taux d'abandon moyen de l'ordre de 19 % (fraudes incluses) est tout simplement insupportable pour un E-Commerçant, c'est « *quasiment tuer le business* !».

Pour venteprivee.com, la généralisation de 3D Secure en mode "full" aurait « *un impact catastrophique sur le chiffre d'affaires* ».

Voyages-sncf.com, qui figure parmi les premiers gros E-Marchands à avoir mis en œuvre 3D Secure de manière systématique et qui est souvent montré en exemple, reconnaît qu'imposer l'utilisation systématique de 3D Secure serait problématique pour une majorité de E-commerçants.

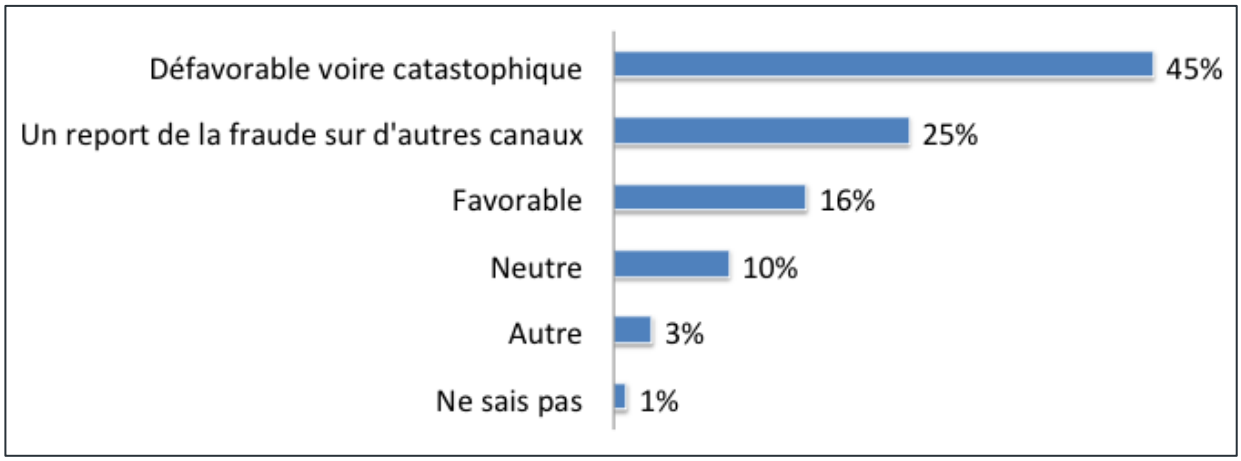
Pour laredoute.com, petits et gros acteurs du e-commerce ne sont absolument pas dans les mêmes problématiques de gestion de la lutte contre la fraude. 3D Secure n'est certainement pas la solution qui couvrirait l'ensemble des cas de figure. Pour laredoute.com, cela reviendrait à imposer aux "gros" acteurs "lourdement" équipés en système de lutte contre la fraude un outil présentant pour eux de fortes contraintes, pour le seul bénéfice espéré de faire baisser la fraude chez les petits qui n'ont pas ou peu de systèmes de protection ! Le remède pourrait être pire que le mal !

Conséquences d'une généralisation de 3D Secure (de façon systématique)

La perception des interviewés sur l'imposition obligatoire de 3D Secure en mode « Full » est partagée par les répondants au questionnaire de la FEVAD.

A la question "Quelles seraient, selon vous les conséquences d'une généralisation de 3D Secure (de façon systématique) sur votre business et pour le e-commerce ?", 45 % des répondants au

questionnaire estime qu'imposer la mise en œuvre de 3D Secure de manière systématique aurait un effet défavorable voire catastrophique sur le développement du E-commerce en France.



Source: sondage auprès des adhérents FEVAD Mai-Juin 2013

B.6.6 Retours d'expérience des E-Marchands sur 3D Secure

B.6.6.1 Le retour d'expérience de Voyages-sncf.com

En 2012, la vente de billets de train a donné lieu à 35 millions d'actes d'encaissement. Le volume d'affaires de Voyages-sncf.com en Europe a atteint 3,6 milliards d'euros en 2012.

Chez Voyages-sncf.com, la quasi-totalité des transactions s'effectue par carte bancaire. Dans certains pays européens, en Allemagne notamment, Voyages-sncf.com propose PayPal comme moyen de paiement alternatif. Les volumétries concernées sont encore faibles.

L'achat de billet de train « à distance » est possible à partir du site dédié à la vente de billets en France, à partir des sites dédiés à la vente de billets en Europe, et sur mobile.

La vente des billets électroniques concentre l'essentiel des efforts de Voyages-sncf.com en matière de lutte contre la fraude. Elle présente deux caractéristiques par rapport au risque de fraude :

- L'absence de points physiques de livraison.
- La délivrance instantanée du billet.

Voyages-sncf.com a exclu la mise en place d'un système similaire à l'aérien pour lequel l'émission du billet peut être retardé le temps nécessaire aux vérifications. Il a été considéré que cette solution aurait trop d'impacts techniques.

Avec le développement du billet électronique, Voyages-sncf.com a constaté le développement de réseaux frauduleux qui achètent des billets « sur demande » en passant par des sites de mise en relations entre vendeurs et acheteurs.

En 2011, Voyages-sncf.com a constaté une envolée de la fraude consécutive au développement très rapide du billet électronique.

Dans une première étape, Voyages-sncf.com a d'abord choisi de ne déclencher 3D Secure que sur l'achat de billets électroniques dont le montant dépassait 150 €. Fin 2011, ce seuil a été supprimé.

Depuis, 3D Secure est déclenché en fonction du mode de retrait choisi par le client et quel que soit le montant du billet. L'authentification 3D Secure n'est pas déclenchée pour les modes de retrait des billets qui nécessitent la saisie du code PIN.

Voyages-sncf.com estime qu'environ 45% de l'ensemble des transactions sont dorénavant authentifiées 3D Secure. Les 55 % restant sont :

- les transactions réalisées à partir du mobile pour lesquelles un traitement spécifique est appliqué ;
- les transactions réalisées sur les bornes et aux guichets ;
- les cartes non éligibles à 3D Secure (la détection des cartes "non éligibles 3D Secure" est réalisée lors de la transaction).

Des résultats indubitables sur la réduction de la fraude …

Incontestablement, la mise en place de 3D Secure a atteint son objectif : le taux de fraude a été réduit d'1/3. "Nous sommes très largement en dessous du seuil de la moyenne nationale de 0,34%[12]".

Voyages-sncf.com observe une tendance globalement en baisse de son taux de fraude sur les moyens de paiement à distance mais reste vigilant sur l'évolution de la fraude sur le mobile. Ce taux est stable mais reste trop élevé.

...sans impact sur le taux d'abandon grâce à un gros effort de pédagogie.

Six mois après la mise en place de 3D Secure, le taux d'abandon sur les billets électroniques (avec 3D Secure) était redevenu équivalant au taux d'abandon sur les billets non électroniques (sans 3D Secure).

Pour parvenir à ce résultat, Voyages-sncf.com estime avoir réalisé de gros efforts de pédagogie auprès de ses clients, d'autant plus que Voyages-sncf.com a figuré parmi les premiers acteurs majeurs en France à mettre en place 3D Secure. Voyages-sncf.com a notamment élaboré une aide en ligne détaillée pour guider les clients quelle que soit leur banque émettrice. Voyages-sncf.com a réalisé ce travail sans l'aide des banques.

Pour Voyages-sncf.com, l'impact quasi nul de la mise en œuvre de 3D Secure sur le taux d'abandon s'explique très largement par :

- les gros efforts de la pédagogie consentis par Voyages-sncf.com auprès de ses clients ;
- la possibilité pour le client de trouver d'autres moyens alternatifs de délivrance du billet que le Web (bornes « libre-service » et guichets).

Pour Voyages-sncf.com, 3D Secure est aujourd'hui un moyen indispensable pour lutter contre la fraude, mais Voyages-sncf.com regrette de devoir faire subir à ses bons clients les contraintes imposées par ce système.

Voyages-sncf.com considère que 3D Secure a permis de limiter fortement la fraude sur les paiements Internet mais reste très contraignant pour les paiements sur mobile et pas toujours efficace pour les cartes étrangères.

[12] le taux de fraude calculé par l'OSCP moyen était de 0,34% en 2011. Il a baissé à 0,29% en 2012.

B.6.6.2 Evolution de la position de Groupe 3 Suisses [13] sur la mise en œuvre de 3D Secure

Le taux de fraude enregistré pour le groupe 3 Suisses varie en fonction des enseignes mais demeure très bas, et très en dessous de la moyenne nationale donnée par l'OSCP. Aussi, la question de la mise en œuvre de 3D Secure ne s'était pas réellement posée jusqu'à récemment. Il faut dire que le groupe était resté sur une expérience très négative de mise en œuvre de 3D Secure à ses débuts.

Pour des raisons spécifiques, une des enseignes du groupe ne pouvait pas avoir accès à l'outil de front office de prise de commandes sur lequel s'appliquent les filtres d'évaluation du risque.

Compte tenu de ces circonstances particulières, la Direction des paiements avait recommandé la mise en place de 3D Secure en mode sélectif. Or, à ce moment là, du fait de contraintes techniques, la mise en place de 3D Secure n'a pu se faire qu'en mode "systématique".

Quand le site a, par la suite, abandonné complètement l'authentification 3D Secure, le taux de transformation a progressé de 30 %. Certes, cet abandon de 3D Secure s'est également accompagné d'une hausse de la fraude.

Le Groupe 3 Suisses en a tiré la conclusion que la mise en place de 3D Secure en mode "systématique" à cette époque pouvait avoir un impact de l'ordre de 20 à 30 % sur le taux de transformation.

Néanmoins, 3D Secure conserve pour le groupe 3 Suisses un intérêt certain s'il est mis en œuvre de façon sélective pour les transactions évaluées à risque.

Pour la Direction des paiements de Groupe 3 Suisses, de la même manière que dans un magasin physique où il ne serait pas cohérent de demander une pièce d'identité à un client habitué, 3D Secure doit être apprécié au regard de la connaissance que le site a de son client.

Pour Groupe 3 Suisses, 3D Secure en mode "sélectif" est une solution intéressante si elle est utilisée de manière très ciblée. Si 3D Secure devait être déployé au sein du Groupe 3 Suisses, 3D Secure serait utilisé comme un «outil supplémentaire de prévention ». Il pourrait permettre par ailleurs un gain de productivité de l'équipe fraude.

Pour autant, le Groupe 3 Suisses est parfaitement conscient que le déclenchement de 3D Secure devra nécessiter un pilotage « fin et régulier ».

B.6.6.3 Evolution de la position de rueducommerce.com sur 3D Secure

Il y a encore deux ans environ, rueducommerce.com était résolument opposé à la mise en place de 3D Secure ! Rueducommerce.com rappelle qu'à l'époque, l'utilisation de 3D Secure en mode sélectif n'était pas encore évoquée.

Cette conviction s'appuyait sur différents retours d'expérience d'autres E-Commerçants ainsi que sur les expériences personnelles des dirigeants du site sur le fonctionnement de 3D Secure.

C'est l'initiative de Voyages-sncf.com de mettre en œuvre 3D Secure qui a fait évoluer la position de rueducommerce.com. Grâce à Voyages-sncf.com, l'utilisation de 3D Secure est devenue réellement "Mass Market".

[13] Anciennement nommé "Groupe 3 Suisses International"

A l'époque, Rueducommerce.com ne percevait pas de pression particulière des banques pour inciter au passage des E-Commerçants à 3D Secure. Ce sont les publications d'articles de presse sur l'augmentation de la fraude sur les moyens de paiement à distance qui ont commencé à alerter Rueducommerce.com et l'ont conduit à revoir sa position auparavant très tranchée sur la question. Ces articles risquaient en effet d'entamer la confiance du Grand Public vis-à-vis du paiement sur internet et particulièrement vis-à-vis de la carte bancaire qui, chez Rueducommerce.com, représente plus de 90 % des transactions.

Un dossier d'opportunité mis à jour devait être étudié en juin 2013, dans le cadre des arbitrages semestriels du site.

Quelle que soit la décision finale, 3D Secure sera forcément déployé sur le mode sélectif. En effet, Rueducommerce.com considère qu'un taux d'échec de l'ordre de 20 % n'est pas économiquement viable. Rueducommerce.com est dubitatif sur une amélioration prochaine et significative du taux d'échec. Il lui apparait à ce jour "incompressible".[14]

B.6.6.4 Le retour d'expérience de mistergooddeal.com sur 3D Secure

En préambule, Mistergooddeal.com rappelle que l'entreprise est naturellement et culturellement portée vers l'innovation. Elle avait suivi le développement de 3D Secure dès son lancement.

Chez mistergoodeal.com, la mise en place de 3D Secure a eu lieu en deux temps.

En 2009, 3D Secure a été mis en place uniquement sur les produits informatiques et le son, deux familles de produits particulièrement fraudées et sur lesquelles la marge est très faible. Dès lors, le risque de répercussion de la mise en œuvre de 3D Secure sur les ventes a été jugé acceptable.

Les résultats sur la fraude ont été spectaculaires. Elle a été divisée par 10 en valeur, quasiment du jour au lendemain ! Mais, revers de la médaille, Mistergooddeal.com a constaté que la fraude se déportait vers les autres familles de produits, de l'informatique vers les lave-linge !

A partir de septembre 2012, la généralisation de 3D Secure a été effective chez mistergoodeal.com sur l'ensemble des produits. En cas d'échec d'authentification 3D Secure du fait d'un problème technique rencontré par la banque émettrice, le client est dirigé vers une page classique de paiement sans 3D Secure. La transaction bascule alors automatiquement dans le processus classique d'évaluation du risque, processus qui a donc été maintenu.

B.6.6.5 Le retour d'expérience de Delamaison.fr sur 3D Secure

Delamaison.fr a commencé par mettre en place 3D Secure en mode systématique (« Full 3DS »).

Fin 2010, en raison d'une brusque montée du taux d'abandon, l'enseigne choisit de retirer 3D Secure.

Très vite, le taux d'impayé augumente fortement. La banque acquéreur de Delamaison.fr l'alerte alors sur l'envolée d'impayés sur des cartes Master Card d'origine étrangère.[15].

---

[14] A noter : ce taux est passé de 19.5% à 17.5% entre avril 2011 et avril 2013 selon les chiffres de l'OSCP. La proportion des paiements 3D-Secure a quant à elle progressée de 17.5% à 27.5% des paiements en volume durant la même période.

[15] Les banques acquéreurs paient des pénalités au réseau Visa et MasterCard quand leurs clients enregistrent des taux d'impayés hors norme. Les réseaux Visa et Master Card ont mis en place

Au vu de l'impact désastreux de la mise en œuvre de 3D Secure en mode "full" sur le taux d'abandon, Delamaison.fr négocie avec sa banque de pouvoir déclencher 3D Secure de façon sélective.

Le point de vue du juriste - L'article 5 du contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS) relatif à la garantie du paiement prévoit que les opérations de paiement sont garanties à la condition, pour le E-Commerçant, de respecter l'ensemble des mesures de sécurité visée au contrat. À défaut, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement et en l'absence de contestations.

L'authentification 3D Secure sera demandée uniquement pour les transactions jugées «à risque».

Actuellement, 20% des transactions par cartes bancaires sont authentifiées avec 3D Secure et Delamaison.fr souhaite faire baisser ce taux.

"Nous cherchons à optimiser le ratio entre le nombre de transactions dont nous demandons l'authentification (et le risque d'abandon afférant) et le taux d'impayés."

Fin 2012, le taux d'abandon brut des transactions 3D Secure chez Delamaison.fr, était de l'ordre de 30 %. Par "taux d'abandon brut", Delamaison.fr entend un taux d'abandon global qui inclut les abandons correspondant à une carte non éligible, un problème technique, un code non saisi par un client de bonne foi ou une tentative de fraude. Delamaison.fr n'a pas les moyens techniques de quantifier chacune de ces causes.

Fort heureusement, Delamaison.fr parvient à relancer une partie de ses clients à la suite d'un abandon grâce à des actions de relances téléphoniques automatisées (détections des commandes abandonnées), ou sur appel du client qui est alors invité à choisir un autre mode de paiement. La dernière possibilité est le « débrayage » manuel de 3D Secure.

Chez Delamaison.fr, le report de la fraude s'est fait vers:

- des moyens de paiements pour lesquels les transactions ne peuvent faire l'objet d'une authentification 3D Secure (PayPal notamment) ;
- les chèques : en 2012, Delamaison.fr a constaté une recrudescence des impayés sur les encaissements par chèque pendant quelques semaines.

B.6.6.6 Cheminement de la décision de Venteprivée.com sur 3D Secure

La décision de mettre en œuvre 3D Secure en mode sélectif a été prise chez venteprivée.com en 2012, du fait de l'augmentation récente de la fraude qui a conduit à revoir la priorité accordée au projet. Il devrait être opérationnel à partir du 3ème semestre 2013.

Le choix du mode sélectif a été pris sur la base des chiffres du taux d'échec communiqué par la Banque de France. Il se justifie aussi par la nature de l'activité de Venteprivée.com qui reste fondée sur l'achat d'impulsion. Dès lors, la mise en œuvre de 3D Secure sur un mode

---

un observatoire des E-Commerçants qui peuvent les amener à "blacklister" un E-Commerçant dont le taux d'impayé dépasserait un certain seuil. Delamaison.fr a eu le sentiment que Master Card en venait à assimiler le E-Commerçant à ses clients fraudeurs !

Les conséquences de ce "blacklistage" pour un E-Commerçant peuvent être dramatiques; toutes les banques acquéreur étant en relation avec les réseaux Visa et MasterCard, le E-Commerçant peut se voir refuser tout contrat VAD.

systématique (Full3D Secure) aurait fait courir un risque beaucoup trop important pour Vente-privee.com.

De plus, le cœur de clientèle de Vente-privee.com est constitué par des clients très fidèles. Vente-privee.com considère posséder l'une des plus importantes bases clients en "One click" de France. Le site ne souhaitait pas " importuner" ce cœur de clientèle extrêmement fidèle en obligeant ces clients à s'authentifier systématiquement.

3D Secure sera actionné pour les nouveaux clients dont les achats seraient identifiés « à risque ». Dans ce cas, Vente-privee.com considère 3D Secure comme particulièrement pertinent.

Il n'en demeure pas moins que, pour Vente-privée.com, 3D Secure n'est qu'un outil parmi d'autres. C'est un indicateur de plus à prendre en compte dans l'analyse de risque de la transaction. Le cœur du système anti-fraude restera *Accertify*.

Vente-privee.com a bénéficié de l'expertise de ses banques acquéreur dans l'étude préalable de mise en œuvre de 3D Secure. "Nous avons un contact quotidien et direct avec le responsable du E-business de la Société Générale !"

B.6.6.7 Cheminement de la décision de Priceminister.com sur 3D Secure

Priceminister.com mettra en place 3D Secure en septembre 2013.

Ce n'est pas la réduction des impayés qui constitue la principale raison de la mise en place de 3D Secure chez Priceminister.com. D'ailleurs, Priceminister.com fait remarquer que 3D Secure est déclenché avant la demande d'autorisation. Dès lors, il n'est pas possible de déclencher 3D Secure pour les seuls refus d'autorisation qui feraient suspecter une fraude tels que "ne pas honorer"," carte perdue ou volée".

Contrairement à la pratique prédominante (au moins jusqu'à présent), PriceMinister.com ne l'activera pas dans le tunnel de vente mais à posteriori. La raison principale de cette décision a été de ne pas perturber en aucune manière le processus de commande.

A la suite de la réception de la demande d'autorisation et du passage des règles d'évaluation du risque, la commande est soit validée soit passée en « observations ».

Seulement dans ce cas, le Client devra accéder à son espace client / suivi des commandes et valider sa commande en s'authentifiant. Il est possible que le client ait à taper de nouveau son numéro de carte bleue. Si le client ne procède pas à cette authentification, alors la commande sera annulée.

Le recours à 3D Secure permettra de supprimer les procédures de rappel du client pour récupérer des pièces justificatives, procédures soumises aux exigences de la CNIL et qui de toute manière, échouaient dans 80 % des cas. Dans les 20 % restants, il faut encore éliminer les dossiers qui reviennent "trop parfaitement complétés" et qui correspondaient très vraisemblablement à des transactions frauduleuses.

Priceminister.com a constaté que 45 % des transactions jugées douteuses mais que le service fraude présentait tout de même à la facturation, sans avoir pu obtenir de justificatif, revenait en impayés.

"Nous voyons 3D Secure comme une manière moderne et efficace de récupérer les justificatifs de la commande ". Grâce à 3D Secure, Priceminister.com espère récupérer la moitié des commandes qui précédemment auraient été annulées.

Priceminister.com estime par ailleurs que 3D Secure sera mieux accepté par le Client comme moyen de vérification de la commande que la demande de pièces justificatives.

Pour Priceminister.com, les avantages perçus de 3D Secure qui ont motivé son choix sont:

- l'augmentation du taux de facturation (la part du chiffre d'affaires réellement facturée par rapport au chiffre d'affaire total) ;
- l'augmentation de la productivité (suppression des demandes de justificatifs) ce qui permettra au personnel de se concentrer sur l'analyse fine des fraudes plutôt que le traitement en masse des cas de suspicion de fraude ;
- la non détérioration de la satisfaction client ;
- la réduction des délais de validation de la commande ;
- la compatibilité du dispositif avec les achats mobiles.

B.6.6.8 Etat des réflexions sur le déploiement de 3D Secure chez Lastminute.com

A la date de l'interview, 3D Secure n'était déployé dans aucun pays dans lesquels Lastminute.com est présent y compris l'Angleterre. Néanmoins une étude d'opportunité avait débuté.

En France, la Direction Financière est très favorable au déploiement de 3D Secure sur un mode sélectif. Pour Lastminute.com France, 3D Secure présente de nombreux avantages notamment la sécurisation des paiements pour les achats de dernière minute.

B.6.6.9 Retour d'expérience de CDiscount.com sur 3D Secure

CDiscount.com est parmi les seuls interviewés à avoir été en mesure de quantifier l'appétence spontanée des clients pour un dispositif d'authentification comme 3D Secure.

En Avril 2009, CDiscount.com a mis en place 3D Secure de façon optionnelle pour les paiements à l'acte. Au moment du paiement, les clients avaient la possibilité de demander l'authentification par 3D Secure. Seulement 3% des clients choisissait de sécuriser leurs transactions par ce moyen. Un an et demi plus tard ce taux est monté à 10 %. Ces résultats factuels nuançaient pour le moins l'appétence des clients pour 3D Secure mise en avant par certaines études consommateurs.

A l'heure actuelle, 3D Secure n'est plus proposé optionnellement aux Clients par soucis de simplification de la page de paiement. Il est déclenché en fonction de règles métier évolutives (paniers sensibles).

3D Secure est également proposé aux clients comme alternative à la fourniture de pièces justificatives. Les analyses de satisfaction clientèle ont montré le très bon accueil des clients pour cette option.

B.6.6.10 Etat de la réflexion de la Redoute sur 3D Secure

"Ce qui est sûr, c'est que ne voulons pas qu'on nous impose 3D Secure. On ne peut pas se permettre d'avoir un taux d'échec de l'ordre de 17 à 20 % : c'est contraire aux règles du commerce ! »

Cette position tranchée trouve en partie son explication dans une expérience malheureuse de la Redoute.com dans la mise en oeuvre de 3D Secure il y a maintenant quelques années.

La Redoute avait alors déployé 3D Secure sur son site Elios.fr, en mode "systématique" : La Redoute a alors enregistré une chute de 20 % de ses ventes.

La Redoute considère au mieux 3D Secure comme une « deuxième chance » de lever une suspicion de transactions frauduleuses.

La Redoute se pose néanmoins la question de savoir s'il proposera 3D Secure de façon optionnelle au client, pour une question d'image. La Redoute n'exclut pas que la possibilité de s'authentifier avec 3D Secure puisse faire partie des futures critères de choix d'un site pour les Clients.

B.6.6.11 Retour d'expérience de Pecheur.com sur 3D Secure

Pecheur.com a mis en place 3D Secure dès 2004 pour lutter contre la fraude sur les cartes étrangères.

Fin 2008 , dès l'annonce de la mise en place du transfert de responsabilité, Pecheur.com a décidé la mise en place immédiate de 3D Secure en mode "full".

Pendant un peu moins d'un an, la mise en œuvre de 3D Secure n'a eu aucun impact sur le taux de transformation. A l'époque, les porteurs enrôlés étaient en effet rares! Les banques émettrices assumaient le risque. Lorsque des contestations avec la banque survenaient - sur des transactions revenues en impayé alors qu'elles avaient été authentifiées 3D Secure- Pecheur.com constatait que même ses interlocuteurs, au sein des banques, ne connaissaient pas l'existence de 3D Secure !

Pecheur.com pense qu'à cette époque, les banques n'avaient pas réalisé les développements SI nécessaires pour isoler les contestations sur des transactions 3D Secure. Pecheur.com se souvient avoir dû "batailler" auprès de sa banque pour obtenir l'application du transfert de responsabilité.

Pour Pecheur.com, la deuxième raison du faible impact de 3D Secure sur le taux de transformation était la situation concurrentielle favorable du site. A cette époque, n'ayant pas d'autres réels choix alternatifs, les clients de Pecheur.com étaient suffisamment motivés pour surmonter l'obstacle de l'authentification ou finissaient par... envoyer un chèque !

La situation a brusquement changé à la rentrée 2009. Pendant l'été, les banques avaient enrôlé massivement leurs clients. Selon Pecheur.com, cet enrôlement massif ne s'était probablement pas fait dans des conditions optimales de qualité en ce qui concerne la collecte des données clients. Brusquement, un nombre beaucoup plus important de clients a dû s'authentifier, dans des conditions de fonctionnement très aléatoires du système, le taux d'échec a alors explosé.

Un second facteur s'est avéré impactant : ces échecs d'authentification se sont multipliés pendant la période de Noel. Or, pour des clients en recherche de cadeaux, la barrière de l'authentification est devenue cette fois rédhibitoire. Le taux d'abandon a atteint 30 %.

Après analyse des statistiques de vente de janvier, Pecheur.com a pris la décision d'arrêter l'utilisation systématique de 3D Secure et de la restreindre aux seules transactions étrangères et aux commandes livrées en point relais.

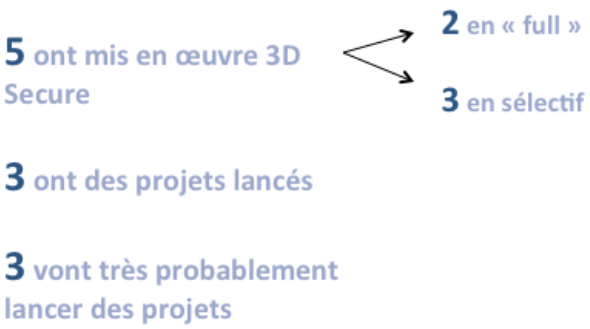
Le déclenchement de 3D Secure est aujourd'hui géré par le prestataire de Pecheur.com, Be2bill. 60 critères de déclenchement de 3D Secure peuvent être pris en compte.

La validation d'une transaction se fait en deux étapes:

- Etape 1: Be2bill valide la transaction en appliquant ou pas 3D Secure ;
- Etape 2 : Validation par Pecheur.com des transactions "à risque" aboutissant à une mise sous quarantaine de certaines commandes.

B.6.7 Déploiement de 3D Secure chez les E-Marchands interviewés

Parmi les 11 E-Marchands interviewés
PECHEUR
LA REDOUTE
CDISCOUNT
GROUPE 3 Suisses
VOYAGES-SNCF
PRICEMINISTER
LASTMINUTE
MISTERGOODDEAL
DELAMAISON
RUE DU COMMERCE
VENTE-PRIVEE



B.6.8 Le mode sélectif est quasiment unanimement privilégié

Mistergooddeal.com et Voyages-sncf.com sont les seuls interviewés à avoir déployé 3D Secure de façon systématique[16]. Et, dans le cas de Voyages-sncf.com, le client qui échouerait à s'identifier bénéficie de moyens alternatifs de retrait de ses billets.

Mistergooddeal.com est donc le seul, parmi les E-Marchands interviewés, à se prononcer aussi nettement pour le développement de 3D Secure en mode systématique qu'il considère comme un moyen important de lutte contre la fraude d'autant plus efficace que son usage serait répandu.

Ainsi, les tenants d'une mise en place de 3D Secure de manière sélective sont largement majoritaires parmi les E-Commerçants interviewés.

L'OSCP souligne cependant que la Banque de France a conduit des actions fortes en 2011 et 2012 demandant aux émetteurs de renforcer l'information et l'équipement de leurs porteurs. Comme en témoignent les chiffres publiés par l'OSCP, la situation s'est sensiblement améliorée tant sur le plan du taux d'équipement que de celui du taux d'échec. Enfin, le déploiement systématique de 3D-Secure en particulier sur Voyages-sncf.com a fortement contribué à éduquer le marché et à généraliser l'usage de l'authentification non rejouable.

B.6.9 Difficultés et coûts de mise en œuvre de 3D Secure très disparates d'un E-Marchand à l'autre

B.6.9.1 Difficultés de mise en œuvre de 3D Secure

Majoritairement, les marchands interviewés n'ont pas relevé de difficultés particulières dans la mise en œuvre technique de 3D Secure, même si les situations peuvent être très différentes

[16] On entend par "systématique" le déclenchement de 3D Secure sur toutes les transactions, sachant que 3D Secure peut néanmoins être débrayé si l'authentification se passe mal.

pour chaque marchand notamment en fonction du nombre de transactions traitées ou de la complexité du SI en place.

Pour Atos Wordline, la difficulté de mise en œuvre de 3D Secure dépend de la localisation de la page de paiement qui peut être soit hébergée par le marchand soit hébergée chez son PSP.

Dans ce deuxième cas de figure, le Marchand doit indiquer à sa banque s'il veut mettre en place un contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS). Son PSP mettra alors en œuvre le process d'activation auprès des Directory Server de Visa et MasterCard (délais 7 jours).

Dans le cas où le marchand opte pour une mise en œuvre de 3D Secure de façon sélective, il lui suffira d'indiquer dans la transaction si cette transaction doit être authentifiée 3D Secure ou pas. Autre option possible pour le E-Marchand : demander à son PSP d'analyser la transaction, et le cas échéant déclencher lui-même l'authentification 3D Secure, en fonction du résultat de l'analyse.

Pour Atos Atos Wordline, quand la page de paiement est déportée, le passage à 3D Secure pour le Marchand ne présente pas de difficultés techniques particulières aussi bien dans un mode "full" que dans un mode " sélectif".

Dans le cas où la page de paiement est hébergée chez le marchand, la mise en œuvre de 3D Secure est plus complexe. Mais, une partie de la complexité peut être prise en charge par le PSP.

Vente-privee.com apporte un éclairage nuancé sur ce constat, non pas sur l'appréciation de la complexité technique intrinsèque de la solution 3D Secure mais sur la complexité du projet de déploiement de la solution: *"Il n'y a pas de complexité technique ou technologique particulière à proprement parler. La complexité est liée à la structure des flux de vente-privée, sa taille et des risques associés liés à l'impact de 3D Secure et des niveaux d'exigences que nous avons sur le déploiement".*

Au fil de l'étude de mise en œuvre, Vente-privee.com s'est aperçu que, contrairement au Full 3D Secure, la mise en place de 3D Secure en mode sélectif pouvait être "tout sauf simple !".

Par défaut, le standard défini par Visa et MasterCard repose sur la mise en œuvre systématique de 3D Secure sur l'ensemble des transactions (Full 3D Secure). Il ne prévoit pas que 3D Secure puisse être activé de manière sélective.

La mise en œuvre de 3D Secure en mode sélectif nécessite donc de passer temporairement par du "Full 3D Secure".

Le passage d'une boutique en mode 3D Secure débrayable doit suivre les étapes suivantes:

- déclaration de la boutique sur les systèmes Visa et MasterCard : délai de 24 heures ;
- passage de la boutique en mode full 3D Secure : délai de 24 heures.

Ainsi, une boutique ne peut passer au mode 3D Secure débrayable que dans un délai minimum de 48 heures, sachant que pendant 24 heures 3D Secure sera activé de façon systématique.

Pour un E-Marchand comme Vente-privée.com, cette contrainte technique a des impacts forts.

La chance de venteprivée.com a été de disposer, sur les principaux pays dans lesquels il est présent, d'au moins deux boutiques gérées chacune par l'une de ses banques acquéreurs. Cela a permis à venteprivée.com d'orienter l'intégralité des flux vers une boutique en attendant que la deuxième passe en 3D Secure débrayable.

L'ensemble de ces contraintes fait dire à venteprivée.com que la mise en œuvre de 3D Secure sur un mode débrayable - au moins pour un E-Marchand de taille important - est "un vrai projet" dont il faut mesurer tous les impacts. Dans la phase de déploiement, il nécessite une

coordination étroite entre le E-Marchand, sa ou ses banques acquéreurs et son prestataire technique de solutions de paiement (plateforme de paiement par exemple).

Cet avis est partagé par rueducommerce.com qui anticipe un "gros chantier informatique" qui devrait mobiliser un nombre important de ressources.

Si elle n'a pas posé de difficultés techniques particulières, la mise en place de 3D Secure a néanmoins représenté une charge de 150 jours hommes pour Voyages-sncf.com.

B.6.9.2 Coûts de mise en œuvre de 3D Secure.

Il est particulièrement difficile de donner un coût moyen de mise en œuvre de 3D Secure pour un E-Marchand, ces coûts pouvant dépendre de facteurs propres à chaque marchand tels que sa taille, la complexité de son système d'information mais également de la manière dont il souhaite mettre en œuvre 3D Secure.

Les résultats de l'étude menée par Rueducommerce.com ont montré qu'ils étaient loin d'être négligeables. C'est le positionnement de 3D Secure dans le dispositif anti-fraude qui a constitué la principale variable de coût. Pour Rueducommerce.com le plus efficace pour rueducommerce.com serait de déclencher 3D Secure en mode débrayable directement dans le tunnel de vente et en temps réel. Mais, la mise en œuvre de 3D Secure dans ces conditions devient relativement coûteuse.

Selon l'estimation de La Redoute, le coût du projet de mise en œuvre de la solution 3D Secure se chiffre en dizaines de milliers d'euros, sachant que la Redoute est déjà certifiée PSI DSS.

B.6.9.3 Autres coûts à prendre en compte

Delamaison.fr souligne l'effort de formation des chargés de clientèle que les commerçants doivent prendre à leur charge. Chez Delamaison.fr, ce sont plus de 50 chargés de clientèles qui ont été formés aux différents parcours d'authentification auquel leurs clients peuvent être potentiellement confrontés. Et d'ajouter au passage : "*Le système bancaire veut nous imposer un système ; que nous, les E- commerçants, devons payer !*"

B.6.10 Le taux d'échec : frein majeur à l'adoption de 3D Secure par les E-Marchands

Le taux d'échec est un des indicateurs suivis très précisément par l'Observatoire de la Sécurité des Cartes de Paiement (OSCP).

L'OSCP rappelle que le taux d'échec communiqué correspond au rapport des transactions non finalisées, quelle qu'en soit la cause, sur le nombre de transactions total initiées en 3D-Secure. Sont ainsi compris dans les motifs d'échec:

- Les abandons légitimes du porteur (changement d'avis, etc.)
- Les problèmes techniques divers (interruption de communication, réseau, etc.);
- Les tentatives de fraude;
- Les saisies erronées;
- Les échecs imputés à des contrôles d'autorisation (provision insuffisante, etc.) lorsque ceux-ci sont intégrés avant la phase d'authentification.

En outre, l'OSCP rappelle que beaucoup de grands e-marchands envoient en 3D-Secure leurs transactions les plus risquées, ce qui impacte défavorablement le taux global d'échec en raison de la forte prédisposition de ces paiements à être rejetés.

B.6.10.1 La réalité "implacable" des chiffres

La 5ème collecte 3D Secure de l'OSCP couvrant la période du 01/11/2012 au 30/04/2013 fait état d'un taux d'échec moyen de 17,47 %, alors que celui-ci était de 20% en 2011.

L'évolution de cet indicateur clé pour les E-Commerçants appelle plusieurs commentaires. Tout d'abord, on constate que la diminution du taux d'échec est lente ! Depuis avril 2011, le taux d'échec n'a finalement que très peu évolué.

Date	Taux d'échec à l'authentification
Avril 2011	19,5 %
Octobre 2011	22 %
Avril 2012	19,7 %
Octobre 2012	17,7 %

Source : baromètre OSCP, 4ème collecte 3D Secure couvrant la période du 01/05/2012 au 31/10/2012.

Ensuite, ces chiffres font la moyenne de l'ensemble des banques. Sans les nommer explicitement, l'OCSP fournit également des résultats banque par banque. Et, on constate une forte disparité d'une banque à l'autre.

Toutefois, les derniers chiffres de l'OSCP en avril 2013 permettent d'observer une nette homogénéisation du taux d'échec avec un minimum à 12,5% et un maximum à 24%.

B.6.10.2 Un taux d'échec jugé « rédhibitoire » pour la plupart des E-Marchands

Le taux d'échec reste un frein majeur dans la mise en œuvre de 3D Secure pour une grande majorité de E-Commerçants. Il apparaît, pour nombre d'entre eux, comme incompatible avec les réalités économiques du E-Commerce à savoir des taux de marge souvent très faibles et des coûts d'acquisition du client élevés.

Delamaison.fr traduit ainsi le sentiment général : "un taux d'abandon moyen de l'ordre de 18 % (même s'il inclut les tentatives de fraudes échouées) est tout simplement insupportable pour un E-Commerçant, c'est quasiment tuer le business !". Il faut également prendre en compte que le E-Marchand peut avoir une perception du taux d'abandon très différente du taux moyen donné par l'OSCP. Ainsi, pour Delamaison.fr, le taux d'abandon était de l'ordre de 40 % début 2011, il est encore à plus de 30 % actuellement.

Ce grief fait par les E-Marchands à 3D Secure n'est pas nouveau. Et, certains E-Marchands déplorent que s'exerce sur eux une forte pression pour qu'ils adoptent 3D Secure alors que parallèlement, ils ne constatent pas d'amélioration significative sur le taux d'abandon.

Pour Vente-privée.com, il est difficilement compréhensible que la Banque de France tolère de telles différences entre les banques sur le taux d'échec d'authentification: "Il n'est pas admissible que certaines banques affichent des taux de l'ordre de 6 % alors que d'autres avaient encore récemment des taux de plus de 40 %! 3D Secure n'est pourtant plus une nouveauté !"

B.6.10.3 Explications sur le niveau très élevé du taux d'échec

Pour un spécialiste de la question comme Be2bill, les raisons du niveau élevé du taux d'échec d'authentification sont multiples. Il est le résultat de l'addition de situations particulières chez les banques émettrices.

Pour Atos Wordline, des raisons conjoncturelles peuvent être avancées pour expliquer le niveau actuel d'échec d'authentification. Si aujourd'hui, quasiment 100% des porteurs peuvent s'authentifier par 3D Secure, une partie d'entre eux ne s'est encore jamais authentifiée car ils n'ont pas effectué d'achat sur des sites 3D Secure. Cette population pourra faire face à des échecs d'authentification, d'autant plus fréquents que certaines banques proposent l'enrôlement en ligne au moment de la transaction. Par ailleurs, les établissements n'ayant pas les mêmes méthodes d'authentification, un même utilisateur multi-bancarisé devra être prêt à jongler entre plusieurs méthodes d'authentification.

Pour remédier à cette situation, certaines banques (dont Crédit Mutuel) seraient ainsi actuellement en train de faire migrer leurs porteurs vers des systèmes d'authentification non rejouables. L'enrôlement de ces clients a lieu en ligne, concomitamment avec l'acte d'achat. Le client doit s'enrôler puis s'authentifier. On comprend qu'un tel parcours d'achat puisse avoir une incidence très négative sur le taux d'échec.

A ces explications conjoncturelles, s'ajoutent des raisons plus fondamentales de choix de méthode d'authentification par les banques. Ainsi, la méthode dite de "la bataille navale" est unanimement décriée par les E-Marchands qui constatent, dans leurs statistiques, que le taux d'échec de la banque qui la propose figure parmi les plus élevés. Même si l'on constate un mouvement d'uniformisation des moyens d'authentification, il est indéniable que les choix divergents des banques à l'origine ont rendu complexe la communication et les explications sur le sujet, ralentissant de ce fait l'adoption de moyens d'authentification comme 3D Secure en France.

B.6.10.4 Le taux d'échec : mélange-t-on des choux et des carottes ?

L'OSCP précise que : "les motifs d'échec de la transaction ne pouvant être analysés, le taux d'échec ne tient pas compte des tentatives infructueuses ayant suivi un échec, mais intègre notamment les abandons porteurs, les problèmes techniques, les tentatives de fraude, les usages abusifs, les mises en opposition et les saisies erronées, ce qui ne constitue pas de réels échecs". Un code retour est systématiquement fourni pour chaque demande d'authentification. Les 5 codes retour émis par les banques émettrices sont les suivants (standards 3D Secure) :

Libellé	Signification	Transfert de responsabilité
3D Success	Authentification réussie	Oui
Echec (mauvais code)	Saisie d'un code erroné	Non
Porteur non enrôlé		Oui
3D Failure	Dépassement du délai imparti	Non
3D Error	Echec pour des raisons techniques	Non

Note : *le tableau ci-dessus est simplifié. Des différences peuvent exister en fonction des réseaux et des régions (intra Europe / hors Europe) ainsi que du type de carte*

Techniquement, ce sont les banques émettrices via leur ACS qui remontent ces données. CB n'a pas de visibilité directe sur les échecs d'authentification.

Pratiquement, il est très difficile de distinguer au sein du taux d'échec ce qui est relatif à la fraude, à un problème technique, ou à un "time out" (dépassement du délai laissé au porteur pour saisir le code). Or, en fonction du code retourné, les raisons de l'échec peuvent être différentes ainsi que les éventuelles responsabilités; banque ou porteur ?

Pour Be2Bill, il y a deux façons d'interpréter un échec d'authentification: positivement (tentative de fraude mise en échec), négativement (incapacité du client à s'identifier).

B.6.10.5 La nécessaire interprétation du taux d'abandon brut

Le taux d'échec annoncé par l'OSCP apparait pour Mistergooddeal.com comme "énorme" par rapport à ce qu'il constate. Chez Mistergooddeal.com, le taux d'abandon "entrée de page d'authentification" est aujourd'hui d'environ 15% et de 17%, tous motifs confondus (plafond bancaire atteint, solde insuffisant, abandon du client...).

Pour Mistergooddeal.com, il est important de rappeler que le taux d'échec d'authentification annoncé par la Banque de France (19,5 %) correspond à un taux d'échec brut.

Ce taux d'abandon brut ne tient pas compte du report vers d'autres moyens de paiement ni des nouvelles tentatives du Client qui, entre deux tentatives, a pu s'enrôler auprès de sa banque. Mistergooddeal.com a pu constater que certains clients pouvaient procéder à une nouvelle tentative d'authentification jusqu'à cinq jours après la première tentative !

Pour certains interviewés, le taux d'échec d'authentification donné par l'OSCP doit être relativisé. Il doit être notamment comparé avec le taux d'échec d'autorisation classique sur les cartes bancaires ou avec le taux naturel d'abandon. Le taux d'abandon classique (client qui va jusqu'à la page de paiement mais qui ne procède pas au paiement lui-même) est d'environ 12% brut chez mistergooddeal.com.

Enfin, Be2Bill rappelle que l'interprétation du taux d'échec d'authentification doit aussi tenir compte des spécificités de chaque secteur. Ainsi, certains commerçants n'ont pas forcément conscience du niveau d'exposition de leurs secteurs d'activité au risque de fraude.

B.6.10.6 Vers une amélioration du taux d'échec : les E-Marchands restent prudents

Depuis la publication des derniers chiffres de l'OSCP, les E-Marchands interrogés constatent l'amélioration récente du taux d'échec d'authentification, mais restent tout de même très prudents. Les débuts extrêmement laborieux de 3D Secure, l'époque où le lien d'aide sur la page d'authentification de certaines banques aboutissait à une erreur 404, reste encore très présents dans les mémoires !

Ainsi Mistergooddeal.com constate depuis huit mois, de réelles avancées dans l'efficacité des systèmes d'authentification mis en place par les banques émettrices, tant d'un point de vue technique que pour l'enrôlement de leurs clients. Cette amélioration s'est notamment traduite par le raccourcissement des délais d'envoi du SMS, qui encore récemment provoquait une augmentation du délai moyen de traitement des appels clients et donc un coût pour le E-Marchand.

CB, confirme que les banques émettrices ont tout intérêt à travailler à la réduction du taux d'échec car même si le SMS n'arrive pas, elles en paient quand même le coût !

B.6.11 Les autres freins à l'utilisation de 3D Secure vus par les E-Marchands

B.6.11.1 Une information des clients jugée très largement insuffisante

Unanimement, les E-Marchands interrogés considèrent que les efforts de pédagogie et d'information déployés par les banques émettrices ou, tout du moins, les résultats obtenus ont été et restent très largement insuffisants. Pour la plupart des interviewés, voyages-sncf.com a plus œuvré pour la vulgarisation de l'usage de 3D Secure que l'ensemble des banques réunies !

De nombreux E-Marchands ont développé un certain ressentiment vis-à-vis des banques à ce sujet. Pour eux, il est anormal qu'ils aient eu à supporter des coûts d'information et de pédagogie que les banques auraient dû logiquement prendre à leur charge en tant qu'instigatrices des méthodes d'authentification. De même, il aurait été logique que les banques émettrices apportent un minimum de support aux marchands sur les méthodes d'authentification qu'elles mettaient en place et ce d'autant plus qu'elles n'avaient pas fait le choix de méthodes d'authentification communes.

L'effort de pédagogie a semble-t-il été beaucoup plus poussé au Royaume-Uni, ce qui constituerait une des raisons expliquant l'usage beaucoup plus répandu de 3D Secure dans ce pays. Pour Be2Bill, la courbe d'apprentissage par le grand public d'une solution comme 3D Secure est forcément longue. Et, en la matière, un gros travail d'explication reste encore à faire.

Contrairement à ce que peuvent penser les E-Marchands interviewés, la Fédération Bancaire Française confirme que les banques ont bel et bien déployé des efforts importants d'information et de pédagogie auprès de leurs clients pour expliquer le fonctionnement de 3D Secure. Mais, force est de constater qu'il est difficile de capter l'attention des clients sur ce type de sujet.

De plus, la Fédération Bancaire Française considère que les banques n'ont pas à supporter à elles seules l'effort de pédagogie. Il revient également aux Pouvoirs Publics de promouvoir l'usage de 3D Secure. Il faut reconnaître que la communication des Pouvoirs Publics vis-à-vis du grand public est perfectible.

B.6.11.2 La non éligibilité de certaines cartes au transfert de responsabilité

Pour CB, le transfert de responsabilité ne pose, en théorie, aucun problème sur les cartes CB. Les seules difficultés concernent certaines cartes étrangères.

Pour les cartes définies comme éligibles par Visa et MasterCard, il est de la responsabilité de la banque émettrice d'enrôler ses clients. Dès lors, même si une transaction n'a pas pu être authentifiée du fait du non enrôlement du client, le transfert de responsabilité du E-Marchant vers la banque émettrice s'applique néanmoins, aux dépens de cette dernière.

Be2Bill confirme la règle établie par Visa et MasterCard selon laquelle toutes les cartes Carte CB-visa MasterCard, Visa seul et MasterCard seul (à l'exception des cartes business) sont éligibles. Pour Be2Bill, les exceptions à cette règle sont clairement des anomalies.

La non éligibilité des cartes business à l'authentification 3D Secure s'explique par le fait qu'une carte business n'est pas forcement nominative; plusieurs employés d'une même société peuvent l'utiliser. Dès lors, il est impossible d'authentifier l'auteur de la transaction de manière unique.

Pour les cartes commerciales hors Europe, l'authentification 3D Secure pourra avoir lieu, donner un résultat positif mais le transfert de responsabilité ne s'appliquera pas pour autant.

Pour Atos Wordline, les cartes non éligibles ne peuvent pas être identifiées uniquement sur leur seule appartenance à une plage spécifique de BIN. Certaines catégorisations de cartes peuvent en effet partager le même BIN.

L'identification des transactions non éligibles à 3D Secure requiert par conséquent une vraie expertise du côté de l'E-Marchand. Souvent, cette expertise est apportée par le PSP. Une fois identifiées, ces transactions sont scorées selon un processus différent des cartes CB avec une intervention plus manuelle.

Pour la grande majorité des E-Marchands rencontrés, au-delà des grands principes, les règles précises d'éligibilités des cartes notamment étrangères nécessitent encore des clarifications. Cet avis semble partagé par la Banque de France qui n'a de cesse de demander un point précis aux banques sur ce sujet.

En attendant cette clarification, ce sont bien les E-Marchands qui font les frais de ce manque de transparence. Certains E-Marchands ont ainsi fait un "apprentissage douloureux" des limites du transfert de responsabilité. En 2009-2010, un interviewé rapporte ainsi qu'une mauvaise compréhension des limites du transfert de responsabilité lui a coûté 300 000 €.

B.6.11.3 L'application du transfert de responsabilité : la vigilance est de mise !

Comme le rappelle Pecheur.com, le transfert de responsabilité est devenu obligatoire à partir du 1er octobre 2008. Mais, en pratique, l'application du transfert de responsabilité est encore loin d'être automatique; la vigilance reste de mise pour les E-Marchands rencontrés !

Opérationnellement, c'est la responsabilité de la banque acquéreur du E-Marchand de contester la réfutation du transfert de responsabilité par la banque émettrice. Pour cela, il reviendra au E-Marchand d'apporter la preuve qu'une transaction a bien été authentifiée 3D Secure. Tant que la preuve n'est pas apportée, le montant de l'impayé reste débité du compte du E-Commerçant.

Pour Pecheur.com, le réflexe premier des banques en cas d'impayés est de s'adresser aux marchands sans avoir préalablement vérifié que la transaction a pu être authentifiée 3D Secure.

Voyages-sncf.com a pu constater que sur certains cas de refus litigieux, c'était la banque émettrice qui n'avait pas procédé à l'authentification 3D Secure. En conséquence, Voyages-sncf.com a décidé de refuser les transactions dont elle savait que la banque ne les authentifierait pas. Voyages-sncf.com précise qu'un nombre très limité de transactions rentre toutefois dans ce cas de figure.

Hormis la non éligibilité de la carte, la raison principale des litiges entre banques et E-Marchands semble être d'ordre technique. Ainsi, pour Atos Wordline, les banques acquéreurs ne sont pas encore toutes outillées pour systématiquement contester les refus de transfert de responsabilité des banques émettrices, ce que semble confirmer venteprivée.com.

Pour Venteprivée.com, "il n'y a pas qu'un 3D Secure, mais des 3D Secure, tant au niveau du parcours client que de l'application de la garantie de paiement". En fonction des banques acquéreurs, les règles sur la garantie de paiement ne sont pas les mêmes. Par exemple, la Société Générale indique dans ses flux d'autorisation du paiement que le paiement est garanti. Ainsi, tout impayé qui se produirait sur une transaction authentifiée est systématiquement rejeté. Tous les partenaires bancaires d'Atos Worldline peuvent faire ce retour d'information au marchand, à chaque transaction.

A priori, la Société Générale a fait en sorte que le rejet des impayés soit systématique dans le cas d'une authentification 3D Secure. La Société Générale aurait considéré que sinon, la gestion des impayés, en Back Office, aurait été impossible. La banque s'appuierait sur une matrice de cas

pour lesquels le transfert de responsabilité s'applique. Ce ne serait pas systématiquement le cas pour la BNP, la deuxième banque acquéreur de Vente Privée.

Pour ces raisons, la vigilance du E-Marchand doit être de mise selon Mistergooddeal.com qui résume ainsi le sentiment largement partagé par les E-Commerçants rencontrés : *"le transfert de responsabilité, dans certains cas, il faut aller le chercher !"* Fort heureusement, le nombre de transactions «en litige» reste finalement faible. Pour Delamaison.fr, elles n'ont représentée que quelques transactions en 2012.

B.6.11.4 Une uniformisation très (trop?) tardive des moyens d'authentification

Pour CB, la tendance générale est à l'uniformisation des moyens d'authentification.

Mais cela n'a pas été le cas pendant très longtemps ce que déplorent unanimement les E-Marchands interviewés. L'hétérogénéité des solutions retenues par les banques pour authentifier leurs clients explique en partie, pour nombre d'entre eux, la relative lenteur du déploiement de 3D Secure en France.

Dans son rapport 2009, l'OSCP recensait au moins six dispositifs différents !

- **la carte matricielle avec chemin secret** (Crédit Mutuel, CIC): le code unique à partir de la saisie de code obtenu sur la carte selon un chemin connu seulement de l'utilisateur ;
- **le "Token"** : le code à usage unique est généré par un algorithme placé dans un petit appareil électronique à la suite d'une pression sur un bouton ;
- le code usage unique reçu par SMS ;
- **le mini lecteur de carte à puce (Banque Populaire)** : le code à usage unique s'affiche sur les heures de la carte bancaire du porteur et saisie de son code PIN ;
- **la clé USB** avec certificat électronique que l'internaute doit connecter à son ordinateur lors du paiement avant entrée du code PIN de la clé, nécessaire à l'authentification.
- Code à usage unique obtenu **par serveur vocal** (Groupama Banque).

Source : Rapport annuel OSCP 2009

Le rapport de l'OSCP publié en 2011 précise toutefois qu'en dépit de la coexistence de plusieurs solutions d'authentification notamment permettant de répondre aux attentes spécifiques par catégorie de porteurs, la majeure partie des paiements 3D-Secure est authentifiée au moyen du SMS OTP.

Pour Rueducommerce.com, CB a manqué l'occasion de généraliser 3D Secure en ne parvenant pas à imposer une solution unique.

CB rappelle qu'à l'origine, en 2008, le système d'authentification était statique (date de naissance ou mot de passe). Selon CB, ce système aurait été rapidement contourné. Les banques ont alors choisi d'expérimenter différentes solutions. Elles ont également cherché à uniformiser les modalités d'authentification pour l'accès aux comptes à distance et pour l'authentification 3D Secure.

Certains E-Marchand interviewés continuent à s'interroger sur le choix d'un mode d'authentification non rejouable. Pecheur.com dresse un parallèle avec le code nécessaire pour les retraits aux distributeurs. Ce code est statique. Il en va de la responsabilité du porteur de le conserver secret. Pourquoi devrait-il en aller autrement pour les cartes bancaires pour lesquelles le code d'authentification est dynamique ?

La FEVAD a toujours soutenu que le déploiement d'une solution d'authentification pour les moyens de paiement à distance aurait été plus rapide si les banques avaient opté pour une solution unique reposant sur un code personnel.

Pour la Fédération Bancaire Française, il est normal que les banques aient opté pour des méthodes d'authentification différentes. Elles ne pouvaient pas encourir le risque qu'un unique moyen d'authentification ait pu être corrompu.

La Fédération Bancaire Française rappelle aussi qu'à l'époque du lancement de 3D Secure, l'usage du téléphone mobile était moins répondu. Les banques ont aussi l'obligation de répondre aux besoins de consommateurs qui n'utilisent pas le portable ou qui se déplacent à l'étranger.

Pour Rueducommerce.com, ce sont aussi les exigences nouvelles (à l'époque) de libre concurrence entre les banques qui ont rendu impossible l'imposition d'une solution unique comme cela avait été le cas avec la suppression du "fer à repasser" et son remplacement par la saisie du code confidentiel.

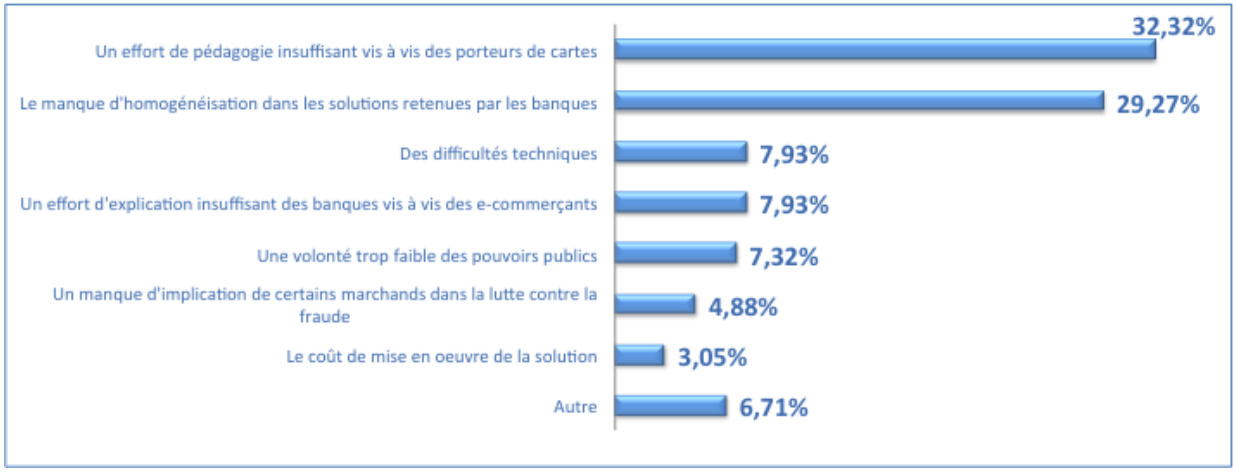
Dès lors, les E-Marchands ont été confrontés à un système non homogène et dont la fiabilité technique variait d'une banque à l'autre !

La Fédération Bancaire Française note qu'avec le développement de l'usage du portable, les réticences liées à l'usage du SMS sont en passe d'être levées. La Fédération Bancaire Française constate que désormais le SMS est le moyen le plus courant pour l'authentification.

Pour CB, l'uniformisation des moyens d'authentification (à priori le SMS) sera rendue inévitable du fait des coûts de déploiement des solutions qui nécessitent l'équipement en masse des clients (clés, boitiers...).

B.6.12 Freins au déploiement de 3D Secure : réponses au questionnaire

Pour un tiers des répondants au questionnaire, l'effort de pédagogie jugé insuffisant des banques et le manque d'homogénéité des solutions d'authentification sont les deux principaux freins au développement de 3D Secure en France.



Source: *sondage auprès des adhérents FEVAD Mai Juin 2013*

B.6.13 Un outil inadapté au M-Commerce

Le constat est quasi unanime parmi les commerçants interviewés sur l'incompatibilité de 3D Secure avec le M Commerce. Pour être tout à fait précis, Vente-privee.com fait la distinction entre les transactions passées à partir d'un Brower web sur une tablette pour lesquelles l'authentification 3D Secure est théoriquement possible (même si l'ergonomie n'est pas optimisée) et les transactions réalisées à partir d'applications (iOS ou Androïd) qui, elles, ne sont pas possibles. En effet, les applications doivent être capables de conserver le contexte quand l'utilisateur bascule sur le mode de réception du SMS.

Or, même si l'ampleur de la progression des ventes sur mobile ou tablette est encore inégale d'un marchand à l'autre, tous s'accordent pour considérer que le M commerce représentera une part très importante des ventes dans un avenir proche. Que 3D Secure ne soit pas adapté au M-Commerce est donc ressenti par les interviewés comme une limite majeure à 3D Secure.

Autre difficulté signalée par Vente-privée.com, les écrans de saisie du code d'authentification ne sont toujours pas optimisés pour le mobile. Pourtant, l'optimisation de ces pages, en fonction du terminal, n'est pas d'une grande complexité technique, ce qu'Atos Wordline confirme. En tant que principal fournisseur des banques en solution d'ACS, Atos Wordline a déjà adressé des propositions d'évolutions techniques aux banques émettrices visant à adapter la page de confirmation aux caractéristiques des mobiles. La décision est entre leurs mains. Certains E-Marchands considèrent comme anormal d'avoir à supporter les coûts de la fraude sur les transactions réalisées sur le mobile à défaut de ne pas encore disposer d'outils adaptés. Un acteur comme Voyages-sncf.com a ainsi pu constater un report préoccupant de la fraude du Web vers le mobile fort heureusement contenue aujourd'hui grâce aux outils de détection du risque mis en place. Or, pour ces E-Marchands, il revient bien au système bancaire de sécuriser les moyens de paiement qu'il propose quel que soit le canal de vente utilisé !

Les E-Marchands fondent de grands espoirs sur les portefeuilles électroniques qui seront lancées prochainement.

B.6.14 Autres limites de 3D Secure vues par les E-Marchands

B.6.14.1 La durée de garantie 3D Secure est contrainte par la durée de garantie de l'autorisation

Atos Wordline rappelle qu'en théorie, la durée de garantie de l'authentification 3D Secure est de 30 jours pour les cartes VISA et de 90 jours pour les cartes MasterCard. Mais, dans les faits, la durée de garantie de l'authentification est contrainte par la durée de garantie de l'autorisation.

La durée de validité d'une demande d'autorisation est généralement de six jours. Or, il ne peut pas y avoir une même demande d'autorisation avec les mêmes identifiants d'authentification. Ainsi, le seul moyen pour le E-Marchand d'allonger la durée de garantie de l'authentification est de négocier l'augmentation du délai de garantie d'autorisation auprès de sa banque acquéreur, ce qui augmente mécaniquement le risque d'acceptation et peut se traduire par une augmentation du taux des commissions perçues par la banque.

Pour Laredoute.com, ces contraintes sont difficilement compatibles avec le principe de débit à l'expédition (recommandé par la FEVAD) notamment pour les cas de commandes livrées tardivement du fait des délais de reassort, les cas des produits avec un fort encombrement, les cas de livraisons retardées à la demande du client. Ainsi, Laredoute.com considère qu'un délai de garantie d'une vingtaine de jours serait optimum.

B.6.14.2 Paiement fractionné : le transfert de responsabilité est limité au premier versement

Selon les règles édictées par Visa et MasterCard, dans le cas d'un paiement échelonné, seul le premier versement est couvert par le transfert de responsabilité dans le cas d'une authentification réussie. Nombreux sont les E-Commerçants à regretter cet état de fait. Ils comprennent difficilement qu'une transaction dont l'auteur a été identifié une première fois ne puisse pas bénéficier du transfert de responsabilité sur l'ensemble des versements. Certains ont même indiqué que cette limite pouvait constituer une faille qui pouvait être exploitée par des fraudeurs.

B.6.14.3 La mise en place de 3D Secure ne dispense pas de maintenir les dispositifs anti-fraude existants

La mise en place de 3D Secure n'aurait qu'un effet dissuasif limité sur les fraudeurs. Ainsi, la mise en place de 3D Secure en mode « systématique » n'a pas totalement dissuadé les fraudeurs chez Mistergooddeal.com qui constate une quinzaine de tentatives par jour.

Pour les banques, la mise en œuvre de 3D Secure ne peut et ne doit pas s'accompagner d'un allègement du dispositif anti-fraude que le E-Marchand aurait mis en place antérieurement. C'est en substance le message très clair qu'a adressé la banque Acquéreur de Mistergooddeal.com lorsque que ce dernier a mis en œuvre 3D Secure de manière systématique : "la mise en place de 3D Secure ne vous empêche pas de contrôler la fraude"....

B.6.14.4 Comme tout système de sécurité, 3D Secure est faillible

Pour CB, la quasi-totalité des fraudes 3D Secure est liée à l'authentification rejouable (élément d'identification statique capturé par le fraudeur au même titre que le N° de carte, cryptogramme…).

CB cite néanmoins deux exemples de contournements « technologiques » de 3D Secure :

Le "rejeu" consiste pour le fraudeur à capter le certificat d'une transaction valide et à l'insérer dans le flux d'une transaction fraudée. Normalement, il revient au E-Commerçant de vérifier que la réponse à la demande d'authentification intègre bien les informations qui ont été fournies dans la demande. Le "rejeu" lorsqu'il se produit peut donc être considéré comme un défaut d'implémentation de 3D Secure imputable au E-Marchand ou à son prestataire. Néanmoins, c'est la banque émettrice qui porte le préjudice.

Autre possibilité, la redirection du SMS dans le cas où le fraudeur arrive, d'une part à capturer tous les éléments liés à la carte, et d'autre part à prendre la main sur la box ADSL du client pour paramétrer le reroutage des SMS. Mais, dans ce cas, on ne peut pas à proprement parler d'une faille de 3D Secure.

En janvier 2013, Mistergooddeal.com a constaté une autre faille dans le procédé d'authentification 3D Secure. Le montant de la transaction à authentifier ne correspondait pas au montant de la transaction que le banquier authentifiait. Ainsi la banque émettrice authentifiait une transaction pour un montant bien inférieur au montant réel de la transaction.

Pour CB et Mistergooddeal.com, les cas de faille de 3D Secure restent fort heureusement extrêmement marginaux, mais révèlent à la fois l'ingéniosité des fraudeurs mais aussi les failles de 3D Secure selon la façon dont il est mis en oeuvre.

B.6.14.5 Le code d'authentification peut être visible même avec un clavier bloqué

Sur la plupart des téléphones, même avec le clavier verrouillé, les messages SMS (tout au moins les premières lignes) sont visibles. En cas de vol de la carte bancaire et du téléphone mobile, le fraudeur dispose alors de tous les éléments requis pour authentifier une transaction 3D Secure. C'est pourquoi, généralement, les ACS prennent garde d'éviter de faire figurer le code d'authentification sur les premières lignes du SMS.

Il serait néanmoins utile de rappeler aux utilisateurs que certains téléphones permettent de paramétrer l'affichage des SMS réceptionnés.

B.6.14.6 Autres limites

Chez Laredoute.com, 33% des cartes de paiement utilisées par les clients du site ne sont pas éligibles à 3D Secure, 3D Secure ne pouvant s'appliquer aux cartes privatives. C'est une difficulté supplémentaire rencontrée par les équipes fraudes pour convaincre en interne de la pertinence de 3D Secure.

B.6.15 Bénéfices ou motivations des E-Marchands pour 3D Secure

B.6.15.1 Réduction de la fraude

Parmi les E-Marchands interviewés, aucun ne remet en cause l'impact positif de 3D Secure sur la fraude. Dans certains cas les résultats sont même très spectaculaires; division de la fraude par 10 en quelques jours chez Mistergooddeal.com, réduction d'1/3 chez voyages-sncf.com.

B.6.15.2 Réduire le risque pour le marchand des fausses répudiations.

Un client s'étant authentifié par 3D Secure sera moins enclin à répudier par la suite une transaction.

B.6.15.3 L'amélioration de la satisfaction client

Pour les E-Commerçants, 3D Secure présente une alternative intéressante aux demandes de pièces justificatives dans le cas de transactions jugées à risque. Très souvent, ces demandes sont très mal ressenties par les clients qui les trouvent, à juste titre, intrusives. Pour des clients connus et récurrents, demander des pièces justificatives présente un gros risque de porter un coup irrémédiable à une relation commerciale patiemment établie.

Priceminister.com constate que la moitié des clients auxquels il a été demandé des justificatifs ne revient plus acheter sur le site ! Or, bien souvent, il s'agit de bons clients réguliers du site !

Mistergooddeal.com ou Cdiscount.com (retours positifs des clients sur le forum www.lafourmiliere.fr, le site de la communauté des clients de Cdiscount.com) confirment que la mise en place de 3D Secure dans ce cadre a eu un impact favorable sur la satisfaction client.

L'amélioration du délai de facturation est aussi un facteur qui a joué dans l'augmentation de la satisfaction client. A présent, notamment grâce à 3D Secure, Mistergooddeal.com est capable de facturer 80 % de ses clients dans les 12 heures suivant leur commande, contre 80 % des commandes facturées dans les 24 heures avant la mise en place de 3D Secure.

B.6.15.4 L'amélioration du taux de facturation

Aussi appelé "taux d'acceptation", le taux de facturation est le rapport entre le chiffre d'affaires enregistré et le chiffre d'affaires réellement "facturable" au Client, déduction faite notamment des transactions jugées frauduleuses.

Ce taux traduit d'une certaine manière la part de risque que le E-Commerçant entend prendre sur les transactions qu'il accepte. Pour le E-Marchand, l'une des façons de réduire le risque est de demander des pièces justificatives ce qui, nous l'avons vu, n'est ni performant, ni très efficace.

Ainsi, Priceminister.com estime qu'une grande partie des commandes que le site doit annuler correspond en fait à des commandes non frauduleuses mais pour lesquelles le risque de fraude n'a pas pu être levé faute d'obtenir les justificatifs du client.

Ainsi, pour Priceminister.com la principale motivation pour mettre en place 3D Secure n'est pas, comme on pourrait s'y attendre, la réduction des impayés mais bien l'amélioration du taux de facturation.

3D Secure est donc considéré comme une façon simple et efficace de réduire la part de risque pris par le E-Marchand et d'abaisser en conséquence le seuil des autres critères de risques qu'il utilise. Avec la mise en place de 3D Secure, Mistergooddeal.com estime que son taux de facturation a gagné 4%, particulièrement sur des commandes à forte valeur.

B.6.15.5 Réduction des coûts de lutte contre la fraude et gains de productivité

Chez Mistergoodeal.com, la mise en place de 3D Secure s'est traduite par une réduction des coûts humains et financiers du dispositif anti-fraude. Parmi les coûts financiers qui ont pu être réduits, figure notamment le recours aux prestations extérieures pour analyser le risque de

fraude sur les transactions, coût qui est proportionnel au nombre de transactions à analyser et qui, avec la mise en place de 3D Secure, a été réduit.

Pour Mistergooddeal.com, l'un des facteurs clés de succès de 3D Secure a été la capacité du service anti-fraude de démontrer la rentabilité économique de mise en place de l'outil, notamment en mettant en avant la réduction des coûts qui en résultait. Ainsi, la perte de 2 % du chiffre d'affaires était largement compensée par la réduction des coûts :

- réduction de la masse salariale (avec la mise en place de 3D Secure, le nombre de personnes travaillant au service fraude est passé de trois à une),
- réduction du nombre de transactions à faire analyser en recourant aux services de prestataires extérieurs.

Il est cependant intéressant de noter que le bénéfice de réduction des coûts de lutte contre la fraude est perçu différemment par les E-Commerçants interviewés.

Ainsi, pour rueducommerce.com, le gain potentiel de productivité du service fraude n'est pas apparu comme un critère de décision sur la mise en place de 3D Secure. Compte tenu des enjeux financiers (moins de 0,1% du CA), le gain de productivité sur la fraude n'est pas prioritaire.

L'argument des gains de productivité potentiels n'est pas non plus mis en avant par les Banques qui tiennent à ce que 3D Secure s'ajoute aux dispositifs déjà en place.

B.6.15.6 Amélioration du taux d'acceptation des autorisations

Chez Mistergooddeal.com, le débit a lieu à l'expédition. L'authentification 3D Secure est déclenchée à la commande. Suite à la réception de la réponse d'authentification, une pré-autorisation est déclenchée. L'autorisation proprement dite n'est demandée qu'au moment de la livraison (en général dans les 24 heures suivant la commande).

Mistergooddeal.com confirme que, suite à la mise en place de 3D Secure, il a constaté une forte diminution du nombre de refus d'autorisation.

Avant la mise en place de 3D Secure, Mistergooddeal.com rejouait certaines demandes d'autorisation (parfois des autorisations à un euro) pour maintenir des taux de commission bancaire bas (répercussion par la banque acquéreur des frais liés au TBTB[17]).

La mise en place de 3D Secure permet également à Mistergooddeal.com de limiter les refus provoqués par des dépassements de plafond, et en particulier pour les commandes avec des montants élevés (3000€), pour lesquels Mistergooddeal.com demandait une pré autorisation suivie d'une autorisation. CB confirme que les transactions ayant fait l'objet d'une authentification positive ont un taux d'autorisation 4 % supérieur à celles qui n'ont pas été authentifiées, alors même que ces transactions présentent en général un risque de fraude supérieur aux autres.

B.6.15.7 Baisse des commissions bancaires

Pour Mistergooddeal.com, la mise en place de 3D Secure s'est traduite par une baisse significative du taux de commission exigé par sa Banque Acquéreur (répercussion par la banque acquéreur des frais liés au TBTB).

---

[17] le TICO (Taux Interbancaire des Cartes en Opposition), qui reflète le taux de fraude entre deux banques a été rebaptisé TBTB (Taux Bilatéral de Transactions Bloquées) pour mieux affirmer son caractère bilatéral et s'adapter au vocabulaire de la Directive des Services de Paiement. Source GIE Cartes Bancaires

B.6.15.8 Grâce à 3D Secure, des contrôles plus qualitatifs

Comme vu précédemment, la mise en place de 3D Secure s'est traduite par des gains de productivité des équipes anti-fraude. Chez Mistergooddeal.com, la mise en place de 3D Secure, le nombre de transactions à vérifier a très fortement diminué. Dès lors, les contrôles sont devenus plus qualitatifs « Ayant moins de transactions à analyser, on a pu se concentrer davantage sur les failles éventuelles de notre dispositif ».

B.6.16 Risque d'image à ne pas mettre en place 3D Secure

B.6.16.1 Risque de déport de la fraude sur les sites qui n'auront pas mis en place 3D Secure

Nul doute que l'absence de dispositif d'authentification forte sur un site constituera un élément d'attractivité pour les fraudeurs. Pour certains interviewés, "ne pas mettre en place 3D Secure, reviendra à agiter le chiffon rouge"....

B.6.16.2 Risques d'image

Pour certains E-Marchands rencontrés, la principale motivation pour mettre en place 3D Secure n'est pas la réduction du taux de fraude : "même s'il peut être toujours amélioré, notre taux de fraude reste faible et nous le maîtrisons". Même s'ils rechignent à l'exprimer aussi clairement, on comprend que la décision de mettre en place 3D Secure pour certains E-Marchand est bien le résultat de la pression combinée de la Banque de France (qu'il est toujours préférable d'avoir à ses côtés) et des médias. Ces E-Marchands sont parfaitement conscients des risques qu'ils prendraient à être désignés (même à tort) par la vindicte populaire comme les responsables de l'augmentation de la fraude parce qu'ils n'auraient pas mis en place « la » solution censée résoudre le problème...

B.6.17 Synthèse des freins, limites et bénéfices perçus de 3D Secure

Le tableau ci-après reprend la perception des E-Marchands interviewés sur les freins, les limites, et les bénéfices de la solution 3D Secure.

Freins à l'adoption de 3D Secure	**Bénéfices perçus à la mise en place de 3D Secure**
• Niveau actuel du taux d'échec d'authentification • Une information des clients jugée encore très nettement insuffisante • La non éligibilité au transfert de responsabilité de certaines cartes étrangères • La gestion opérationnelle du transfert de responsabilité • Une uniformisation très (trop) tardive des moyens d'authentification	• Réduction de la fraude • Amélioration de la satisfaction client • Amélioration du taux de facturation • Réduction des coûts de lutte contre la fraude et gains de productivité • Amélioration du taux d'acceptation des autorisations • Baisse des commissions bancaires • Des contrôles plus qualitatifs
Limites de la solution	Risques à ne pas mettre en place 3D Secure
• Inadaptation de 3D Secure au M-Commerce • Durée de garantie de 3D Secure contrainte par la durée de garantie de l'autorisation • Paiements fractionnés: transfert de responsabilité limitée au premier versement • Effet dissuasif limité sur les fraudeurs • Pas d'allégement des dispositifs anti fraude existant grâce à 3D Secure • Faillibilité de 3D Secure	• Risque de déport de la fraude sur les sites qui n'auront pas mis en place 3D Secure • Risques de détérioration de l'image

B.6.18 Bonnes pratiques de mise en œuvre de 3D Secure

B.6.18.1 Avant le déploiement

Un soutien indéfectible de la Direction Générale...

Comme évoqué dans un chapitre précédent, la fraude est un sujet transverse à l'entreprise qui nécessite des arbitrages fréquents, notamment entre les Directions des Ventes et du Marketing (qui ont intérêt à développer le chiffre d'affaires) et la Direction Financière qui est garante du résultat, déduction faite des fraudes.

Pour Mistergooddeal.com, l'un des facteurs clé de succès dans le déploiement de 3D Secure a été le support très fort de la Direction Générale qui a été à l'origine du projet.

Beaucoup de pédagogie auprès du marketing, une étude économique poussée

Chez Mistergooddeal.com, l'équipe fraude a dû démontrer aux équipes marketing que l'impact de 3D Secure était faible voire neutre en termes de chiffre d'affaires et, qu'en revanche, l'impact financier était très positif.

Pour mener cette étude, le service fraude a dû s'appuyer sur une analyse informatique détaillée des données extraites du dataware.

Un des points clés de la démonstration a été d'aller au-delà du taux d'abandon brut tel qu'il est donné par l'OSCP qui, pour une Direction des Ventes ou du Marketing, peut effectivement apparaitre comme rédhibitoire. L'équipe anti-fraude de Mistergooddeal.com s'est donc évertuée à calculer un taux d'abandon net.

Or, ce calcul est particulièrement laborieux puisqu'il nécessite une étude "ligne à ligne" des logs de commandes des clients. Et, malheureusement, aucun outil ne permet d'automatiser ce calcul.

Pour Mistergooddeal.com, avec la mise en place de 3D Secure, ce sont tous les indicateurs marketing (taux de rebond, taux de transformation) qui doivent être réinterprétés. Sans un minimum de pédagogie, ces chiffres ont effectivement de quoi effrayer les équipes marketing !

B.6.18.2 Pendant le déploiement

Une très bonne coordination à établir entre le E-Marchand, le PSP et les banques acquéreurs

Le retour d'expérience de Vente-privee.com repris plus haut dans le document tend à montrer qu'un projet de déploiement de 3D Secure en mode sélectif peut être complexe.

Pour venteprivée.com, "la mise en œuvre de 3D Secure sur un mode sélectif - au moins pour un E-Marchand de taille important - est "un vrai projet" dont il faut mesurer tous les impacts. Dans la phase de déploiement, il nécessite une coordination étroite entre le E-Marchand, sa ou ses banques acquéreurs et le PSP".

Qualité de l'accompagnement Client et robustesse des mécanismes de récupération du client

Un autre élément déterminant dans le succès de la mise en œuvre de 3D Secure chez mistergooddeal.com a été l'attention portée à l'ensemble des procédures permettant de "récupérer" le client en cas d'échec de l'authentification (call back) ainsi que l'information fournie aux clients.

Chez CDiscount.com, en cas d'échec de paiement, la récupération de la transaction est systématique. La politique de l'enseigne est de présumer de la bonne foi du client. En cas

d'échec de paiement par carte bancaire, jusqu'à 6 autres moyens de paiement sont proposés au client.

Compte tenu de l'hétérogénéité qui persiste encore sur les solutions d'authentification mises en place par les banques émettrices, il en va de l'intérêt de l'E-Marchand de prévoir un accompagnement suffisant du client (explication des parcours client d'authentification en fonction des banques, briefing des chargés de clientèle...). Comme évoqué précédemment, les méthodes d'authentification mises en place par les banques évoluant, cela nécessite que le E-Marchand fasse évoluer régulièrement son dispositif d'accompagnement.

B.6.18.3 Lors de l'exploitation

Détection des cartes non éligibles au transfert de responsabilité

Pour un E-Commerçant, la détection des cartes non éligibles au transfert de responsabilité n'est pas simple (cf. « Limites de 3D Secure »). Le E-Commerçant aura tout intérêt à s'appuyer sur l'expertise de son PSP.

Attention au report de la fraude sur les autres moyens de paiement !

Quasiment tous les marchands interviewés ont constaté un report de la fraude sur les autres moyens de paiement mis à la disposition des clients lorsqu'ils ont mis en œuvre 3D Secure.

Par exemple, chez Delamaison.fr, le report de la fraude s'est fait suivant deux directions :

- vers des moyens de paiements pour lesquels les transactions ne peuvent faire l'objet d'une authentification 3D Secure (PayPal notamment) ;
- vers les chèques. En 2012, Delamaison a constaté une recrudescence des impayés sur les encaissements par chèque pendant quelques semaines.

B.6.19 3D Secure, un outil déjà daté ?

Rueducommerce.com traduit l'avis général des interviewés en considérant que l'insistance à promouvoir 3D Secure est finalement un "combat d'arrière-garde". Pour Rueducommerce.com, 3D Secure aurait été parfaitement adapté à la situation, il y a sept ou huit ans... La solution ultime ne peut pas être 3D Secure du simple fait de son incompatibilité avec la cinématique d'achat du M-commerce.

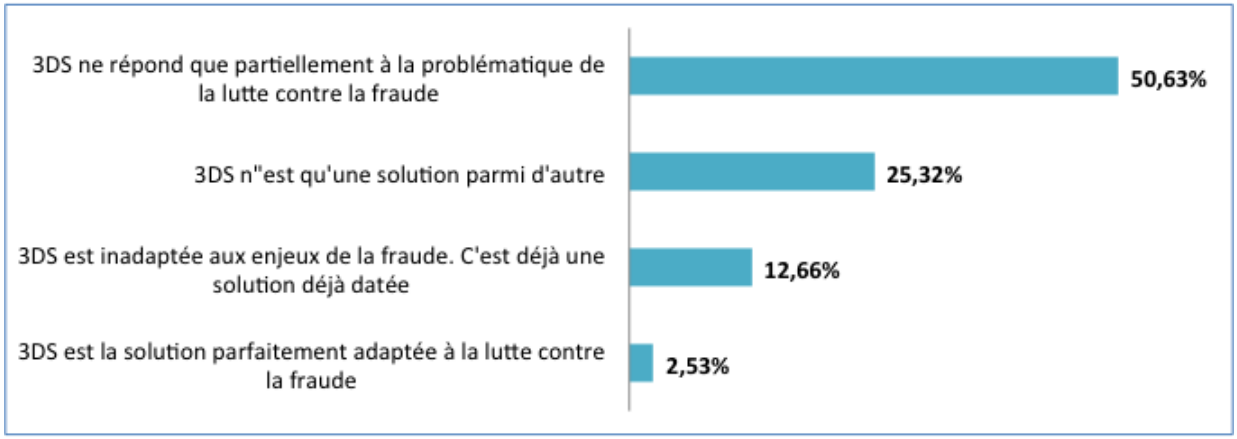
La perception de CB sur l'avenir de 3D Secure est évidemment plus nuancée. Selon CB, l'authentification forte va devenir la norme mais sur un nombre limité de transactions. 3D Secure n'est qu'un protocole technique permettant de mettre en œuvre une authentification du client par sa banque, et son ergonomie pourra être considérablement améliorée dans le cadre des nouvelles solutions de paiement, en particulier les portefeuilles (wallets) qui seront prochainement proposés par les banques.

Le nombre de commerçants qui adopteront 3D Secure va augmenter, mais la proportion de transactions 3D Secure déclenchées par ces commerçants pourra être faible puisqu'elle ne concernera que les transactions que le E-Marchands aura identifiées comme risquées.

Plus prosaïquement, concernant le M-Commerce, CB anticipe que Visa et MasterCard chercheront à privilégier à moyen terme leur offre de portefeuille électronique dont les enjeux financiers sont pour eux sans commune mesure avec la solution 3D Secure.

B.6.20 Appréciation globale des répondants au questionnaire sur 3D Secure

Pour la majorité des répondants au questionnaire FEVAD, 3D Secure n'apporte qu'une réponse partielle à la problématique de la lutte contre la fraude. Seuls 2,5% des répondants peuvent être considérés comme des inconditionnels de la solution 3D Secure. A l'autre extrémité, 13 % des répondants considèrent cette solution comme inadaptée aux enjeux de la fraude.



Source : *sondage auprès des adhérents FEVAD Mai Juin 2013*

B.7 PERCEPTION DES E-MARCHANDS SUR LA COOPERATION ENTRE LES PARTIES PRENANTES DE LA LUTTE ANTI-FRAUDE

B.7.1 Perception de la coopération avec la Banque de France et CB

Dans leur ensemble, les E-Marchands interviewés saluent le travail effectué par la Banque de France dans le cadre de l'Observatoire de la Sécurité des Cartes de Paiement, et proposent même des thèmes de réflexion à engager (Cf. Partie "Recommandations et pistes de travail" de ce document).

Au cours des derniers mois, la Banque de France et CB ont rencontré un certain nombre de E-Marchands (dont certains E-Commerçants interviewés dans ce Livre Blanc) pour évoquer avec eux les raisons de la hausse de la fraude sur les moyens de paiement.

Dans leur ensemble, les E-Marchands convoqués ont compris et ressenti positivement cette démarche.

Pour Rueducommerce.com par exemple, la mission de la Banque de France étant de maintenir la confiance des utilisateurs dans les moyens de paiement, elle est parfaitement dans son rôle quand elle cherche à pousser une solution qui limite la fraude.

Rueducommerce.com considère comme très utile le renforcement des échanges avec CB et la Banque de France. En tant que "gros remettant" de transactions par cartes bancaires, il apparait à Rueducommerce.com comme normal qu'un organisme de contrôle veuille faire un point avec lui et attire son attention sur les moyens de sécurisation des paiements comme 3D Secure. Car, pour Rueducommerce.com, l'intention de la réunion était clair : inciter les E-Marchands à mettre en place 3D Secure.

Pour Groupe 3 Suisses néanmoins, "l'attention ne devrait pas porter uniquement sur les sites E-Marchands qui maîtrisent leur fraude mais plutôt sur les quelques sites qui enregistrent des taux de fraude bien au-delà de la moyenne, jusqu'à 2 ou 3 % pour certains. La recommandation à ces sites pourrait être de mettre en œuvre un minimum de filtres sur leurs pages de paiement et éventuellement d'utiliser 3D Secure en mode systématique".

Lors de ces entretiens, les E-Marchands ont clairement perçu la volonté de la Banque de France de pousser la solution 3D Secure.

Pour Rueducommerce.com, la Banque de France reste néanmoins dans une attitude "ouverte". Elle cherche à comprendre pourquoi les E-Marchands sont si réticents à utiliser 3D Secure et cherche réellement à en comprendre ses limites. Pour Rueducommerce.com, la Banque de France ne cherche pas à imposer le 3D Secure de façon systématique et reste favorable à une mise en place de 3D Secure sur un mode débrayable.

Il demeure néanmoins un point sur lequel l'attente des interviewés vis-à-vis de la Banque de France reste très forte (et encore insatisfaite), c'est celui de la réduction du taux d'échec d'authentification 3D Secure.

Vente-privee.com résume ainsi la pensée de l'ensemble des participants au Livre Blanc: « il est difficilement compréhensible que la Banque de France puisse tolérer de telles différences entre les banques sur le taux d'échec d'authentification qu'elles rapportent. Il n'est pas admissible que

certaines banques affichaient encore récemment des taux de l'ordre de 6 % alors que d'autres avaient encore des taux de plus de 40 %. 3D Secure n'est pourtant plus une nouveauté ! »

Des échanges réguliers qu'entretiennent la FEVAD et la Banque de France, on comprend que le sujet est particulièrement suivi et que des résultats probants sont attendus. Donc acte !

B.7.2 Perception de la coopération avec les Banques

Les E-Marchands interviewés perçoivent clairement l'intérêt des Banques à lutter contre la fraude VAD. En revanche, certains d'entre-deux sont plus circonspects sur la méthode et les moyens que les banques mettent en œuvre pour y parvenir...

B.7.2.1 Perception des E-Marchands sur le rôle des banques dans la lutte contre la fraude

Rueducommerce.com rappelle qu'au-delà des enjeux primordiaux de maintien de la confiance des clients dans la sécurité des moyens de paiement, il ne faut pas perdre de vue que la fraude, pour les banques acquéreur, représente également un coût opérationnel important (coût administratif, coûts informatiques...) qu'elles cherchent à minimiser pour augmenter leur productivité et préserver leurs marges.

Ainsi, les banques sont dans la même logique de recherche de productivité que les E-Marchands. Elles cherchent à limiter le traitement des exceptions qui leur coûtent cher (traitement des appels clients notamment).

CB rappelle que la banque acquéreur n'a évidemment aucun intérêt à laisser filer la fraude. C'est d'abord la banque acquéreur qui se voit répercuter le coût de l'impayé et qui essaie ensuite de le répercuter au E-Marchand. Si ce dernier est défaillant, c'est la banque acquéreur qui supporte l'impayé.

La Fédération bancaire Française (FBF) confirme que les banques consacrent de lourds investissements à la lutte contre la fraude et à la sécurisation des moyens de paiement. Leurs motivations sont:

- la préservation de la confiance des porteurs dans leur banque : la carte doit rester le moyen préféré de paiement des consommateurs ;
- les coûts que représente le traitement de la fraude par les banques.

La FBF rappelle que la banque est le secteur d'activité qui investit le plus dans les nouvelles technologies de l'information et de la communication : 16% des dépenses informatiques dans le monde sont effectuées par les banques selon une étude de Gartner. Selon une autre étude menée par le cabinet Celent, les dépenses des banques européennes en TIC augmenteront de 0,3% en 2012 pour s'élever à 59,2 milliards de dollars. Pour 2013, les dépenses sont évaluées à 59,5 milliards de dollars.

B.7.2.2 Perception des E-Marchands sur la position des banques vis-à-vis du déploiement de 3D Secure et ses conditions de mise en œuvre

Lors des interviews, certains E-Marchands ont déclaré avoir parfois du mal à comprendre la stratégie opérationnelle suivie par les banques pour faire reculer la fraude. En la matière, l'exemple du déploiement de 3D Secure en France est, pour eux, assez significatif.

Pour Laredoute.com, l'hétérogénéité des solutions d'authentification et le manque d'effort d'information et de pédagogie auprès des porteurs sont deux éléments qui illustrent bien les carences du déploiement de 3D Secure par les banques.

Le Groupe 3 Suisses s'interroge sur l'intérêt, pour les banques, de favoriser le développement de 3D Secure ciblé sur les transactions les plus risquées. En effet, cela reviendrait pour elles à assumer le risque financier d'un éventuel impayé.

Des entretiens, il ressort également que les Banques n'exercent pas toutes la même pression sur les E-Marchands pour qu'ils adoptent 3D Secure. En revanche, elles ont globalement averti que si le taux de fraude venait à se dégrader alors elles répercuteraient le coût de fraude sur leur taux de commission.

En ce qui concerne les moyens mobilisés pour le déploiement de 3D Secure, la Fédération Bancaire Française, répond que l'investissement des banques sur le projet de mise en place de 3D Secure se chiffre en millions d'euros : "Des équipes entières ont été mobilisées pour la mise en œuvre de ce dispositif".

CB rappelle quant à lui que le coût du transfert de responsabilité pour les banques émettrices peut être évalué à 7 millions d'euros par an pour les transactions domestiques.

CB confirme en outre que l'envoi du SMS constitue un coût récurrent important pour les banques. Pour le limiter, les banques émettrices se sont dotées de solutions d'évaluation du risque. CB rappelle que la possibilité de ne pas envoyer de SMS a été prévue dès le début par les Access Control Server (ACS) comme un paramètre. Dans un premier temps, cette souplesse permettait de faire face à des difficultés techniques (disposer d'une solution alternative à l'envoi du SMS). Depuis, cette fonctionnalité est utilisée dans la gestion du risque et répond à la contrainte économique du coût des SMS.

Selon CB, le besoin des banques émettrices d'évaluer le risque de la transaction va s'accroître à l'avenir.

B.7.2.3 Un support des Banques aux E-Marchands en matière de lutte contre la fraude jugé pauvre voire inexistant

Lors des entretiens, plusieurs E-Marchands ont fait part d'attentes encore insatisfaites vis-à-vis de leur banque Acquéreur. Il semble nécessaire de rappeler ici en quoi consiste principalement le rôle d'une banque Acquéreur.

Un établissement acquéreur réceptionne des fonds pour le compte des E-Marchands. Le marchand reste le principal responsable vis-à-vis des réseaux interbancaires de la bonne gestion de sa fraude. L'établissement acquéreur assume, quant à lui, une responsabilité de l'accompagnement du E-Commerçants dans la gestion de cette problématique.

Le point de vue du juriste - La définition donnée par le Comité Français d'Organisation et de Normalisation Bancaires (CFONB) donne la définition suivante de l'acquéreur (*acquirer*) : « *entité qui tient les comptes de dépôt des accepteurs de cartes* [tout commerçant, tout prestataire de services et tout professionnel libéral] *et qui acquiert les données relatives aux transactions effectuées. L'acquéreur est responsable de la collecte des remises et du règlement des accepteurs* ». L'article préliminaire du contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS) dispose que l'acquéreur CB est tout établissement de crédit ou de paiement membre du GIE Cartes Bancaires, avec lequel l'accepteur CB a signé un contrat d'acceptation.

Parmi les prestations fournies par l'acquéreur figurent notamment la gestion de l'ensemble de la gamme des paiements possibles, paiements «simples», paiements «fractionnés», remboursements, annulations ainsi que la gestion du taux d'impayés des marchands.

Le principal reproche que formule une bonne majorité des E-Commerçants interviewés est la pauvreté voire, selon certains, carrément l'absence de support qu'ils disent recevoir de leur Banque dans leur lutte contre la fraude.

Ainsi, Delamaison.fr considère n'avoir reçu aucun support de sa banque dans la définition ou la mise en œuvre de son dispositif de détection des comportements à risque. "On a rencontré des experts de la monétique, certainement pas des experts du E-commerce ! La banque a cherché à nous imposer une solution sans nous apporter le moindre support."

Pour le Groupe 3 Suisses, "les banques pourraient mieux accompagner les marchands sur les techniques anti-fraude et communiquer davantage sur les particularités et les restrictions d'usage des cartes qu'elles émettent. Un accompagnement plus présent sur les aspects techniques et réglementaires de la part des banques serait apprécié par les E-Marchands.

Selon le constat de Vente-privée.com, la qualité de la communication des banques sur le sujet de la fraude est très variable d'une banque à l'autre. Vente-privee.com regrette l'absence de liens directs avec des structures dédiées à la lutte contre la fraude, dans les grands établissements bancaires.

Au-delà de la communication sur les bonnes pratiques en matière de fraude jugée insuffisante, c'est aussi la pauvreté du support apporté par les Banques aux E-Marchands qui est décrié.

Vente.privee.com regrette que les banques acquéreur ne proposent pas aux E-Marchands un "framework de reporting ou d'analyse de fraude" qui leur permettrait de mieux analyser les risques de fraude auxquels ils sont exposés. Les informations qui pourraient être utiles pour le E-Marchand sont par exemple la typologie des fraudes, la répartition des fraudes en fonction des montants d'achat, la nationalité des cartes émettrices. En somme, des informations permettant de dresser un « profil type de la transaction frauduleuse ». Pour Vente-privee.com, c'est le CB qui serait légitime pour définir de tels "frameworks".

Be2bill souligne que la seule récupération des informations de sa banque acquéreur constitue déjà, pour la plupart des E-Commerçant une vraie difficulté. En effet, selon Be2bill, les banques traditionnelles n'ont pas la culture de l'analyse de la donnée Web et, force est de constater, qu'elles n'ont pas non plus la réactivité adéquate qui est pourtant essentielle dans la lutte contre la fraude sur Internet. Be2bill résume ainsi ce constat : "le métier d'un banquier n'est pas d'analyser de la data".

Selon la Fédération Bancaire Française, les contraintes de marché ont focalisé les négociations commerciales entre le marchand et le banquier uniquement sur le prix (montant des commissions) sans tenir compte du niveau de service souhaitable ou attendu. Il est important qu'au moment de contractualiser, ce soit l'ensemble des prestations de service qui soit pris en compte par le commerçant, et pas seulement le taux facturé.

Le point de vue du juriste - Il est à noter que le cadre des négociations contractuel entre les E-Marchands et les banques va prochainement évoluer avec la publication annoncé du règlement annoncé relatif aux commissions d'interchange (CMI) pour les opérations par carte, qui prévoit un plafonnement entre 0,2 et 0,3 % des CMI, intégrées dans ce que l'on appelle les « commissions de service commerçant » (composées, outre la CMI, par la commission liée au système de paiement et au traitement du paiement et par la marge de l'acquéreur), versées à l'acquéreur par le commerçant accepteur pour chaque opération.

B.7.2.4 Inégalité dans l'accès à l'information en fonction de la taille du E-Marchand ?

Un point est mentionné par les E-Marchands de taille plus modeste : la difficulté d'accéder au fichier des plages BIN qui, pour rappel, permet notamment d'identifier le pays d'origine de la carte. Manifestement, l'accès à ce fichier que détiennent les banques Acquéreur est d'autant plus facile qu'on est un gros E-Marchand !

Dans le cadre de 3D Secure, on comprend que certaines banques émettrices puissent être réticentes à la transmission large du fichier BIN, puisque ce fichier permet à un marchand de corréler le taux d'échec d'authentification avec la banque émettrice.

Avec l'identité de la banque émettrice de la carte, il est possible d'appliquer une politique de gestion du risque différenciée par banque intégrant leur taux moyen d'échec d'authentification.

Vente-Privee.com fait partie des E-Marchand qui ne rencontrent pas de difficultés particulières pour obtenir ce fichier. Pour Vente-Privee.com, la réticence des banques acquéreurs à fournir le fichier BIN[18] est liée à la possibilité qu'auraient ainsi les E-Marchands de refuser certains types de cartes (ou les cartes émises par certaines banques dans certains pays) ce qui serait contraire aux règles d'acceptabilité définies par Visa et MasterCard.

B.7.3 Coopération entre CB et les E-Marchands

CB précise qu'il rencontre soit des acteurs dont le taux de fraude est très élevé soit des acteurs qui enregistrent des montants de fraude élevés compte tenu de leur chiffre d'affaires, même si leur taux de fraude est bas.

Pour le moment, les échanges qu'entretient CB avec les E-Marchands sont plutôt de nature « informative ». Il s'agit, pour CB, de comprendre la situation à laquelle le E-Marchand fait face. Selon CB, ces échanges sont également l'occasion de fournir aux E-Marchands des "bonnes pratiques" en matière de lutte contre la fraude.

Le délai pour qu'une fraude soit remontée dans les systèmes étant d'environ un 1,5 mois, CB constate que les E-Marchands ont très souvent réagi avant son intervention ou celle de banque Acquéreur. Dans ce cas, CB reconnait que son rôle se limite parfois à constater que le E-Marchand a bien pris les mesures correctives appropriées.

CB entend la demande des E-Marchands de disposer de certaines statistiques qu'il possède. Ce type de demande se heurte néanmoins à des contraintes juridiques ou statutaires fortes. Ainsi, CB ne peut envoyer les statistiques de fraude aux E-Marchands qu'à la demande de la banque acquéreur. De même, il apparaît difficilement possible à CB de fournir des statistiques à des organisations professionnelles telles que la FEVAD.

Enfin, CB tient à préciser qu'il ne lui revient pas d'imposer une solution particulière aux E-Marchands. Lors de ses rencontres avec les E-Marchands, CB promeut une approche sélective de 3D Secure en fonction notamment du montant des achats.

À noter encore la mise en place récente par le GIE Cartes Bancaires d'une procédure d'agrément pour les plateformes techniques du commerce électronique et de paiement sur internet.

[18] BIN : pour *Base Identification Number*, numéro d'identification unique et international de la carte

B.7.4 Perception de la coopération avec les prestataires techniques de solutions de paiement

Le PSP est responsable du "tuyau". C'est lui qui prend en charge la prestation technique, qui assure le flux entre la page de paiement et l'acquéreur. En collaboration avec le Marchand, le PSP a la capacité d'activer des filtres ou des méthodes d'évaluation du risque et ainsi de bloquer certaines transactions en "temps réel".

Le point de vue du juriste - Définition juridique des Prestataires de services de paiement (PSP)

Tels que définis par la directive 2007/64/CE du 13 novembre 2007 concernant les services de paiement (DSP), définition reprise à l'article L. 521-1 du Code monétaire et financier, les prestataires de services de paiement (PSP) sont essentiellement les traditionnels établissements de crédit (les banques) auxquels s'ajoutent les nouveaux établissements de monnaie électronique et les établissements de paiement. Ils ne doivent pas être confondus avec les prestataires (techniques) de solutions de paiement, non réglementés (au sens de réglementation bancaire et financière).

A la différence de la banque acquéreur, le PSP (dans l'acception faite de ce terme dans ce document et non dans la définition juridique ci-dessus) n'a pas d'accès aux données dites « bancaires » au sens d'un acquéreur et n'a aucune visibilité sur la sinistralité.

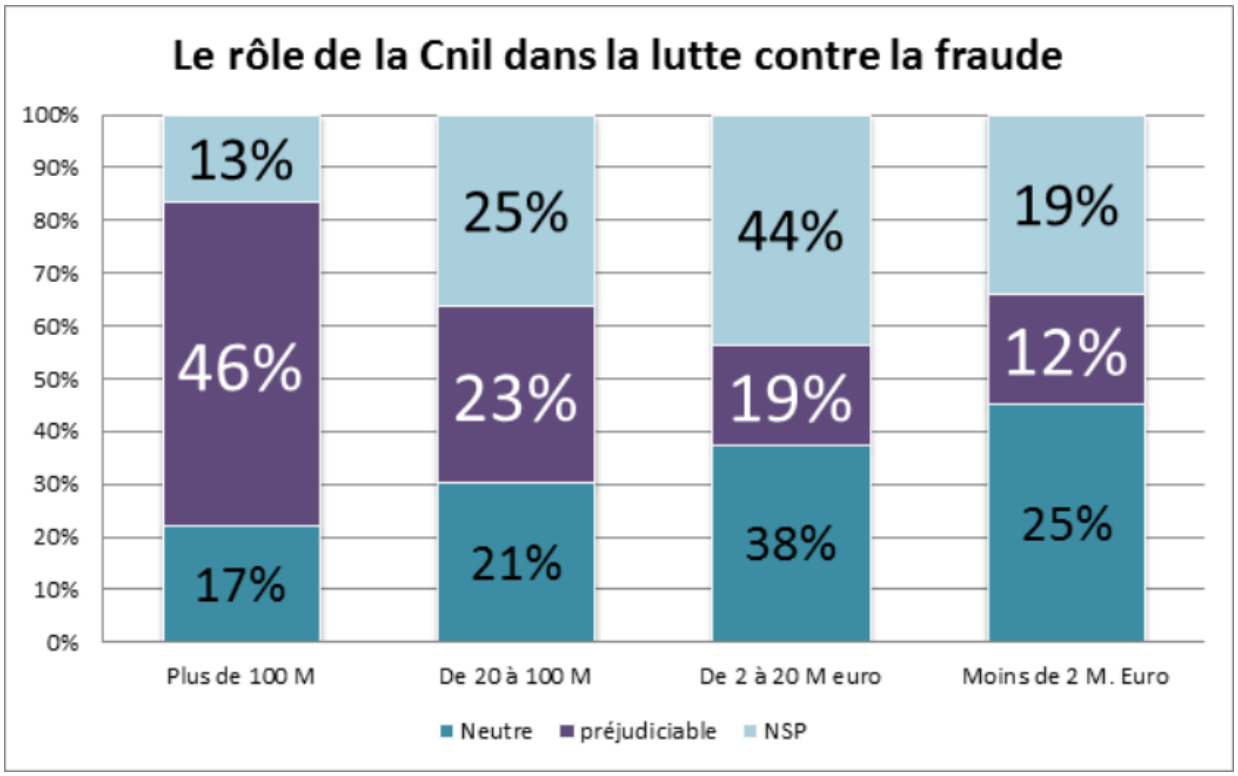
Lors des entretiens, les E-Marchands n'ont que très marginalement évoqué leur relation avec leur PSP. Il est vrai que les interviewés font majoritairement partie des sites les plus importants en France et qu'ils bénéficient vraisemblablement de relations particulières avec eux. Certains ont quand même exprimé leurs attentes, de la part de leur PSP, d'un peu plus de « transparence » sans véritablement préciser sur quel sujet en particulier. Un E-Commerçant a notamment déclaré travailler depuis des années avec le même prestataire mais continuer à découvrir certaines choses...".

B.7.5 Perception de la coopération avec la CNIL

Dans leur réponse au questionnaire quantitatif, plus d'1/3 des E-Marchands (majoritairement les plus gros) s'estime contraints par les exigences de la CNIL dans la lutte contre la fraude.

Question :

« Comment jugez-vous l'impact des exigences de la CNIL vis-à-vis de la protection des données personnelles dans le cadre de la lutte contre la fraude ? »



Source : *sondage auprès des adhérents FEVAD Mai-Juin 2013*

Les reproches sont de deux ordres :

- la doctrine : un corpus de règle qui manque de clarté et de prévisibilité laissant une part importante à l'interprétation ;
- le délai de la procédure de déclaration et d'autorisation jugé incompatible avec les exigences de lutte contre la fraude.

Le point de vue du juriste - La CNIL considère que l'utilisation du numéro de carte bancaire par un professionnel de la vente à distance, dans un fichier ayant pour finalité de lutter contre la fraude au paiement en conservant la trace d'agissements lui ayant porté préjudice, est légitime, sous la réserve que ce fichier ait fait l'objet d'une demande d'autorisation préalable et que cette utilisation du numéro de carte bancaire soit subordonnée à une information claire des personnes fichées ainsi qu'à la possibilité pour ces personnes de s'opposer, pour des motifs légitimes, à un tel traitement (Délibération n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance).

Dans une délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée (norme destinée à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux liberté) concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects, la CNIL reconnaît la finalité d'un traitement de gestion des impayés et du contentieux, à condition qu'elle ne porte pas sur des infractions et/ou qu'elle n'entraine pas une exclusion de la personne du bénéfice d'un droit, d'une prestation ou d'un contrat.

B.7.5.1 Des positions de la CNIL parfois difficilement comprises par les E-Marchands et parfois jugées contre-productives !

Un E-Marchand, quelque peu exaspéré par les délais d'instruction de son dossier, a déclaré : « à force de vouloir protéger les données personnelles, on peut se demander si finalement les exigences imposées par la CNIL ne profitent pas aux voleurs! ». Pour de nombreux interviewés, la dimension économique semble très peu présente dans les décisions prises par la CNIL.

Le Groupe 3 Suisses souhaite que chacun reste vigilant sur le risque de « mouvement contradictoire » entre la volonté légitime d'augmenter la sécurisation des paiements d'une part et d'autre part le souhait de renforcer la protection des données personnelles notamment en limitant leur conservation.

Mutualisation des données rendue nécessaire dans le cadre de la lutte contre la fraude

Les contraintes imposées par la CNIL sur la mutualisation des données fait partie des griefs récurrents des E-Commerçants vis-à-vis de la CNIL. Ils sont rejoints par les PSP.

Les E-Commerçants constatent la globalisation de la fraude et souhaiteraient disposer d'outils mutualisés leur permettant d'y répondre en disposant par exemple d'un système qui leur permettrait de partager l'information sur les tentatives de fraude réalisées sur une carte bancaire à partir de leur site.

Le Groupe 3 Suisse considère que la mutualisation des données entre les différentes filiales du groupe serait à même d'améliorer très sensiblement la performance des dispositifs anti- fraudes; idem pour l'intégration de contrôles sur les proxy ou sur les adresses IP.

Or, selon la CNIL, il est interdit de partager une information sur une transaction frauduleuse avec une autre enseigne. Ainsi, une carte bancaire à l'origine d'une fraude, ne peut, selon la CNIL, être interdite par d'autres enseignes d'un même groupe. En pratique, ce cloisonnement est

inapplicable opérationnellement puisque les équipes anti-fraude sont parfois mutualisées entre les enseignes d'un même groupe.

Même revendication du côté des PSP. En l'état actuel de la réglementation, la CNIL interdit même la mutualisation des données entre clients d'un même PSP.

Pour Be2Bill, "les règles imposées par la CNIL ne sont pas claires pour le moment". Si Be2bill est bien évidemment en accord avec les principes de protection des données personnelles, Be2bill se dit capable de certifier l'usage frauduleux d'une carte, à la suite d'une investigation adéquate.

Dans ce cas précis, il lui semble logique et judicieux de tout mettre en œuvre pour prévenir un usage frauduleux chez un autre marchand.

Pour Be2bill, le point clé sera d'être capable de rassurer la CNIL sur sa capacité à faire la différence entre des cas avérés de fraude et des litiges commerciaux, qui nécessitent effectivement le maintien de la protection des données.

Pour Be2bill, la mutualisation de l'information sur la fraude est une demande générale de l'ensemble de ses clients qui peut et doit aller de pair avec la confidentialité des données personnelles.

Dans certains pays européens, aux Pays-Bas, au Royaume-Uni, en Irlande par exemple, il est courant que les PSP alertent les banques émettrices de l'usage frauduleux d'une carte et évitent ainsi la réitération de fraudes.

Vente-privee.com constate qu'en Allemagne, pays dans lequel la protection des données personnelles est un sujet considéré avec la même importance qu'en France, l'approche de la lutte contre la fraude est beaucoup plus pragmatique : "En Allemagne, le scoring est considéré comme normal. Tout le monde est scoré ! C'est une réalité. Un acteur comme Arvato Infoscore étudie des millions de transactions par jour. Le système allemand fonctionne sur un mode déclaratif".

Le délai de conservation des données

L'un des points d'achoppement entre Rueducommerce.com et la CNIL a porté sur la durée de conservation des données.

Rueducommerce.com considérait comme indispensable de pouvoir garder pendant cinq ans la trace d'un impayé notamment dans le cas des achats fractionnés. Le délai prescrit par la CNIL était de deux ans seulement. Finalement, un accord a été trouvé sur un délai de trois ans.

Le point de vue du juriste - Dans sa délibération n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance, la CNIL n'indiquait aucune durée de conservation : « *La Commission considère en conséquence que la durée de conservation d'un numéro de carte bancaire ne saurait excéder le délai nécessaire à la réalisation de la transaction ou à la finalité de lutte contre la fraude au paiement du traitement mis en œuvre conformément aux lois et règlement en vigueur* ».

Aux termes de délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects, on lit : « *Les données relatives aux cartes bancaires doivent être supprimées une fois la transaction réalisée, c'est-à-dire dès son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour la durée prévue par l'article L 133-24 du code monétaire et financier, en l'occurrence 13 mois suivant la date de débit. Ce délai peut être étendu à 15 mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé. Ces données peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers par exemple). Ce consentement*

peut être recueilli par l'intermédiaire d'une case à cocher (non précochée par défaut), par exemple et ne peut résulter de l'acceptation de conditions générales. Les données relatives au cryptogramme visuel ne doivent pas être stockées. Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celles-ci doivent être supprimées ».

Sa délibération n° 2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société Fnac Direct est plus ambigüe, et ouvre la voie à une durée de conservation des données… presqu'indéterminée. Car si elle observe que la durée de conservation des données bancaires devrait être de 13 mois selon l'article L. 133-24 du CMF, elle ajoute que cette durée ne concerne que les porteurs de carte souhaitant obtenir remboursement auprès de leurs banques de toutes sommes contestées relatives à des opérations de paiement non autorisées. De sorte que cette disposition n'est pas applicable aux commerçants, puisqu'une banque saisie d'une contestation par son porteur cherchera à se retourner contre le commerçant à l'origine de la transaction litigieuse, « *ce recours n'étant alors pas enfermé dans le délai prescrit par ce texte* ».

Notons toutefois que l'article 6.1 du contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS entre le commerçant et sa banque) stipule que « *toute réclamation doit être formulée par écrit à l'Acquéreur "CB", dans un délai maximum de 6 mois à compter de la date de l'opération contestée, sous peine de forclusion. Ce délai est réduit à 15 jours calendaires à compter de la date de débit en compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé* ». L'incertitude règne donc en la matière.

La CNIL perçoit dans la conservation des données un risque de constitution de "listes noires "qui recenseraient les clients pour lesquels toute commande serait dès lors impossible. Mais, pour Rueducommerce.com cette crainte est infondée puisque l'achat reste toujours possible par d'autres moyens de paiement.

Groupe 3 Suisses souhaiterait pouvoir conserver le numéro de carte bancaire ainsi que le CVV2 (ou CV2X ou cryptogramme visuel) de la prise de commande jusqu'à l'expédition. Si cela était possible, Groupe 3 Suisses s'engagerait à ne pas conserver ces données au-delà de la libération du colis. Une commande peut, en effet, faire l'objet de plusieurs livraisons et donc de plusieurs paiements (cas des « livraisons retardées »). La notion de durée de transaction est donc plus longue en VAD qu'en magasin.

Le point de vue du juriste - S'il y a bien une prohibition stricte en droit des paiements en ligne, c'est bien celle de la conservation du cryptogramme visuel (les trois numéros au dos de la carte). L'interdiction est clairement fulminée par le standard PCI DSS, reprise en ces termes par le « référentiel sécuritaire accepteur » du contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS) : « Les données du Titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un Titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur "CB" ».

Certaines exigences de la CNIL se traduisent en contraintes opérationnelles parfois lourdes

Pour Vente-privee.com, certaines des contraintes imposées par la CNIL peuvent avoir des incidences opérationnelles lourdes. Vente-privee.com cite la directive de la CNIL qui impose que la décision de refus de vente ne puisse pas être prise sans intervention humaine (même si le processus qui a conduit à cette décision peut être, lui, automatisé).

Autre exemple: l'obligation faite aux E-Marchands de prévenir le client dans un délai suffisant avant de l'inscrire sur une liste qui l'empêcherait d'utiliser un certain type de moyen de paiement pour un achat! Cette exigence qui pourrait s'entendre du point de vue du droit de la consommation apparaît difficilement compatible avec les mesures anti-fraude que déploient les E-Marchands.

Reconnaissance du terminal : Device FingerPrint

Certaines solutions permettent l'identification unique du terminal en consignant certaines de ses caractéristiques dans une base de données.

Pour répondre aux exigences de la CNIL, un E-Commerçant interviewé a dû retirer l'usage du "Device FingerPrint (DFP)"[19] de son dossier de demande d'agrément. Or, l'identification du terminal appelant est une donnée clé dans l'identification d'une fraude potentielle. Elle est utilisée dans d'autres pays, aux Etats-Unis notamment.

Certains interviewés souhaiteraient que puisse s'engager une réflexion avec la CNIL sur les conditions d'utilisation du DFP dans le cadre des mesures mises en œuvre pour lutter contre la fraude.

Le point de vue du juriste - Remarquons que la CNIL considère que l'utilisation du numéro de carte bancaire par un professionnel de la vente à distance, dans un fichier ayant pour finalité de lutter contre la fraude au paiement en conservant la trace d'agissements lui ayant porté préjudice, est légitime, sous la réserve que ce fichier ait fait l'objet d'une demande d'autorisation et que cette utilisation du numéro de carte bancaire soit subordonnée à une information claire des personnes fichées ainsi qu'à la possibilité pour ces personnes de s'opposer, pour des motifs légitimes, à un tel traitement (Délibération n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance).

Dans une délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée (norme destinée à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux liberté) concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects, la CNIL reconnaît la finalité d'un traitement de gestion des impayés et du contentieux, à condition qu'elle ne porte pas sur des infractions et/ou qu'elle n'entraine pas une exclusion de la personne du bénéfice d'un droit, d'une prestation ou d'un contrat.

B.7.5.2 Des délais d'instruction des dossiers de conformité jugées trop longs

S'il y a bien un sujet qui suscite l'ire des E-Commerçants, c'est bien celui des délais d'instruction des dossiers d'autorisation de traitement automatisé des données à caractère personnel !

Rueducommerce.com a été contrôlé par la CNIL en novembre 2011. L'examen par la CNIL du traitement anti-fraude imaginé par Rueducommerce.com a pris 4 mois, un délai qui est jugé "incompatible avec les enjeux business". Même constat chez vente-privee.com : l'obtention de l'autorisation de la CNIL a pris 6 mois.

B.7.6 Perception de coopération avec les services de police et services judiciaires

La perception de la coopération avec les services de police et judiciaires est assez différente d'un E-Marchand à l'autre. Deux attitudes se distinguent : les E-Marchands qui choisissent de ne

coopérer avec les services policiers que sur réquisition, et les E-Marchands qui collaborent pro activement.

Ainsi, rueducommerce.com entretient des relations bilatérales avec les services policiers et juridiques : Rueducommerce.com répond systématiquement à toute demande des autorités judiciaires et, réciproquement, transmet les informations dont il dispose sur d'éventuels trafics. Rueducommerce.com se félicite de la qualité des relations qu'il entretient avec les services de gendarmerie (contact établi grâce à la FEVAD). Rueducommerce.com a le sentiment que depuis 2006-2007, le sujet de la fraude sur Internet intéresse de plus en plus les services de police : «Cela va dans le bon sens ».

Cet avis est partagé par vente-privee.com pour qui la collaboration avec les services judiciaires fonctionne « bien». Le site fait partie des E-Marchands qui ont une attitude très pro active vis-à-vis des services de Police. Il est ainsi déjà arrivé que vente-privee.com participe à la mise en place de flagrants délits, à la demande des autorités judiciaires. Par principe, Vente-privée.com pose systématiquement plainte en cas de fraude. En 2012, Vente-privée.com a déposé 272 plaintes.

Pecheur.com a fait le constat que la fourniture à la gendarmerie des éléments en sa possession permettait effectivement l'identification des fraudeurs et leur arrestation, même si le délai moyen de résolution d'une affaire pouvait prendre plusieurs mois. Sur demande de la Police, Pecheur.com est capable de fournir un certain nombre d'informations sur la transaction comme la durée, la date et l'heure de connexion, le numéro d'autorisation, l'adresse IP...

Pour d'autres E-Marchands, la collaboration avec les services de police semble plus compliquée. Deux motifs reviennent fréquemment; la difficulté à identifier les bons interlocuteurs et la difficulté à mobiliser les services de Police sur des dossiers dans lesquels soit la probabilité d'arrestation des fraudeurs est faible soit les montants en jeu sont peu élevés au regard des moyens qu'il faudrait mobiliser pour les faire aboutir.

Enfin, certains E-Marchands soulignent une difficulté très pratique qu'ils rencontrent pour déposer plainte : le manque de temps! Car, seule une personne habilitée dans l'entreprise peut déposer plainte. Or, ce sont souvent les personnes les moins disponibles ! Ces E-Marchands regrettent que la procédure ne puisse s'effectuer à distance.

En attendant, la proposition de directive du 7 février 2013 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (directive SRI) invite les États membres à veiller à ce que les administrations publiques et les acteurs du marché notifient une autorité nationale compétente en matière de sécurité des réseaux et systèmes informatiques, les incidents ayant un impact significatif sur la sécurité des services essentiels qu'ils fournissent (art. 14, 2). Dans la lignée de ce projet, la proposition de directive du 24 juillet 2013 concernant les services de paiement (directive DSP 2) soumet les prestataires de services de paiement (PSP) à cette exigence de notification, étant ajouté que « *lorsque l'incident de sécurité risque d'avoir un impact sur les intérêts financiers des utilisateurs des services de paiement fournis par le prestataire de services de paiement, celui-ci notifie l'incident dans les meilleurs délais aux utilisateurs de services de paiement et il les informe des mesures qu'ils peuvent prendre de leur côté pour atténuer les effets dommageables de l'incident* » (art. 85).

B.8 LES EVOLUTIONS DES MODALITES DE PAIEMENT ET DES MOYENS D'AUTHENTIFICATION VUS PAR LES E-MARCHANDS

B.8.1 Le Tsunami mobile

B.8.1.1 Oui, mais quand ?

S'il y a consensus pour considérer que le M Commerce constitue bien l'enjeu majeur à venir du commerce à distance, l'estimation de la survenue de ce Tsunami annoncé est moins unanime.

Pour certain, le mobile est déjà un enjeu

Chez Vente-privée.com, les ventes réalisées à partir du mobile (Smartphones et tablettes) représentent déjà 30 % des transactions.

Chez Voyages-sncf.com, le mobile a représenté 162 millions d'€ du volume d'affaire en 2012, et les ventes sur mobiles connaissent une très forte croissance.

Chez Laredoute.com, les ventes sur mobiles doublent chaque année. Les ventes réalisées sur Smartphone représentent de 3 à 4% des transactions et entre 7 et 8% pour les tablettes.

Pour d'autres, la vague est annoncée mais n'a pas encore déferlée...

Depuis fin octobre 2012, l'application mobile de Rueducommerce.com permet de commander en ligne. Les ventes réalisées sur le mobile sont encore marginales. En revanche, leur taux de progression est très rapide. Rueducommerce.com constate que ses clients préparent leur achat sur le mobile, même si pour l'instant, une faible minorité va jusqu'à commander. « L'utilisation du mobile ; on voit que cela vient ! »

Chez Mistergooddeal.com, les ventes sur mobile représentent entre 3 et 4 % de l'ensemble des ventes, ce qui représente un chiffre important compte-tenu du fait que Mistergooddeal.com n'a encore pas spécifiquement optimisé ce canal de vente. Les clients qui achètent sur le mobile sont particulièrement motivés.

La situation est similaire pour le Groupe 3 Suisses qui n'a pas de site optimisé pour les mobiles, ni d'application, ce qui n'empêche pas le Groupe 3 Suisses d'étudier de façon très précise, la mise en place d'une solution de paiement mobile.

B.8.1.2 Le canal de vente mobile est-il plus fraudé ?

Aucune vision claire ne se dégage sur ce point à la lumière des interviews. Chez Vente-privee.com, le taux de fraude sur le mobile est, pour l'instant (avant la mise en œuvre de 3D Secure) inférieur au taux de fraude sur Internet. Mistergooddeal.com ne perçoit pas encore les impacts du développement des ventes sur le mobile sur son dispositif de lutte contre la fraude.

En revanche Priceminister.com constate que le taux de fraude sur le mobile « explose», même si les ventes sur mobile sur ce canal de vente sont encore marginales. Chez Voyages-sncf.com, c'est bien la progression très rapide des ventes sur mobile qui a motivé la mise en place de la solution Retail & Decision.

B.8.1.3 Quelles possibilités de lutte contre la fraude pour les ventes sur le mobile en l'absence de solutions dédiées ?

Face à la progression du M-Commerce, bon nombre de E-Commerçants se sentent démunis. Un certain nombre de dispositifs anti-fraude repose notamment sur l'adresse IP qui, dans le cas d'une connexion par mobile ou tablette n'est pas adaptée.

Aussi, tous les E-Marchands interviewés fondent-ils beaucoup d'espoirs sur les portefeuilles électroniques (wallets).

La Banque de France, définit ainsi les portefeuilles électroniques : « Les portefeuilles électroniques permettent d'effectuer des paiements sur Internet rapidement et simplement, sans avoir à saisir des numéros sensibles (i.e. numéro de carte de paiement, sa date de validité et son cryptogramme visuel). Ces données ne sont en effet demandées que lors de la création du portefeuille électronique. Par la suite, l'utilisateur de la solution doit uniquement saisir ses identifiants (par exemple le numéro de téléphone portable ou le courriel de l'utilisateur + mot de passe) pour réaliser des transactions ».

Vente-privee.com dit regarder les initiatives de lancement de nouveaux wallets avec "beaucoup d'intérêt". Pour Vente-privee.com, les wallets sont une occasion intéressante de pouvoir combiner trois objectifs ; une solution de paiement largement "mass market", la garantie de paiement pour le E-Marchand au travers du transfert de responsabilité, la garantie d'un taux de transformation performant du fait de l'adaptation du paiement à l'ergonomie du terminal.

Selon Atos Wordline le futur wallet V.me de Visa sera bien compatible avec le mobile et utilisera des moyens d'authentification comparables à 3D Secure. Cela devrait être aussi le cas pour le wallet de Mastercard. L'authentification ne sera pas systématique. C'est en fonction du résultat de l'analyse du risque intégré à la solution V.me que sera déclenchée ou non une authentification forte.

B.8.2 Vision des E-Marchands sur quelques évolutions des moyens de paiements et de l'authentification en ligne

Même si ce n'est clairement pas leur métier de prédire quels seront les moyens de paiement de demain, quelques E-Commerçants ou prestataires de solutions de paiement interviewés, se risquent à donner quelques pistes.

Vers la disparition du chèque et son remplacement par les virements ?

Ruedu.commerce.com prédit que, dans un avenir proche, la part des chèques devrait reculer, voire disparaître, au profit des prélèvements SEPA et, si la carte bleue continuera d'exister, elle pourrait être supplantée par d'autres moyens de paiement.

Il est à noter que, parmi les 20 recommandations préconisées par le rapport Pauget-Constant de mars 2012 sur l'avenir des moyens de paiement en France, figure expressément celle d' « *accélérer et accompagner la réduction du rôle du chèque* » en fixant « *au plan national pour 2017 un objectif intermédiaire de réduction de moitié en cinq ans du nombre de chèques émis en France* » (p. 98).

Le développement des virements en ligne

Pour Atos Wordline, ce type de solution présente un double avantage pour les marchands; la garantie de paiement et des coûts de transactions moindres que pour la carte bancaire.

Ce type de moyen de paiement est relativement peu développé en France. Il l'est davantage à l'étranger. La solution iDEAL aux Pays-Bas a retenu l'attention du rapport Pauget-Constans sur l'avenir des moyens de paiement en France, lui consacrant une annexe détaillée.

Atos Wordline fait remarquer que certaines solutions des virements en ligne ne viennent pas directement du monde bancaire. Ces moyens de paiement s'appuient sur des solutions bancaires mais n'ont pas été initiés par les banques. Même si les banques demeurent en périphérie du fonctionnement de ces solutions de paiement, ce type de solution présente un réel risque de désintermédiation pour elles. Et, ces nouveaux moyens de paiement sont objectivement beaucoup moins rémunérateurs pour les banques que la carte bancaire.

Les moyens de paiements prépayés

Il s'agit principalement des cartes achetées chez les buralistes ou les agents de change. Le coût d'acquisition est certes plus élevé pour le marchand que pour les cartes bancaires. Mais, en contrepartie, le Marchand bénéficie de la garantie de paiement.

Il est à noter que certains E-Commerçants sont confrontés à des schémas de fraudes liées à l'utilisation de cartes prépayées anonymes. Ce sujet a été évoqué par les E-Marchands lors de leur rencontre avec la Banque de France, et le GIE Cartes Bancaires. Il est apparu souhaitable que les E Commerçants puissent plus facilement identifier les cartes prépayées afin de renforcer la vigilance sur ces cartes et être en mesure de les bloquer lorsqu'un cas de fraude est détecté.

Il est à noter que l'Observatoire a poursuivi en 2012 son analyse relative à l'utilisation des cartes prépayées anonymes et que son président a saisi par lettre le ministre de l'Économie et des Finances pour souligner les risques que représentent ces produits en termes de fraude et de financement du terrorisme et suggérer une évolution du cadre normatif en conséquence.

Ce sujet est suivi au sein des groupes de travail de l'Observatoire.

Le point de vue du juriste - Le développement du prépayé en France, qui n'est cependant pas sans risque en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, devrait (enfin) bénéficier de la transposition, en droit français, de la deuxième directive Monnaie électronique (DME 2) par une loi du 28 janvier 2013. De véritables établissements de monnaie électronique pourront ainsi émettre et gérer de la monnaie du même nom, que ce soit sous forme de cartes prépayées ou directement de services électroniques.

Développement de la pratique de l'authentification en ligne

Selon Atos Wordline, cette pratique est appelée à se développer pour plusieurs raisons.

La première raison est le développement de la banque en ligne et la convergence entre les moyens d'authentification à son compte en banque et l'authentification des transactions, comme c'est déjà le cas en Belgique, dans les pays nordiques, et en Suisse.

La deuxième raison est que des sites à fort trafic comme Gmail ont maintenant recours à des moyens d'authentification pour autoriser leurs clients à accéder à leur compte ou pour modifier leurs paramètres de comptes, familiarisant ainsi de plus en plus les utilisateurs avec ces pratiques.

La troisième raison est le développement de l'usage des Wallets.

Le point de vue du juriste - Deux projets de textes européens devraient contribuer à ce développement :

- une proposition de règlement du 4 juin 2012 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, devant entre autres permettre aux États membres de « *susciter la confiance nécessaire dans leurs systèmes d'identification électronique respectifs et faciliter la reconnaissance et l'acceptation mutuelles des des moyens d'identification électronique relevant de leurs systèmes notifiés* » (cons. 13) ;

- une proposition de directive du 24 juillet 2013 concernant les services de paiement (DSP 2), dont l'article 87 dispose : « Les États membres veillent à ce qu'un prestataire de services de paiement applique l'authentification forte du client lorsque le payeur initie une opération de paiement électronique, sauf dérogation spécifique fondée sur le risque lié au service de paiement fourni, prévue par les orientations de l'ABE [Autorité bancaire européenne] ».

Partie C
RECOMMANDATIONS DES E-MARCHANDS
(A EUX-MEMES) ET AUX AUTRES ACTEURS PARTIE-PRENANTES, POUR RENFORCER COLLECTIVEMENT LA SECURITE DES PAIEMENTS SUR INTERNET

C.1 RECOMMANDATIONS AUX E-MARCHANDS

Mesurer l'impact de la fraude dans sa globalité

Pour les E-Marchands interviewés, considérer la fraude comme un coût financier inévitable et l'intégrer dans son calcul de marge, c'est en mésestimer totalement les conséquences à moyen et long terme.

Même si la culture de la lutte contre la fraude est très fréquemment inscrite dans les gènes des principaux acteurs de l'internet (et notamment de ceux pour qui Internet ne constitue qu'un puissant canal additionnel de vente par rapport à une activité de commerce classique), il faut bien reconnaitre que, pour certains "pur-players", la fraude reste considérée comme "un mal inévitable" qu'ils intègrent dans le calcul de leur marge[20]. C'est notamment le cas pour certains "pur-players" de contenus digitaux, pour qui le coût de la fraude était finalement très marginal par rapport aux revenus qu'ils génèrent.

Pour la FEVAD, un tel raisonnement court-termiste est particulièrement dangereux pour l'ensemble du secteur dans la mesure où il joue sur un élément absolument fondamental pour la pérennité du E-Commerce, à savoir la confiance du consommateur dans les moyens de paiement.

Déposer systématiquement plainte, avec le cas échéant constitution de partie civile

Les E-Marchands ne déposent pas systématiquement plainte en cas de fraude. Bien souvent, le E-Marchand considère le dépôt de plainte uniquement sous l'aspect économique et pratique. Est-ce réellement rentable de consacrer des moyens (et notamment du temps) à rassembler les preuves de la fraude par rapport à la probabilité (souvent très faible) d'être indemnisé et de voir

[20] Selon la Fédération Bancaire Française, cette pratique n'est évidemment pas l'apanage de certains E-Marchands français, elle serait notamment très répandue aux États-Unis

le ou les fraudeurs finalement interceptés et condamnés. A ce calcul, s'ajoutent les difficultés pratiques déjà évoquées à déposer plainte pour la personne autorisée au sein de l'entreprise.

Là encore, ne pas déposer plainte, c'est laisser se développer un sentiment d'impunité parmi les fraudeurs et entretenir un phénomène de nature à saper inexorablement l'ensemble de l'écosystème de l'E-Commerce. Il faut ici saluer l'attitude de certains E-Marchands rencontrés pour qui le dépôt systématique de plaintes relève d'une question de principe.

Il y a également une autre évidence à rappeler : ne pas déposer plainte, c'est tout bonnement considérer que la fraude n'a pas existé, notamment dans les statistiques suivies par les pouvoirs publics.

Dans le déploiement et l'exploitation de 3D Secure, mettre en œuvre les bonnes pratiques identifiées dans le Livre Blanc

Dans ce Livre Blanc, les E-Marchands qui ont mis en œuvre 3D Secure ont accepté de donner leur retour d'expérience et de partager un certain nombre de bonnes pratiques qu'ils en ont tirées. Ces recommandations sont totalement désintéressées. Elles n'ont d'autres finalités que de faciliter l'adoption de 3D Secure par les E-Marchands qui ne l'ont pas encore mis en place (ou s'interrogent encore), dans les meilleures conditions possibles compte tenu des limites de la solution qui ont été identifiées. Ces recommandations visent également à permettre aux E-Marchands d'exploiter pleinement les bénéfices de la solution 3D Secure, au sein de leur dispositif de lutte contre la fraude étant entendu qu'une authentification renforcée ne garantit en rien le marchand contre une fraude ; au mieux, elle le garantit contre un futur "charge back".

Mieux utiliser et exploiter les informations « de base » déjà disponibles auprès des PSPs ou des banques

Alors que certains E-Marchands interviewés considèrent ne pas disposer de suffisamment d'outils pour piloter leur lutte contre la fraude, certains prestataires de solutions de paiement rencontrés dans le cadre de ce Livre Blanc, déplorent quant à eux une sous-utilisation des outils de lutte contre la fraude qui sont pourtant librement accessibles dans les back-offices des Marchands. Mais, pour être réellement efficaces, les PSP rappellent que ces outils et les règles associées doivent faire l'objet de mises à jour régulières par les E-Marchands.

Les reportings qu'envoient les prestataires aux E-Marchands seraient eux-aussi sous-exploités. Ils contiennent notamment les journaux "de rapprochement des impayés Clients" sur lesquels apparaît l'information sur la couverture de la transaction par la garantie de paiement (et le transfert de risques). Une bonne exploitation de l'ensemble de ces données permettrait aux marchands d'avoir une vision précise du niveau de risque que présente chacun de ses clients.

De même, les techniques de fraudes et les technologies permettant de les empêcher évoluant rapidement, les E-Marchands doivent s'astreindre à un effort de veille permanent, si possible en collaboration étroite avec la Banque de France et le GIE Cartes Bancaires.

Envisager l'externalisation partielle ou total des dispositifs de lutte contre la fraude

La question de l'externalisation de la lutte contre la fraude peut se poser pour certains E-Marchands dont les moyens sont focalisés sur d'autres sujets et qui, même s'ils en mesurent les enjeux, considéreraient que cette compétence n'est pas "au cœur de leur métier".

Des acteurs sur le marché proposent aujourd'hui des prestations de conseil en définition de stratégies de lutte contre la fraude adaptées au contexte et spécificités du E-Marchand. Ces missions de conseil peuvent aller jusqu'à l'accompagnement et la mise en œuvre; voire dans certain cas l'externalisation complète de la lutte contre la fraude.

On l'a vu à d'autres occasions, la promotion des prestataires de services tiers (services d'initiation de paiement en particulier) par la future DSP 2 (proposition directive du 24 juillet 2013) devrait faciliter cette externalisation.

Se mobiliser collectivement contre la fraude - Partager l'information

La globalisation de la fraude et le développement des réseaux de fraude rend nécessaire un renforcement de la coopération entre les professionnels du secteurs sur l'échange des bonnes pratiques (ce Livre Blanc veut en être une illustration) mais également un renforcement des échanges d'informations entre les sites, dans le respect bien évidemment des exigences de la CNIL, dont les E-Marchands souhaiteraient qu'elles évoluent (cf. Pistes de réflexions à engager avec la CNIL plus loin dans ce document).

Certains E-Marchands interviewés souhaiteraient même la mise en place d'une "Plate-forme d'échanges d'information relatives à la fraude", pourquoi pas avec le GIE Cartes Bancaires qui en détient l'historique, qui serait partagée entre E-Marchands.

C.2 RECOMMANDATIONS AUX PRESTATAIRES DE SOLUTIONS DE PAIEMENT

Proposer des solutions de lutte contre la fraude adaptée aux E- marchands de petite taille

Même si, comme cela a été souligné dans ce Livre Blanc, la lutte contre la fraude passe d'abord par la mise en place de solutions "simples et de bons sens", son évolution permanente et le mouvement de professionnalisation de la fraude, maintenant bien engagé, nécessitent potentiellement une forte mobilisation d'expertise et de moyens, particulièrement pour les E-Marchands de taille "moyenne" qui sont particulièrement visés par la fraude mais qui n'ont pas forcement autant de moyens que les "gros" à mobiliser sur le sujet.

Dans le contexte du développement de la fraude, largement décrit dans ce document, il est particulièrement important que les PSP puissent proposer aux E-Marchands de taille "moyenne" des solutions de lutte contre la fraude qui soient adaptées à leurs moyens.

Ces solutions devraient certainement reposer sur la mutualisation de ressources et d'informations entre les sites E-Marchands, dans le respect des recommandations de la CNIL (cf. point suivant).

C.3 PISTES DE REFLEXION A PARTAGER AVEC LES BANQUES ET/OU CB

C.3.1 Spécifiquement sur 3D Secure et les moyens d'authentification

Réduire le taux d'échec d'authentification pour le rendre compatible avec les exigences économiques du E-Commerce

Le niveau de taux d'échec d'authentification reste le frein majeur au développement de 3D Secure en France. Même si, beaucoup de E-Marchands en conviennent, il s'agit d'un taux d'échec "brut", 18% des authentifications qui n'aboutissent pas est un taux qui reste

"incompatibles avec les règles économiques du E-Commerce". Des échanges qu'a eu la FEVAD avec elle il ressort que la Banque de France souhaite maintenir la pression sur les banques afin de faire rapprocher le taux d'échecs 3D-Secure de celui constaté lors des paiements non 3D-Secure. Au-delà du taux moyen, c'est bien l'écart très important d'une banque à l'autre qui "choque" particulièrement les E-Marchands. Ces écarts tendent à prouver, si cela était encore nécessaire, qu'une réduction très importante du taux d'échec d'authentification est possible et qu'elle ne dépend que de la mobilisation des moyens appropriés par les banques.

Accélérer l'uniformisation des moyens d'authentification

Les E-Marchands notent, avec un certain soulagement, le mouvement d'uniformisation des moyens d'authentification engagé par les banques qui, ils en sont conscients, a également été permis par la généralisation de l'usage du téléphone mobile.

C'est le deuxième message clé qu'ils veulent réaffirmer dans le cadre de ce Livre Blanc : la sécurisation des moyens de paiement ne peut se faire au détriment de la fluidité du parcours client (dont l'échec d'authentification est la pire des extrémités).

Les E-Marchands se disent prêts à collaborer avec les banques pour trouver ensemble des solutions qui contribueraient à l'atteinte de ces deux objectifs.

A court terme, les E-Marchands voient dans l'accélération de l'uniformisation des moyens d'authentification un facteur de développement de l'usage de 3D Secure.

Pour les E-Marchands, les moyens d'authentification nécessitant le déploiement de matériel spécifique (clé, grille...) sur l'ensemble du parc clients des banques ont montré leurs limites. Ils rappellent cette évidence: un client en attente du renouvellement par sa banque de son moyen d'authentification physique est un client momentanément perdu pour le E-Commerce.

Enfin, les E-Marchands appellent de leurs vœux le déploiement de nouveaux moyens d'authentification qui s'inscrivent en cohérence avec le principe de simplicité et de fluidité de l'acte de paiement. Les banques et CB étudient d'ailleurs la mise en œuvre de nouvelles méthodes d'authentification mieux adaptées au mobile, notamment dans le cadre des solutions de portefeuille à venir.

Intensifier l'effort de communication et de pédagogie sur les moyens d'authentification renforcée

Pour les E-Marchands, le travail de communication et de pédagogie à fournir sur les bénéfices et l'utilisation des moyens d'authentification reste encore très important même s'ils ne contestent pas l'effort initié par les Banques ni la difficulté de l'exercice.

Pour eux, il s'agit là aussi d'un point clé dans le développement de l'usage de 3D Secure. Ils restent également persuadés que cet effort de communication et de pédagogie est de nature à rassurer les clients sur la sécurisation des moyens de paiement.

Veiller à une meilleure transparence dans la garantie de paiement

La garantie de paiement (et le transfert de risques associé) demeure un élément très fort de l'attrait de la solution 3D Secure pour le E-Marchand. Il semble qu'il est dans l'intérêt mutuel des banques et des E-Commerçants de lever les ambiguïtés sur les limites de celle-ci, tout simplement par une communication claire et transparente sur les dites règles et, dans la pratique, par une information claire fournie aux E-Marchands sur les transactions ayant bénéficié du transfert de risque et celles qui n'en n'ont pas bénéficié.

Informer systématiquement les E-Marchands lors de l'ouverture d'un contrat VAD, sur les possibilités de mise en œuvre de 3D Secure, notamment le mode sélectif

A l'ouverture de tout nouveau contrat d'acceptation en paiement à distance sécurisé par cartes (contrat VADS), le mode de mise en œuvre proposé par défaut est le mode systématique ou « full 3DS ». Il paraîtrait souhaitable que la banque puisse indiquer au E-Marchand (notamment les E-Marchands de petite taille) les répercussions possibles de 3D Secure sur le taux de transformation, et idéalement puisse l'informer des autres modalités possibles de mise en œuvre de la solution (3D Secure sélectif).

Allongement du délai de validité du transfert de responsabilité

Certains E-Marchands souhaiteraient engager une réflexion sur la règle définissant la durée de validité du transfert de responsabilité après une authentification positive.

C.3.2 Sur le support aux E-Marchands

Faciliter l'accès des E-Marchands (notamment les E-Marchands de petite taille) aux données leur permettant notamment de paramétrer et piloter leur dispositif de lutte contre la fraude

Que l'on soit "petit" ou "gros" remettant, l'accès à certaines informations pourtant essentielles au paramétrage des dispositifs de lutte contre la fraude semble plus ou moins compliqué, comme par exemple l'accès au fichier BIN ou au fichier OPOTTOTA.

Les E-Marchands souhaiteraient engager une réflexion avec les banques sur les modalités d'accès aux informations qui leur permettraient de paramétrer encore plus efficacement leurs dispositifs de lutte contre la fraude, tout en tenant compte du caractère parfois extrêmement sensibles de ces informations.

Définir un reporting standard sur les statistiques de fraude que fournirait la banque acquéreur au E-Marchand

Certains E-Marchands regrettent le manque de statistiques fournies par leur banque acquéreur. Certains suggèrent la définition d'un reporting standard sur les statistiques de fraude qui devrait être transmis systématiquement par la banque acquéreur aux E-Marchands ce qui leur permettaient de dresser des « profils types » de transactions frauduleuses.

Informer les E-Marchands sur les nouveaux produits de paiement lancés par les banques

Un certain nombre de difficultés rencontrées par les équipes techniques des E-Marchands en charge du paramétrage des moyens de paiement vient parfois de leur méconnaissance des spécificités et surtout des limites des nouvelles cartes ou des solutions de paiement émises par les banques. Ces E-Marchands souhaiteraient bénéficier d'un meilleur accompagnement des banques sur ce sujet.

Développer le niveau de compétence et l'expertise des responsables de compte sur la lutte contre la fraude et/ou développer des cellules dédiées à la lutte contre la fraude et plus généralement au E-Commerce

Comme évoqué dans le chapitre relatif à la perception des E-Marchands sur la collaboration avec les banques, les E-Marchands expriment très nettement le besoin d'un support plus fort des banques sur le sujet de la lutte contre la fraude.

Là encore, les situations sont différentes en fonction du pouvoir de négociation du E-Marchand vis-à-vis de sa banque.

Le point de vue du juriste - L'ouverture du marché des paiements réalisée par la directive de 2007 sur les services de paiement (DSP) permet toutefois aujourd'hui (on ne le sait pas assez) de « faire jouer la concurrence » avec notamment les nouveaux établissements de paiement et, demain, avec les prestataires de services de paiement (PSP) tiers que sont les PSP initiateurs de paiement (ou d'information sur les comptes).

Même s'il est compréhensible que les interlocuteurs commerciaux des E-Marchands au sein des banques ne puissent maîtriser tous les sujets, il serait néanmoins apprécié que les E-Marchands (et notamment de petite taille) puissent avoir accès plus facilement à des cellules d'expertises dédiées à la lutte contre la fraude au sein des banques, cellules d'autant plus justifiées aujourd'hui que le e-commerce est très largement entrer dans les usages de consommation et les pratiques marchandes (voir chiffres clés Fevad).

C.4 RECOMMANDATIONS ET PISTES DE REFLEXION AVEC LA BANQUE DE FRANCE

Dans leur ensemble, les E-Marchands interviewés saluent le travail réalisé par la Banque de France notamment dans le cadre de l'Observatoire de la Sécurité des Cartes de Paiement (OSCP)

On saluera à cet égard l'action de communication engagée en décembre 2012 par l'OSCP, par la publication d'une brochure « Commerçants, comment renforcer la sécurité des paiements sur Internet ? », où il est fait mention du mécanisme d'authentification renforcée et de la solution 3D Secure. Parallèlement, la Banque de France a elle-même publié en novembre 2011, à destination des particuliers, un document sur la protection des identifiants bancaires (numéros de compte, numéros de carte bancaire, identifiants de la banque en ligne).

Poursuivre la promotion d'une approche par les risques pour impacter graduellement la fluidité du parcours client : inciter à l'usage sélectif de 3D Secure

Les E-Marchands collectivement soutiennent l'objectif de la Banque de France d'assurer la sécurisation des moyens de paiement et comptent assumer pleinement leurs responsabilités dans l'atteinte de cet objectif, qui est absolument essentiel pour eux.

Mais ils rappellent que la généralisation des moyens de sécurisation des paiements sera d'autant plus rapide et efficace que ces moyens s'inscriront de façon la plus fluide possible dans les parcours de paiements et que ces moyens de sécurisation perturberont le moins possible les habitudes d'achat des consommateurs.

La FEVAD, qui en fût très tôt l'instigatrice, recommande une approche de la sécurisation des moyens de paiement par les risques (proportionnalité des moyens de sécurisation au risque de la transaction), seule approche qui permette de concilier fluidité du parcours et maîtrise de la fraude.

Définir et contrôler les engagements d'amélioration des banques notamment sur la réduction du taux d'échec d'authentification

Les E-Marchands constatent que malgré les intentions affichées et le temps écoulé depuis le lancement de 3D Secure, le taux d'échec d'authentification moyen reste élevé.

Ils subissent en parallèle une pression de plus en plus forte pour mettre en œuvre 3D Secure.

Ils leur semblent que cette pression serait d'autant plus efficace si elle s'accompagnait d'engagements fermes des banques sur des délais de réduction du taux moyen d'échec, objectifs dont la réalisation pourrait être vérifiée par la Banque de France.

Poursuivre, renforcer et (le cas échéant) organiser le dialogue entre les parties prenantes (notamment via l'OSCP) particulièrement sur les points suivants:

Lors des entretiens, les E-Marchands interviewés ont réaffirmé l'importance à leurs yeux soit de poursuivre soit d'engager des réflexions avec l'ensemble des parties prenantes sur les thèmes suivants:

- La clarification des limites de la garantie de paiement en fonction des cartes de paiement
- L'extension de garantie 3D Secure à l'ensemble des transactions, dans le cas d'un paiement fractionné.
- La définition et le suivi de la qualité de service (QoS) de la demande d'authentification : définition d'un délai maximum d'affichage de la page d'authentification, adaptation de la page de saisie du code aux spécificités du terminal appelant (rendering) …
- Les moyens à mobiliser pour réduire la fausse répudiation (incluant une réflexion sur la communication à faire sur les conséquences économiques de ce type de fraude et ses conséquences pénales pour le fraudeur)
- Les modalités d'accès des E-Marchands de petite taille aux informations et aux moyens techniques leur permettant de bénéficier de dispositifs anti-fraude adaptés à leurs moyens
- L'harmonisation des législations européennes sur l'utilisation des moyens de paiement (qui néanmoins progresse avec le projet de DSP 2).

C.5 PISTES DE REFLEXION A ENGAGER AVEC LA CNIL

C.5.1 Quel équilibre trouver entre "protection des données personnelles" et "lutte contre la fraude" ?

Pour les E-Marchands, la protection des données personnelles est un enjeu majeur pour le développement de l'économie numérique et ils y souscrivent totalement.

Néanmoins, il leur paraît maintenant utile de revisiter les modalités de mise en œuvre des procédures de protection des données personnelles à la lumière des nouvelles exigences de lutte contre la fraude sur internet. Il leur semble qu'il en va de l'intérêt du consommateur d'être assuré de la protection de ses données personnelles comme de la sécurisation des moyens de paiement qu'il utilise.

Réaliser un benchmark des bonnes pratiques européennes (Allemagne, Royaume-Uni...)

Des E-Marchands interviewés ont émis l'idée d'enrichir la réflexion à partir d'exemples concrets empruntés à d'autres pays européens pour identifier d'éventuelles bonnes pratiques qui pourraient être répliquées en France.

Constituer un groupe de travail spécifique pour partager les réflexions et l'expertises des E-Marchands

La plupart des E-Marchands interviewés se sont dits prêts à participer à un éventuel groupe de réflexion sur l'évolution de l'équilibre à trouver entre protection des données personnelles et efficacité des systèmes de lutte contre la fraude. Ce sujet devrait être abordé prochainement au sein de l'Observatoire de la sécurité des cartes de paiement.

C.5.2 Engager une réflexion avec la CNIL sur certains thèmes spécifiques

Au-delà du thème générique de réflexion précédemment cité, les E-Marchands souhaiteraient que puissent s'ouvrir des débats plus spécifiques sur les thèmes suivants :

- Les conditions de mutualisation de certaines données notamment entre filiales d'un même groupe et entre clients d'un même prestataire

Le point de vue du juriste - On s'inspirerait utilement des règles gouvernant la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) qui, s'agissant des organismes financiers (dont les prestataires de services de paiement (PSP), prennent en compte l'appartenance à un groupe pour une mise en œuvre efficace des obligations de LCB-FT. Les articles L. 561-4 et R. 561-29 du Code monétaire et financier n'imposent-ils pas aux PSP, notamment, appartenant à un même groupe d'échanger les informations nécessaires à la vigilance dans le groupe en matière de LCB-FT, y compris pour les informations relatives à la clientèle et ce compris entre entités étrangères ? Ne pourrait-on pas prévoir une telle information croisée, en tout cas au sein d'un groupe, entre PSP et entre PSP et commerçants ?

- La durée de conservation de certaines données nécessaires à l'évaluation du risque de fraude.
- Les conditions de mise en place d'une base de données accessible aux E-Marchands les renseignant sur la mise en opposition des cartes de paiement frauduleuses, sur le principe de la base Préventel dans le secteur des communications électroniques.
- Les conditions d'utilisation des méthodes de reconnaissance du terminal (Device FingerPrint). A cet égard, le fait qu'un terminal constitue un prolongement de l'identité d'une personne ou d'un comportement frauduleux, n'est pas nouveau. Cette problématique est aussi ancienne que l'usage de la téléphonie fixe ou de la carte à puce. Au lieu de camper sur une position d'interdiction qui favoriserait des stratégies de dissimulation ou de délocalisation, il serait préférable que la CNIL ouvre une concertation en vue d'un encadrement clair des méthodes de Device FingerPrint, qui soit valable au sein de l'Union européenne. A l'heure où les terminaux mobiles s'équipent de lecteurs d'empreintes digitales stockées à l'autre bout du monde, il paraît anachronique de souhaiter interdire l'identification d'un terminal.

C.5.3 Engager une réflexion avec la CNIL sur les modalités d'instruction des dossiers d'autorisation

Comme évoqué lors de la description de la perception des E-Marchands de la collaboration avec la CNIL, le délai d'instruction des dossiers d'autorisation est globalement jugé très long (de l'ordre de six mois jusqu'à plus d'une année) et, peu compatible avec la réactivité que nécessite la lutte contre la fraude.

La CNIL a régulièrement affirmé que la protection de la vie privée et des données personnelles n'a pas pour objet de protéger les comportements frauduleux, mais d'éviter les exclusions illégitimes ou mutualisées parmi plusieurs secteurs professionnels et de fixer des durées de conservation proportionnées et impératives.

Il conviendrait que cette approche s'illustre dans l'instruction des demandes d'autorisation.

Aussi, les E-Marchands identifient deux pistes de réflexion pour raccourcir les délais d'instruction :

- Fixer un délai maximum d'instruction des dossiers permettant aux E-Marchands d'obtenir une réponse dans les délais impartis par la loi à la CNIL (deux mois) pour se prononcer sur une demande d'autorisation.
- Passer d'un régime d'autorisation « ad hoc » à un régime d' « autorisation unique » établi en concertation avec les acteurs concernés, afin de viser a minima les dispositifs de prévention des fraudes et impayés, à l'image de ce qui est fait en matière de LCB-FT.

En effet, la légitimité de l'objectif de sécurité économique n'est pas contestée par la CNIL. Les critères de prévention des fraudes sont principalement attachés à la transaction financière envisagée et aux coordonnées de paiement et à l'identification de l'acheteur et de son terminal.

Enfin, les durées de conservation de listes d'exclusion sont, en tout état de cause, actuellement limitées par la CNIL dans le cadre des procédures d'autorisation « ad hoc ». En conséquence, le raccourcissement des délais d'instruction par la CNIL pourrait résulter de la normalisation de la doctrine de la CNIL, celle-ci étant aujourd'hui stabilisée et répétée dans tous les dossiers qu'elle examine.

C.5.4 Repenser la responsabilité du E-Marchand en matière de traitement des paiements et de prévention des fraudes

Lorsqu'un E-Marchand recourt aux services d'un PSP, il ne décide généralement pas des modalités de sécurisation et de conservation des données traitées par le PSP, lesquelles sont essentiellement régies par les réglementations bancaire et financière et par les normes de traitement des paiements et de sécurité appliquées par le PSP.

Il parait de plus en plus fictif de considérer que le E-Marchand serait « responsable du traitement » des données réalisé par le PSP. Les finalités de traitement de ces données résultent du contrat d'adhésion proposé par le PSP au E-Marchand. Les modalités et moyens de traitement des données de transaction et de paiement sont également déterminés par le PSP, comme les mesures de sécurité et les durées de conservation qu'il met en œuvre.

Il est de même fictif de considérer que le E-Marchand a le pouvoir de donner des instructions à un PSP sur la manière dont ce dernier s'organise dans le traitement des données qui lui sont transmises aux fins de traiter un paiement.

Or, le propre d'un « responsable de traitement » est de pouvoir, s'il le souhaite, se substituer au sous-traitant qui agit pour son compte, puisque ledit « responsable » est réputé décider de tout. En l'espèce, le E-Marchand ne décide de rien ou presque, si ce n'est de devoir recourir à un PSP pour traiter les paiements électroniques destinés au E-Marchand.

Aussi paraît-il nécessaire que la CNIL ouvre une réflexion sur la meilleure régulation des systèmes de prévention des fraudes intégrés au traitement des paiements par des PSP. En effet, il parait peu pertinent de soumettre à la CNIL des centaines de demandes d'autorisation identiques présentées par autant de E-Marchands, alors que les traitements de données concernés seront mis en œuvre par une poignée de PSP, représentant peu de demandes d'autorisation à examiner.

A cet égard, la CNIL n'a jamais exigé d'un marchand qu'il lui soumette une demande d'autorisation pour les mécanismes de prévention des fraudes mis en œuvre par la banque qui lui fournit un terminal de paiement. Il devrait en être de même dans le domaine des paiements électroniques associés à des solutions de prévention des fraudes proposées par les PSP à des E-Marchands.

Du point de vue des PSP, la validation par la CNIL de leurs services et mécanismes de prévention des fraudes, faciliterait la commercialisation de leurs services auprès de n'importe quel E-Marchand, en évitant à chacun de ces derniers de supporter les délais et la charge d'une demande d'autorisation répliquant celle d'un autre E-Marchand client du même PSP.

C.6 ATTENTES VIS-A-VIS DES SERVICES DE POLICE ET DES POUVOIRS PUBLICS EN GENERAL

C.6.1 Modalités de dépôt des plaintes et durcissement des peines encourues

Les E-Commerçants rencontrés formulent trois demandes:

1) Revoir les modalités de dépôt de plaintes pour les particuliers et pour les E-Marchands

Pour les particuliers : rendre obligatoire le dépôt d'une plainte pénale sans lequel la banque devrait s'interdire l'enregistrement et la comptabilisation d'une contestation d'un paiement réalisé à distance ou, a minima, inciter à nouveau au dépôt de plaintes pour les particuliers.

Pour les E-Marchands : faciliter le processus de dépôt de plainte

2) Durcir les sanctions et les peines encourues dans le cadre de la fraude au E-Commerce

Activité criminelle parmi d'autres, la fraude sur les moyens de paiement à distance exige un investissement moindre que pour d'autres filières criminelles. De plus, les peines encourues sont plus faibles comparées à celles occasionnées par d'autres délits « physiques ». Il est ainsi plus facile et moins risqué de déployer des compétences dans le secteur de la cybercriminalité, que dans d'autres activités illégales. Les E-Commercants appellent de leur voeux un durcissement des sanctions à l'encontre des fraudeurs aux moyens de paiement.

3) Sans remettre en cause l'administration de la politique pénale de chaque procureur, obtenir une meilleure homogénéisation des décisions de l'autorité judiciaire sur l'ensemble du territoire national

C.6.2 Renforcement de la coopération fonctionnelle entre les principaux acteurs de la sécurité des moyens de paiement en VAD (CB, PSP, Prestataires) et de la coopération judiciaire internationale

Il s'agit pour les E-Commerçants d'un point essentiel, notamment dans le cadre du mouvement de globalisation de la fraude et de sa structuration en réseau. Pour faire face à ces nouveaux enjeux, le renforcement de la coopération fonctionnelle entre les principaux acteurs de la sécurité des moyens de paiement à distance (CB, PSP, Prestataires) est indispensable. Il passe notamment pour les trois points repris ci-après:

- Faciliter la coopération avec les services de police : Créer un « guichet unique » permettant d'orienter le Marchand vers le service compétent ou, à défaut diffuser l'information sur « qui contacter en cas de fraude» aux E-Marchands

Le point de vue du juriste - On notera avec intérêt que la proposition de directive SRI (directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union) prévoit la création, dans chaque État membre, d'une autorité nationale compétence en matière de sécurité des réseaux et systèmes informatiques (art. 6), à laquelle devraient être notifiées les incidents ayant un impact significatif sur la sécurité des services essentiels qu'ils fournissent (art. 14) ; que la proposition de deuxième directive sur les services de paiement (DSP 2) fait expressément référence, concernant la sécurité du paiement, à la procédure ainsi mise en œuvre par la directive SRI.

- Renforcer la coopération entre services de police et E-Marchands: organiser des échanges croisés (formations, séminaires) entre eux.
- Veiller au maintien de moyens suffisants pour traiter les demandes d'information avec une réactivité adéquate.

Au niveau international, il apparait également souhaitable de renforcer la coopération judiciaire internationale notamment avec les pays avec lesquels la France n'a pas d'accords.

Partie D
ANNEXES

D.1 QUELQUES DEFINITIONS

D.1.1 Fichier OPPOTOTA

Le fichier OPPOTOTA est le fichier qui recense l'ensemble des cartes mises en opposition[21] Ce fichier est partagé entre les membres CB. Be2bill fait remarquer que le délai entre la mise en opposition d'une carte et son signalement effectif dans le fichier OPPOTOTTA varie et peut-être supérieur à plusieurs jours. Et, dans ce laps de temps, un certain nombre de transactions frauduleuses peuvent être réalisées.

Le processus d'autorisation de la transaction comprend la vérification de l'absence de la carte sur le fichier OPPOTOTA.

D.1.2 Demande d'autorisation

Pour chaque demande d'autorisation, la transaction transite d'abord par le PSP qui la transmet à la banque acquéreur (acquéreur du marchand) qui elle-même transmet la demande, via un réseau d'autorisation (leRSB le réseau CB) à la banque émettrice de la carte.

A réception de la demande d'autorisation, la banque émettrice vérifie qu'elle est bien l'émettrice de la carte. Elle vérifie également que la date de validité de la carte est cohérente avec son numéro, et que le cryptogramme est correct.

La banque émettrice peut également procéder à d'autres vérifications (chaque banque ayant sa propre politique); notamment le plafond de la carte. [22]

La classification des codes de retour d'une autorisation est standardisée. Mais, chaque banque peut avoir une interprétation différente de cette classification.

La réponse à la demande d'autorisation est transférée via l'eRSB à l'acquéreur qui la renvoie au prestataire de paiement et au marchand.

Lorsque la transaction est autorisée, le E-Marchand a donc la garantie du transfert effectif des fonds ("capture des fonds") entre la banque émettrice et sa banque acquéreur (quel que soit le solde du compte) si le délai entre la date d'authentification et la capture est inférieur à 13 jours calendaires (hors secteur de la location).

---

[21] cartes contrefaites, perdues, volées, non parvenues etc.

[22] en général, plafond de 1500 € et 300 € de retrait sur sept jours glissants / par mois glissants

D.1.3 Code BIN

Un fichier des BIN est géré directement par les banques acquéreurs, sur la base de classifications de produits fournies par les systèmes cartes.

Il est principalement utilisé par les banques acquéreurs pour vérifier l'acceptabilité de la carte et le système carte, voire le type de programme auquel elle appartient pour permettre son traitement dans les systèmes monétiques.

Un fichier des BIN comporte une centaine de colonnes et plusieurs centaines de milliers de lignes. Il recense des plages de numéro de carte. Il comporte notamment les informations suivantes:

- le type de produit auquel correspond la carte (Business, Electron, Infinite...) ;
- le pays d'origine de la carte ;
- l'identité de la banque émettrice ;
- le système de la carte (CB, Visa, MasterCard, etc).

L'exploitation de ce fichier est relativement limitée dans le cadre de la fraude. Il apporte des éléments d'information parmi d'autres.

A noter, les cartes virtuelles dynamiques ne sont pas identifiables dans le fichier BIN.

D.1.4 Access Control Serveur (ACS)

Ce sont les ACS qui authentifient le porteur de la carte en fonction de règles imposées par la banque. Chaque banque possède son propre ACS. Le socle technique de la plupart des ACS en France a été fourni par Atos Wordline. Atos Wordline gère 80 % des ACS en France.

D.2 PCI DSS[23]

Les mesures PCI s'appliquent à l'ensemble des acteurs de la chaîne d'acceptation et d'acquisition, c'est à dire aux commerçants, aux banques acquéreurs et aux prestataires de service des uns et des autres. Il est en effet fondamental, prévient le GIE CB, que, « *quelle que soit la taille des acteurs concernés (banques, commerçants, prestataires), des investissements adaptés soient consentis dans la sécurisation des données sensibles des transactions par carte. Assurer la confidentialité de ces informations, c'est garantir aux titulaires de cartes CB une protection contre les risques de fraude mais aussi contre les possibles atteintes à la vie privée* ». C'est pourquoi, observe le Groupement, la communauté bancaire et CB partagent les objectifs du référentiel PCI-DSS.

Les mesures dites PCI sont développées par l'organisme « PCI SSC » (Payment Card Industry Security Standard Council), créé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. International. Elles s'appliquent de manière mondiale à l'ensemble des acteurs de la filière d'acceptation et d'acquisition (banques acquéreurs, commerçants, prestataires de service exploitant des plates-formes de paiement, etc.) participant aux systèmes de paiement par carte membres de PCI, à la fois pour les transactions transfrontalières, mais aussi pour les transactions domestiques dans le cas de cartes

[23] Source : Rapport annuel 2009 de l'Observatoire de la sécurité des cartes de paiement

co-badgées avec un système national. Compte tenu de ce champ d'application, ces mesures prennent, de fait, argement le caractère de standards Les mesures PCI visent à lutter contre le détournement des données de carte afin d'éviter leur réutilisation frauduleuse. Plusieurs séries de mesures de sécurité ont été édictées par PCI SSC, parmi lesquelles on retiendra principalement pour les besoins de cette étude les mesures appelées « PCI DSS » (PCI Data Security Standard), qui visent à protéger les données transmises au travers des systèmes d'information de la chaîne d'acquisition du paiement par carte, ou stockées dans ces systèmes :

PCI DSS se compose de 12 types de mesures, réparties en 6 thèmes :

Création et gestion d'un réseau sécurisé

1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes

2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Protection des données des titulaires de cartes

3. Protéger les données de cartes stockées

4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics

Gestion d'un programme d'analyse des vulnérabilités

5. Utiliser des progiciels antivirus et les mettre à jour régulièrement

6. Développer et gérer des systèmes et des applications sécurisés

Mise en œuvre de mesures de contrôle d'accès strictes

7. Restreindre l'accès aux données des titulaires de cartes aux seules personnes qui doivent les connaître

8. Affecter un identifiant unique à chaque utilisateur d'ordinateur

9. Restreindre l'accès physique aux données des titulaires de cartes

Surveillance et test réguliers des réseaux

10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes

11. Tester régulièrement les processus et les systèmes de sécurité Gestion d'une politique de sécurité des informations

12. Gérer une politique de sécurité des informations

La vérification de la mise en œuvre de ces mesures donne lieu à une certification de conformité. Pour ce faire, des audits sont conduits par des organismes spécialisés accrédités par PCI SSC, auprès des commerçants et des prestataires techniques, selon différentes méthodes tenant compte du volume de transactions réalisées. Les modalités de ces audits et de la certification qui en résulte sont propres à chaque système de paiement par carte. A titre d'illustration, pour MasterCard Worldwide, elles se déclinent selon 4 niveaux en fonction de l'importance des acteurs concernés :

– niveau 1 : pour les acteurs gérant plus de 6 millions de transactions cartes par an (tous canaux de commerce confondus) ou ayant déjà subi une compromission, le programme prévoit que l'acteur concerné doit effectuer un audit annuel de sécurité sur site de son système d'information et une analyse trimestrielle des vulnérabilités de son réseau de télécommunication ;

– niveau 2 : les acteurs gérant entre 1 et 6 millions de transactions cartes par an sont tenus de répondre à un questionnaire annuel d'auto-évaluation et de réaliser une analyse trimestrielle des vulnérabilités réseaux ;

– niveau 3 : les acteurs gérant plus de 20 000 transactions cartes en commerce électronique et moins de 1 million de transactions cartes par an au total sont eux aussi tenus de répondre à un questionnaire annuel d'auto-évaluation et de réaliser une analyse trimestrielle des vulnérabilités réseaux ;

– niveau 4 : il est recommandé aux autres acteurs de répondre à un questionnaire annuel d'auto-évaluation établi par PCI SSC et de procéder à un test d'évaluation trimestriel des vulnérabilités du système d'information et du réseau de télécommunication.

On peut enfin remarquer que l'article 3.13 du contrat d'acceptation en paiement à distance sécurisé par cartes CB ou agréées CB (contrat VADS) prévoit que l'accepteur (le commerçant) doit respecter les exigences du référentiel de sécurité PCI DSS jointes en annexe du contrat.

Plus d'informations sur PCI DSS : https://www.pcisecuritystandards.org/ (en français voir https://fr.pcisecuritystandards.org)

D.3 RESSOURCES DOCUMENTAIRES SUR LA LUTTE CONTRE LA FRAUDE ET SON ENCADREMENT REGLEMENTAIRE

Sur le thème de la sécurité, référence doit être faite au **rapport Pauget-Constant « L'avenir des moyens de paiement en France »** de mars 2012, qui relève que la sécurité est, pour les consommateurs, une condition essentielle au développement de nouveaux moyens de paiement (pp. 46 et s.) ; que la sécurité et la garantie de paiement sont les attentes essentielles des commerçants (pp. 50 et s.) et que l'objectif premier des autorités est d'assurer la sécurité des solutions de paiement et la confiance (pp. 56 et s.). Dès lors, parmi les 20 propositions émises pour une stratégie des moyens de paiement en France, apparaît comme premier objectif prioritaire de faciliter les paiements sécurisés en ligne (pp. 94 et s.).

De son côté, l'OSCP a publié le 17 décembre 2012, à l'attention des commerçants, **une brochure sur la sécurité des paiements sur Internet**, qui rappelle les bonnes pratiques en la matière, dont les conditions d'un déploiement réussi de l'authentification renforcée, par laquelle les clients valident leurs paiements par la saisie d'un code unique, généralement transmis par SMS.

La sécurité des paiements en ligne passe aussi par une protection renforcée des données carte (numéro, date de validité, cryptogramme visuel). À cet effet, la CNIL a publié une **délibération n° 03-004 du 19 juin 2003 relative au stockage et à l'utilisation de ces données dans le secteur de la vente à distance**. Elle y reconnait que l'utilisation du numéro de carte bancaire par un professionnel de la vente à distance, dans un fichier ayant pour finalité de lutter contre la fraude au paiement en conservant la trace d'agissements lui ayant porté préjudice, est légitime. Pour autant, les E-Commerçants devraient s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des individus.

Existe par ailleurs le Forum européen SecuRe Pay (Security of Retail Payments), créé en 2011 sous l'égide de la Banque centrale européenne (BCE), dont l'objectif principal est de contribuer à l'harmonisation des mesures de sécurité en Europe. Ses premières recommandations, de janvier 2013 : **"Recommendations for the Security of Internet Payments",** portent en particulier sur des "specific control and security measures for internet payment", dont la principale concerne la nécessité de protéger l'initiation des paiements sur Internet et l'accès aux données sensibles concernant les paiements par une forte authentification du client afin de garantir que l'initiateur d'un paiement est un utilisateur autorisé et non un fraudeur.

Enfin, **la proposition de révision de la directive sur les services de paiement (dir. 2007/695/CE, 13 nov. 2007, dite DSP), publiée le 24 juillet 2013**, fait de la sécurité des paiements électronique l'un de ses objectifs prioritaires : "Payment Services Directive – Innovation and security should go hand in hand" s'est ainsi félicitée l'European Banking Federation (EBF). Cette proposition de DSP 2 invite en particulier les États membres à veiller à ce qu'un prestataire de services de paiement (PSP) applique l'authentification forte du client qui initie une opération de paiement électronique, obligation s'appliquant aussi à un PSP tiers qui initierait une opération de paiement au nom du payeur (art. 87). De manière générale, la promotion d'un marché unique des paiements de détail dans le cadre du SEPA (Single Euro Payment Area) exige la sécurité des systèmes et moyens de paiement. Car l'un des facteurs d'une plus grande intégration du marché est bien « une sécurité de paiement accrue et des clients plus confiants » : « À l'image des progrès réalisés en matière de paiement sécurisé sur les points de vente, un marché intégré augmenterait la sécurité des systèmes de paiement à distance, tels que le e-paiment et le m-paiement, ainsi que la confiance du consommateur à leur égard » (Livre vert,

Vers un marché intégré des paiements par carte, par internet et par téléphone mobile, 11 févr. 2012, p. 3).

Voir aussi :

- Directive sur les Services de Paiement (PSD)
  http://ec.europa.eu/internal_market/payments/framework/index_fr.htm

- Recommandations de la BCE concernant la sécurité des paiements sur internet (Recommandations for the security of internet payments)
  http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- Le rapport de l'OSCP 2013
  http://www.banque-france.fr/observatoire/rap_act_fr_12.htm

- Plaquette « Conseils aux commerçants » (OSCP)
  http://www.banque-france.fr/observatoire/commercants-securite-paiements-internet.htm

- Conseils aux porteurs
  http://www.banque-france.fr/observatoire/conseil.htm

- Signalement à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication : https://www.internet-signalement.gouv.fr/

- Pré-plainte en ligne : https://www.pre-plainte-en-ligne.gouv.fr/ ;

D.4 SECURITE / PAIEMENTS / MONETIQUE : LES ADHERENTS FEVAD

Comme évoqué dans la préface, ce Livre Blanc n'est pas un manuel des techniques de lutte contre la fraude. Ce n'est pas non plus un inventaire des solutions de lutte contre la fraude (il existe excellents ouvrages sur ces sujets).

Ce Livre Blanc est avant tout le ressenti "sur le terrain" de la lutte contre la fraude telle qu'elle est vécue au quotidien par les E-Marchands. C'est pourquoi nous n'avons pas interrogé tous les acteurs du paiement, ni même tous les membres de la Fevad mais principalement des marchands.

Nous publions cependant ici la liste des acteurs du paiement membres de la Fevad qui nous font confiance, soutiennent souvent nos manifestations, nourrissent et accompagnent notre réflexion au cours des nombreux échanges, réunions et rencontres organisées par la Fevad tout au long de l'année.

D.4.1 Réseaux interbancaires

D.4.1.1 AMERICAN EXPRESS PAYMENT SERVICES LIMITED

American Express Company est un groupe international présent dans le voyage et les services financiers. Fondé en 1850, il occupe des positions de premier plan dans les cartes de paiement et de crédit, les chèques de voyage, le voyage et les produits d'assurance. American Express est à la fois un réseau d'acceptation et la première société non bancaire émettrice de cartes de paiement au monde, en termes de nombre de cartes (plus de 102 millions de cartes en circulation et acceptées dans plus de 200 pays) et de montant de dépenses (888 milliards de dollars / chiffres à fin 2012). Les marques prestigieuses avec lesquelles elle a également initié il y a plus de 10 ans des partenariats (Air France 1998) lui confèrent incontestablement une longueur d'avance sur le marché co-branding. www.americanexpress.fr

D.4.1.2 GROUPEMENT DES CARTES BANCAIRES "CB"

CB est un système de paiement et de retrait par carte, interbancaire et universel. CB c'est près de 10 milliards de transactions par an, quelque 130 banques ou établissements de paiement membres, 1,2 million de commerçants en France et plus de 60 millions de porteurs. Le système CB est géré par un Groupement d'Intérêt Economique qui en garantit la fiabilité, l'ergonomie et la sécurité. Il assure quatre missions principales : la vérification de la conformité, la gouvernance et la promotion du système CB, ainsi que le développement de produits et services. Pour l'année 2012, les paiements CB sur internet ont représenté 390 millions de transactions pour un chiffre d'affaires de 34 milliards d'euros. Les paiements e- et m-commerce représentent 9 % de l'ensemble des paiements CB. www.cartes-bancaires.com

D.4.1.3 VISA EUROPE FRANCE

Visa est le système de paiement leader en Europe. En facilitant les paiements, Visa Europe apporte aux consommateurs, aux commerçants, aux banques et à tous les fournisseurs de services plus de rapidité, de sécurité et de simplicité. Visa lancera prochainement V.me by Visa. Ce "portefeuille" permettra aux clients de regrouper plusieurs cartes de paiement dans un seul

portefeuille numérique, afin de procéder à des paiements sécurisés en ligne sans avoir à saisir toutes les données de la carte. V.me offre toutes les mesures de sécurité attendues de la part des réseaux internationaux de cartes de paiement les plus reconnues. La technologie permet de réduire les risques de transactions frauduleuses et le produit offre la même protection pour les commerçants que Verified by Visa. De plus, V.me by Visa dispense le commerçant du contrôle des informations de paiement au cours du processus de commande. En outre, V.me by Visa respecte les exigences PCI-DSS - un ensemble de normes qui accroissent la sécurité des données financières de vos clients.

http://www.visa.fr/ / https://fr.v.me/

D.4.2 Prestataires de solutions de paiement

D.4.2.1 ADYEN

Adyen a conçu une solution de paiement en ligne qui possède une solide expérience notamment sur les points suivant : internationalisation, transformation et sécurité.

Penser international, agir localement : Adyen se connecte à plus de 200 méthodes de paiement pertinentes à travers l'Amérique du Nord, Amérique latine, Europe, Asie-Pacifique et de l'Océanie.

Conversion, des méthodes éprouvées qui fonctionnent : Adyen travaille à l'optimisation des taux de conversion en cherchant à simplifier vos processus de paiement électronique (personnalisation des pages de paiement, One clic, A / B testing …). Enfin, les solutions Adyen offrent une grande souplesse d'intégration en proposant des solutions pour tous les scénarios possibles. www.adyen.com

D.4.2.2 BUYSTER

Buyster est une société Anonyme (SA) à conseil d'administration qui dispose d'un statut d'Etablissement de Paiement accordé par l'Autorité de Contrôle Prudentiel de la Banque de France et d'un capital de 10, 2 Millions d'euros. Buyster est né de la volonté de 4 entreprises françaises d'associer leurs expertises complémentaires au travers d'un partenariat : les trois opérateurs mobiles : Bouygues Telecom, Orange et SFR qui apportent leur expertise télécom et réseau ; Atos, expert en matière de traitement électronique des transactions de paiements sécurisés, dont il est le leader européen. Grâce à une cinématique de paiement mobile unique sur le marché, Buyster est LA solution de paiement adaptée aux nouvelles formes du e-Commerce : mobile, tablettes tactiles, TV connectée … Buyster propose une garantie de paiement qui protège les e-commerçants contre les risques de répudiation, quelle que soit la cinématique (paiement sur ordinateur ou mobile, paiement express). Cette garantie de paiement peut vous être proposée en standard grâce à notre dispositif d'authentification forte et un système de lutte contre la fraude. www.buyster.fr/

D.4.2.3 CARDS OFF SA

Cards Off est un Établissement de Paiement qui sécurise de bout en bout les transactions sur internet grâce à un système unique et breveté, indépendamment des solutions de paiement utilisées par les cyberacheteurs. Cards Off, en tant que tiers certificateur et de confiance, garantit l'ensemble des acteurs (vendeurs, acheteurs transporteurs et banques) de la chaîne e-commerce. La plateforme technique développée par CardsOff permet de sécuriser l'ensemble du processus de vente de bout en bout en permettant de s'affranchir de l'utilisation en ligne des

numéros de carte bancaire. La solution de paiement Cards Off permet tout à la fois de verrouiller, d'accompagner et de fluidifier l'ensemble du processus d'achat en ligne, de la passation de la commande jusqu'à la livraison. www.cardsoff.com

D.4.2.4 FIA-NET

FIA-NET, le leader français des solutions de confiance pour l'e-commerce et de lutte contre la fraude à la carte bancaire sur Internet. FIA-NET propose des services dédiés aux sites e-commerce et aux cyber-consommateurs. Certissim et le Sceau de Confiance FIA-NET apportent aux e-commerçants et aux cyber-acheteurs la confiance nécessaire au développement du e-commerce. Créée en 2000, FIA-NET compte aujourd'hui 1 700 sites marchands clients, 17 millions d'internautes référencés en base et 23 millions de transactions analysées par an. www.fia-net.com

D.4.2.5 LIMONETIK

Limonetik est une plateforme de paiement online spécialisée dans les paiements enrichis et adaptée au top 200 des sites marchands. Son métier : connecter aux sites marchands tous les modes de paiement (cartes cadeaux, prépayées, e-wallet, points de fidélité, chèques papier, …) et rendre possible des paiements mixtes (non bancaire et bancaire).

Limonetik privilégie une approche résolument marketing : proposer des remises sur la page de paiement, ou des applications clef en mains pour recruter ou fidéliser les acheteurs (carte cadeau, couponing, fidélité…). www.limonetik.com

D.4.2.6 LYRA NETWORK / PAYZEN

Lyra Network , opérateur monétique, a constitué un réseau pour l'acheminement et le traitement des flux bancaires en provenance des terminaux de paiement ou d'internet, via une solution s'appuyant sur les infrastructures de plusieurs opérateurs télécoms. Lyra Network a réalisé 45 M Euros de chiffre d'affaires en 2011 et reste le leader de l'acheminement des flux bancaires français en provenance des terminaux de paiement, notamment grâce à la fiabilité technique et la performance de ses solutions. Son réseau lui a permis de traiter en 2011, 100 millions/ mois de paiements à destination des banques et des centres privatifs, soit plus de 40% du marché. PayZen, une marque de Lyra Network, est une solution de paiement en ligne. PayZen est connectée avec de multiples acquéreurs en Europe et en Amérique du sud. www.payzen.com

D.4.2.7 MONEXT / PAYLINE

La vocation de Monext est de faciliter les transactions de paiements électroniques, avec ou sans carte, que ce soit en point de vente, sur Internet ou sur mobile. Chaque jour que cela soit pour payer une heure de parking, prendre les transports en commun, faire le plein d'essence, faire ses courses, acheter en ligne, ou mettre sa carte en opposition, des millions de personnes ont recours à leurs prestations. Monext accompagne les établissements financiers et les commerçants, en France et en Europe, dans l'optimisation de leur chaîne de valeur monétique en leur proposant des solutions sécurisées, fiables et immédiates. www.monext.fr / www.payline.com/

D.4.2.8 NATIXIS PAIEMENTS

Natixis Paiements est un acteur de référence, en France et en Europe, du traitement des opérations de paiement (monétique, opérations de masse et unitaires, chèques…). Natixis Paiements est l'opérateur des métiers de flux et de monétique du Groupe BPCE. Spécialiste des moyens de paiement classiques et monétiques, elle développe des solutions innovantes et performantes de :

- processing (plus de 6,5 Md d'opérations de masse par an, 16 M€ de cartes sous gestion),
- back office (expertise opérations internationales et impayés),
- sécurité des moyens de paiement, marketing opérationnel et accompagnement commercial.

www.natixis.com

D.4.2.9 OGONE SAS

Ogone est l'un des principaux opérateurs internationaux de services de paiement en ligne et mobile. Ses solutions sont utilisées par plus de 42 000 entreprises dans le monde pour gérer, collecter et sécuriser leurs paiements, et se protéger contre la fraude. Bénéficiant d'une connectivité avec plus de 200 banques et acquéreurs sur les cinq continents, la plateforme Ogone permet aujourd'hui de consolider la gestion de plus de 80 moyens de paiement internationaux, locaux ou alternatifs. Ce portefeuille étendu d'options de paiement contribue à améliorer le taux de conversion des commerçants à la fois sur leur marché domestique et à l'international. Au travers de sa filiale Tunz.com, qui dispose d'une licence de monnaie électronique, Ogone est également en mesure de proposer des solutions clé en main de porte-monnaie électronique (e-wallets). Ogone fait partie du Groupe Ingenico, acteur majeur sur le marché des solutions de paiement multicanal (points de vente physique et digitaux). Ogone, dont le siège social est basé en Belgique, est également implanté en France, aux Pays-Bas, en Allemagne, en Autriche, en Suisse, au Royaume-Uni, aux Emirats Arabes Unis, aux Etats-Unis et en Inde. www.ogone.com

D.4.2.10 ONEY

Oney est une marque de Banque Accord, filiale à 100% du groupe Auchan, spécialisée depuis 10 ans dans la distribution de solutions de paiement et de financement multicanal. Oney propose des solutions de paiement et de financement sécurisés, multicanal, multidevice. Oney propose également une solution de lutte contre la fraude liée aux règlements par cartes bancaires en ligne, Sell Secure. www.oney-ecommerce.com

D.4.2.11 PAYPAL

PayPal permet à une entreprise ou un utilisateur disposant d'une adresse email d'envoyer et de recevoir des paiements en ligne de manière pratique, sécurisée et peu coûteuse. Son réseau se base sur l'infrastructure financière existante de comptes et cartes bancaires afin de créer une solution de paiement en temps réel mondiale. PayPal propose un produit parfaitement adapté aux petites sociétés, boutiques en ligne, personnes physiques et autres intervenants pour lesquels les mécanismes de paiement traditionnels ne sont pas suffisants. Il est l'un des principaux réseaux de paiement pour les sites d'enchères en ligne, comme eBay. PayPal est également de plus en plus utilisé sur d'autres sites de commerce électronique, pour la vente de biens comme des objets électroniques ou de l'électroménager, de services comme des voyages ou de la conception de sites, ainsi que pour la vente de contenu numérique. www.paypal.fr

D.4.2.12 PAYBOX SERVICES

Paybox fait partie du groupe Point qui est un fournisseur majeur de solutions de paiement en Europe spécialisé dans les services de paiement aux marchands. Paybox adresse tout type d'entreprise depuis les commerces indépendants de proximité jusqu'aux grandes enseignes internationales requérant des solutions de paiement multi-canal tels que les hotels, restaurants... Depuis 1987, date de sa création, Point se positionne comme un précurseur et un acteur de référence dans son domaine que les autres fournisseurs de paiement suivent. Point est présent dans 11 pays européens. Chaque filiale de Point bénéficie d'experts connaissant parfaitement leur marché local. www.paybox.com

D.4.2.13 RENTABILIWEB / BE2BILL

Depuis 10 ans, Rentabiliweb, spécialiste de la monétisation d'audiences et de contenus, est également expert dans l'édition des sites de divertissement sur Internet. Rentabiliweb est une entreprise cotée en bourse avec un effectif de 200 salariés dans le monde et un chiffre d'affaire de 100 millions d'Euros l'année dernière. A partir de son expérience, Rentabiliweb intègre les problématiques liées au e-commerce en général et celles du paiement en ligne en particulier. Un constat est vite établit : les systèmes de paiement en ligne sont indissociables du marketing et aucun acteur du marché ne répond à ce besoin. Début 2011, Rentabiliweb devient ainsi le premier établissement de paiement agréé par l'Autorité de Contrôle Prudentiel (code banque : 16378 / numéro d'agrément N° 16378C). La société est désormais habilitée par la loi à fournir des services de paiement au sens de l'article L314-1 du code monétaire et financier. En juin de cette même année, coopté par BPCE, Rentabiliweb devient membre du GIE Carte Bancaire, qui regroupe plus de 130 établissements de crédit ou de paiement. Rentabiliweb a alors lancé Be2bill le 23 janvier 2012. www.rentabiliweb-group.com/

D.4.2.14 SKRILL / MONEYBOOKER

Skrill est l'un des plus importants systèmes de paiement en ligne utilisé par plus de 135 000 marchands. Son réseau de paiement s'étend sur plus de 100 options de paiement, comporte 41 devises et couvre 200 pays et territoires. À travers un seul partenaire et une seule connexion, vous pouvez instantanément investir de nouveaux marchés et développer vos affaires.

Skrill comprend que chaque besoin commercial est unique et qu'une taille unique ne convient pas à tous. Qu'il s'agisse d'une simple intégration ou d'une solution sur-mesure, d'options de paiement local ou d'un choix de devises, Skrill vous permet de décider de ce qui vous convient le mieux. La seule caractéristique standard fournie par Skrill est son support technique intégral, ses mesures anti-fraude gratuites et éprouvées et la fiabilité de son service client. www.moneybookers.com

D.4.2.15 SOCIETE GENERALE / Sogenactif

Sogenactif est une solution d'encaissement sécurisée sur Internet conçue en partenariat avec Atos Worldline. Vous pouvez l'intégrer à votre site Internet qu'il soit déjà opérationnel ou en cours de construction. Sogenactif comprend le raccordement à une plate-forme technique sécurisée pour l'enregistrement du paiement en ligne, l'accès à une interface de back office, Sogenactif Gestion ainsi que le contrat monétique commerçant pour la comptabilisation des transactions et le crédit en compte.

www.sogenactif.com

D.4.2.16 WORLDLINE

Worldline, une filiale d'Atos, est le leader européen et un acteur mondial de référence dans le secteur des paiements et des services transactionnels. Worldline met en place des services nouvelle génération, permettant à ses clients d'offrir au consommateur final des solutions innovantes et fluides. Acteur clef du B2B2C, riche de 40 ans d'expérience, Worldline est idéalement placé pour servir et contribuer au succès de toutes les entreprises et administrations, dans un marché en perpétuelle évolution. Worldline propose un Business Model unique et flexible, construit autour d'un portefeuille d'offres évolutif et global permettant une prise en charge end-to-end. Les activités de Worldline sont organisées autour de trois axes : Merchant Services & Terminals, Mobility & eTransactional Services, Financial Processing Services & Software Licensing. En 2012, les activités de Worldline au sein du groupe Atos ont généré un revenu (pro-forma) de 1,1 milliard d'euros. L'entreprise emploie plus de 7 100 collaborateurs dans le monde entier. http://worldline.com/fr/

D.4.3 Autres prestataires

D.4.3.1 CYBERSOURCE FRANCE SAS

CyberSource assiste les omni-commerçants, qui distribuent leurs produits et services via plusieurs canaux, dans la gestion du cycle de vie de leurs paiements, depuis le traitement jusqu'à la détection pertinente des comportements frauduleux et l'optimisation des processus d'évaluation des commandes à risque. Plus de 370.000 marchands font confiance à CyberSource à travers le monde. Créée en 1994, CyberSource emploie 1100 salariés dans ses différentes implantations et est filiale à 100 % de Visa Inc. www.cybersource.fr

D.4.3.2 RETAIL DECISIONS EUROPE LIMITED

ReD fournit des solutions de lutte contre la fraude pour tous les types de transaction de paiement. Red est présents dans toutes les parties de la chaîne de paiements, en collaboration avec les commerçants, les émetteurs, les acquéreurs, les PSP, les processeurs. Sa clientèle comprend 300 sociétés de premier ordre dans les industries suivantes : banque, commerce de détail, voyage, télécommunication, jeux, pétrole et bien d'autres secteurs. ReD a protégé plus de 17 milliards de transactions en 2011 et a recueilli des données provenant de plus de 190 pays, sur six continents. Red est implanté en Amérique du Nord, en Europe, au Moyen-Orient et en Afrique, en Amérique latine et en Asie Pacifique. ReD travaille en étroite collaboration avec des partenaires mondiaux, régionaux et locaux. www.redworldwide.com/emea/francais

D.4.3.3 VERIZON

www.verizonbusiness.com/fr

Verizon est leader mondial pour les solutions destinées à transformer le business des entreprises et des administrations. Verizon associe à ses solutions de communications et solutions informatiques intégrées, et à l'expertise de services professionnels, des réseaux IP et mobiles hautement intelligents pour permettre aux entreprises d'accéder à leurs informations, de partager des contenus et de communiquer, en toute sécurité. Verizon intervient notamment dans la mise en conformité du standard PCI DSS, la gestion des programmes de sécurité, l'évaluation et l'analyse des failles …

D.5 LES OFFRE "3 EN 1" : EXEMPLE DE BE2BILL

Comme vu au chapitre B.5.3.4, certains nouveaux acteurs comme Be2bill (Rentabiliweb) proposent des offres combinant trois types de prestations : prestation d'établissement de paiement acquéreur, de solutions de paiement et prestations d'agence web.

Be2bill décrit ce qui fait, selon lui, l'intérêt de ce type d'offre pour le E-Marchand.

Le statut combiné d'établissement acquéreur et de prestataire technique permet à Be2bill d'accéder aux données du système interbancaire, telles les mises en opposition de cartes, ou encore au cheminement des flux monétiques. L'exploitation de ces informations se fait au cœur de l'outil de paiement à travers le paramétrage et le scoring d'un moteur de filtres. Au final, c'est une solution pertinente de lutte contre la fraude qui est mise en place.

En choisissant une formule intégrée, le marchand gagne un temps précieux. Be2bill souligne que le fait de récupérer des informations de sa banque acquéreur constitue une vraie difficulté pour le marchand.

Pour Be2bill, les banques traditionnelles sont moins agiles dans la culture de l'analyse des données Leur réactivité essentielle dans la lutte contre la fraude sur Internet, peut en souffrir. Be2bill résume ainsi ce constat : « Notre service se différencie de celui des banquiers en fournissant, entre autre, un service d'analyse de la data, ce qui est capital aujourd'hui pour gérer la fraudes et optimiser la conversion. »

A leur décharge, les banques sont limitées dans l'exploitation des données de leurs clients parce qu'elles sont soumises au secret bancaire auquel leurs clients sont très attachés ! Ce qui ne veut pas dire que les banques n'ont pas d'outils adéquats pour lutter contre la fraude.

Déclenchement des demandes d'autorisation "à bon escient"

La combinaison et l'exploitation des données obtenues par son double statut PSP et établissement qu'acquéreur et de prestataire de solutions de paiement permet à Be2bill de filtrer en temps réel les transactions suspectées d'être frauduleuses (sur la base de schémas de fraudes connus, de la blacklist du marchand, des données des cartes en opposition remontées par les réseaux interbancaires). Les bénéfices pour le marchand sont multiples:

- d'un point de vue économique : le marchand économise le coût des demandes d'autorisations non abouties.
- d'un point de vue opérationnel : détecter très en amont une vente frauduleuse permet au marchand de ne pas réserver la marchandise pour une commande qui s'avérera frauduleuse. 98,5% de la fraude est bloquée en temps réel.
- pour les E- commerçants confrontés à des taux de fraude élevés, maîtriser la sinistralité devient indispensable pour réduire le coût des impayés et éviter d'atteindre un seuil d'alerte avec les réseaux (Visa / Mastercard), qui pourrait conduire à des pénalités financières de la part de ces derniers.
- Cela permet enfin d'éviter les bien-connus « faux positifs » afin de continuellement tendre vers l'objectif attendu de tous : 100% de Fraudes contrecarrées et 0% de faux positifs.

Le filtre évolutif et dynamique mis en œuvre par Be2bill peut :

- déclencher une demande d'authentification 3D Secure (sur le mode d'un 3D Secure sélectif) ;
- refuser une transaction (analysée comme frauduleuse) ;
- gérer des exceptions pour optimiser certains filtres reconnus efficaces pour lutter contre la fraude et dont les faux positifs sont identifiés et anticipés ;

- refuser et "*blacklister*" les éléments constitutifs d'une transaction frauduleuse.

L'objectif de Be2bill est d'exploiter les data pour comprendre l'évolution du trafic du marchand et utiliser les outils appropriés pour gérer les anomalies en temps réel.

Enfin, l'agence web et la plus grande souplesse pour « charter » le tunnel de commande, peut apporter des résultats significatifs sur le taux de transformation.

D.6 ADRESSES UTILES

D.6.1.1 Le monde bancaire

Observatoire de la Sécurité des Cartes de Paiement (OSCP)

L'Observatoire de la sécurité des cartes de paiement a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. Les dispositions légales relatives à l'Observatoire figurent à l'article L.141-4 du Code monétaire et financier. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) par le bon fonctionnement des systèmes de paiement par carte. L'OSCP publie tous les ans un rapport son rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'Économie et des Finances et transmis au Parlement. Il comprenait cette année :

- un état des lieux de la sécurisation des paiements par carte sur Internet (1re partie) ;
- une présentation des statistiques de fraude pour 2012 (2e partie) ;
- une synthèse des travaux conduits en matière de veille technologique (3e partie), avec deux études : une sur la sécurité des paiements par carte sans contact et l'autre sur les techniques de fraude visant les transactions par carte ;
- une étude sur les évolutions réglementaires et les recommandations en Europe et à l'international sur la sécurité des cartes de paiement (4e partie).

La Fevad participe activement aux travaux de l'observatoire.
http://www.banque-france.fr/observatoire/home.htm

Groupement Cartes Bancaires (CB)

CB est un Groupement d'Intérêt Economique (GIE) qui regroupe près de 130 établissements de crédit ou de paiement. Il assure quatre missions principales : la vérification de la conformité, la gouvernance et la promotion du système CB, ainsi que le développement de produits et services.

Le fondement majeur du système CB est l'interbancarité. Il s'agit de l'écosystème qui permet à la carte CB d'être acceptée quelle que soit l'enseigne de la banque du commerçant et celle du client.

L'acceptent : plus de 1.150.000 magasins de proximité, 160.000 automates, 140.000 paiements en Vente à Distance dont 47% sur internet, et 50.000 distributeurs automatiques de billets.

Cette même carte, selon ses fonctionnalités, pourra aussi être utilisée partout à travers le monde grâce aux partenariats que le système CB a noués avec des systèmes internationaux. À l'étranger le porteur d'une carte CB co-badgée avec un système international partenaire peut retirer de l'argent sur près de 2 millions de DAB et peut également l'utiliser chez plusieurs dizaines de millions de commerçants.

Cette universalité du paiement par carte implique pour CB d'être toujours en mouvement et de coller au plus près des nouveaux usages et des nouvelles technologies, voire de les initier. Ainsi la carte CB a largement contribué au développement du commerce en ligne et représente aujourd'hui plus de 80% des transactions de paiements sur internet. (source : Rapport d'Activité 2012 Du Groupement des Cartes Bancaires CB) / http://www.cartes-bancaires.com/

D.6.1.2 Les forces de police et de gendarmerie

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)

L'OCLCTIC est chargé :

- d'animer et coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication ;
- de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigations ;
- d'apporter, à leur demande, une assistance aux services de police, de gendarmerie et de douane en cas d'infractions liées aux hautes technologies ;
- d'intervenir d'initiative, avec l'accord de l'autorité judiciaire saisie, pour s'informer sur place des faits relatifs aux investigations conduites ;
- de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs.

Grâce aux connaissances spécialisées de ses fonctionnaires, l'OCLCTIC apporte son soutien technique aux enquêteurs en charge des perquisitions informatiques. L'OCLCTIC traite les affaires judiciaires qui concernent plus spécifiquement les atteintes aux systèmes de traitements automatisés de données, les fraudes aux télécommunications, les fraudes aux cartes de paiement et à microprocesseurs, ainsi que toutes les formes de criminalité qui utilisent les nouvelles technologies. On peut citer les piratages informatiques, le phishing et les autres formes de captation de données bancaires sur internet, le piratage des distributeurs de billets ou de carburant.

Son domaine d'action comprend également la lutte contre les atteintes aux systèmes d'information gouvernementaux ou de sociétés sensibles économiquement ou techniquement.

En fonction des nécessités, l'office peut effectuer une surveillance active des réseaux (site web, forum de discussions...) et procéder à toute vérification utile ainsi qu'à la localisation de serveurs.

http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Office-central-de-lutte-contre-la-criminalite-liee-aux-technologies-de-l-information-et-de-la-communication

La brigade d'enquêtes sur les fraudes aux technologies de l'information

Elucider les crimes et délits informatiques, voilà la mission dévolue à la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI). Zoom sur cette unité de la police judiciaire.

Créée en février 1994, la BEFTI compte aujourd'hui 25 policiers spécialisés dans les nouvelles technologies. Elle est composée de trois groupes « enquêtes et initiative » et d'un groupe d' « assistance ».

Les investigations des groupes d'enquêtes portent sur les crimes et délits informatiques :

- intrusion dans un ordinateur ou un réseau ;
- contrefaçon de logiciels ou de bases de données ;
- téléchargements illégaux ;
- piratage de réseau téléphonique ;
- défiguration de sites sensibles ;
- modification ou suppression de données ;
- défaut de sécurisation des données personnelles,
- collectes frauduleuses, illicites ou déloyales de données à caractère personnel.

http://www.prefecturedepolice.interieur.gouv.fr/La-prefecture-de-police/Missions-de-police/La-direction-regionale-de-la-police-judiciaire/La-brigade-d-enquetes-sur-les-fraudes-aux-technologies-de-l-information

L'Institut de recherche criminelle de la gendarmerie nationale (IRCGN)

La gendarmerie nationale s'est engagée résolument ces dernières années, dans la lutte contre les nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Cette nouvelle typologie de crimes et de délits a nécessité la mise en place aux niveaux central et territorial de formations et de moyens spécifiques.

La réussite de la montée en puissance de ces unités conditionne grandement la capacité générale de la gendarmerie, en matière de cybercriminalité, à remplir avec efficacité et synergie sa mission à tous les échelons, tant au niveau central qu'au niveau de la chaîne territoriale

http://www.gendarmerie.interieur.gouv.fr/fre/Sites/Gendarmerie/Presentation/PJ/Cybercriminalite

D.6.1.3 Les associations

Merchant Risk Council (MRC)

Le MRC est l'organisation mondiale phare qui soutient et préconise l'excellence opérationnelle auprès des professionnels de la fraude, des paiements, de la sécurité et des risques dans le secteur du commerce en ligne. L'organisation compte dans ses rangs quelque 400 commerçants parmi les principales sociétés de commerce en ligne au monde et plus de 50 prestataires de solutions leaders dans leur catégorie. Les membres du MRC déclarent 45 % de pertes de chiffre d'affaires imputables à la fraude de moins que les non-membres. Ils réalisent 50 % d'examens manuels en moins que leurs homologues non affiliés au MRC et comptabilisent 50 % de refacturations en moins liées à des fraudes. Le MRC soutient et félicite les associations leader comme la Fevad dans leurs travaux nationaux comme ce livre blanc publié par la FEVAD.

Contact : linda@merchantriskcouncil.org
https://www.merchantriskcouncil.org/Pages/home.aspx

Fédération Bancaire Française (FFB)

La Fédération bancaire française (FBF) est l'organisation professionnelle qui représente toutes les banques installées en France. Elle compte 390 entreprises bancaires adhérentes de toutes origines (commerciales, coopératives ou mutualistes), françaises ou étrangères. Elle a pour mission de promouvoir, dans l'intérêt de ses membres, l'activité bancaire et financière aux niveaux français, européen (la FBF a une implantation à Bruxelles) et international, et de définir les positions, propositions ou préoccupations de la profession vis-à-vis des pouvoirs publics et des autorités du domaine économique et financier.

Elle est également l'intermédiaire entre la profession bancaire et tous les publics de la banque : monde politique et institutionnel, médias, consommateurs, associations professionnelles, enseignants,... La FBF a aussi pour mission d'informer les banques adhérentes de l'actualité de la profession et des évolutions réglementaires, et répondre à toute question relative à leurs activités. / http://www.fbf.fr/

www.fevad.com

fédération e-commerce et vente à distance

60 rue La Boétie - 75008 Paris
tél. 01 42 56 38 86 - contact@Fevad.com

Fevad - siret 784 854 994 00034 - crédits photos : Shutterstock; Fevad - création : Zapping 06 42 79 09 12