

Le Forum des droits
sur l'internet

Les paiements sur l'internet

**Deuxième rapport de
l'Observatoire de la
Cyber-Consommation**

Introduction.....	3
I – Le paiement par carte bancaire sur l’internet : de multiples procédés garantissant une protection à l’acheteur.....	5
A – Un consommateur protégé face à des risques identifiés et jugulés	5
1 – L’inexistence du piratage de la carte bancaire sur l’internet.	5
2 – Les protections élaborées afin de rassurer le client et lutter contre la fraude	7
B – Les conséquences des mesures de sécurisation du processus de paiement en ligne	12
1 – La réalité de la fraude à la carte bancaire sur l’internet	13
2 – La nécessaire participation du cyber-consommateur à la protection de son environnement numérique	13
3 – Les difficultés rencontrées par les acteurs marchands dans le secteur du paiement en ligne	16
II – Le micro-paiement et le porte-monnaie électroniques : deux outils alternatifs dédiés au paiement de petites sommes.....	22
A – Les outils existants en matière de paiement de petites sommes	23
1 – Le recours à des numéros à revenus partagés	23
2 – Le porte-monnaie électronique	26
3 – Le paiement par courrier électronique	29
4 – Le paiement à partir d’outils physiques.....	30
5 – Le rétro-paiement : le « <i>cash-back</i> ».....	31
B – Les difficultés pratiques rencontrées par les consommateurs et les acteurs du paiement de petites sommes	32
1 – L’escroquerie au <i>dialer</i>	33
2 – L’information du consommateur lors d’achats de biens immatériels par mobile ou de l’obtention de codes d’accès.....	34
3 – L’éclatement du secteur du micro-paiement	35
4 – La difficile compréhension du dispositif bancaire français.....	35
Conclusion.....	37
Annexe 1 :.....
Composition de l’Observatoire de la Cyber-Consommation	38
Annexe 2 :.....
Liste des personnes auditionnées ou consultées.....	39
Annexe 3 :.....
Rapport d’activité de l’Observatoire permanent de la Cyber-Consommation .	41

Introduction

L'année 2004 a encore constitué une année de forte progression du commerce électronique. Selon le baromètre de la FEVAD (Fédération des entreprises de vente à distance) publié le 20 janvier 2005¹, les ventes en ligne ont augmenté de plus de 53% par rapport à l'année précédente. L'ACSEL (Association pour le commerce et les services en ligne), quant à elle, indiquait en février 2005² une hausse de 65% du chiffre d'affaire du commerce électronique français pendant la même période, ce dernier ayant dépassé le seuil symbolique des 2 milliards d'euros. Le panier moyen de l'internaute se situe aujourd'hui autour de 54 euros, celui-ci achetant de plus en plus régulièrement.

Dans un tel contexte, la question du paiement sur l'internet est primordiale à la fois pour l'acheteur et le vendeur. D'une part, le consommateur a besoin d'être rassuré face à l'usage d'outils informatique et technique qu'il ne maîtrise pas forcément. D'autre part, le professionnel a besoin de solutions de paiement efficaces, rapides et fiables permettant au consommateur de réaliser de la manière la plus fluide possible son acte d'achat.

Cette angoisse de l'acheteur se reflète parfaitement dans les divers chiffres publiés. Ainsi selon une étude menée par le Credoc³, pour 32% des Français interrogés, la sécurité des paiements sur l'internet ne semble pas assurée. En 2001, 48% des personnes interrogées et 44% en 2003 exprimaient cette crainte⁴. Si la peur de donner son numéro de carte bancaire ne constitue pas le premier obstacle des Français à l'achat en ligne, elle demeure en quatrième place derrière l'absence de connaissance de l'enseigne (77%), l'absence de contact avec le produit (73%) ou de conseils de la part du vendeur (65%).

Néanmoins, une fois le pas franchi, le taux d'usage des cartes de paiement est particulièrement important. Selon la FEVAD, 80% des achats sont payés par ce moyen (carte bancaire ou carte privative), 14% par chèque, 5% par prélèvement, virement ou mandat et seulement 1% par des mécanismes de contre-remboursement ou de paiement à la livraison.

*
* *

C'est la problématique des paiements que l'Observatoire permanent de la Cyber-Consommation, créé en septembre 2003 dans le but d'assurer une veille sur les nouveaux enjeux de la cyber-consommation, a souhaité étudier dans son présent rapport. Celui-ci se concentre sur la question des paiements en ligne prise dans son acception la plus large possible et non pas simplement dans sa seule définition juridique d'extinction d'une créance. Le rapport n'a pas examiné les problématiques liées la non-acceptation du paiement en numéraire pour des contrats conclus en ligne⁵.

Composé d'experts indépendants⁶, l'Observatoire a opéré son analyse à l'aide de deux outils complémentaires. Tout d'abord, un appel à témoignages a été mis en place et son contenu est accessible – de manière permanente – sur le site du Forum des droits sur l'internet. Il est destiné à collecter les expériences, les pratiques voire les craintes des internautes en matière de commerce électronique.

Ensuite, les membres de l'Observatoire ont procédé à l'audition de plus de quarante acteurs du paiement en ligne : institutions publiques, associations de consommateurs, banques, intermédiaires techniques et prestataires financiers⁷. En particulier, et en raison du caractère à la fois technique et évolutif de ce secteur, de très nombreux prestataires ont été entendus.

Les conclusions de l'Observatoire sont plutôt rassurantes. En effet, il apparaît que de multiples techniques permettant de protéger le consommateur ont été mises en œuvre dans le secteur du paiement par carte bancaire sur l'internet. Parallèlement, de multiples solutions alternatives se sont développées, particulièrement dédiées au paiement de petites sommes

⁶ La composition de l'Observatoire est disponible en annexe.

⁷ La liste des personnes auditionnées est disponible en annexe.

I – Le paiement par carte bancaire sur l'internet : de multiples procédés garantissant une protection à l'acheteur

Avec plus de 80% des paiements⁸, la carte bancaire demeure l'outil le plus utilisé sur la toile mondiale en matière d'achats en ligne. Il convient de ne pas confondre le terme générique de carte bancaire avec celui de la carte bleue. En effet, la carte bleue est le nom commercial adopté en France par la société responsable de l'émission de produits Visa et de l'adaptation de ceux-ci au réseau français. La carte bancaire estampillée « carte bleue » demeure le leader du marché en France où elle se trouve en concurrence avec les réseaux d'EuroCard et Mastercard.

A – Un consommateur protégé face à des risques identifiés et jugulés

Les chiffres le montrent : pour 32% des internautes, les craintes en matière de sécurité des paiements sur l'internet constituent, encore aujourd'hui, un obstacle à l'achat en ligne. De nombreux particuliers vivent encore avec cette angoisse lors de la saisie de leur numéro de carte bancaire sur un site marchand, même si ce chiffre a atteint en 2004 son plus bas niveau.

Cette peur exprimée par les internautes constitue l'une des réactions à la méconnaissance du réseau mondial, celui-ci pouvant être parfois perçu comme un « trou noir » au sein duquel ils seraient absorbés.

A travers l'audition de nombreux acteurs par les membres de l'Observatoire mais également grâce aux contributions reçues, les conclusions suivantes ont pu être tirées.

1 – L'inexistence du piratage de la carte bancaire sur l'internet.

Trois grandes familles de craintes ont pu être déterminées : le détournement du numéro de carte bancaire à l'occasion d'une transaction en ligne, la génération automatique d'un numéro et la récupération d'un numéro de carte dans la vie courante. Dans les trois cas, l'inquiétude principale des porteurs d'une carte est celle du risque financier : celui d'être victimes de retraits intempestifs sur leur compte bancaire leur causant ainsi un dommage financier.

a) Le mythe du détournement du numéro de carte bancaire lors d'un achat en ligne

Premier risque perçu par l'internaute lors de son achat en ligne, la peur du détournement du numéro de carte bancaire est liée à la nature même de l'achat sur l'internet. Dès lors que l'internaute ne maîtrise pas matériellement la réalisation de la transaction, il peut légitimement s'interroger sur le risque d'utilisation frauduleuse de son numéro après son achat.

Cette crainte pourrait s'exprimer ainsi : un internaute donne son numéro de carte bancaire dans un espace sécurisé du site marchand lors de la passation d'une commande, valide le formulaire, et voit son numéro être intercepté puis utilisé par un « pirate ».

L'ensemble des auditions menées par l'Observatoire confirme cependant qu'aucune interception d'un numéro de carte bancaire, à l'occasion d'un achat en ligne sur un site marchand doté d'un espace sécurité, n'a eu lieu en France. En effet, ni les cyber-

⁸ FEVAD, Chiffres clés de la vente à distance et du e-commerce, année 2004.

marchands, ni les banques, les autorités bancaires ou les services de police judiciaire n'ont fait part de la survenance de tels faits.

Ceci s'explique par deux éléments cumulatifs. D'une part, dans le schéma de paiement en ligne institué en France, le cyber-marchand ne conserve que dans de très rares occasions (cas des paiements récurrents par exemple, enregistrement d'un profil pour réaliser des achats en un clic, etc.) le numéro de carte bancaire ayant servi à la transaction. D'autre part, le mécanisme de cryptage mis en place autour des espaces de paiement en ligne demeure très difficilement contournable.

En conséquence, la **Crainte des internautes de voir leur numéro piraté lors d'un achat sur l'internet n'est pas fondée**. Bien évidemment, le consommateur devra respecter certaines précautions comme toujours s'assurer que son numéro de carte bancaire lui est demandé au sein d'un espace sécurisé (l'adresse du site commence alors par https au lieu de http).

Autre conseil, l'internaute devra veiller à toujours bien sélectionner son vendeur. En effet, toutes les techniques de protection, actuellement mises en place, n'empêcheront pas un escroc d'obtenir un numéro de carte bancaire du consommateur lui-même. Ainsi, des cyber-acheteurs peuvent être tentés, face à des prix relativement faibles, de passer une commande sur un site non fiable et ainsi de communiquer à un tiers son numéro de carte bancaire. Par ailleurs, et nous le verrons ci-après, certaines techniques d'escroquerie (*phishing*) recourent à l'envoi de courriers électroniques destinés à tromper le consommateur et à obtenir directement de lui ses données bancaires

b) La crainte du générateur automatique des numéros de carte bancaire

La génération automatique d'un numéro de carte bancaire est un type de fraude indépendant de l'internet ; nul besoin en effet pour l'internaute d'être cyber-acheteur pour la rencontrer.

Cette fraude repose sur des outils informatiques qui créent, à la demande et de manière totalement aléatoire, des numéros de carte bancaire qui s'avèrent par la suite être associés à des comptes bancaires existants, lesquels seront débités des transactions réalisées avec ces numéros.

Même si ce risque n'est pas lié à l'achat en ligne, les internautes – non spécialistes du secteur des nouvelles technologies – font l'amalgame et associent ce phénomène à l'internet.

En tout état de cause, il est apparu clairement lors des auditions que ce phénomène demeure marginal. Par ailleurs, les protections mises en œuvre par les acteurs du secteur du paiement en ligne, et décrites ci-après, permettent de juguler les risques engendrés par cette pratique délictueuse. Enfin, l'internaute victime d'une telle fraude conserve la possibilité d'obtenir le remboursement des sommes indûment prélevées.

c) La récupération d'un numéro de carte bancaire lors d'un paiement de proximité

Dès lors que le numéro de carte bancaire ne peut être intercepté lors d'une transaction en ligne, comment les escrocs peuvent-ils se procurer de telles informations ? A cette interrogation, de nombreux acteurs pointent du doigt une faille existante : le paiement de proximité. En effet, à l'occasion d'un paiement par carte bancaire dans le monde physique, le porteur se voit remettre par le marchand un récépissé (facturette) sur lequel figurait, auparavant, le numéro complet de la carte. Suite au travail mené par le GIE

Cartes bancaires, l'ACSEL et la FEVAD – ce numéro n'est plus inscrit sur le reçu délivré au client depuis le 31 décembre 2001⁹.

Seulement, il demeure inscrit sur les récépissés conservés par le vendeur. En effet, cela peut lui permettre – en cas de problème informatique – de pouvoir ressaisir manuellement l'ensemble des transactions réalisées par carte bancaire. La conservation d'un tel document, sans protection supplémentaire, constitue l'une des causes de récupération d'un numéro de carte bancaire. De même, on retrouve cette faiblesse en matière d'achat par téléphone, le numéro de la carte bancaire étant confié par le consommateur lui-même à un opérateur sans avoir la garantie que ce numéro ne sera pas utilisé à d'autres fins.

Des enquêtes judiciaires ont ainsi démontré que des escrocs avaient collecté de telles informations dans certains commerces (magasins informatiques par exemple, stations services), réalisant eux-mêmes la copie de l'information ou l'obtenant d'un complice.

Face à un tel problème, de nombreux acteurs ont émis le souhait que soit lancée **une réflexion** entre acteurs du monde de l'internet, du monde physique et du milieu bancaire **pour parvenir progressivement à l'effacement du numéro de carte bancaire de tout support physique et en particulier du récépissé conservé par le vendeur.**

Cette récupération peut également prendre d'autres formes. Ainsi, un internaute a confié à l'Observatoire avoir vu son numéro être récupéré à la suite d'un achat réalisé dans un magasin par un vendeur qui s'est absenté quelques secondes avec la carte bancaire pour en réaliser une photographie.

Dans ces situations, il revient au consommateur de toujours surveiller sa carte bancaire en France ou à l'étranger. A ce titre, on peut relever l'action de sensibilisation menée par les autorités australiennes¹⁰ à destination de leurs ressortissants. Parmi les nombreux conseils qu'elles ont avancés, on relève qu'elles invitent à ne jamais laisser un serveur emporter la carte bancaire lors du paiement de l'addition dans un restaurant.

Des actions identiques de sensibilisation pourraient être menées en France par les pouvoirs publics en complément de celles menées par les banques, tout en prenant soin de ne pas effrayer les consommateurs dans l'utilisation quotidienne de leur carte bancaire.

2 – Les protections élaborées afin de rassurer le client et lutter contre la fraude

Face à ces risques et interrogations, les pouvoirs publics, le secteur bancaire et les acteurs de l'internet ont apporté progressivement des réponses aux internautes leur permettant, d'une part, de pouvoir procéder à un achat sur l'internet sans crainte et d'autre part, d'être garantis en cas de fraude.

⁹ Cette mesure a été prise à la suite d'un protocole d'accord signé entre ces trois acteurs le 10 juillet 2001. Elle faisait suite notamment à un avis du Conseil national de la consommation du 23 mai 2001 sur la sécurité des cartes de paiement, *BOCCRF*, 22 juin 2001, http://www.finances.gouv.fr/DGCCRF/boccrf/01_07/a0070005.htm

¹⁰ « NSW Police launches credit card fraud ad campaign », *SMH.com.au*, 25 novembre 2004
<http://www.smh.com.au/news/Business/NSW-Police-launches-credit-card-fraud-ad-campaign/2004/11/24/1101219611189.html>

a) L'indemnisation du consommateur en cas de fraude

Parallèlement au droit communautaire¹¹, le législateur français a, tout d'abord, souhaité renforcer la protection du consommateur en cas de fraude à la carte bancaire. Ainsi, la loi du 15 novembre 2001 sur la sécurité quotidienne a modifié le Code monétaire et financier en créant un mécanisme de remboursement du titulaire de la carte en cas d'utilisation frauduleuse de son numéro, à distance et sans utilisation physique de sa carte¹².

Pour obtenir le remboursement du débit frauduleux et des éventuels frais bancaires que l'opération a pu engendrer¹³, le consommateur doit contester, par écrit, le prélèvement auprès de sa banque, dans le délai de 70 jours qui suit l'opération, voire 120 jours si le contrat le liant à celle-ci le prévoit¹⁴. La banque sera ensuite tenue de procéder au crédit du compte dans un délai d'un mois qui suit la réception de la contestation¹⁵.

b) La mise en place du SSL contre l'interception du numéro

La première mesure technique mise en place a été de procéder à la généralisation du protocole SSL en matière de transaction bancaire. Le SSL (*Secure Socket Layer*) est un protocole développé par Netscape en 1996, puis adopté progressivement par l'ensemble des acteurs en matière de sécurisation des transmissions de données sur la toile mondiale. Cette mesure de sécurité repose sur trois leviers : l'authentification, le cryptage et l'intégrité des données.

Concernant l'authentification, un certificat numérique est associé à un nom de domaine déterminé. Ce certificat est attribué après la réalisation – par un organisme indépendant – d'un certain nombre de vérifications, notamment sur l'identité du demandeur. Ce certificat doit ainsi permettre de garantir aux internautes la « légitimité » du site avec lequel ils souhaitent contracter.

¹¹ Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, JOCE L 144 du 4 juin 1997, p. 19. Son article 8 précise, en effet, que « *Les États membres veillent à ce que des mesures appropriées existent pour que le consommateur: 1°) puisse demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte de paiement dans le cadre de contrats à distance couverts par la présente directive, 2°) en cas d'utilisation frauduleuse, soit recrédité des sommes versées en paiement ou se les voie restituées* ». Cette disposition a été confirmée par la directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, JOCE L 271 du 9 octobre 2002, p. 16

<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2002:271:0016:0024:FR:PDF>

Voir également, Etudes de législation comparée du Sénat, « La sécurité des transactions réalisées par carte bancaire », octobre 2003

<http://www.senat.fr/lc/lc125/lc125.html>.

¹² Article L. 132-2 du Code monétaire et financier : « *Il ne peut être fait opposition au paiement qu'en cas de perte, de vol ou d'utilisation frauduleuse de la carte ou des données liées à son utilisation, de redressement ou de liquidation judiciaires du bénéficiaire* » ; Article L. 132-4, al. 1 du même code : « *La responsabilité du titulaire d'une carte mentionnée à l'article L. 132-1 n'est pas engagée si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de sa carte* ».

¹³ Article L. 132-5 du Code monétaire et financier : « *En cas d'utilisation frauduleuse d'une carte mentionnée à l'article L. 132-1, l'émetteur de la carte rembourse à son titulaire la totalité des frais bancaires qu'il a supportés* ».

¹⁴ Article L. 132-6 du Code monétaire et financier : « *Le délai légal pendant lequel le titulaire d'une carte de paiement ou de retrait a la possibilité de déposer une réclamation est fixé à soixante-dix jours à compter de la date de l'opération contestée. Il peut être prolongé contractuellement, sans pouvoir dépasser cent vingt jours à compter de l'opération contestée* ».

¹⁵ Article L. 132-4, al. 3 du Code monétaire et financier : « *Dans les cas prévus aux deux alinéas précédents, si le titulaire de la carte conteste par écrit avoir effectué un paiement ou un retrait, les sommes contestées lui sont recréditées sur son compte par l'émetteur de la carte ou restituées, sans frais, au plus tard dans le délai d'un mois à compter de la réception de la contestation* ».

Le cryptage consiste à rendre incompréhensible à toute personne les données saisies ou envoyées depuis une page donnée. En pratique, le SSL est destiné à crypter et à signer les informations transmises via le protocole « https ».

Enfin, concernant l'intégrité des données, une fois qu'une connexion à une page SSL est réalisée, le contenu de toutes les communications envoyées vers le serveur de la banque est protégé de toute manipulation.

Ainsi, lorsque l'internaute accède au formulaire de saisie de son numéro de carte bancaire dans un espace sécurisé, il se situe dans un environnement où l'interception de son numéro demeure impossible.

c) L'effacement total ou partiel du numéro de carte bancaire lors d'un achat en ligne

Outre le renforcement de la sécurité de la transaction au niveau du site marchand, d'autres solutions ont également été élaborées, principalement sous l'impulsion du milieu bancaire, tendant à éviter la circulation du numéro de carte bancaire réelle lors de la passation de la commande sur l'internet¹⁶.

➤ La création d'un « numéro virtuel de carte bancaire », la e-Carte Bleue

La e-Carte Bleue permet au consommateur, après inscription à ce service, de créer en temps réel un nouveau numéro de carte bancaire à chacune de ses transactions. Ce e-numéro est valable pour un montant déterminé par le porteur et est désactivé une fois utilisé. Elle se positionne comme un outil de protection du consommateur à double titre : elle évite toute réutilisation du numéro en cas d'interception et elle permet au client de ne pas subir de surfacturation.

Lancée en avril 2002, elle est aujourd'hui proposée aux clients de certaines banques françaises (Société générale, la Poste, Crédit Lyonnais, Groupe Banque populaire et groupe Caisse d'Epargne). D'autres banques françaises proposent des produits analogues (P@yweb Card et Virtualis au Crédit mutuel) de même que certains établissements étrangers.

La e-Carte Bleue compte 30 000 transactions par semaine, 5 000 nouveaux porteurs chaque semaine et devrait atteindre les 350 000 utilisateurs à la fin du mois de mars 2005. Depuis son lancement, le service a enregistré plus de 1,4 millions de transactions pour un montant total de 110 millions d'euros.

Afin de pouvoir utiliser la e-Carte Bleue, l'internaute doit tout d'abord s'inscrire auprès de sa banque (soit en ligne, soit par l'intermédiaire d'un formulaire papier à remplir). Le service est, selon les banques, gratuit ou payant (abonnement mensuel ou paiement à la transaction). Une fois l'inscription enregistrée, la banque délivre à l'internaute un identifiant de 8 caractères, puis par courrier, un mot de passe de 8 caractères également.

Ensuite, pour utiliser l'outil, l'internaute devra soit télécharger une application, soit se connecter sur un site dédié. Il pourra alors, grâce à ses codes d'accès, générer un numéro de e-Carte Bleue en indiquant le montant de la transaction, la date limite de validité de ce numéro (3 mois pour un e-numéro de type « usage unique ») et également préciser s'il s'agit d'un paiement récurrent (cas des abonnements). Dans ce dernier cas, l'internaute devra prendre soin de préciser le montant total des mensualités.

¹⁶ Cette volonté avait déjà été mise en avant par le Conseil national de la consommation dans son avis précité du 23 mai 2001 qui demandait « que soient développés les systèmes de paiement en ligne sécurisés n'impliquant pas la circulation des numéros de carte en ligne ».

Une fois son numéro créé, l'internaute ne pourra l'utiliser que sur un seul site marchand en utilisant le montant inscrit en une ou plusieurs fois. Cette carte virtuelle fonctionne également sur les sites étrangers.

L'objectif de la e-Carte Bleue est double : convaincre les internautes qui n'achètent pas de franchir le pas et permettre aux internautes qui se limitent dans leurs achats « *d'oser profiter de toutes les opportunités* ».

Aujourd'hui, la quasi-totalité des cyber-marchands accepte la e-Carte Bleue (l'ensemble des transactions a concerné plus de 35 000 marchands). Néanmoins, certaines structures ne permettent pas d'utiliser ce moyen de paiement en raison de contraintes techniques. Tel est le cas, en particulier, lorsque l'obtention du bien ou du service ne peut s'opérer que sur présentation physique de la carte bancaire (retrait d'un billet de train réservé et payé en ligne auprès d'une borne automatique, retrait de places de spectacle au guichet). Ces contraintes sont en cours de disparition : depuis le 10 mars 2005, les commandes de billets de train imprimables ou livrés à domicile sont possibles sur Voyages-Sncf.com.

De manière générale, les taux de refus de la e-Carte Bleue demeurent très faibles. Ils sont dus principalement à l'absence de l'indication du cryptogramme visuel créé avec le numéro de carte bancaire, d'erreurs de saisie ou de dépassement des plafonds indiqués par l'internaute.

Une critique, néanmoins, demeure. En effet, certains consommateurs se plaignent du caractère souvent payant de la solution proposée par leur banque alors que légalement, il demeure protégé contre les risques d'utilisation frauduleuse de son numéro de carte bancaire.

➤ L'indication partielle du numéro sur l'internet : le système Sympass

Sympass est une société, créée en 2001, cherchant à répondre à la réticence des internautes de confier leur numéro de carte bancaire sur l'internet. Elle a donc développé un outil reposant sur le principe du double clavier : celui de l'ordinateur et celui du téléphone. Lors d'un achat en ligne, l'internaute saisit uniquement les 8 premiers numéros de sa carte ainsi qu'un numéro de téléphone. Il reçoit alors immédiatement un appel téléphonique d'un service vocal lui demandant de saisir sur son clavier téléphonique les 8 derniers chiffres.

Ce système est disponible depuis décembre 2003 dans l'offre de paiement en ligne proposée par la Caisse d'Epargne (offre Secret plus) et depuis la fin de l'année 2004 dans celle de Paybox (solution technique de paiement en ligne). Plus de 25 acteurs marchands français ou étrangers proposent cette solution (dont CDiscount, Interflora, Nomatica, Vivacances, Digital-Shopping), entraînant l'enregistrement de plus de 1200 transactions par jour. Sympass compte aujourd'hui 170 000 utilisateurs uniques, objectif atteint en l'espace de 20 mois avec une croissance de 20 000 nouveaux utilisateurs par mois.

Suite à une enquête réalisée auprès d'utilisateurs de la solution, il apparaît que 30% des utilisateurs payaient déjà auparavant par carte bancaire, les 70% restant, n'ayant jamais acheté ou préférant le paiement par chèque. La solution offre ainsi au cyber-marchand la possibilité de réduire le nombre de transactions acquittées par chèque bancaire ou postal¹⁷ mais également de connaître une progression du nombre de clients. En effet,

¹⁷ Un tel mode de paiement impose aux cyber-marchands de nombreuses contraintes (blocage d'une partie du stock pendant un délai indéterminé, coût de traitement, etc.) sans pour autant garantir le paiement (un nombre non négligeable de chèques n'est jamais envoyé).

38% des utilisateurs y ont eu recours plus de deux fois au cours du trimestre, 20% plus de quatre fois.

Concernant la fraude, la société a indiqué lors de son audition que celle-ci était inexistante sur ce mode de paiement. Ceci s'explique principalement par le fait que les fraudeurs ne souhaitent pas donner de numéro de téléphone susceptible de les identifier.

- Le paiement par carte sans indication du numéro, la solution ID Tronic de la Caisse d'Épargne

Outre la solution « Secret + » (qui intègre le mécanisme Sympass), la Caisse d'Épargne a développé un outil de paiement en ligne appelé ID Tronic. Celui-ci tend à répondre à une promesse faite au consommateur : acheter avec une carte bancaire sans en donner le numéro. Pour pouvoir bénéficier de ce service, l'internaute – client ou non de la Caisse d'Épargne – doit s'inscrire (en ligne, par téléphone ou par courrier) en indiquant son RIB et ses coordonnées. Il doit également confier un numéro de téléphone portable.

En pratique, lors d'un achat via ID Tronic (la solution doit alors être proposée par le site marchand), l'utilisateur rentre, soit le code d'accès fourni lors de son inscription, soit son adresse de courrier électronique. Un SMS lui est alors envoyé sur son téléphone mobile lui indiquant un mot de passe à saisir sur l'écran de paiement en ligne. Le paiement sera alors confirmé et l'identité de l'utilisateur authentifiée.

Le taux de recours à cet outil a représenté en 2003, 2 millions d'euros, aucune fraude et un taux d'usage 10 fois supérieur à celui de l'e-Carte Bleue (25 000 transactions enregistrées par ID Tronic pour 1 500 sites). Cette solution permet également d'acheter par l'ensemble des sites internationaux mettant en œuvre la solution 3D-Secure.

d) L'assurance du cyber-consommateur et du cyber-vendeur

Parallèlement à ces diverses solutions de paiement, les banques ont également élaboré des mécanismes d'assurance du client lors d'une transaction sur l'internet. Ainsi, certaines d'entre elles commercialisent auprès du grand public des produits garantissant le remboursement de l'internaute en cas de fraude de son numéro de carte bancaire.

D'autres, sociétés d'assurance principalement, proposent aux clients finaux de garantir leurs transactions sur l'internet. Tel est le cas de la société Fia-Net qui gère aujourd'hui 2 millions de transactions par an.

Elle offre un double service. Cette société assure gratuitement les internautes qui achètent sur un site étiqueté Fia-Net en les remboursant des sommes indûment prélevées en cas d'utilisation frauduleuse de leur numéro de carte bancaire suite à son interception lors de la transaction sur le site en question. Néanmoins, cette indemnisation n'a jamais été mise en œuvre dès lors qu'aucun cas d'interception de numéro de carte bancaire sur un site français n'a pu être prouvée. Par ailleurs, elle demeure redondante avec les dispositions introduites par la loi sur la sécurité quotidienne qui protègent le consommateur dans une telle situation.

La société a donc surtout pour vocation de protéger le marchand, tenu par nature de contracter avec un client qui lui est souvent inconnu. En adhérant à Fia-net, le cyber-marchand s'acquitte d'une cotisation calculée en fonction du chiffre d'affaire et bénéficie d'un mécanisme de « *scoring* » de chaque transaction. Il s'agit d'une note basée sur l'analyse de la transaction, sa nature et sur le risque que peut faire peser sur celle-ci le consommateur.

Si le client présente un danger particulier, le marchand en est informé, et pourra décider de ne pas poursuivre le processus contractuel. Si la vente a malgré tout lieu, le vendeur ne sera pas assuré pour cette transaction.

Dans tous les cas, l'internaute conserve la possibilité d'apporter la preuve de son honnêteté (production d'une copie de documents d'identité).

- e) La mise en place du contrôle du cryptogramme visuel pour lutter contre la récupération du numéro lors d'un paiement de proximité.

Le 10 juillet 2001, l'ACSEL, la FEVAD et le GIE Cartes Bancaires ont signé un protocole d'accord dans lequel ils s'engageaient à rétablir la confiance des consommateurs en garantissant la transparence et la sécurité des paiements par carte bancaire afin de favoriser le développement de la vente à distance et du commerce électronique.

Ce texte prévoyait de généraliser les solutions de paiement sécurisées notamment par carte à puce et la mise en place à court terme, de mesures prenant en compte les modalités de fonctionnement de la carte bancaire. En particulier, les parties s'engageaient à rendre opérationnel le contrôle complémentaire des trois derniers chiffres mentionnés au dos de la carte (cryptogramme visuel), pour toutes les cartes Visa et Mastercard, à partir de l'été 2002. Ce contrôle est devenu obligatoire à compter du 1^{er} janvier 2004.

Cette décision faisait suite à l'avis du 23 mai 2001 du Conseil national de la consommation sur la sécurité des cartes de paiement demandant « *que soient généralisées l'existence d'un numéro ou d'un cryptogramme visuel au verso des cartes bancaires, et son utilisation pour les demandes d'autorisation* »¹⁸.

Elle a pour effet de permettre au cyber-marchand de vérifier que l'acheteur est bien en possession, physiquement, de la carte bancaire et non de son seul numéro. Afin de garantir cette sécurité, le GIE Cartes Bancaires interdit strictement aux marchands de conserver ce cryptogramme afin que celui-ci ne soit disponible que sur la carte bancaire.

Pour autant, la communication autour de cette nouvelle protection n'en demeure pas moins difficile au regard de la grande diversité de situations. Alors que les cartes Visa et Mastercard font figurer le cryptogramme au dos de la carte, d'autres cartes de paiement (American Express par exemple) le font apparaître sur la face de la carte, aux côtés du numéro de celle-ci.

Après plusieurs mois d'utilisation, les consommateurs ont pris l'habitude de le reporter dans le formulaire de paiement et les commerçants constatent une régression de certains types de fraudes visées par son emploi.

B – Les conséquences des mesures de sécurisation du processus de paiement en ligne

La fraude sur l'internet existe effectivement, mais pas dans les proportions que l'internaute peut s'imaginer. De même, le type de fraude dont sont victimes les consommateurs et les cyber-marchands n'est pas celle que le grand public se représente. Bien au contraire, la fraude est souvent liée à des pratiques totalement extérieures à l'internet ou à des abus pratiqués par certains internautes.

¹⁸ Voir note n° 9

1 – La réalité de la fraude à la carte bancaire sur l'internet

D'après les chiffres publiés¹⁹ par l'Observatoire de la sécurité des cartes de paiement, placé auprès de la Banque de France, la fraude totale relative aux paiements et retraits effectués dans les systèmes français (en ligne ou de manière physique) s'est élevée en 2003 à 273,7 millions d'euros, en hausse de 11 % par rapport à 2002. Rapporté au montant total des transactions effectuées dans les systèmes français, ce montant de fraude représente un taux global de 0,086 %, contre 0,082 % en 2002.

Selon ce rapport, le nombre de paiements nationaux frauduleux est de 940 000 en 2003 ; rapporté au nombre total de paiements nationaux, le taux de paiements nationaux frauduleux est de 0,021%. Le montant moyen d'un paiement national frauduleux se situe autour de 80 euros.

Concernant spécifiquement la fraude sur l'internet, il est à noter que la Banque de France relève « *une baisse de l'utilisation de numéros usurpés* » entre 2002 et 2003. Sur les 940 000 paiements frauduleux nationaux, 250 000 sont des paiements réalisés à distance (internet, minitel, téléphone) pour un montant total de 22,8 millions d'euros. Cela a correspondu à 31% du montant des paiements frauduleux nationaux en 2003 contre 34% en 2002.

Ce constat de la baisse du niveau de fraude en matière de vente à distance est corroboré par les chiffres publiés par Fia-Net, dans le cadre de son rapport annuel analysant les sinistres subis par les cyber-marchands. La société constate que « *la fraude à la carte bancaire sur l'internet connaît son premier recul depuis l'an 2000* ». Par rapport à 2002, elles ont diminué de 40% en volume et 57% en valeur. Pour l'assureur, les fraudeurs à la carte bancaire sont désormais organisés en de véritables réseaux.

2 – La nécessaire participation du cyber-consommateur à la protection de son environnement numérique

La fraude – comme nous l'avons indiqué précédemment, demeure faible compte tenu des mécanismes élaborés par les divers acteurs. Seulement, cet environnement sécurisé a pour effet de diminuer les réflexes de l'internaute alors qu'il fait face, dorénavant, à de nouvelles techniques d'escroquerie.

a) Le *phishing* ou « hameçonnage »

Le *phishing*²⁰ ou « hameçonnage » repose toujours sur le même principe : les fraudeurs utilisent la marque, le logo ou les couleurs d'une entreprise importante afin d'inciter les internautes à leur confier différents éléments d'identification (numéro de carte bancaire, codes d'accès aux services en ligne, identifiants de connexion à l'internet, etc.).

Souvent, pour obtenir ces informations, les fraudeurs ont recours à l'envoi de messages électroniques non sollicités, aux couleurs de l'entreprise concernée, incitant les destinataires à cliquer sur un lien les redirigeant vers un site où ces informations leur sont demandées.

¹⁹ Statistiques de fraude pour l'année 2003, complément au rapport annuel d'activité 2003, Observatoire de la sécurité des cartes de paiement

http://www.observatoire-cartes.fr/telechar/fraude_2003.pdf

²⁰ Terme provenant de la contraction de « *phishing* » (pêche) et de « *phreaking* » (piratage de ligne téléphonique)

Dear valued Citizens Bank member,

Due to concerns, for the safety and integrity of the online banking community, we have issued the following warning message.

It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.


Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.


To confirm your bank account records please [click here](#).

Thank you for your time,
Citizens Bank Billing Department.

[Privacy](#) | [Security](#) © 2004 Citizens Financial Group. All rights reserved. [Terms of Use](#) | [Site Map](#)

Exemple 1 : le lien pointe vers un faux site

De :  PayPal Customer Department [Service@PayPal.com]
À : Service.Financial@paypal.com
Cc :
Objet : PayPal Important Warning Message

 **PayPal** *The way to send and receive money online*

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This notification expires on October 05, 2004.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run.

Thank you for using PayPal! <http://uirowopw.com/hell.html>

Sincerely,
Paypal customer department!

Exemple 2 : l'adresse apparaissant dans le courriel semble correcte, mais en fait, renvoie vers un tout autre site (uirowopw.com) et le message est en anglais

Le phénomène était jusqu'ici cantonné aux internautes anglophones, les principales entreprises concernées par cette usurpation d'identité étant de grandes sociétés américaines. Les membres de l'Observatoire ont constaté en 2004 une augmentation importante de cas de *phishing* portant sur de grandes entreprises françaises : fournisseurs d'accès à l'internet, banques françaises ou géants du commerce électronique. La France a été, ainsi, classée au cinquième rang des pays à risque en décembre 2004 par l'*Anti-Phishing Working Group*²¹. Le mois précédent, elle était située au 10^{ème} rang²².

En France, la réaction est importante. Des plaintes ont été déposées par des particuliers ou des entreprises victimes et des poursuites judiciaires ont été intentées à l'encontre de particuliers français tentant de soustraire des informations aux internautes. Une première condamnation est intervenue le 2 septembre 2004 à Paris où un étudiant strasbourgeois a été, sur le fondement de la tentative d'escroquerie et de l'accès frauduleux dans un système de traitement automatisé de données, condamné à 1 an de prison avec sursis et à 8.500 euros de dommages intérêts pour avoir usurpé l'identité d'une grande banque française²³.

Désormais victimes, les entreprises françaises s'organisent. Ainsi, les banques françaises ont développé des campagnes d'information et de sensibilisation de leurs clients. Certains acteurs du commerce électronique ont également conçu des barres d'outils²⁴ permettant à l'internaute de détecter s'il se trouve sur un site fiable.

Pour sa part, l'Observatoire de la cyber-consommation a alerté en janvier 2005 les internautes de ce phénomène en dispensant quelques conseils pratiques de vigilance :

- 1°) Ne pas cliquer sur des liens dans les courriels ; toujours aller soi-même sur un site en saisissant son adresse internet lors de la saisie de données sensibles (numéro de carte bancaire, identifiants personnels) ;
- 2°) toujours vérifier, dans la barre d'adresse du navigateur, l'adresse du site internet avant de saisir les informations demandées ;
- 3°) toujours partir de la page d'accueil d'un site pour accéder aux autres pages, notamment celles où sont demandées des identifiants ;
- 4°) lors de la consultation de sites sécurisés (sites bancaires, par exemple), s'assurer de l'activation du cryptage des données (l'adresse du site doit commencer par https et non par http). Sur Internet Explorer, le navigateur le plus répandu actuellement, en https, un cadenas apparaît en bas à droite de la page et en double-cliquant dessus, l'internaute peut s'assurer que la société bénéficiaire du certificat correspond à celle du site ;
- 5°) en cas de doute, prendre contact directement avec l'entreprise concernée (votre banque, votre fournisseur d'accès à l'internet, etc.) pour lui signaler le message suspect ou transmettre ces messages aux services « *anti-phishing* » de votre prestataire

b) La vulnérabilité du poste client

Autre situation, moins visible pour l'internaute : la vulnérabilité de son poste informatique. En effet, certains « pirates » ont développé des logiciels s'installant sur l'ordinateur d'un internaute et permettant de récupérer un numéro de carte bancaire lors de sa saisie, par exemple à l'occasion d'un achat en ligne.

²¹ Phishing Attack Trends Report - December 2004

<http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf>

²² Phishing Attack Trends Report - November 2004

<http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20November%202004.pdf>

²³ Tribunal de grande instance de Paris, 13^{ème} Chambre, 2 septembre 2004, Ministère public, Crédit Lyonnais et Caisse nationale du Crédit agricole c/ Radhouan M. et autres

<http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=873>

²⁴ C. Guillemin, « Des barres d'outils pour Internet Explorer et Firefox protègent du "phishing" », *ZdNet*, 4 janvier 2005

<http://www.zdnet.fr/actualites/telecoms/0,39040748,39196431,00.htm>

Ces « *keyloggers* », véritables chevaux de Troie, s'implantent sur le matériel informatique d'un particulier soit en même temps qu'un autre logiciel non fiable, soit par la voie d'un virus propagé, par exemple, par courrier électronique.

Cette infection est souvent due à un manque flagrant de protection de l'ordinateur utilisé par l'internaute : absence d'anti-virus ou non mise à jour de celui-ci, non installation d'un pare-feu (*firewall*)²⁵. Pour contrecarrer cette lacune, certains intermédiaires assistent le consommateur dans la protection de son matériel. Ainsi, les principaux fournisseurs d'accès permettent de souscrire, parfois de manière payante, à une option « anti-virus » bloquant la réception de virus en pièce jointe d'un message. De même, Microsoft offre dorénavant, dans les dernières versions de son système d'exploitation Windows XP, un pare-feu intégré.

Ces initiatives demeurent néanmoins limitées²⁶, et il apparaît que des **actions de sensibilisation doivent être menées afin d'informer le particulier sur la vulnérabilité de son ordinateur** et sur les outils disponibles sur le marché pouvant renforcer la protection de son poste informatique.

3 – Les difficultés rencontrées par les acteurs marchands dans le secteur du paiement en ligne

Outre le consommateur, relativement protégé, l'autre victime d'une fraude est le cyber-marchand. Ce dernier risque de perdre à la fois le bien envoyé à l'escroc mais également le montant de la commande qui doit alors être remboursé à l'internaute lésé. Au cours des auditions, il est apparu que les protections développées produisaient certains dommages collatéraux résultant d'une utilisation abusive des voies de droit ouvertes au consommateur ou de limitations imposées par la réglementation bancaire.

a) La répudiation du paiement par le client

Effet ricochet de la protection instituée par les dispositions de la loi du 15 novembre 2001 sur la sécurité quotidienne, certains acteurs marchands se plaignent de la répudiation abusive d'un paiement opéré suite à un achat pourtant réalisé par le client.

Les dispositions du Code monétaire et financier²⁷ précisent que l'opposition à un paiement réalisé par carte bancaire ne peut avoir lieu qu'en cas de perte, de vol ou d'utilisation frauduleuse de la carte ou des données liées à son utilisation, de redressement ou de liquidation judiciaire du bénéficiaire.

Il apparaît que certains cyber-consommateurs, en cas d'insatisfaction vis-à-vis d'un achat en ligne (non livraison, exécution non conforme du contrat, non remboursement, etc.), en contestent le paiement auprès de leur banque. Lors d'auditions, des acteurs ont fait part de quelques cas d'obtention d'un double remboursement par le client insatisfait (suite au retour d'une commande, le marchand peut opérer le remboursement du client qui parallèlement l'obtient également de sa banque). Néanmoins ces cas, demeurent limités.

²⁵ Le pare-feu (*firewall* en anglais) est un logiciel permettant de protéger un ordinateur des intrusions provenant notamment du réseau Internet.

²⁶ A noter que certaines banques proposent aux clients de leurs services financiers en ligne de nouveaux mécanismes d'authentification ne nécessitant plus une saisie directe sur le clavier de leur identifiant ou de leur mot de passe : A. Garcia, « Des claviers virtuels pour défendre la banque sur Internet », *01Net*, 4 avril 2005 <http://www.01net.com/article/272521.html>

²⁷ Articles L. 132-2 et suivants du Code monétaire et financier.

En outre, quelques consommateurs utilisent également ce texte pour rompre de manière unilatérale un contrat conclu. Cette situation peut s'expliquer par **un phénomène incident à la dématérialisation de la passation d'un contrat de vente en ligne : le sentiment du caractère non-obligatoire d'une relation contractuelle nouée en ligne.**

En effet, lorsqu'un consommateur procède à un achat dans un magasin non virtuel, celui-ci se sent engagé en raison du phénomène d'immédiateté : paiement et réception du bien sont quasiment instantanés. Sur l'internet, cette instantanéité demeure marginale et n'existe que pour l'achat de biens numériques ou la prise d'abonnement à des services à ligne.

En revanche, lors de la commande en ligne de biens matériels, le paiement peut être différé par rapport à la commande soit, du fait du marchand (retrait opéré à la date d'envoi de la commande) soit, du fait du client lui-même (non envoi du chèque). Ces contraintes limitent le caractère souvent impulsif de l'acte d'achat et **le consommateur peut trouver dans ce paiement différé, une faculté permettant de procéder à l'annulation unilatérale du contrat.**

Or et d'un point de vue strictement juridique, en vertu des dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique qui ont inséré un article 1369-2 au sein du Code civil, le contrat est conclu dorénavant dès lors que le consommateur a eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation. L'internaute entre donc dans une relation contractuelle dès cette validation définitive, avant même qu'il indique au cyber-marchand ses données bancaires. Ainsi, et à défaut de paiement, un consommateur s'expose à la mise en cause de sa responsabilité contractuelle permettant de réparer le préjudice subi par le cyber-marchand (immobilisation du bien par exemple).

Finalement, l'internet a changé l'appréhension, par le consommateur, de la relation contractuelle. Lors d'un engagement souscrit sur le réseau, il n'a plus la sensation d'entrer dans un schéma contraignant. Au contraire, certains internautes pensent même avoir la possibilité de résilier unilatéralement leurs contrats aussi simplement qu'ils l'ont conclu.

Les exemples reçus par l'Observatoire de la cyber-consommation sont nombreux à confirmer ce point. Tel est le cas d'un internaute achetant un voyage en ligne et qui, dès le lendemain, l'annule, ayant décidé de ne plus partir à l'endroit sélectionné. On peut aussi citer le cas d'internautes souscrivant un nouveau contrat d'accès à l'internet pour bénéficier d'une offre promotionnelle proposée par l'un des acteurs du secteur sans respecter la durée minimale de leur contrat initial ou les formalités imposées en matière de résiliation de celui-ci.

Dès lors, il est évident que ce changement de paradigme dans la conception de la relation contractuelle amène l'internaute à se diriger, automatiquement, vers sa banque pour obtenir un remboursement ou un blocage de la transaction alors que le droit ne le lui permet pas d'opérer ainsi en cas de problème purement contractuel.

Un autre élément explique également ce phénomène du recours à la banque. **Dès lors que l'acheteur n'arrive pas à contacter le cyber-marchand, n'obtient aucune réponse à ses réclamations ou s'expose à des frais pour contester** (service clientèle accessible via un numéro d'appel surtaxé...), il va naturellement **se diriger vers le seul intermédiaire facilement accessible et joignable de la transaction commerciale : sa banque.**

Ce rôle plus important souhaité de la banque a trouvé un écho auprès des instances communautaires. En effet, la Commission européenne a envisagé de fixer un nouveau cadre juridique pour les paiements dans le marché intérieur lors d'une communication du 2 décembre 2003 au Conseil et au Parlement européen. Dans ce texte, les services de Bruxelles s'interrogent sur la possibilité d'instaurer une forme de « *responsabilité solidaire entre le prestataire de services de paiement et le commerçant en cas de non-livraison d'un produit (voire de non-conformité d'un produit livré)* ».

Le texte prévoit, en outre, « *l'introduction de règles spécifiques de révocabilité pour les paiements effectués dans le domaine du commerce électronique, qui disposeraient par exemple que les paiements effectués dans le cadre de contrats de vente à distance sont révocables jusqu'à ce que le commerçant fournisse au prestataire de services de paiement la preuve que la livraison a eu lieu* ». Un tel mécanisme existe, d'ores et déjà, au Royaume-Uni, en Finlande et en Suède²⁸.

b) La conservation du cryptogramme visuel par les cyber-marchands

Avec l'indication obligatoire lors d'un paiement en ligne, du cryptogramme visuel (CVV chez Visa pour *Card Verification Value* et CVC chez Mastercard pour *Card Verification Code*), certains acteurs marchands ont été confrontés à une problématique nouvelle.

Celle-ci intéresse les cyber-marchands devant « récurer » leur client, c'est à dire opérer un prélèvement régulier sur le compte bancaire du consommateur par l'intermédiaire de son numéro de carte bancaire. Tel est le cas, par exemple, de certains contrats d'accès à l'internet ou de l'accès à certains services ou contenus (salons de discussions payants, archives de journaux, etc.).

Dans de telles situations, le cyber-marchand est dans l'obligation de procéder à la conservation du cryptogramme visuel afin de pouvoir le présenter avec le numéro de carte bancaire à chaque mensualité. Or, les règles imposées par le GIE Cartes bancaires, ainsi qu'une délibération de la CNIL²⁹, interdisent la conservation de ce numéro. Un moratoire avait donc été institué afin de permettre à ces acteurs de présenter, lors de chaque transaction, uniquement le numéro de carte bancaire non accompagné du cryptogramme qui n'était pas alors conservé.

Après une discussion avec les acteurs du secteur, le GIE Carte Bancaires a modifié sa réglementation en la matière. Applicable dès le 1^{er} juillet 2005, celle-ci rappelle tout d'abord le principe de non conservation du cryptogramme. Ensuite, elle précise qu'en matière de paiement récurrent, deux phases sont à distinguer : lors du premier paiement, dès lors que le consommateur fournit son cryptogramme, celui-ci sera adressé avec les autres données bancaires. A partir du deuxième paiement et pour les paiements suivants, la demande d'autorisation adressée par le marchand n'aura plus besoin de comporter le cryptogramme.

Si cette mesure tente de concilier les différentes contraintes, elle demeure délicate à manier. Elle impose en effet aux cyber-marchands de s'identifier auprès de leur banque comme pouvant réaliser des paiements récurrents. Par ailleurs, elle impose aux prestataires bancaires de mettre en place des solutions techniques permettant de gérer la double facette de la demande d'autorisation selon le type de paiement opéré.

²⁸ Selon les chiffres apportés par Visa Europe, en 2003, 21% des cas de remboursement des porteurs de la carte étaient fondés sur une inexécution contractuelle contre 79% pour les cas de fraude à la carte bancaire.

²⁹ 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, <http://www.cnil.fr/index.php?id=1357>

c) L'authentification du porteur de la carte lors d'un achat à distance, la logique 3D-Secure

Compte tenu des nouveaux cas d'escroquerie, comme le *phishing*, et du fait que l'ensemble des gardes-fous élaborés ne prémunissent pas les cyber-marchands de tout type de fraude, le milieu bancaire réfléchit actuellement à un renforcement de la sécurité dans le domaine du paiement en ligne. L'objectif est de procéder à l'authentification du porteur de la carte lors de l'achat³⁰. Suite à la mise en place du standard 3D Secure par Visa international, le GIE Cartes bancaires a décidé de travailler sur le développement d'un standard domestique : 3D-CB.

Il s'agit d'un moyen permettant d'authentifier à la fois le porteur de la carte et le commerçant, en vérifiant leur identité. Ainsi, lors d'une transaction en ligne, les porteurs de carte doivent confirmer leur identité à l'aide, par exemple, d'un mot de passe – de la même manière qu'ils s'authentifient à l'occasion d'un paiement de proximité. La banque émettrice authentifie alors le porteur de carte et confirme à la banque du commerçant l'identité de l'acheteur.

A noter le changement important en terme de responsabilité interbancaire dans le mécanisme 3D-Secure pour des transactions internationales. En effet, le marchand qui accepte une transaction *via* cette nouvelle norme sera dorénavant garanti contre la fraude à l'inverse de ceux qui auront toujours recours au mode de transaction faisant intervenir simplement l'indication du cryptogramme visuel. La responsabilité pèsera donc sur la banque du porteur de la carte qui devra, en cas d'impayé, supporter ce risque.

Déployée par Visa et Mastercard sous les noms *Verified by Visa* et *Secure Code*, elle concerne aujourd'hui plus de 55 000 cyber-marchands dans le monde dont 28 200 pour la zone Visa Europe. En France, la solution est utilisée par plusieurs centaines de commerçants et sera progressivement déployée au cours de l'année 2005, en priorité pour les paiements transfrontaliers. La concertation opérée entre les banques et les cyber-marchands en 2004 a progressivement convaincu les acteurs de l'intérêt de cette solution pour anticiper les situations de fraudes aggravées dans certains secteurs particuliers³¹.

Côté émission, plusieurs banques françaises proposent cette solution. Tel est le cas par exemple de la Caisse d'Épargne avec son produit ID Tronic (authentification par mot de passe envoyé par SMS) et des émetteurs e-Carte Bleue/*Verified by Visa* (authentification par les identifiants de connexion et mot de passe indiqués pour la génération du numéro virtuel).

Seulement, et les auditions l'ont montré, nombreux sont les acteurs (cyber-marchands mais également banques) à s'opposer au déploiement de cette solution, invoquant des arguments tantôt économiques, tantôt pratiques. A l'inverse, d'autres se déclarent favorables à cette solution. Cette opposition n'est pas uniquement française, la Belgique connaissant des difficultés similaires³².

³⁰ Cette idée avait déjà vu le jour dans l'avis précité du Conseil national de la consommation du 23 mai 2001 qui demandait « *que soient mis en place au bénéfice des commerçants, en particulier dans le secteur de la vente à distance, des systèmes de vérification de l'identité du porteur* ».

³¹ Une telle solution pourrait ainsi avoir un intérêt dans le secteur du voyage en ligne où le montant de chaque fraude constatée est naturellement élevé et où la nécessité d'authentification du voyageur est importante.

³² E. Wery, « La Belgique adopte l'architecture 3D-Secure pour les paiements électroniques sur l'internet », *Droit-technologie.org*, 22 novembre 2004 : http://www.droit-technologie.org/1_2.asp?actu_id=1007

➤ Les avantages de 3D-Secure en France

Tout d'abord, la première argumentation met en avant les assurances apportées par cette solution en faveur du bien fondé des autorisations bancaires données sur l'internet par un acheteur. Dès lors que l'internaute est identifié comme étant à l'origine de la vente, il ne sera plus en mesure de contester la réalité de l'achat. Ce mécanisme offre ainsi un certain rééquilibrage des responsabilités entre l'acheteur et le vendeur tout en limitant les abus et les impayés qui y sont afférents³³.

Ensuite, plusieurs cyber-marchands de petite et moyenne tailles ont indiqué à l'Observatoire de la cyber-consommation qu'ils seraient relativement favorables à une telle solution, faute d'avoir les moyens d'assumer les pertes résultant des cas de fraude qu'ils subissent ou de procéder à des investissements substantiels pour la souscription d'un contrat d'assurance ou à des solutions d'analyse des commandes reçues. Pour eux, un tel mécanisme d'authentification de l'acheteur leur permettrait de développer de manière acceptable financièrement leur activité commerciale sur le réseau mondial.

➤ Les contraintes de la mise en œuvre de 3D-Secure

Les craintes émises à l'encontre de la mise en place de cette nouvelle norme proviennent à la fois de cyber-marchands et d'intermédiaires impliqués dans la gestion des paiements en ligne.

Du côté des principaux acteurs marchands, 3D-Secure est perçu comme une solution qui risque de freiner le développement du commerce électronique en installant une barrière dans la fluidité actuelle du paiement en ligne. En effet, dès lors que l'internaute devra s'identifier au préalable auprès de sa banque, le nombre de vente sur impulsion risque de diminuer. Par ailleurs, certaines banques pourraient rendre payant ce service, risquant d'altérer le dynamisme du commerce électronique. Les partisans de la solution répliquent que l'inscription ne devra s'opérer qu'une seule et unique fois et donc que cet effet s'estompera progressivement comme ce fut le cas lors de l'instauration de l'utilisation du code confidentiel pour les paiements par carte à puce.

D'autres acteurs craignent que toutes les banques ne veuillent pas jouer le jeu. En effet, avec la nouvelle norme, la banque du porteur de la carte sera dorénavant responsable en cas de contestation de la transaction bancaire. Ainsi, afin de diminuer son implication, elle pourrait être tentée, lors de l'interrogation par le cyber-marchand, de ne pas systématiquement valider l'authentification de son client (notamment si le mécanisme choisi n'est pas sans risque, comme par exemple, une simple authentification par identifiant et mot de passe statiques). En réponse, d'autres acteurs mettent en avant le fait que la norme 3D-Secure ne sera déployée qu'avec la garantie que l'ensemble des acteurs du secteur bancaire jouera le jeu.

Deux structures auditionnées ont également indiqué que cette nouvelle norme ne permettra pas de résoudre complètement la question de la fraude sur l'internet. En effet, si la méthode d'authentification choisie repose sur l'apparition d'une « *pop-up* »³⁴ sur le site marchand au sein de laquelle le consommateur devra indiquer un code confidentiel attribué par sa banque, aucun système ne permet à l'heure actuelle d'identifier la personne générant cette *pop-up* et un risque de récupération des mots de passe par des sites malveillants est présent. Enfin, des solutions simples et gratuites ont pour effet de bloquer l'affichage de ces *pop-up* (barres d'outil Google, Yahoo!, option de Windows XP SP2, etc.). C'est en raison de l'ensemble de ces contraintes que les banques qui ont

³³ Selon les chiffres communiqués par Visa lors de son audition, les taux de remboursement que le marchand doit supporter passent de 0,22% (en cas de paiement via la technologie SSL) à 0,03% (pour les marchands ayant recours à la technologie 3D-Secure avec authentification du consommateur).

³⁴ Une *pop-up* est une nouvelle fenêtre du navigateur s'ouvrant de manière automatique.

déployées la solution, ont plutôt opté en faveur d'une création dynamique du mot de passe et une indication de celui-ci dans l'interface même de paiement.

Par ailleurs, un commerçant peu scrupuleux pourrait utiliser la marque 3D-Secure afin de rassurer ses clients sans leur offrir toutes les garanties qui sont dues, et entraînant ainsi, une augmentation non négligeable des litiges devant être supportés par les banques des porteurs de carte.

Enfin, les intermédiaires techniques du secteur (prestataires de solution de paiement) demeurent réservés vis-à-vis de cette solution dès lors qu'elle va nécessiter de nombreux investissements. Or, ils conservent tous en mémoire les pertes engendrées par de précédentes solutions, aujourd'hui abandonnées (CyberCom, CB sur mobile, e-comm).

C'est pour analyser les conditions de mise en œuvre de l'authentification du porteur que le GIE Cartes bancaires et les acteurs de la vente à distance ont constitué un groupe de travail afin de trouver un accord permettant un déploiement de cette nouvelle norme. Seulement, et pour reprendre des propos tenus par un des acteurs auditionnés, *« s'il est facile d'équiper des sites, en revanche il est plus difficile de convaincre des millions d'utilisateurs »*.

II – Le micro-paiement et le porte-monnaie électroniques : deux outils alternatifs dédiés au paiement de petites sommes

A côté de la carte bancaire, l'internet a vu émerger de nouveaux outils permettant à l'internaute de procéder au paiement de biens ou de services. Le point commun de ces outils est qu'ils ont tous accompagné le développement de produits ou de services de faible valeur sur l'internet.

Aujourd'hui, le secteur du paiement de petites sommes, le micro-paiement, est très diversifié : achat d'articles de presse, de sonneries de portable, de logos permettant de personnaliser son téléphone, achat de morceaux musicaux sur les plates-formes payantes, de jeux en ligne, etc.

Ce marché est en pleine expansion. Il a représenté, aux Etats-Unis, 1,6 milliards de dollars en 2003 et 1,8 milliards de dollars en 2004, soit une progression de 13,7%. En Europe, le chiffre d'affaire atteignait, en 2003, 544 millions d'euros en Europe. Les analystes estiment qu'il représentera en 2007, 5,5 milliards de dollars aux USA et 2,37 milliards d'euros en Europe soit une progression de plus de 40% par an³⁵ (due principalement aux secteurs des jeux en ligne³⁶, de la musique ou de la vidéo à la demande³⁷).

Avec de telles transactions particulières, les outils disponibles sont variés (outils spécifiques, recours aux modes de paiement habituels – carte bancaire, chèque, etc.). Néanmoins, pour certains acteurs, le recours à la carte bancaire pour l'achat de ces biens ou services de ce type n'est pas aisé. Les frais bancaires demeurent élevés au regard du montant de la transaction, même si les banques ont souhaité adopter une démarche compétitive en diminuant le montant des commissions perçues vis-à-vis de certains contenus (plates-formes de téléchargement de fichiers musicaux par exemple). Par ailleurs, ces contenus numériques s'adressent principalement à un jeune public dépourvu généralement de tout outil de paiement bancaire.

En conséquence, plusieurs outils ont été développés pour opérer dans le secteur du micro-paiement. Il pourrait être défini comme le paiement d'un achat de moins de 15 €. Ce montant correspond, en effet, au seuil d'exigibilité d'une facture par le consommateur en application de l'arrêté n° 83-50/A du 3 octobre 1983 relatif à la publicité des prix de tous les services³⁸. Certains acteurs estiment que ce montant pourrait être porté jusqu'à 40 €.

Tous ces dispositifs veillent enfin à répondre aux principales caractéristiques de cette forme particulière de paiement à savoir la rapidité et la facilité d'utilisation pour le consommateur, l'anonymat relatif de l'utilisateur et le faible coût pour le vendeur.

³⁵ Chiffres et données communiqués par Biz-n-Cash lors de son audition.

³⁶ Selon *Jupiter Research*, le chiffre d'affaire sur les seuls téléphones mobiles devrait atteindre en 2009, 6,9 milliards de dollars pour les paris sportifs, 7,9 milliards pour les loteries et 4,5 milliards pour les casinos. Cf. « Paris sur le mobile », *Biz-n-Cash*, 7 mars 2005, <http://www.biz-n-cash.fr/actualite-665.html>

³⁷ Selon l'*Online Publishers Association*, le premier secteur aux Etats-Unis, en 2004, est celui des sites de rencontre (469,5 millions) suivi des loisirs (dont la musique en ligne) réalisant un chiffre d'affaire de 413,5 millions de dollars. Cf. « Chiffres US de la vente de contenus en ligne », *Biz-n-Cash*, 14 mars 2005, <http://www.biz-n-cash.fr/actualite-671.htm>

³⁸ Ce texte réglementaire ne vise que le cas des prestations de service qui constituent, actuellement, la quasi-totalité du marché.

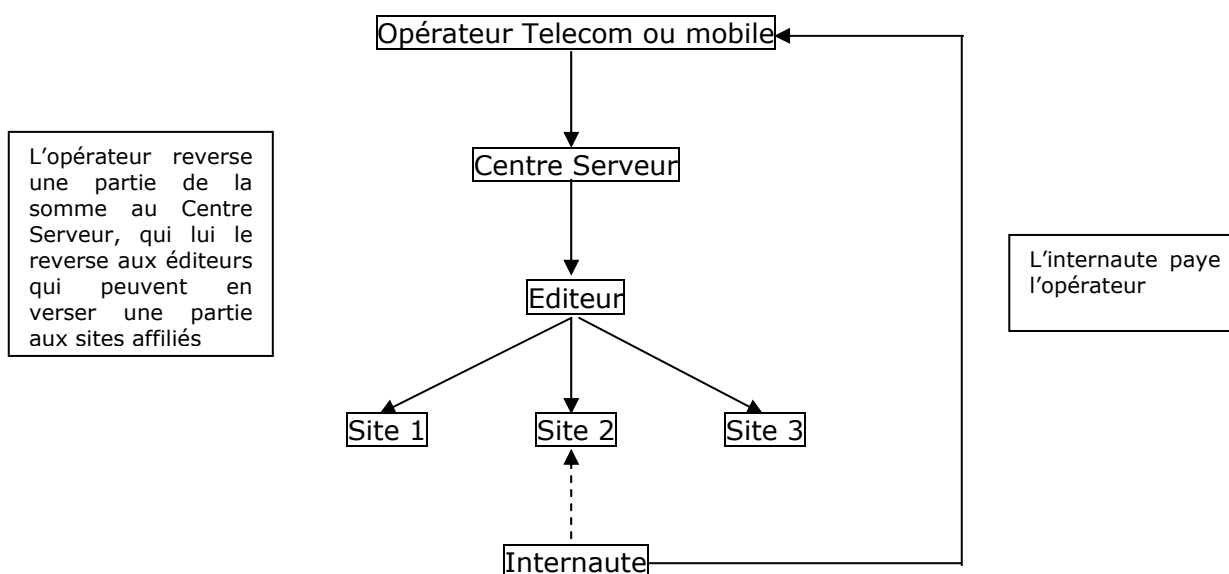
A – Les outils existants en matière de paiement de petites sommes

Plusieurs technologies sont actuellement présentes sur le marché français du paiement en ligne. Elles proviennent, soit de la transposition au secteur de l'internet d'outil issus de la télématique, soit sont le fait de réelles innovations.

1 – Le recours à des numéros à revenus partagés

Cette première technologie recouvre un grand nombre d'outils : *dialers*, numéros audiotel ou SMS+. Elle est la transposition d'outils développés à l'origine pour la télématique. En pratique, l'ensemble de ces systèmes se rapproche du schéma suivant :

Schéma : Les acteurs des numéros à revenus partagés



Pour autant, le recours à ces technologies demeure très encadré. En effet, l'ensemble de ces services est soumis aux règles déontologiques élaborées par le Conseil supérieur de la télématique (CST) ou validées par ce dernier (cas de la charte SMS+).

a) Les kits de connexion ou *dialers*

Les kits de connexion sont des outils qui servent à rémunérer des contenus immatériels de faible montant avec une livraison immédiate. Les règles déontologiques du CST limitent le recours à ces outils aux cas de rémunération de contenus internet (pas d'achat de biens matériels par exemple).

Dans le domaine des *dialers*, deux catégories de produits existent : ceux renvoyant vers un numéro surtaxé français (Audiotel, Kiosque Micro, etc.) et ceux renvoyant vers des numéros internationaux.

Le kiosque micro est l'un des outils disponibles en la matière. Il a été développé par France Telecom et est la transposition du schéma minitel à l'internet. Interrogé par l'Observatoire CyberConso, France Telecom indique que le Kiosque micro est aujourd'hui un outil destiné à disparaître dès lors qu'il n'y a pas eu de report du marché qui existait sur le minitel vers l'internet, les principaux sites étant dorénavant accessibles

gratuitement (SNCF par exemple) et qu'il ne s'adresse qu'au marché du bas débit en forte diminution.

Néanmoins, certains services demeurent attachés à ce mode de rémunération, et des éditeurs utilisent cette solution afin de fournir des services interdits par les règles déontologiques du Conseil supérieur de la télématique, comme les contenus adultes, et ce malgré les saisines et les coupures qui s'ensuivent.

Mais finalement, l'ensemble des acteurs interrogés s'accordent pour dire que l'industrie du kit de connexion est une industrie qui connaît depuis plusieurs mois une baisse très importante, au profit d'autres mécanismes de paiement. Plusieurs éléments peuvent expliquer ce phénomène : la généralisation du haut débit, la mise sur liste noire des kits de connexion par les logiciels anti-*spyware*, les *supers-proxy* des fournisseurs d'accès à l'internet ou, plus récemment, le passage du système d'exploitation phare de Microsoft à une version plus sécurisée : Windows XP Pack SP2 (qui a pour effet de bloquer un certains nombres d'applications et en particulier la technologie ActiveX). Ainsi, en mars 2004, un des acteurs interrogés a connu une chute du temps de connexion sur son kit de l'ordre de 50%.

b) Le recours à des services vocaux à tarification majorée

Il existe deux types de recours à des services vocaux à tarification majorée.

Tout d'abord, ils peuvent constituer un mode d'obtention d'un code par le truchement d'un service vocal à tarification majorée, permettant à l'utilisateur d'accéder à un contenu numérique (service, bien immatériel comme téléchargement de sonneries, personnalisation du téléphone portable, jeux en ligne, téléchargement de logiciels, etc.). Cette forme de paiement a trouvé son public ; le leader français (Allopass) annonçant devoir délivrer près de 2 millions de code chaque mois à la fin de l'année 2005.

Par ailleurs, une seconde solution existe. Dans un premier temps, l'internaute relève sur le site auquel il souhaite accéder, un code. Dans un deuxième temps, il appelle un service à tarification majorée auquel il indique ce code par l'intermédiaire du clavier téléphonique, ce qui lui permet d'accéder à la partie réservée du site tant que dure la communication avec le service à tarification majorée (cas par exemple de l'audiotel décroché).

En France, l'un des principaux acteurs est Allopass. Il propose ces divers outils de micro-paiement. Le paiement est alors facturé à l'internaute par l'opérateur de télécommunications qui reverse, après déduction d'une commission, les sommes collectées à Allopass, laquelle société fait de même à l'égard de l'éditeur du site. Actuellement, plus de 100 000 sites internet français ont recours à ces solutions de paiement et leur nombre ne cesse de progresser.

Néanmoins, cette forme de paiement en ligne demeure relativement marginale auprès des grandes enseignes au regard du commissionnement institué (prélèvement de 30% par l'opérateur téléphonique). Ces solutions séduisent plus les particuliers ou les petits éditeurs de site à la recherche d'une solution de paiement facile à installer.

c) Le SMS+

Les SMS+ (SMS Premiums) permettent aux détenteurs d'un téléphone mobile soit de recevoir directement sur le mobile un contenu commandé par SMS surtaxé (logo, sonnerie, information), soit d'obtenir, par retour de SMS, un code permettant d'accéder à un contenu sur l'internet (équivalent au code audiotel).

Ces numéros sont gérés par l'association SMS+ (groupement des trois opérateurs mobiles français et d'éditeurs de contenus comme l'ACSEL, le GESTE, etc.) qui est chargée de gérer les numéros disponibles de manière coordonnée avec l'ensemble des opérateurs mobiles et de traiter les demandes de réservation de numéros courts déposées par les éditeurs de services. Elle fixe également les règles déontologiques et les paliers tarifaires applicables à chaque service. Ces dernières s'inspirent fortement de celles du Conseil supérieur de la télématique et ont été approuvées par ce dernier. Les opérateurs sont ainsi en mesure de rappeler à l'ordre les éditeurs de service et ont la possibilité d'ordonner la coupure du numéro incriminé en cas de violation desdites règles déontologiques.

En effet, l'association SMS+ ne gère pas le déploiement du numéro attribué. En effet, il est nécessaire pour le titulaire du numéro de se mettre en rapport avec chaque opérateur mobile pour la signature d'un contrat, signature devant intervenir dans les trois mois sous peine de perdre le numéro. Outre ces éléments, le coût d'attribution du numéro s'élève à 700 € HT. Finalement, peu d'acteurs sont réellement présents sur le secteurs, la majorité des éditeurs préférant sous-louer leurs numéros. En effet, ils n'ont pas forcément tous les moyens techniques de développer leurs propres services et préfèrent faire appel à certains prestataires.

Le SMS+ obéit à un mécanisme de six paliers tarifaires, s'appliquant en fonction des services offerts. Sur les paliers les plus élevés, l'éditeur du site ne peut demander aux utilisateurs l'envoi que d'un nombre limité de SMS+ pour accéder au contenu. Par exemple, sur le palier le plus cher, l'éditeur ne peut facturer son contenu plus de 3 euros (deux SMS+ à 1,50 €). En pratique, cela signifie que l'utilisateur devra envoyer deux SMS+ successifs pour récupérer deux codes distincts qu'il devra, alors, saisir pour accéder au contenu.

Tranche de numéro court	Fourchette tarifaire TTC (hors coût du transport)
3XXXX (Palier P3)	0,00 €
4XXXX (Palier P4)	0,05 €
5XXXX (Palier P5)	0,06 à 0,20 €
6XXXX (Palier P6)	0,21 à 0,35 €
7XXXX (Palier P7)	0,36 à 0,50 €
8XXXX (Palier P8)	0,51 à 1,50 €

Tableau 1 : fourchettes tarifaires (source : Association SMS+)

Paliers	Tarif TTC pour le client (hors coût du transport)	Nombre maximum de SMS à envoyer pour accéder au service
P8	1,50 €	2
P8	1,00 €	3
P7	0,50 €	4

Tableau 2 : Nombre maximum d'échanges payants autorisés pour délivrer l'intégralité du service aux utilisateurs (Source : Association SMS+)

Par ailleurs, pour les prestations délivrées directement sur le téléphone mobile, sont uniquement autorisés sur les paliers les plus élevés, les services de personnalisation du mobile de l'utilisateur et les services d'information thématique en mode micro-abonnement.

Concernant la délivrance de codes d'accès, les paliers les plus importants ne pourront pas être utilisés par les sites fournissant certains services (annonces entre particuliers, annonces de rencontre et annonces d'emploi)

Dans ce secteur, le mécanisme de reversement est le suivant :

Prix pour l'utilisateur (payé à son opérateur) : coût du SMS standard en fonction de l'opérateur du client + coût du contenu surtaxé (en fonction du palier).

Sur le prix payé par l'utilisateur :

Paiement de la prestation à l'opérateur : en moyenne 30% du palier (cela varie en fonction des opérateurs et des paliers) + coût du SMS standard (varie en fonction de l'opérateur et de l'offre souscrite par l'abonné)

Reversement à l'éditeur du site et au prestataire technique : en moyenne 70% du palier
L'éditeur supporte, en outre, le coût éventuel de la réponse par SMS (non systématique) : 0,6/0,8 cts.

Ce système a pour effet de générer un taux de reversement moins important pour l'éditeur du site par rapport à un numéro audiotel. Ainsi, par exemple :

	Audiotel	SMS
Coût utilisateur	1,68	1,65 (0,15+1,50 pour le palier)
Reversement final pour l'éditeur	1,18	0,78

Par ailleurs, et outre son utilisation à l'occasion de jeux télévisés, il semble que l'usage du SMS+ sur l'internet pour l'obtention d'un mot de passe soit peu exploité. Cela tient, d'une part, au fait que le taux de reversement est moins important pour l'éditeur qu'un numéro audiotel classique et d'autre part, au fait que peu de personnes disposent d'un téléphone portable professionnel leur permettant d'éviter de supporter personnellement le coût de ce service. Pour autant, du côté des éditeurs ayant franchi le pas, il apparaît que l'utilisation d'une solution SMS+ permet une progression des ventes d'environ 10 à 15% en raison de sa commodité d'usage (contrairement aux mécanismes d'Audiotel décroché, il n'y a pas de numéro à écouter et à inscrire, celui-ci étant directement envoyé sur l'écran du téléphone portable).

2 – Le porte-monnaie électronique

En France, les réflexions sur un porte-monnaie électronique sur carte à puce datent du début des années 90 et ont conduit au lancement de plusieurs pilotes à la fin des années 90 (Modeus, Moneo, Mondex). Pour favoriser l'interopérabilité entre ces différents systèmes, les banques ont créé en 1999 la Société Financière du Porte-Monnaie Electronique Interbancaire (SFPMEI) pour y centraliser l'émission et la garantie de la monnaie électronique. Après la fusion de ces différents projets en un seul (Moneo), la SFPMEI a conservé ce rôle. La SFPMEI est un établissement de crédit agréé par les autorités bancaires françaises. Elle est la filiale des 11 principales banques.

Parallèlement à Moneo, des porte-monnaie totalement dématérialisés ont vu le jour. Ces outils ne sont pas dédiés exclusivement au micro-paiement. De par leur nature, les consommateurs peuvent y avoir recours pour le paiement de sommes plus importantes.

- a) Moneo : le porte monnaie électronique sur carte à puce

Moneo est un porte-monnaie électronique sur carte à puce destiné au paiement de biens ou de services de faibles montants dans le monde physique (jusqu'à 30 €). Début 2005, il représente environ 1,2 millions de porte-monnaies chargés, 100 000 points de paiement installés et 400 000 paiements réalisés par semaine.

Avec le développement du commerce électronique, certaines banques promotrices du système réfléchissent à l'utilisation de Moneo pour effectuer des paiements sur l'internet. Toutefois, cela imposerait au consommateur de posséder un lecteur pour lire la carte. Or, depuis l'échec du projet Cyber-Comm³⁹, peu d'acteurs souhaitent investir dans ce domaine. Pourtant, un tel lecteur à carte pourrait constituer une externalité positive puisqu'il serait possible d'envisager d'autres usages (lecture de la carte vitale ou de la future carte d'identité électronique). Le choix d'un tel système a notamment été fait, en Suisse, par UBS qui a acquis 100.000 lecteurs pour ses clients. D'autre part, devant le succès encore limité de Moneo, les banques, dans leur majorité, ne semblent pas considérer ce domaine comme prioritaire.

Concernant les paiements de faibles montants dans le monde virtuel, il existe, pour la SFPMEI, une réelle attente pour une solution permettant d'effectuer, à partir de son compte courant bancaire, des paiements de faibles montants dans le monde virtuel (internet, téléphonie mobile). Le marché de cette solution se situerait entre la carte bancaire (gros montants, authentification de l'utilisateur) et les kiosques des opérateurs télécoms (très faibles montants). Cette solution pourrait être tant prépayée (comme pour le porte-monnaie sur carte à puce) que post-payée.

b) Paynova : le porte-monnaie électronique prépayé

Paynova est une société fondée en Suède en 2001. Après une première étape de développement technologique, elle a lancé son mécanisme de micro-paiement à la fin de l'année 2001. Depuis septembre 2003, elle développe ses activités en dehors de la Suède (France, Allemagne, Belgique, Danemark). En France, elle a fondé sa filiale en juillet 2004.

Elle offre à tout consommateur la possibilité d'ouvrir un porte-monnaie virtuel pouvant être utilisé sur divers sites internet. Il devra indiquer ses nom et prénom ainsi qu'une adresse de courriel, puis créditer son porte-monnaie par carte bancaire. Le montant de ses achats est, initialement, limité à 120 euros. Pour dépasser ce plafond, le client doit accepter une vérification par l'intermédiaire d'un débit sur son compte bancaire⁴⁰. Le plafond est alors porté à 3 000 euros.

Lors de l'achat sur internet, le consommateur choisira parmi les solutions de paiements proposés par le commerçant, l'outil Paynova. Il devra alors se connecter sur son porte-monnaie virtuel pour procéder au paiement.

Pour le cyber-marchand, Paynova a pour mission de collecter les sommes sans créer de masse monétaire. La somme est débitée du portefeuille de l'acheteur et créditée dans un compte séquestre différent de celui de Paynova. L'intérêt pour le marchand est d'avoir une garantie du paiement : l'argent est disponible dans le porte-monnaie du client, et ce dernier est authentifié lors de la transaction (solution 3D-Secure).

³⁹ Projet de système de paiement en ligne reposant sur l'utilisation du protocole SET mis au point par les grands émetteurs internationaux de cartes en 1997. Au cours de l'année 2000, les grands émetteurs ont commencé à étudier des solutions alternatives à ce protocole qui a été abandonné dans le courant de l'année 2001. En particulier, cet outil nécessitait le recours à un lecteur de carte à puce pour le paiement par carte bancaire sur l'internet.

⁴⁰ Une somme est prélevée sur son compte bancaire. La transaction fait alors apparaître, dans le relevé de compte, un « code » qui devra être communiqué à Paynova.

Paynova compte environ 160.000 comptes et 500 cyber-marchands en Europe. Lancée officiellement sur le marché français le 1er septembre 2004, une vingtaine de marchands français propose cette solution de micro-paiement, pas forcément de manière exclusive.

Pour Paynova, ce produit s'adresse principalement aux PME qui peuvent avoir des difficultés à convaincre les banques pour obtenir un contrat « vente à distance ». Elle serait également susceptible d'intéresser les cyber-marchands saisonniers (clubs, lobbying, associations), les spécialistes des « petits prix » (sonneries) et les acteurs alimentaires (pour la vente de produits français à l'étranger). Enfin, il est à noter que certains cyber-vendeurs sont exclus (sites de charme, jeux en ligne).

c) Click&Buy : le porte-monnaie électronique « post-payé »

Présente depuis 2002 en France via un contrat de distribution confié à NetFront, la société allemande FirstGate a fondé en septembre 2004 sa filiale française pour offrir aux marchands et aux internautes l'accès à sa plateforme de paiement Click&Buy.

Click&Buy fonctionne comme un outil de paiement à débit différé : l'internaute lors de son inscription fournit une seule fois ses informations bancaires, consomme les contenus et services chez les marchands puis est débité une fois par mois du montant global de ses dépenses. Afin de couvrir les risques pris par l'outil de paiement et par les marchands, un mécanisme de surveillance est mis en œuvre (validation du numéro de carte bancaire, demande de réservation sur le système bancaire, interdiction d'une double utilisation du même numéro de CB sans contact préalable avec le service client).

Le *scoring* effectué lors de l'adhésion de l'internaute permet à FirstGate de fixer le seuil d'engagement maximal admissible. Si les dépenses de l'internaute dépassent ce seuil, il est averti et un débit intermédiaire est déclenché auprès de sa banque en utilisant le moyen de paiement communiqué. Cette limite d'engagement augmente en fonction de la fidélisation de l'internaute et de l'absence d'incidents sur son compte Click&Buy. Elle peut aussi diminuer dès qu'un incident survient sur celui-ci ; tout incident provoquant le blocage temporaire du compte forçant ainsi l'internaute à régulariser la situation ou à prendre contact avec le service clientèle.

En cas d'impayé, le compte de l'internaute est bloqué, des messages de relance lui sont envoyés ; si la situation n'est pas régularisée le dossier est transmis au service contentieux pour une prise de contact téléphonique voire transmission à une société de recouvrement international (cession de la créance).

A noter qu'en France, si le système repose actuellement sur la carte bancaire, l'utilisation d'autres supports de paiements est prévue. En Allemagne, le virement est très utilisé. Dans d'autres pays (Royaume-Uni, Suisse), le paiement peut s'opérer par l'intermédiaire de la facture téléphonique en raison de partenariats signés avec British Telecom et SwissCom.

Les taux de reversement aux marchands oscillent entre 70 et 80% pour les micro-paiements (0,10€ à 4,99€) et entre 90 et 97% pour les macro-paiements (à partir de 5€). En outre, la société offre des services complémentaires se positionnant ainsi au niveau international comme une « plate-forme sécurisée d'intermédiation commerciale ».

Aujourd'hui la société affiche 4,8 millions d'utilisateurs dans le monde. Si les premiers marchands ont été principalement des sites de presse en ligne (La Tribune, les Echos en France, Financial Times en Angleterre, ...), d'autres grandes entreprises dans la vente de contenus et de services sur Internet ont adopté cette solution au niveau international

(BetandWin, AstroCenter, Gameloft, PlayBoy, OD2, MSN Music, Symantec, ...). Environ 3500 marchands dans le monde utilisent Click&Buy.

La tenue des comptes (marchand et internaute) est faite dans l'une des sept devises gérée par Click&Buy (Euro, livre sterling, franc suisse, dollar américain, couronne norvégienne, couronne danoise et couronne suédoise) et le « *roaming* » des internautes effectuant leurs achats en devise est géré automatiquement par le moteur de change de l'outil.

3 – Le paiement par courrier électronique

Dans le secteur du paiement par courrier électronique, plusieurs acteurs sont présents en France. Ce système tend à devenir la norme en matière de paiements réalisés entre particuliers, notamment à l'occasion d'achats réalisés sur les sites de « vente aux enchères »⁴¹ n'offrant pas d'outils intégrés de ce type.

a) Visa Direct

Lancé en Europe à l'été 2004, Visa Direct est l'outil développé par Visa pour les virements entre particuliers. Cet outil permet aux utilisateurs d'envoyer de l'argent aux porteurs de carte Visa.

Visa Direct a été lancé afin de faciliter les paiements transfrontières de faible montant entre les particuliers. Pour effectuer un virement, l'expéditeur peut utiliser différents canaux (internet, agence bancaire, banque à domicile). Plusieurs moyens de transferts sont possibles tels que l'adresse de courrier électronique ou le numéro de compte du bénéficiaire. La somme virée est alors directement versée sur le compte courant du bénéficiaire.

Ce service peut être mis en place par les banques qui souhaitent le proposer à ses clients. Depuis fin 2004, cinq banques européennes proposent le service Visa Direct à leurs clients dont Carta Si en Italie, BBVA en Espagne et Corner Banca en Suisse. De nombreuses autres banques étudient actuellement les opportunités de lancement courant 2005.

b) Paypal

PayPal est une solution de paiements en ligne et une filiale de *eBay Inc.* En Europe, PayPal Europe Limited s'est constituée au Royaume-Uni où les autorités bancaires (FSA) lui ont accordé une licence ELMI (*Electronic Money Institution*) en application de la directive du 18 septembre 2000 (2000/46/CE)⁴². PayPal a ensuite demandé le passeport de cette licence dans la plupart des pays de la Communauté européenne. En France, le passeport lui a été agrémenté en avril 2004 par le Comité des établissements de crédit et des entreprises d'investissement (CECEI).

PayPal compte aujourd'hui 64 millions d'utilisateurs à travers le monde ; en France, PayPal acquiert environ 20 000 nouveaux utilisateurs par semaine, et aux Etats-Unis, un internaute sur trois possède un compte PayPal. En 2004, PayPal a traité 18,4 milliards de dollars de volumes de paiement. La simplicité d'utilisation et la sécurité qu'offre ce

⁴¹ Le terme usuel utilisé pour désigner ces plates-formes est celui de « ventes aux enchères ». Juridiquement, il convient de parler de « courtage en ligne sous formes d'enchères », les ventes aux enchères étant soumises à un régime juridique particulier (article L. 321-1 et suivants du Code du commerce).

⁴² Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, JOCE n° L 275 du 27 octobre 2000, p. 39.

http://europa.eu.int/eur-lex/pri/fr/oj/dat/2000/l_275/l_27520001027fr00390043.pdf

moyen de paiement expliquent son succès tant sur eBay que sur d'autres sites marchands : L'ouverture de compte ne prend quelques minutes et est gratuite, les vendeurs n'ont pas accès aux coordonnées bancaires de l'acheteur, et PayPal renforce la sécurité et la traçabilité des transactions car il se substitue aux paiements par chèques, mandats et en espèce. Sur eBay, sous certaines conditions, les acheteurs bénéficient aussi gratuitement de la « Protection des acheteurs PayPal », qui les protège contre la non-réception des objets ou lorsque ceux-ci ne sont pas livrés dans l'état décrit par le vendeur, à hauteur de trois transactions par an pour une valeur maximale de 400 € par transaction.

PayPal est un émetteur de monnaie électronique et non une banque, et n'offre donc pas en conséquence de cartes bancaires, de compte rémunéré, ou autres services financiers. En France, l'utilisateur peut approvisionner sa transaction PayPal au moment de payer son achat, et sa carte bancaire est alors débitée du montant, qui est ensuite crédité sur le compte PayPal du vendeur quasi-instantanément. Le vendeur, qui reçoit l'argent, a le choix entre conserver la somme sur son compte PayPal ou la faire virer sur son compte bancaire (virement gratuit pour les sommes supérieures à 100 €).

En pratique, la majorité des vendeurs procèdent à ce virement : les soldes des comptes demeurent faibles. Par ailleurs, passé un certain solde, PayPal adresse le message suivant à ses utilisateurs : « *Sachez que votre solde de compte représente une créance chirographaire Europe Limited auprès de PayPal, qu'il existe un risque pour ce solde en cas d'insolvabilité de PayPal Europe Limited et qu'il n'est pas couvert par le système de compensation des services financiers du Royaume-Uni ou par tout autre système d'assurance publique ou privé* ». Pour des raisons liées à la lutte contre le blanchiment d'argent et autres fraudes, les virements supérieurs à 9 500 euros par transaction sont interdits.

Par ailleurs, pour mitiger les risques de fraude, PayPal demande à ses utilisateurs de procéder à une vérification dès lors que l'historique de volumes de paiement du compte atteint certains seuils (750 euros pour l'envoi, 7 500 Euros pour la réception de fonds) : PayPal demande à ses utilisateurs de lui verser une somme d'environ 1,5 euro – ensuite remboursée lors du prochain paiement effectué. Un code de sécurité à 4 chiffres est alors transmis à l'utilisateur par le biais de son relevé bancaire, qu'il/elle doit ensuite saisir sur son compte PayPal afin de devenir « vérifié ».

Interrogée par l'Observatoire de la cyber-consommation, PayPal indique ne pas être un outil destiné aux paiements de faible montant (inférieur à 1 euro), au regard des taux de commission applicables, qui sont à la charge des vendeurs. Il vise une grande variété d'utilisateurs (utilisateurs de eBay, vendeurs de logiciels, offreurs de contenus numériques ou d'autres services marchands). A cette fin, il offre un vaste choix d'outils aux vendeurs (intégration facile du bouton de paiement PayPal sur un site marchand), système de paiement récurrents/abonnements, panier, outils pour gérer les dons). En offrant des paiements en 6 devises (Euro, Dollars Australiens, Canadiens et US, Livre Sterling, et Yen), PayPal aide les TPE et PME à développer leurs ventes à l'export. Sur eBay, PayPal est entièrement intégré ce qui facilite les paiements et leur suivi pour les acheteurs et les vendeurs.

4 – Le paiement à partir d'outils physiques

Outre le développement d'outils en ligne, certains acteurs français proposent aux consommateurs des produits de paiement en ligne reposant sur des supports physiques, sous forme de cartes prépayées par exemple. Trois acteurs proposent de telles solutions : Kertel (filiale de Iliad), EasyCode et Néosurf.

Le principe est commun à l'ensemble des solutions : l'internaute acquiert dans un point de vente (les bureaux de Poste ou les débitants de tabac par exemple), une carte chargée d'un montant prédéterminé. Sur cette carte figure un ou plusieurs codes que le consommateur devra indiquer lors de son achat en ligne.

Encore mal connus, ces outils s'accordent difficilement à l'une des caractéristiques principales de l'achat en ligne : l'impulsion. Pour autant, certains acteurs ont su faire valoir d'autres atouts en proposant par exemple, en partenariat avec un site de charme, de distinguer des cartes adultes et des cartes « tout public », transformant ce moyen de paiement en outil de vérification de l'âge de l'internaute pour l'accès à certains contenus réservés. Enfin, d'autres prestataires proposent ces solutions à destination d'un public n'ayant pas forcément d'outils de paiement facilement accessibles (mineurs, entreprises)⁴³.

5 – Le rétro-paiement : le « cash-back »

Dernier phénomène en développement sur l'internet : le cash-back. Il permet à un internaute de gagner de l'argent lors de ses achats. A chaque achat, une partie du montant payé lui est, en effet, reversé par virement ou chèque bancaire, voire mis à sa disposition pour acquérir biens et services sur des sites partenaires. Ce phénomène de « rétro-paiement »⁴⁴ est en pleine expansion en France où trois acteurs cohabitent sur ce marché.

De manière générale, l'ensemble des acteurs s'accordent pour dire que leurs outils ont un double effet : d'une part, ils incitent fortement à l'achat et, d'autre part, ils induisent un effet d'entraînement assurant un niveau de réachat important dépassant le simple stade de la fidélisation.

Fidéliser, c'est en effet réussir à créer les conditions qui donnent au consommateur à la fois l'envie et l'occasion de revenir. Si les occasions tiennent avant tout à la dynamique commerciale du marchand, l'envie est créée par de tels services, qui récompensent les acheteurs pour la régularité de leurs achats en les rémunérant.

a) eBuyClub

eBuyClub, fondé à la fin de l'année 2000, est le premier acteur à avoir développé cet outil en France. Le principe est simple : le site rétrocède au consommateur une partie du montant des achats réalisés (entre 1 et 15%) chez un certain nombre de cyber-marchands. Cette rétrocession s'opère de manière trimestrielle par l'envoi de chèque si le montant des rétrocessions cumulées dépasse les 30 euros.

Par ailleurs, ce *cash back* s'applique aux achats personnels et à ceux réalisés par l'ensemble des membres de « l'équipe » à laquelle adhère l'internaute. Il s'agit d'un modèle incitatif à l'achat en ligne. Il permet au consommateur de faire « fructifier » ses achats sur l'internet. Il incite également fortement les internautes à transformer leurs visites sur des sites en actes d'achat. Enfin, la constitution d'équipes a pour effet de créer un phénomène « d'autodynamisation » incitant les membres à réaliser des achats sur l'internet.

⁴³ Cf. Interview de Laurent Fiscal, Directeur général de VirginMega.fr, « La carte prépayée peut être un outil éducatif », *01Net*, 17 mars 2005, <http://www.01net.com/article/271204.html> ; voir aussi : Carte prépayée Infogreffe, <http://www.carteinfogreffe.fr>.

⁴⁴ Les acteurs de cash back ne gèrent pas d'argent pour le compte de tiers, ce sont des intermédiaires qui récompensent les membres de leurs communautés pour l'importance et la régularité de leurs achats chez les marchands dont ils sont partenaires. Il s'agit donc d'une formule proche de la carte de fidélité et non de paiement au sens juridique du terme.

eBuyClub regroupe actuellement environ 180 sites. Il dénombre 150 000 membres qui ont un panier moyen relativement important.

La société propose également sa solution en « marque blanche » à divers acteurs (Mastercard).

b) CashCash

CashCash est une société ayant pour objectif de rendre le consommateur « actionnaire » grâce à ses achats. Elle propose sur l'internet le système cashcash.fr consistant à offrir à un internaute un compte rémunéré automatiquement à partir des achats qu'il réalise.

En pratique, à chaque achat, l'internaute reçoit des euros donnés au nom d'une marque (le taux de reversement par la marque au profit de l'acheteur est au maximum de 20%). Ces points sont ensuite placés afin de constituer une épargne que l'internaute est libre d'utiliser quand il le souhaite. Le système compte environ 10 000 membres et est référencé par 90 marques « marchands » et 15 marques « produits ».

A terme, et si une législation plus adaptée est mise en œuvre, CashCash souhaiterait proposer aux marques d'abonder un compte épargne afin de rémunérer les internautes pour certains de leurs projets⁴⁵.

Parallèlement à ses activités directes auprès du consommateur, CashCash commercialise sa plate-forme de fidélisation en marque blanche aux marques, FAI et autres acteurs de l'internet.

c) CashStore.fr

Cashstore.fr a été lancé en juin 2004 et compte après huit mois d'activité 100 000 utilisateurs. Le site est basé sur le couplement du modèle de cash back et du modèle de réseau social. En effet, chaque utilisateur peut s'inscrire en équipe. Ainsi, à chaque achat, il cumule non seulement de l'argent en retour mais encore son équipe se partage un bonus additionnel. Le but est d'accélérer le cumul d'argent et de créer un réel effet d'entraînement. Le site permet d'obtenir un remboursement variant entre 3 et 20% du montant de la commande chez 85 sites marchands sélectionnés pour leur politique de prix, la qualité de leur service et leur solidité financière.

A noter que les sommes cumulées ne sont exigibles en euros par les acheteurs contre paiement par chèque qu'à partir de 30 € de cash back cumulés.

Le site est par ailleurs le seul à proposer une autre utilisation des sommes gagnées par les internautes. En effet, au lieu de leur permettre de recevoir ces sommes par chèque bancaire à partir de 30 €, le site leur propose, dans le cadre d'un partenariat exclusif avec le site PriceMinister de les transférer sur leur porte-monnaie PriceMinister pour faire des achats sur ce site.

B – Les difficultés pratiques rencontrées par les consommateurs et les acteurs du paiement de petites sommes

⁴⁵ Aux USA, des services identiques sont proposés et ont été accompagnés de mesures fiscales avantageuses. C'est le cas par exemple de Upromise.com (financement des études), Babymint.com, Nesteggz.com (épargner pour la retraite) ou Stockback.com

Avec le développement de ces outils destinés au paiement de petites sommes, plusieurs acteurs ont fait part à l'Observatoire de la cyber-consommation de quelques difficultés voire dans certains cas de réelles fraudes touchant les consommateurs.

1 – L'escroquerie au dialer

Depuis le mois de juin 2004, le nombre de plaintes d'utilisateurs ayant été victimes de surfacturations téléphoniques est en permanente augmentation⁴⁶. En pratique, des internautes découvrent, soit après un message d'alerte de leur opérateur de télécommunications, soit en recevant leur facture téléphonique, qu'ils ont été connectés, malgré eux, sur des numéros surtaxés ou étrangers (appels vers des numéros étrangers, vers des numéros satellitaires).

Il s'agit d'une pratique frauduleuse consistant à forcer l'installation sur le poste informatique de l'internaute d'un kit de connexion vers des numéros surtaxés ou situés à l'étranger. Cette action s'opère sans information préalable du consommateur sur les coûts de connexion et de manière tellement invisible que l'internaute ne constate aucune différence avec sa connexion habituelle. Des consommateurs ayant pris contact avec l'Observatoire de la cyber-consommation ont ainsi indiqué qu'ils avaient été victimes d'une telle pratique à la suite de l'affichage d'une simple *pop-up* ou de l'installation d'un logiciel.

Ces problématiques, déjà identifiées dans le premier rapport de l'Observatoire du 30 mars 2004, ont entraîné la publication par le Forum des droits sur l'internet d'un premier bulletin d'alerte à la fin du mois de juin 2004 pour avertir les internautes de ces pratiques frauduleuses. Depuis cette date, plusieurs plaintes ont été déposées. D'autres pays occidentaux ont également tiré le signal d'alarme⁴⁷.

Le nombre de victimes potentielles est important. En effet, pour qu'un internaute puisse être victime d'une telle pratique, il doit être doté d'un modem analogique branché sur une prise de téléphone active. Trois catégories d'internautes sont susceptibles d'être visés :

- Les internautes dotés d'un raccordement analogique « bas débit » à l'internet par le réseau téléphonique commuté (RTC) ;
- Les internautes dotés d'un raccordement à un réseau numérique à intégration de services (RNIS) ;
- Les internautes dotés d'une connexion ADSL mais ayant en outre un modem analogique connecté à une prise téléphonique. Il peut s'agir, soit d'un ancien modem externe non débranché ou d'un modem interne à l'ordinateur raccordé au réseau téléphonique. Tel est notamment le cas des internautes ayant fréquemment recours à la fonction « Minitel/Fax » de leur ordinateur et donc laissant en permanence branché leur modem analogique au réseau téléphonique. C'est aussi le cas des internautes qui installent leur ordinateur et qui branchent par défaut leur modem interne même s'ils ne configurent que leur connexion haut-débit.

⁴⁶ Cf. Rapport d'activité de l'Observatoire de la cyber-consommation, en annexe. Cette tendance est également confirmée, notamment par l'AFUTT, qui relève dans le rapport 2004 de son Observatoire des plaintes dans le secteur des télécommunications : « une augmentation de près de 20% des plaintes portant sur la téléphonie fixe due principalement à deux graves dérives commerciales : les souscriptions non sollicités et le défaut d'information préalable à la connexion par 'dialers' », <http://www.afutt.org/Particuliers/CPRobservatoire2004.html>.

⁴⁷ En Allemagne, l'autorité de régulation des télécommunications a ainsi procédé à la fermeture de plusieurs dizaines de numéros de téléphone. En Irlande, un blocage à destination de 13 pays du Pacifique a été ordonné par le régulateur national. Enfin, les Pays-Bas se sont déclarés favorables à l'adoption d'une législation spécifique destinée à lutter contre ces techniques de fraude.

La question de l'encadrement des *dialers* n'est pas aisée à appréhender compte tenu du nombre d'acteurs pouvant intervenir :

- l'internaute qui a été victime de l'installation, souvent transparente, du *dialer* ;
- l'opérateur téléphonique facturant les communications enregistrées sur la ligne téléphonique de l'internaute ;
- le fournisseur d'accès à l'internet qui a fourni, dans le cadre du contrat le liant à l'internaute, un accès à l'internet permettant le téléchargement d'un *dialer* mais qui se retrouve mis à l'écart de l'opération dès lors que l'internaute est déconnecté ;
- l'opérateur technique ou le centre serveur fournissant la solution technique ;
- l'éditeur de contenu ayant utilisé le *dialer*.

De manière générale, l'internaute victime se trouve désemparé face à cette fraude. En effet, l'opérateur téléphonique lui demande de s'acquitter du montant complet de la facture, considérant qu'il ne peut être tenu responsable d'un piratage du poste informatique. Pour l'heure, certains opérateurs font bénéficier de gestes commerciaux partiels les internautes qui en sont victimes.

De même, les fournisseurs d'accès à l'internet ne sauraient être tenus responsables dès lors que ces surfacturations sont indépendantes de la prestation qu'ils offrent. Des juridictions de premier degré ont pu néanmoins faire peser une obligation d'information sur ces derniers, mais cette question est aujourd'hui pendante devant la Cour de cassation.

Pour les membres de l'Observatoire de la cyber-consommation, il **semble nécessaire qu'une réflexion soit menée afin de mettre en œuvre auprès de l'ensemble des opérateurs de télécommunications** (opérateur historique ou opérateurs alternatifs) **des gardes-fous permettant de prémunir ou de garantir le consommateur des désagréments liés aux connexions forcées sur des numéros surtaxés.**

En particulier, une action de communication pourrait être menée par ces opérateurs, en collaboration avec les fournisseurs d'accès à l'internet, sur les dangers encourus et les solutions alternatives offertes (accès sélectif modulable⁴⁸ du numéro appelé par l'ordinateur par exemple).

A défaut, et si la France continue d'être victime de ces pratiques, des mesures plus strictes pourraient ensuite être examinées, comme celles adoptées par quelques pays européens (Irlande notamment) et étrangers (Australie), tendant à imposer aux opérateurs de télécommunications le blocage des appels vers certains numéros identifiés comme étant à l'origine de cas de fraude.

2 – L'information du consommateur lors d'achats de biens immatériels par mobile ou de l'obtention de codes d'accès

Entre 2003 et 2004, le trafic généré par l'envoi de SMS+ par les consommateurs est en constante progression. Ainsi, plus de 228 millions de SMS+ ont été envoyés par des utilisateurs de téléphone mobile, soit une progression de 66% par rapport à 2003. Côté chiffre d'affaire, celui s'élève en 2004 à plus de 135 millions d'euros soit une progression de 92% par rapport à l'année précédente⁴⁹.

Parmi les témoignages collectés par le l'Observatoire de la cyber-consommation dans le cadre de son activité, quelques internautes l'ont saisi de difficultés rencontrées lors du

⁴⁸ Outil proposé par l'opérateur téléphonique permettant de bloquer l'accès à certains numéros.

⁴⁹ Association SMS+, Bilan d'activité 2004, <http://www.smsplus.org/index.php?idRubrique=1013>

recours à des services faisant appel au SMS+ (obtention de sonnerie, de logos, de code d'accès).

En effet, concernant l'obtention d'outils de personnalisation du téléphone mobile, des internautes nous ont indiqué n'avoir pas été correctement informés par les sites internet ou les publicités véhiculées par les autres médias, sur l'éventuelle incompatibilité de telle ou telle sonnerie ou logo avec leur modèle de téléphone. Ils ont donc adressé un SMS surtaxé obtenant en retour, dans le meilleur des cas, un outil incompatible avec leur téléphone voire dans certains cas, aucun élément.

De la même manière, plusieurs internautes ont fait part à l'Observatoire de la cyber-consommation de la difficulté d'obtenir gain de cause lorsque, suite à l'obtention d'un code d'accès (par SMS+ ou téléphone), ces derniers se voyaient renvoyer un message d'erreur par le site sur lequel le code était indiqué.

Malgré l'absence d'éléments chiffrés sur les taux d'erreur, il apparaît que **contrairement au paiement par carte bancaire** où un interlocuteur est facilement identifiable en cas de problème (cyber-marchand, banque), **les consommateurs se sentent mal informés des recours éventuels** (opérateur téléphonique, éditeur du site ou du service, opérateur de paiement, etc.) **lorsque survient un incident dans le cadre de ces transactions particulières.**

3 – L'éclatement du secteur du micro-paiement

Autre problématique soulevée par les acteurs auditionnés : l'éclatement des acteurs du micro-paiement. Contrairement à l'Allemagne où une concentration forte des acteurs peut être constatée, la France – et les éléments rappelés ci-dessous le montre – connaît un marché très concurrentiel où les offres sont multiples.

Dans un tel schéma, il devient difficile au consommateur d'avoir une réelle lisibilité aussi bien des offres existantes que de leur coût total. Autre conséquence forte pour le consommateur : celui-ci n'est plus maître de son mode de paiement.

En effet, contrairement au secteur du paiement par carte bancaire où un grand nombre de cartes est accepté (Visa, MasterCard, cartes privatives), le micro-paiement ne connaît pas d'interopérabilité. En conséquence, l'internaute devra souscrire à de nombreuses solutions de paiement, en fonction des cyber-marchands auprès de qui il souhaite contracter.

Cette situation a un effet direct pour le cyber-marchand : l'internaute risque de ne pas transformer son intention en acte d'achat dès lors que parmi les solutions de paiement proposées, aucune ne remporte son choix.

Plusieurs acteurs se sont déclarés favorables à la mise en place de mécanismes d'interopérabilité entre les solutions de micro-paiement existantes sur le marché. Cela pourrait passer par l'élaboration de standards communs, comme cela a pu être le cas pour la carte bancaire, ou par la mise en place de solutions commerciales offrant un choix au consommateur final.

Tel est le cas par exemple de la plate-forme Abacoo, développée par Biz N'Cash. Il s'agit d'une plate-forme unifiée de micro-paiement proposant aux marchands d'intégrer un outil laissant à l'internaute le choix de sa solution (porte-monnaie électronique, paiement par courrier électronique, Audiotel, SMS+, etc.).

4 – La difficile compréhension du dispositif bancaire français

Dernier élément soulevé par les acteurs interrogés et en particulier par ceux qui ne sont pas originaire du secteur bancaire. Ces derniers témoignent de la difficile compréhension de la loi bancaire en particulier face à de nouvelles pratiques comme celles du rétro-paiement.

De même, les acteurs ayant développés des produits innovants de paiement sur l'internet s'interrogent sur leur soumission au régime juridique des établissements financiers, notamment suite à la transposition en droit français de la directive « monnaie électronique ».

Enfin, certains plaident en faveur de la création d'un nouveau statut en droit bancaire français. Ce nouveau statut d'intermédiaire aurait vocation à s'appliquer aux structures intervenant dans la chaîne du paiement en ligne sans pour autant avoir directement des activités financières.

Cette idée est également envisagée par l'Union européenne dans le cadre de la préparation de son texte relatif au cadre juridique applicable aux moyens de paiement qui souhaite créer un nouveau statut d'institution de paiement à destination des sociétés dont les activités se limitent à fournir des services de paiement. Ces établissements seraient alors soumis à des obligations moindres.

Conclusion

Grâce aux nombreuses technologies et outils développés par le secteur bancaire et des prestataires, la France a réussi à faire diminuer fortement le niveau de la fraude à la carte bancaire à l'occasion de transactions réalisés en ligne.

Seulement, les nouvelles techniques utilisées par les délinquants nécessitent de nouvelles actions à laquelle doivent prendre part de manière active les utilisateurs, qui sont actuellement incontournables sur le secteur.

En particulier, l'Observatoire de la cyber-consommation constate la nécessité :

- de **développer la sensibilisation des internautes en matière de *phishing*** au travers de la diffusion de plusieurs conseils pratiques simples ;
- de **réaliser des actions d'information du particulier sur la vulnérabilité de son ordinateur** et sur les outils disponibles sur le marché pouvant renforcer la protection de son poste informatique (virus, espioniciels, etc.)

Dans le secteur du micro-paiement, et même si celui-ci demeure relativement varié et éclaté créant pour le consommateur une certaine confusion et un manque de lisibilité, les problèmes constatés sont de deux ordres.

Pour l'Observatoire de la cyber-consommation, une réflexion plus poussée devrait ainsi être menée en matière **d'information du consommateur lors d'achats de biens immatériels par mobile** (compatibilité du téléphone, etc.) ou d'obtention de codes d'accès.

De manière plus urgente, il apparaît enfin qu'une étude soit réalisée afin de **renforcer la protection du consommateur vis-à-vis des dérives actuellement constatées dans le secteur des *dialers***. Cette analyse devra être menée en partenariat avec l'ensemble des acteurs afin de renforcer l'information et la sensibilisation des internautes aux problèmes auxquels ils peuvent être exposés sur l'internet et mettre au point des gardes-fous permettant de prémunir ou garantir le consommateur des désagréments liés à ces connexions forcées sur des numéros surtaxés.

Annexe 1 : Composition de l'Observatoire de la Cyber-Consommation
--

Pour mener ses travaux, l'Observatoire de la Cyber-Consommation était composé de :

Jean-Luc DANIEL

Bureau droit de la consommation, Direction générale à la concurrence, à la consommation et à la répression des fraudes ;

Didier ETIENNE

Mission pour l'économie numérique, Ministère de l'économie, des finances et de l'industrie ;

Patricia FOUCHER

Juriste, Institut national de la consommation ;

Cédric MANARA

Professeur de droit à l'EDHEC Business School ;

Cécile MOULARD

Directrice Marketing Europe, Ilius ;

Christian NATALI

Commissaire, Brigade d'enquête sur les fraudes liées aux technologies de l'information (BEFTI), Préfecture de police de Paris ;

Hervé SOYMIE

Secrétaire général, Conseil supérieur de la télématique ;

Benoît TABAKA

Chargé de mission, Forum des droits sur l'internet, rapporteur de l'Observatoire permanent de la Cyber-consommation.

Annexe 2 : Liste des personnes auditionnées ou consultées
--

Pour la réalisation de ce rapport, les membres de l'Observatoire de la Cyber-Consommation ont procédé à l'audition ou à des entretiens avec les personnes suivantes :

Pierre ACHACHE, Président, Oxone Technologies ;

Catherine BARBA, Directrice générale, CashStore.fr ;

Michel BAUJARD*, Président, Syndicat professionnels des médias de télécommunication (SPMT) ;

Eric BAROUILLET, Directeur, Firstgate "Click & Buy" France ;

Denis BEAU, Secrétaire général, Observatoire de la sécurité des cartes de paiement, Banque de France ;

Thomas BINCAZ, Directeur marketing et développement, Fidelipius ;

Olivier BON, Responsable Ligne de solutions Kiosque, France Telecom ;

Martine BRIAT*, Responsable des affaires juridiques et bancaires, Groupement des Cartes Bancaires ;

Joël BURTIN, Directeur général, Oxone Technologies ;

Jean-Pierre BUTHION*, Responsable des produits et services, Groupement des Cartes Bancaires ;

Olivier CHEDEVILLE, Directeur marketing de la banque à distance, Société générale ;

Dominique CLAUDEL, Directeur des études stratégiques "Banque de détail", Société générale ;

Christopher COONEN, Directeur général, Paypal France ;

Manuel CRUZ, Président du Directoire, Jet Multimédia ;

Fredrik DANELIUS, Paynova France ;

Eric DAUDON*, Directeur technique, Société Eurovox - Allopass ;

Jean-Marie DELBARY, Société CarpeDiem ;

Jean-Marie DRAGON, Responsable monétique, Direction Marketing et Développement, La Poste ;

Jean-Pierre DUBORD, Directeur adjoint, Entité Carte, Experian ;

Bernard DUTREUIL, Directeur du département Systèmes et moyens de paiement, Fédération bancaire française ;

Roland ENTZ, Directeur général France, Visa ;

Emmanuel FLEURY, Commissaire principal, Chef adjoint de la Brigade sur les fraudes aux moyens de paiement, Direction de la Police judiciaire ;

Laurent GOMIS*, Chargé de mission, Confédération Logement et Cadre de Vie (CLCV) ;

Anne-Sophie GUILLET, Juriste, France Telecom ;

Jacques HARASSE, Département Systèmes et moyens de paiement, Fédération bancaire française ;

Abdallah HITTI, Directeur, Paynova France ;

Léon-Charles HOTTIER, Directeur général, Société financière du porte-monnaie électronique interbancaire (SFPMEI) ;

Denis JEANTEUR, Directeur, Sympass ;

Jacques LAMBERT, Association française des utilisateurs de télécommunications (AFUTT) ;

Sébastien LE CHARPENTIER, Responsable Marketing et Nouvelles technologies, SAS Carte Bleue ;

Mathilde LENOIR, Directeur général, Biz-n-Cash.fr ;

Sandrine LEONARDI, Directrice financière, CashStore.fr ;

Grégory LEVIS, Directeur technique, Biz-n-Cash.fr ;

Frédéric LOOS, Directeur commercial, Paybox Services ;

Paul NAHON*, Directeur général, Société Eurovox - Allopass ;

Christian NATALI, Commandant de police, Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Direction de la Police judiciaire ;

Gilles NECTOUX, Président directeur général, eBuyClub.com ;

Bernard OVINK, Vice Président, Responsable eCommerce, Visa ;

Thierry PEYRE, Directeur associé, Mobile Trend ;

Jacques SCHUHMACHER, Direction de la Distribution, Commerce et Moyens de paiement électroniques, Caisse nationale des Caisses d'Epargne ;

Sandra WOËHLING*, Juriste, UFC-Que Choisir ;

Mung Ki WOO, Directeur technique, Société financière du porte-monnaie électronique interbancaire (SFPMEI).

Les personnes dont le nom est suivi d'un astérisque(*) ont fait l'objet d'une audition lors des consultations précédant le premier rapport de l'Observatoire.

Annexe 3 : Rapport d'activité de l'Observatoire permanent de la Cyber-Consommation

Le Forum des droits sur l'internet a créé, en septembre 2003, Cyberconso, l'Observatoire de la cyberconsommation. L'objectif de cet Observatoire était d'identifier les problématiques juridiques qui pouvaient exister en matière de commerce électronique.

A cette fin, l'Observatoire a mené une enquête sur les pratiques des consommateurs et des professionnels de la vente à distance au regard du cadre juridique applicable. De septembre 2003 à mars 2004, l'Observatoire a collecté les témoignages de près de 400 internautes. Il a également procédé à l'audition de nombreux acteurs du commerce électronique : marchands, comparateurs de prix, intermédiaires techniques et représentants des consommateurs.

Le premier rapport a été remis le 30 mars 2004 aux autorités publiques. Trois constats ont été réalisés : le droit de la vente à distance est adapté au commerce électronique, sous réserve de certains aménagements ; une nouvelle forme de commerce électronique se développe (relations commerciales entre particuliers) posant de nouvelles questions quant à l'encadrement de ces relations ; les consommateurs souhaitent être mieux alertés sur les fraudes observables sur l'internet.

1.- Les fonctions de l'Observatoire de la Cyber-Consommation

Faisant suite à son premier rapport, il a été décidé de faire évoluer les fonctions de l'Observatoire. Outre son activité de veille sur les pratiques du commerce électronique, l'Observatoire CyberConso a pour fonction de publier des bulletins d'alerte à destination des consommateurs.

1.1 – Le travail de veille des pratiques de la Cyber-Consommation

La première fonction de l'Observatoire est de mener à bien un travail de veille sur les pratiques de la CyberConsommation. L'objectif est d'identifier les problématiques qui demeurent en la matière afin, ensuite et si besoin, qu'un processus de concertation puisse être mis en oeuvre afin d'apporter des solutions. Les internautes sont également sollicités en ligne afin de leur permettre de faire part à l'Observatoire de l'ensemble de leurs remarques, commentaires ou problèmes concernant le commerce électronique.

Le premier thème choisi par l'Observatoire, pour son travail entre mars 2004 et mars 2005, a été celui du paiement en ligne (paiement traditionnel par carte bancaire, nouveaux acteurs du marché, micro-paiement).

1.2 – Le travail d'alerte des internautes sur les fraudes constatées

A ce jour, de multiples fraudes (ou supposées fraudes) se développent sur l'internet. Souhaitant combler une carence constatée, l'Observatoire émet périodiquement des bulletins d'alerte à destination des internautes et des médias sur des fraudes avérées et qui se seraient développées. A cette fin, les membres de l'Observatoire se réunissent toutes les six semaines afin d'analyser les dernières pratiques auxquelles sont confrontés les internautes.

Au cours des derniers mois qui se sont écoulés, l'Observatoire a émis 2 bulletins d'alerte.

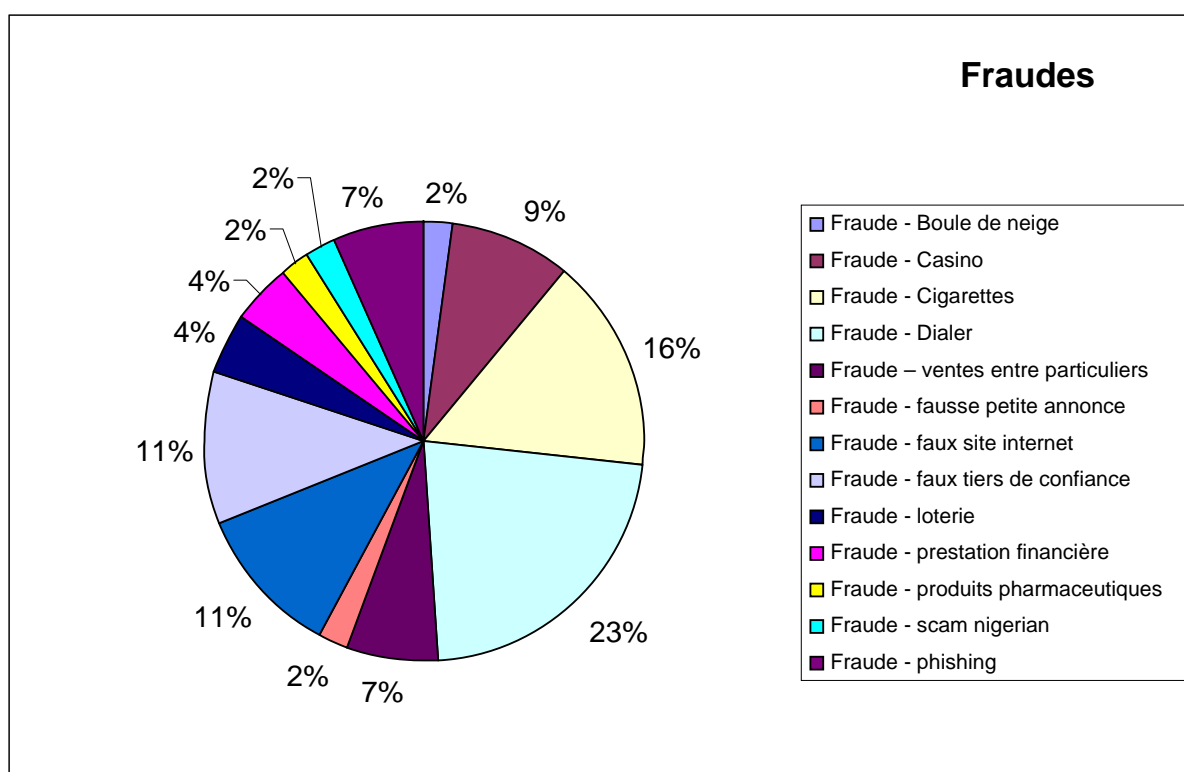
Le premier a été publié au début du mois de juillet 2004 et portait sur les problèmes rencontrés par les internautes en matière de surfacturation téléphonique suite à l'installation d'un logiciel sur leur ordinateur.

Le deuxième bulletin a été publié au cours du mois de janvier 2005 et portait sur une nouvelle infraction se développant sur l'internet : le phishing. Des conseils pratiques étaient, également, dispensés par l'Observatoire.

2. – Synthèse des fraudes répertoriées par les membres de l'Observatoire

Afin de mener à bien son travail d'alerte, l'Observatoire synthétise les plaintes reçues des internautes afin de réaliser une typologie des cas de fraude rencontrés. Au cours de l'année 2004, les chiffres suivants ont été obtenus.

NB : les données suivantes ne constituent pas une analyse scientifique des cas de fraude rencontrés sur l'internet mais uniquement un agrégat d'informations chiffrées en provenance des membres de l'Observatoire.



3. - Contacts clés selon les problèmes et fraudes rencontrés sur l'internet

NB : Le recours aux associations de consommateur et aux juges n'est mentionné que dans la rubrique « Problèmes contractuels ». Ils sont naturellement compétents pour intervenir également vis-à-vis des autres problématiques

Problématiques	Contacts IDF	Contact province
Problèmes contractuels	Associations de consommateurs Juges Service de médiation	Associations de consommateurs Juges Service de médiation
Problèmes liés au droit de la consommation sanctionnés pénalement	DDCCRF Brigade de Répression de la Délinquance économique (BRDE)	DDCCRF DRPJ/DIPJ/SRPJ
Vente à la boule de neige	DDCCRF Brigade de répression de la délinquance astucieuse (BRDA)	DDCCRF DRPJ/DIPJ/SRPJ
Casino en ligne	Renseignements généraux/Brigade de répression du banditisme CST/CTA (si revenu partagé)	Renseignements généraux DRPJ/DIPJ/SRPJ CST/CTA (si revenu partagé)
Cigarettes en ligne	Direction des douanes	Direction des douanes
<i>Dialers</i>	Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) CST/CTA	OCLCTIC/DRPJ CST/CTA
Enchères	BRDA DDCCRF CST/CTA (si revenu partagé)	DRPJ/DIPJ/SRPJ DDCCRF CST/CTA (si revenu partagé)
Fausses petites annonces	BEFTI	OCLCTIC
Faux sites internet	BEFTI	OCLCTIC
Faux tiers de confiance	BEFTI	OCLCTIC

Problématiques	Contacts IDF	Contact province
Loteries en ligne	BRDA DDCCRF CST/CTA (si revenu partagé)	DRPJ DDCCRF CST/CTA (si revenu partagé)
Phishing	BEFTI	OCLCTIC
Prostitution	Brigade de Répression du proxénétisme (BRP)	DRPJ/SRPJ/DIPJ
Médicaments	Brigade de Répression de la Délinquance contre la personne (BRDP)	DRPJ/SRPJ/DIPJ
Spamming	BEFTI CNIL DDCCRF CST/CTA (publicité en faveur de services à revenus partagés)	DRPJ/SRPJ/DIPJ CNIL DDCCRF CST/CTA (publicité en faveur de services à revenus partagés)
Protection des données personnelles	CNIL BEFTI	CNIL DRPJ/SRPJ/DIPJ
Protection des mineurs / Pédophilie	Brigade de protection des mineurs (BPM) CST/CTA (si le site utilise un moyen de paiement à revenus partagés)	OCLCTIC DRPJ/SRPJ/DIPJ CST/CTA (si le site utilise un moyen de paiement à revenus partagés)
Fraude aux paiements	Brigade des fraudes aux moyens de paiement (BFMP)	DRPJ/SRPJ/DIPJ