Fraude à la carte bancaire sur internet: l'UFC-Que Choisir donne les codes pour une sécurité renforcée !

Sommaire

I – Constats : une fraude internet en augmentation constante 3

1 - Un taux de fraude sur les CB qui monte 3

2 - La fraude des cartes sur internet, une fraude non maîtrisée 4

3 - Internet : 5% des transactions, mais 33% du coût de la fraude ! 5

4 - Qui paie cette fraude ? 7

II – Les causes de cette fraude à la carte bancaire 9

1 – Origine du problème : l'usurpation des données de cartes bancaires 9

2 – L'échec du 3D Secure en France 12

3 – L'exemple Anglais : le 3D Secure fait baisser la fraude quand il est massivement utilisé 16

III – La fraude à la carte bancaire, une plaie au quotidien pour les consommateurs 21

1 – En théorie, une règlementation très protectrice sur les fraudes internet 21

2 – Dans les faits, de nombreux freins au remboursement des consommateurs 22

3 – Autre conséquence : l'assurance des moyens de paiement, peu utile et surfacturée 26

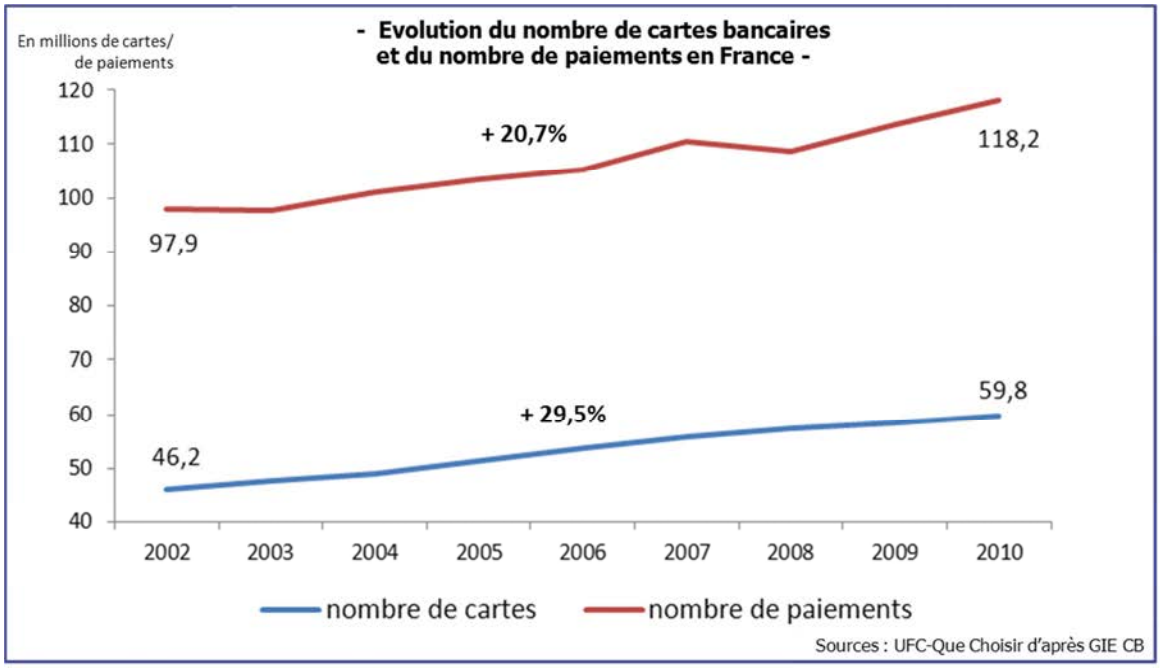
IV – Conseils aux consommateurs pour éviter les fraudes à la carte bancaire sur internet 27

V – Demandes de l'UFC-Que Choisir sur la sécurité de la carte bancaire sur internet 29

I – Constats : une fraude internet en augmentation constante

1 - Un taux de fraude sur les CB qui monte

La carte bancaire est le premier moyen de paiement en France depuis 2002. A cette date, 46,2 millions de cartes bancaires « CB » étaient en circulation. Depuis cette date, le nombre de cartes bancaires a encore augmenté de 30% pour atteindre près de 60 millions de cartes « CB » en 2010, auquel il faut ajouter les cartes bancaires non marquées « CB » (environ 4 millions de cartes). Le nombre de paiements a également augmenté sur la période dans une proportion similaire : +20,7%.



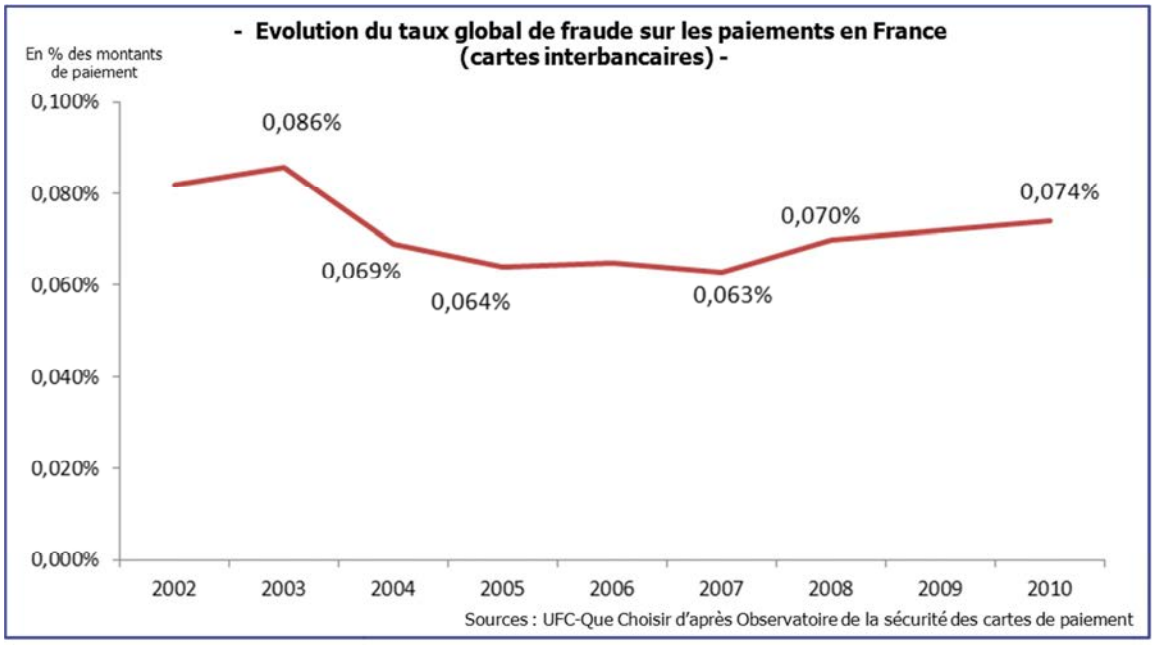
Aujourd'hui, la carte bancaire est à l'origine de 45% des paiements de proximité. Cette domination est encore plus poussée sur les paiements à distance, puisque 80% des paiements à distance se font par carte bancaire (chiffres FEVAD).

La carte bancaire est donc, plus que jamais, un moyen de paiement de masse utilisé par l'ensemble des Français et un instrument privilégié de la vie économique.

Cependant, en dépit de cette massification encore accrue des paiements par carte bancaire, la sécurité des paiements par carte bancaire a connu une évolution contrastée. Pour cet aspect, nous nous appuierons sur les études de l'Observatoire de la sécurité des cartes de paiement, comité regroupant consommateurs, commerçants, émetteurs et autorités publiques, qui réalise chaque année un audit du fonctionnement des systèmes de paiement par carte, et de la fraude à la carte bancaire en particulier.

Des statistiques de l'Observatoire nous observons :

- Qu'entre 2003 et 2007, le taux moyen de fraude sur les paiements par carte bancaire en France a diminué. Cette diminution correspondant à la généralisation des systèmes EMV (Europay Mastercard Visa) tant en France -le GIE Cartes Bancaires n'a adhéré au système qu'en 2006, mais son système en était déjà très proche- qu'en Europe, où beaucoup de pays utilisaient avant cela des cartes bancaires à pistes magnétiques. Ce standard généralise l'usage de la carte à puce et du code confidentiel « PIN », système beaucoup plus sécurisé que les cartes à pistes magnétiques -la puce n'étant pas copiable- ce qui accroît fortement la sécurité des paiements de proximité.



- Cependant, en dépit de la mise en place du standard EMV, la fraude sur la carte bancaire recommence à augmenter sans discontinuer depuis 2007 : entre cette date et 2010, le taux de fraude a ainsi connu une hausse de 17,5%.

Quelles sont les causes de cette hausse, et ses conséquences pour les consommateurs ?

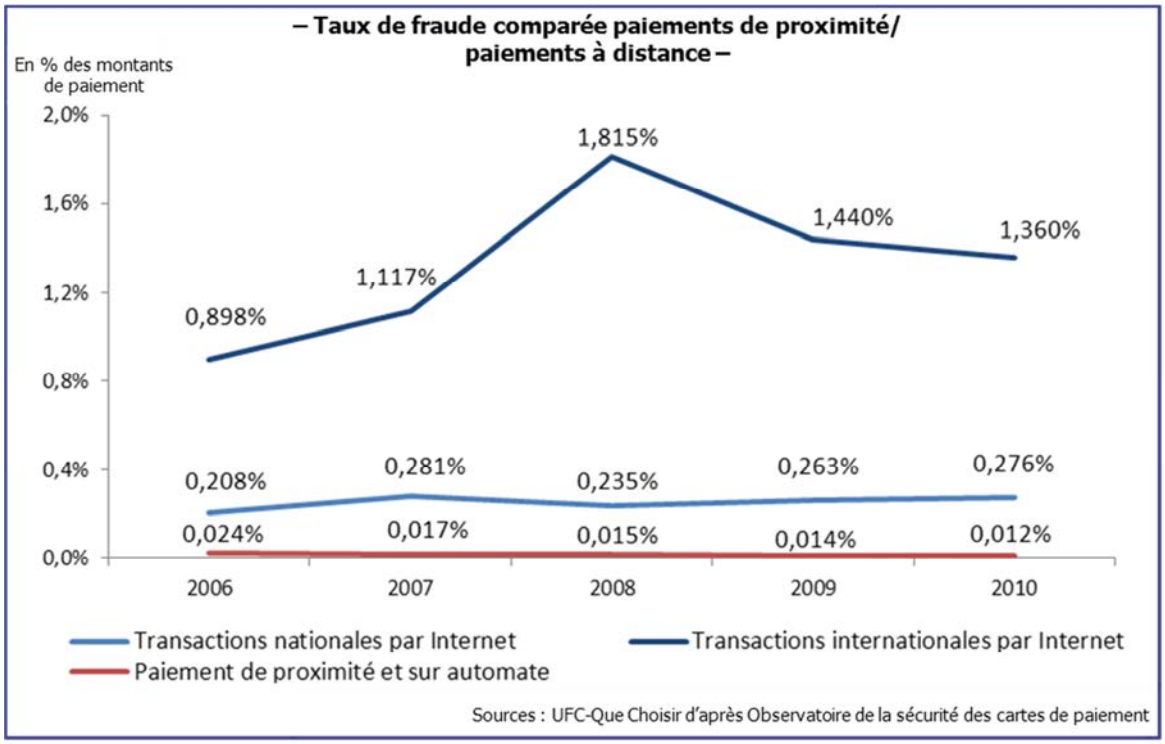
2 - La fraude des cartes sur internet, une fraude non maîtrisée

Le détail des chiffres contenus dans les rapports annuels de l'Observatoire de la sécurité des cartes de paiement permet de comprendre l'origine de cette hausse de la fraude, qui est concentrée sur les paiements sur internet. En effet :

- Le taux de fraude des paiements de proximité est divisé par deux sur la période. Déjà très bas (0,024%), le taux de fraude sur les paiements de proximité est aujourd'hui totalement marginal (0,012%). A ce niveau de fraude, on peut dire que la sécurité de la carte bancaire pour les paiements de proximité est maîtrisée. Il convient cependant de noter que le taux de fraude sur les retraits est aujourd'hui deux fois plus élevé que sur les paiements (0,024%), et en hausse depuis 2005.
- En revanche, le taux de fraude sur les paiements internet nationaux est 23 fois plus élevé : 0,276% du montant de ce type de paiement. Il y a donc, sur internet, 1 euro de fraude tous

les 360 euros dépensés. Au total sur ce type de paiement il y a plus d'une fraude (1,18 fraude) à chaque minute de l'année ! Ainsi, en seulement 5 ans, le taux de fraude sur les paiements nationaux a augmenté de 32,7%. Ces paiements représentent en montant 97% du total des paiements internet en France.

- Le taux de fraude sur les paiements internationaux est encore plus élevé : 1,36% en 2010 ! Ce taux a doublé entre 2006 et 2008 (+102% en trois ans !), avant de connaître une diminution qui, si elle est significative (-25%), ne compense pas la hausse vécue en début de période. Entre 2006 et 2010, la hausse de la fraude sur les paiements internationaux est très importante (51,5%). Au final, le taux de fraude actuel est incroyablement élevé : 1,36% !



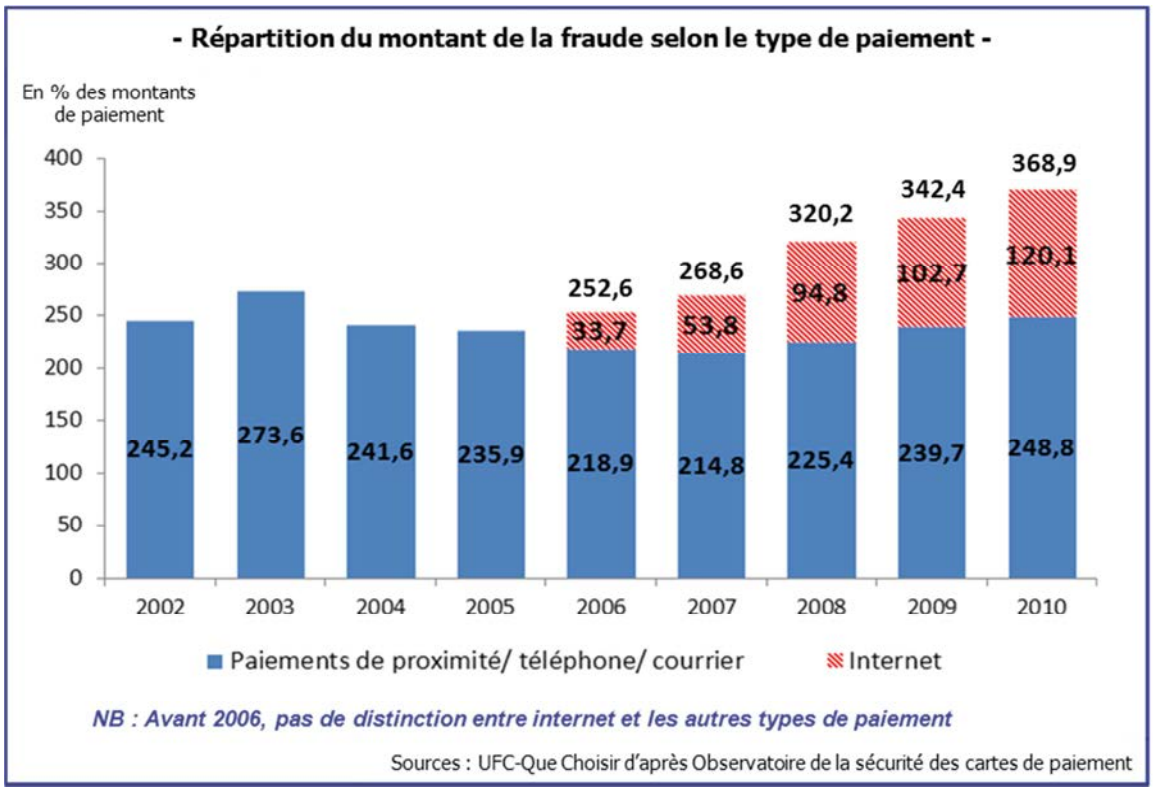
A noter également que la fraude sur les paiements à distance hors internet -donc les paiements effectués par courrier ou par téléphone- est également en hausse. Sur les paiements nationaux, cette fraude est ainsi passée de 0,194% en 2002 à 0,231% en 2010, et sur les paiements internationaux, de 0,684% à 1,193%. Cependant, les montants en jeu étant bien plus limités (27,3 millions d'euros pour la fraude nationale, soit le tiers de la fraude sur internet : 7,8 millions d'euros sur la fraude internationale, un chiffre en baisse), nous nous focaliserons sur la fraude internet, dont l'enjeu nous semble plus considérable.

Ainsi, l'étude de ces statistiques révèle clairement que la hausse globale de la fraude sur les paiements par carte bancaire entre 2002 et 2010 est due à une forte hausse de la fraude sur les paiements internet. Mais quel est le coût de cette fraude ?

3 - Internet : 5% des transactions, mais 33% du coût de la fraude !

La fraude globale sur les paiements par carte bancaire a coûté en 2010 près de 370 millions d'euros. Ce coût global a augmenté de 50% depuis 2002, un chiffre bien supérieur (comme signalé plus haut) à la croissance du nombre de paiements par carte bancaire sur la période (+20,7%).

Le coût de la fraude sur internet est détaillé dans les rapports annuels de l'Observatoire des moyens de paiement depuis l'année 2006, année qui coïncide d'ailleurs avec la montée en puissance du e-commerce. Force est de constater qu'internet constitue une part grandissante des montants fraudés.



Ainsi, en 2006, le montant des fraudes internet ne représentait que 13,3% du total de la fraude sur la carte bancaire. En 2010, soit seulement 5 ans plus tard, la fraude sur internet représentait 120,1 millions d'euros, et un tiers de la fraude totale ! Ce chiffre est d'autant plus important que les paiements par internet ne représentent que 5% du total des paiements effectués en France. Ainsi, internet représente 5% des paiements, mais 33% de la fraude ! En recoupant le montant total de la fraude internet en 2010 et le montant moyen d'une fraude cette année-là (119 euros pour une carte interbancaire), on se rend compte qu'au total il y a eu plus d'1 million de fraudes sur internet en 2010, soit deux fraudes par minute en France !

Le graphique ci-dessus est particulièrement parlant : alors que la fraude « traditionnelle » est assez stable depuis dix ans –aux alentours de 240 millions d'euros– période où le nombre d'opérations a augmenté de 20,7% sur la période, la fraude internet est venue progressivement s'ajouter à la fraude traditionnelle pour devenir le poste unique de croissance de la fraude.

Ce montant et cette proportion de fraude est d'autant plus inquiétant que le marché français du paiement en ligne n'en est qu'à ses débuts : 31 milliards d'euros en 2010. A cette même date, le Royaume-Uni, pays à la population et au PIB très proche de celui de la France, a effectué 63,4 milliards d'euros de paiements (54 milliards de livres) en ligne en 2010, ce chiffre continuant bien sûr à croître.

Par conséquent, à taux de fraude inchangé, une France qui rattraperait les pratiques de paiements à distance du Royaume-Uni aurait un montant de fraude de 536 millions d'euros, dont 268 millions rien que sur la fraude sur internet.

Pour un commerce électronique représentant 25% de l'ensemble du commerce, chiffre considéré comme plausible d'ici 2020 dans la plupart des études (voir notamment l'étude du Crédoc de

novembre 2010 *Quel commerce pour demain ? La vision prospective des acteurs du secteur*, où les professionnels tablent sur un e-commerce à 25%), la fraude atteindrait les 850 millions d'euros !

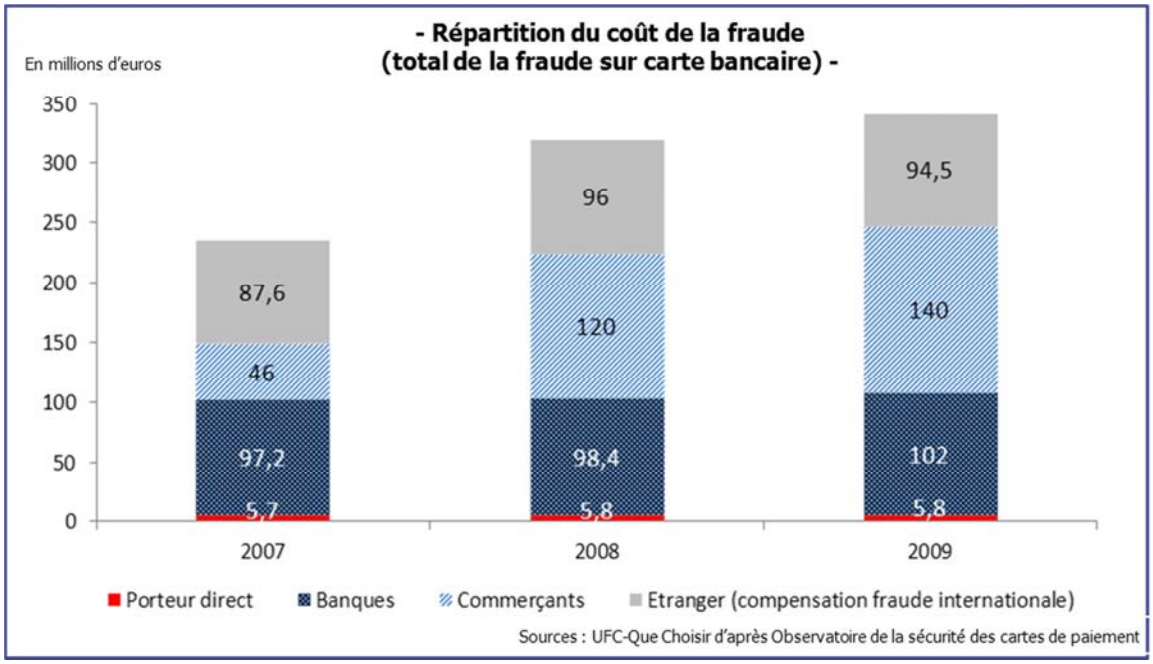
Il semble ainsi indispensable de juguler la fraude sur internet, sans quoi le montant des fraudes risquerait d'être préjudiciable à la fois au consommateur, mais aussi au commerce électronique dans son ensemble.

4 - Qui paie cette fraude ?

Le montant de la fraude sur la carte bancaire pourrait n'avoir aucune importance sur le commerce si celle-ci n'était payée que par les banquiers, distribuant après tout les moyens de paiements à leur clientèle. Or, ce n'est pas le cas.

Les chiffres de l'Observatoire de la sécurité des cartes de paiement montrent que la fraude est supportée par 4 types d'acteurs : l'étranger, le banquier, le commerçant et le client (le porteur de la carte). D'après ce même observatoire, pour l'année 2009, la répartition du coût de la fraude se ferait de la manière suivante :

- Les acteurs étrangers (commerçants ou banquiers) supportent une part importante de la fraude, du fait des conventions internationales existantes dans le domaine bancaire qui partagent les responsabilités lors des paiements dans le cadre de l'EMV et du 3D Secure. En 2009, ces acteurs étrangers ont supporté 94,5 millions d'euros
- En dehors de cette part, les 247,9 millions d'euros restants sont partagés de la manière suivante :
  - 56,5% sont supportés par les commerçants, soit 140 millions d'euros ;
  - 41,1% sont supportés par les banquiers, soit 102 millions d'euros ;
  - 2,3% sont supportés par les consommateurs, soit 5,8 millions d'euros. Il s'agit de la fraude payée directement par le consommateur, c'est-à-dire l'ensemble des sommes détournées avant opposition pour les paiements traditionnels, des sommes non remboursées ou non réclamées par les clients pour les paiements en ligne et de la « franchise » payée par les consommateurs fraudés en cas de faute lourde (NB : ces sujets seront approfondis un peu plus loin dans l'étude).



Or, dans la réalité, et comme toute « consommation intermédiaire », les sommes payées par le commerçant et le banquier sont refacturées au « consommateur final » qu'est le client.

Ainsi :

- Le commerçant paie la fraude à travers le TICO (Ticket commerçant), qui est inclus dans la commission d'interchange payée par le commerçant à sa banque… Et répercutée au consommateur sur le prix de vente !
- Le banquier refacture le coût de la fraude à son client via ses différents tarifs bancaires, et en particulier via l'assurance des moyens de paiement (voir plus bas).

Les consommateurs sont donc bien les principales victimes. En réalité, les banquiers qui distribuent à leurs clients des cartes bancaires dont la sécurité sur internet semble problématique, ne supportent pas le coût du produit défectueux qu'est la carte bancaire dans les paiements sur internet… Dès lors qu'ils n'en subissent pas les coûts, les banquiers n'ont donc aucune incitation à améliorer la sécurité de la carte bancaire.

Nous voyons ainsi que la hausse globale de la fraude à la carte bancaire constatée dans les statistiques de l'Observatoire de la sécurité des cartes de paiement est principalement due à la fraude internet, laquelle présente des taux de fraude incroyablement plus élevés.

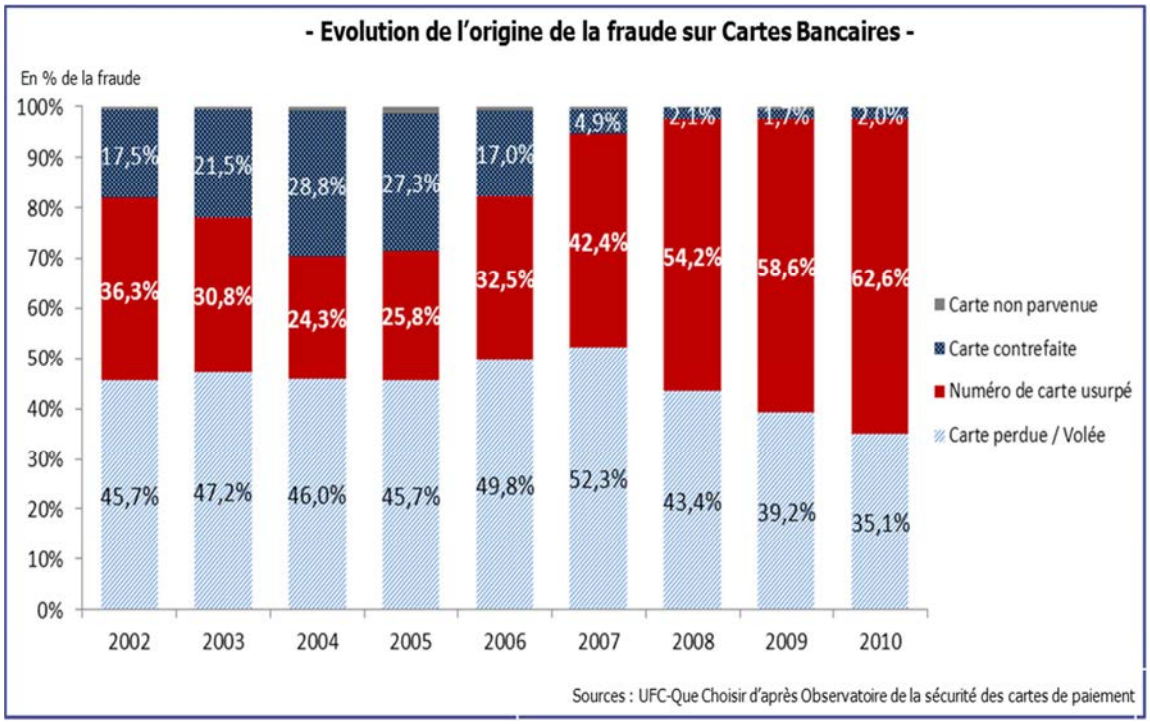
Après ce constat, nous allons chercher à comprendre pourquoi la fraude à la carte bancaire sur internet est bien plus élevée que la fraude à la carte bancaire sur les paiements de proximité.

II – Les causes de cette fraude à la carte bancaire

1 – Origine du problème : l'usurpation des données de cartes bancaires

Là encore, l'étude des statistiques de l'Observatoire de la sécurité des cartes de paiement permet de comprendre l'origine principale de la fraude sur les cartes bancaires. En effet on constate :

- Qu'entre 2002 et 2007, la fraude était issue principalement des pertes ou vols des cartes bancaires. Ce poste représentait quasiment la moitié de la fraude. Les cartes contrefaites constituaient également un poste important : à cette époque en effet, la piste magnétique de la carte bancaire pouvait être copiée pour être utilisée dans les pays frontaliers utilisant des terminaux de paiement à piste, ou en France sur les quelques systèmes utilisant la piste (autoroutes par exemple). L'usurpation des numéros de cartes étaient également importantes, mais sans dépasser les vols ou pertes de cartes.



- L'année 2008 constitue un tournant radical dans les causes de la fraude : les numéros de cartes usurpés deviennent fortement majoritaires dans les causes de la fraude, alors que les cartes perdues ou volées déclinent fortement, et que les cartes contrefaites, déjà en déclin sur les deux années précédentes, deviennent très marginales. En 2010, l'usurpation des numéros de cartes constitue près des deux tiers de la fraude issue de la carte bancaire (62,6%).

L'Observatoire de la sécurité des cartes de paiement décrit l'usurpation du numéro de carte comme une situation où *« le numéro de carte d'un porteur est relevé à son insu ou créé par «moulinage» (à l'aide de générateurs aléatoires de numéros de carte) et utilisé ensuite en vente à distance »*. Le centre du problème de la fraude à la carte bancaire semble donc bien être l'utilisation du numéro de carte pour effectuer les paiements sur internet.

<u>Les données fixes de carte bancaire, facilement copiables</u>

Les systèmes de paiements de proximité par carte bancaire utilisent un double dispositif :

- La puce, infalsifiable ;
- Alliée au code PIN, confidentiel.

Ce double dispositif permet d'obtenir une sécurité convenable sur les paiements de proximité, la puce protégeant les porteurs d'une copie de leur carte, le code confidentiel (et le blocage automatique au bout de 3 essais manqués) assurant au système que l'utilisation de la carte est bien faite par le porteur.

Jusqu'à très récemment, rien de tel n'a été développé pour les paiements en ligne par carte bancaire. La plupart des paiements internet en France se basent encore aujourd'hui uniquement sur des données statiques :

- Les numéros de la carte bancaire figurant au recto de la carte ;
- La date de validité de la carte bancaire ;
- Le cryptogramme visuel (CVx2, les trois derniers chiffres à l'arrière de la carte).

Ce dernier élément a été ajouté au début des années 2000 dans le but de renforcer la sécurité contre les copies de cartes (ce numéro n'étant pas en relief, il est plus difficile à copier au « fer à repasser »).

- Exemple d'informations fixes demandées lors d'un paiement en ligne -

Ces données présentent la particularité d'être valables aussi longtemps que dure la carte, c'est-à-dire tant qu'aucun remplacement pour fraude, perte ou vol –qui entraînent l'attribution d'une nouvelle carte avec de nouveaux numéros– n'est effectué. Elles peuvent ainsi durer plusieurs années, voir des décennies… En réalité, jusqu'à ce que la carte fasse l'objet d'une opposition !

Ce qui laisse autant de temps aux fraudeurs pour capturer les données de carte bancaire, puis les utiliser tant que le client ne se rend pas compte de la fraude.

<u>Méthodes de récupération des données de cartes bancaires</u>

Les fraudeurs disposent de différents moyens pour récupérer les données de carte bancaire d'un client :

- Les « Spywares » (ou espiogiciels) : ce sont des programmes malveillants qui s'installent automatiquement –souvent depuis un logiciel gratuit précédemment téléchargé– sur l'ordinateur, afin d'enregistrer les mots de passe ou codes confidentiels tapés par l'utilisateur sur son clavier. Ces données sont ensuite envoyées directement au fraudeur par le programme ;
- Via le Phishing (ou hameçonnage), qui consiste pour un fraudeur à se présenter, le plus souvent dans un mail, comme un des fournisseurs du consommateur (sa banque, sa société de cartes de crédit ou sa compagnie de téléphone) afin de lui soutirer des renseignements personnels : le plus souvent son numéro de carte bancaire et/ou le code confidentiel de cette carte, mais également ses numéros de compte bancaire, sa date de naissance, etc. En dépit de leur orthographe française souvent approximative, les messages qui sont envoyés ressemblent beaucoup –et de plus en plus– à de « vrais messages », notamment parce qu'ils reproduisent les logos des fournisseurs et proviennent d'adresses mails très proches de celles de ces même fournisseurs. Beaucoup de consommateurs se laissent ainsi abuser par ce type de message : le fait qu'ils fournissent eux-mêmes leurs données de cartes bancaires aux fraudeurs rend très difficile le remboursement des montants fraudés, alors même que ce type de message se multiplie.

- Exemple d'email de Phishing (ou hameçonnage) -

Expéditeur: Verified By Visa <alert@verifiedbyvisa.fr>
Date: 14 mai 2011 00:28:03 HAEC
Destinataire:
Objet: votre carte bancaire est supendue
Répondre à: Cher@server.webglobal.es, Utilisateur@server.webglobal.es

Verified by VISA MasterCard SecureCode

Cher utilisateur Visa / MasterCard ,

Il a été porté a notre attention que votre Carte VISA / MasterCard doit être protéger dans le cadre de notre engagement continu pour protéger votre carte et à réduire les cas de fraude.

Nous avons determiné que quelqu'un a peut-être utilisé Votre Carte sans votre autorisation. Pour votre protection, nous avons suspendu votre Carte de credit. Pour lever la suspention de votre Carte de Credit et augmenter sa protection, **Cliquez ici ,**suivez la procedure indiquée pour Mettre à jour votre Carte de Credit.

N.B: Echec d'activation entraînera la suspension de votre carte

Nous vous remercions de votre cooperation dans le cadre de ce dossier.

Merci,
Support Clients Service.

Copyright 1999-2011 VerifedbyVisa . Tous droits reserves.

Des serveurs de stockage des données sûrs… en théorie !

Dernière possibilité de récupération des données : l'attaque directe des serveurs des commerçants, où sont stockées les données de cartes bancaires.

Depuis 2005, les grands émetteurs de cartes bancaires (Visa, Mastercard, American Express, etc.) ont mis en place un standard commun nommé PCI DSS qui constitue un ensemble de bonnes pratiques (regroupées en 12 exigences) pour la sécurisation des sites conservant les données de cartes bancaires sur internet. Aujourd'hui, un commerçant qui souhaite stocker des données de cartes bancaires doit obligatoirement passer par ce standard (obligation découlant de l'article 226-17 du code pénal et des articles 34 et 34bis de la Loi informatique et libertés).

A noter que ce standard international représente une contrainte et un coût important pour les commerçants : en effet la norme PCI DSS repose sur une certification obligatoire, assurée par des cabinets de certification anglo-saxons très onéreux. De même, du fait de l'aspect international de la certification, les commerçants français sont obligés de certifier les paiements par piste, très fréquents aux Etats-Unis mais totalement marginaux en France. Là-encore, ces coûts sont répercutés sur le prix de vente au consommateur.

Or, malgré ce coût, la norme PCI DSS n'est pas pour autant synonyme de sécurité absolue. Ainsi :

- Entre octobre 2006 et avril 2008, un célèbre pirate informatique, Albert Gonzales, est parvenu à s'immiscer dans les serveurs de l'opérateur de paiement Heartland Payment Systems et du supermarché Hannaford Brothers et à dérober 130 millions de numéros de cartes bancaires, qu'il revendait à des fraudeurs entre 10 et 100 dollars l'unité ;
- Fin avril 2011, Sony avait dû fermer sa plateforme de jeux Playstation Network après une attaque informatique et le vol des données de 77 millions de comptes joueurs, dont 10 millions contenant des données de cartes bancaires.

Par conséquent, malgré la norme PCI-DSS, les données de cartes bancaires peuvent être dérobées et utilisées pour des paiements frauduleux.

Cependant, contrairement aux opérateurs téléphoniques, qui depuis le « Paquet télécom » 2009 (transposé en droit français en 2011), doivent notifier –quand elles surgissent– les violations de données personnelles des abonnés, tous les autres opérateurs conservant des données de cartes bancaires n'ont aucune obligation d'informer les consommateurs de la survenance d'une effraction sur leurs serveurs. Ce qui empêche les consommateurs de prendre les mesures de précaution qui s'imposent : surveillance de leurs comptes, déclaration de fraude le cas échéant ou opposition à la carte bancaire.

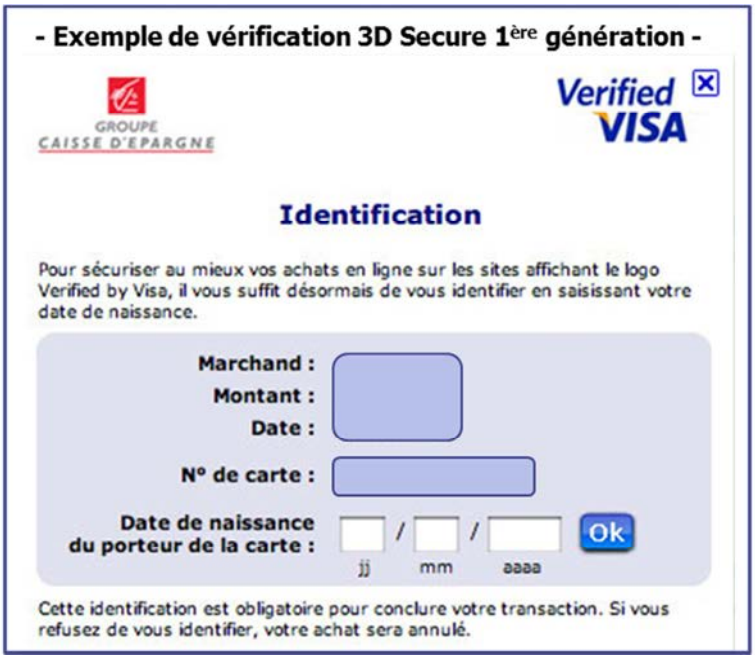
Le problème des numéros de carte bancaire, et les interrogations liées à la sécurité sur internet ont poussé les opérateurs de cartes bancaires à renforcer les contrôles des paiements par carte bancaire en mettant en place le 3D Secure.

2 – L'échec du 3D Secure en France

Le dispositif 3D Secure, mis en place en France à partir de 2008, part de l'idée qu'étant donné que les données fixes de la carte peuvent être facilement capturées et réutilisées pour effectuer des paiements frauduleux, il convient de s'assurer, lors du paiement sur internet, que c'est bien le possesseur de la carte qui effectue le paiement. Ce qui passe donc par la mise en place d'un mécanisme d'authentification du porteur appelé « authentifiant ». En échange de la mise en place de ce mécanisme par les commerçants, les banques acceptent de supporter le coût de la fraude résiduelle.

La première génération de 3D Secure : un système mort-né

La première génération du 3D Secure ajoutait ainsi aux informations de la carte bancaire (saisies sur le site du e-commerçant), une seconde page internet issue de la banque du client et lui demandait de confirmer par la saisie d'une information personnelle (le plus souvent sa date de naissance, mais également un mot de passe ou la réponse à une question personnelle…) qu'il était bien le propriétaire de la carte.



Cette première génération de 3D Secure a été fortement critiquée tant par les professionnels de la monétique que par les commerçants et les consommateurs. En effet :

- Avec la naissance et la généralisation des réseaux sociaux (Facebook, etc.), nombre de données personnelles sont devenues publiques : c'est le cas en particulier de la date de naissance, qui fait partie des informations de base de Facebook mais souvent également de tous les sites professionnels ou para-professionnels (hébergeant des C.V par exemple) ;
- Ce système nécessite de passer par une page en plus (celle de la banque), ce qui offre une occasion supplémentaire pour un pirate informatique de faire surgir une page d'hameçonnage (phishing) avant la vraie page de la banque afin de récolter l'authentifiant ;
- Ces données d'authentification sont toujours inscrites à l'aide du clavier : ce dispositif n'entraîne par conséquent aucune sécurité supplémentaire pour un ordinateur « vérolé » par un spyware (logiciel espion). Le client se fera capturer en même temps les codes de la carte bancaire et l'authentifiant.
- Surtout, ces données sont toujours des données « statiques », fixes, et à durée de vie longue. Il suffit donc que l'authentifiant soit capturé une fois pour qu'il puisse resservir durant toute la durée de la carte bancaire.

En plus de ces problèmes de sécurité, l'échec du 3D Secure a été consacré par la faible adhésion des commerçants au système. En effet, pour que le 3D Secure fonctionne, deux entités doivent avoir adopté le 3D Secure : la banque du client, mais également le commerçant faisant l'objet de la transaction.

Or, si les banques ont toutes adopté ce système, seul un faible nombre de commerçants a adopté cette première génération du 3D Secure. En particulier, les « grands commerces » électroniques, les quelques dizaines de sites réalisant la plupart des transactions sur internet, ont refusé de l'adopter. Ceux-ci ont en effet déclaré que l'adoption du 3D Secure avait entraîné une perte de 10 à 30% du chiffre d'affaires selon le type de commerçants : perte due selon eux, à la complexité supplémentaire induite par l'authentification du paiement, qui décourage la « fluidité de l'achat » et augmente ainsi les abandons d'achats.

Par conséquent, de nombreux commerçants ont préféré supporter le coût de la fraude plutôt que d'adopter le 3D Secure, d'autant plus que, comme nous l'avons vu, ce coût est in fine supporté par les consommateurs.

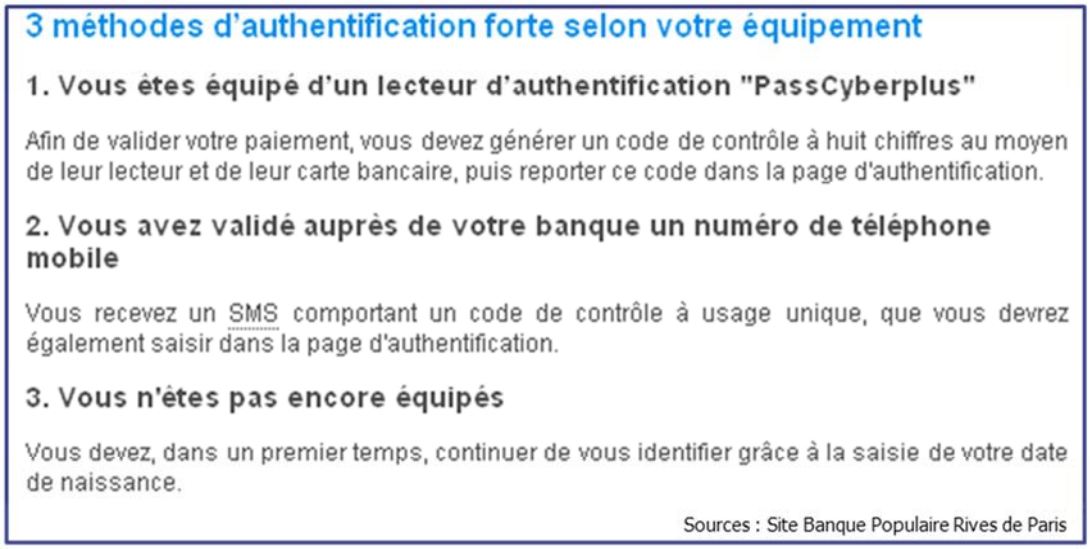
La seconde génération de 3D Secure : un système d'authentification forte mais aucune concertation

Face à l'échec de la première génération, les systèmes de carte bancaire et les banques ont mis en place une seconde génération de 3D Secure, basée sur une sécurisation plus poussée du numéro d'authentification. Dans ce nouveau système, le numéro de téléphone utilise une authentification « forte » car utilisant un numéro dit « dynamique » car non-rejouable. Le numéro non-rejouable présente un avantage essentiel par rapport à la première version du 3D Secure : un authentifiant qui serait capturé par un fraudeur durant un paiement ne peut être réutilisé.

Un grand nombre de banques a adopté le 3D Secure. Cependant cette mise en place ne s'est pas faite de manière concertée… Il existe ainsi plusieurs systèmes d'authentification différents :

- Un code à usage unique obtenu par SMS (BNP, Société Générale, Crédit Agricole, etc.) ;
- Une combinaison de codes à usage unique délivrés au moyen d'une carte papier (Crédit Mutuel, CIC) ;
- Un code délivré par un lecteur de carte fourni au client (Banque Populaire) ;
- Un code à usage unique obtenu par serveur vocal (certains cas de Groupama Banque)

A noter que certaines banques font coexister plusieurs systèmes, ce qui rend plus difficile la compréhension du système. Par exemple, Banque Populaire laisse le choix entre l'utilisation d'un lecteur de carte ou l'envoi d'un SMS. Ce qui concrètement, donne lieu à un texte explicatif compliqué pour le client :



3 méthodes d'authentification forte selon votre équipement

1. Vous êtes équipé d'un lecteur d'authentification "PassCyberplus"

Afin de valider votre paiement, vous devez générer un code de contrôle à huit chiffres au moyen de leur lecteur et de leur carte bancaire, puis reporter ce code dans la page d'authentification.

2. Vous avez validé auprès de votre banque un numéro de téléphone mobile

Vous recevez un SMS comportant un code de contrôle à usage unique, que vous devrez également saisir dans la page d'authentification.

3. Vous n'êtes pas encore équipés

Vous devez, dans un premier temps, continuer de vous identifier grâce à la saisie de votre date de naissance.

Sources : Site Banque Populaire Rives de Paris

A noter également que dans un certain nombre de cas, comme indiqué ci-dessus, l'utilisation des dispositifs rejouables (date de naissance, codes confidentiels, questions secrètes) est toujours d'actualité, ce qui complexifie encore plus la procédure. Au final, ce sont donc 8 procédures différentes qui peuvent se présenter au consommateur selon sa banque, son équipement, et la souscription ou non du commerçant au 3D Secure.

Cette complexité a entraîné, là encore, une faible adhésion des e-commerçants à cette seconde génération du 3D Secure. Certes, 40% des e-commerçants l'ont adopté, mais ceux-ci ne représentent qu'environ 10% des paiements par carte et 15% des montants. Les grands e-commerçants, c'est-à-dire la vingtaine de sites internet qui réalise la grande majorité des transactions en ligne, n'ont pas adopté ce système. Pour la plupart des paiements en France donc, les authentifiants ne sont donc jamais utilisés et le paiement est effectué simplement avec les numéros fixes de carte bancaire.

L'argument des commerçants est que la multiplication des systèmes d'authentification, due à l'absence de concertation entre les banques et entre banquiers et commerçants, fait que les clients sont déroutés au moment de l'authentification. Ils préfèreraient alors abandonner le paiement, voire même faire leurs achats sur des sites n'utilisant pas le système d'authentification.

D'autres problèmes se posent également. Par exemple, pour les comptes joints, il n'est souvent possible, que de mettre seulement 1 seul numéro de téléphone pour l'envoi du SMS de confirmation : par conséquent le conjoint qui n'a pas entré son numéro ne peut pas utiliser la carte de son compte joint sur internet. Le 3D Secure pose également un problème pour les paiements récurrents, différés ou fractionnés : le code d'authentification non rejouable n'étant valable que trois jours, ces paiements ne sont pas validés et le commerçant doit alors recontacter son client pour effectuer de nouveau le paiement, avec un nouveau code d'authentification.

Cette critique des commerçants vis-à-vis du 3D Secure n'est pas infondée : en effet l'efficacité du dispositif souffre de la multiplication des dispositifs, qui a empêché la mise en place d'une campagne d'information claire des consommateurs sur le processus d'authentification des paiements sur internet. Sans information, ceux-ci ont donc « découvert » en direct avec plus ou moins de bonheur les dispositifs mis en place par leur banque, lors des achats. Les clients ont donc pu être déroutés par ces nouvelles demandes, certains clients craignant même que la page supplémentaire d'authentification soit une page de hameçonnage ou que le SMS envoyé soit un spam !

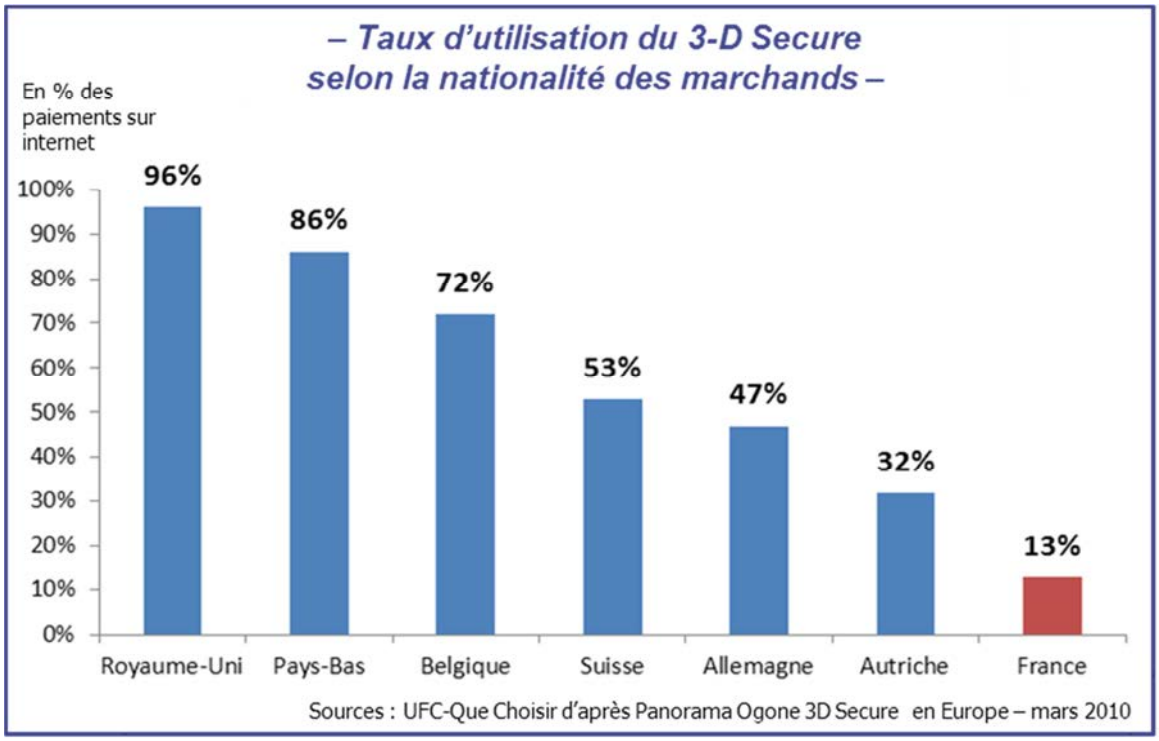
Ceci étant, il est probable qu'une partie (sans doute faible), des tentatives d'achats -et du chiffre d'affaires perdu- bloquées par le 3D Secure soit des tentatives de fraude… Et qu'une autre partie

des abandons d'achat résulte du freinage des « achats impulsifs » fréquents sur internet, freinage résultant de cette page de validation supplémentaire créée par le 3D Secure.

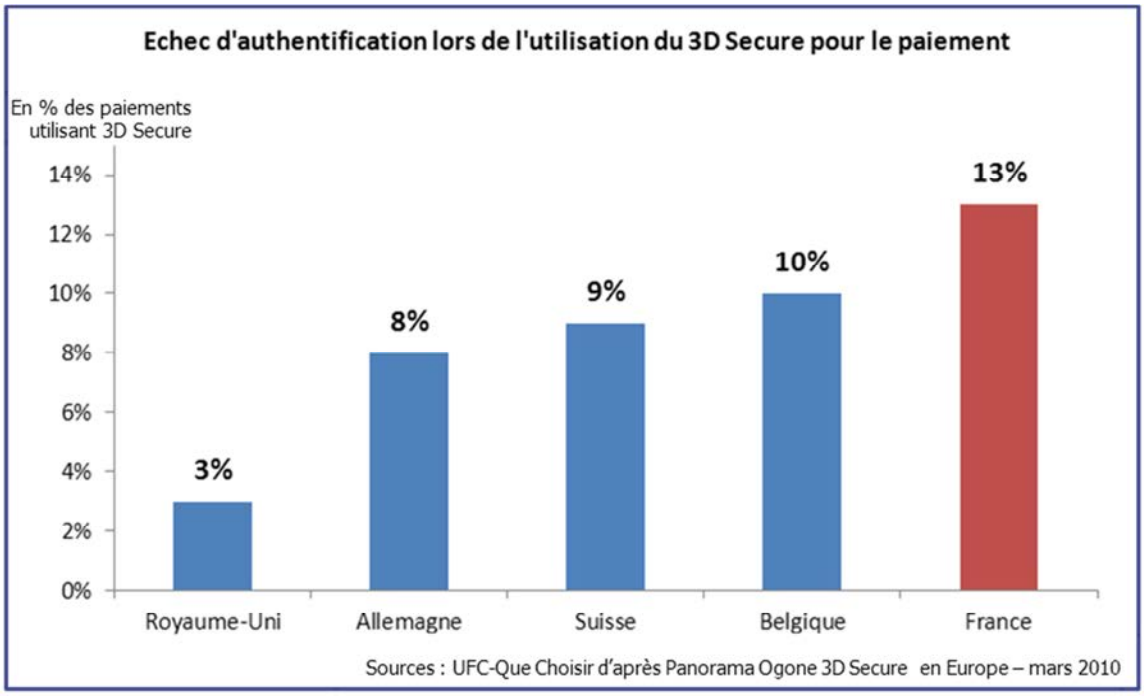
3 – L'exemple Anglais : le 3D Secure fait baisser la fraude quand il est massivement utilisé

L'échec du 3D Secure en France est d'autant plus regrettable que cette technologie semble -sans être évidemment la panacée- permettre de diminuer la fraude à la carte bancaire sur internet.

Les comparatifs internationaux montrent que le 3D Secure est bien plus développé chez nos voisins européens qu'il ne l'est en France. Ainsi le Panorama effectué par Ogone –opérateur de paiement internet présent dans 7 pays d'Europe– montre que de ces 7 pays, la France est celui qui utilise le moins le 3D Secure. Dans les 6 autres pays, l'utilisation du 3D Secure est en moyenne 5 fois plus élevée qu'en France !



La palme de l'utilisation du 3D Secure revient au Royaume-Uni, où la quasi-totalité (96% d'après Ogone) des transactions sur internet utilise ce système. Ce pays est également celui où, quand le système 3D Secure est utilisé, le taux d'échec d'authentification, c'est-à-dire le nombre de fois où les clients n'arrivent pas à utiliser les dispositifs de sécurité, est le plus faible : seulement 3%, contre 13% pour la France qui arrive là-encore en dernière position. En prenant en compte cette autre donnée, le taux des paiements entièrement 3D Secure qui arrivent jusqu'au bout du processus n'est en France que de 11,3%.



Au vu de cette utilisation massive et de ce faible taux d'échec d'authentification, nous nous sommes penchés sur le système retenu au Royaume-Uni pour comprendre les raisons de cette adhésion unanime –là où en France la plupart des commerçants rejette le 3D Secure– et pour évaluer son impact sur la baisse de la fraude sur internet.

Un cercle vertueux entre procédure unique et adoption massive des commerçants

Le système mis en place au Royaume-Uni présente une différence fondamentale avec le système Français : il s'agit d'une procédure unique, mise en place suite à la concertation de l'ensemble du marché. Le dispositif retenu est en effet identique entre tous les opérateurs de carte bancaire (Visa, Mastercard, American Express), et entre toutes les grandes banques britanniques (HSBC, RBS, Lloyds, Barclays…).

Quant au dispositif d'authentification lui-même, il s'apparente à la première génération du 3D Secure. Il s'agit en effet d'un mot de passe secret défini préalablement par le consommateur auprès de sa banque (via son espace personnalisé sur internet par exemple) qui lui sera demandé comme authentifiant lors de la seconde étape du paiement.

– Exemple d'authentification par 3D Secure au Royaume Uni –

L'avantage de ce système unique est qu'il a permis une appropriation facile par le consommateur anglais : le système du mot de passe est connu dans le cas d'autres utilisations sur internet : pour tous les espaces personnels mais également dans les processus de récupération d'identifiant (en cas de perte d'un code d'identification donné par le professionnel).

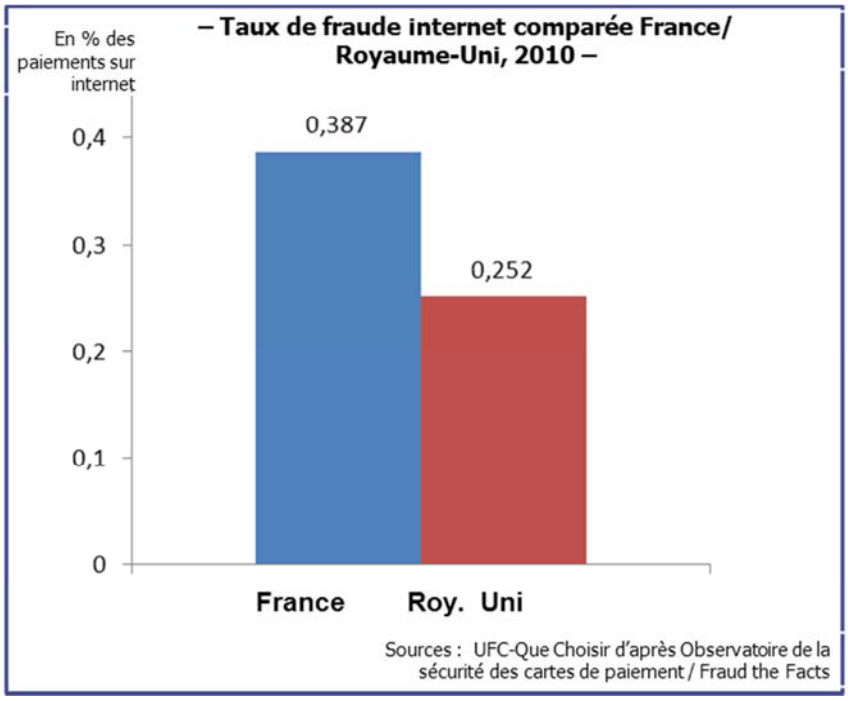
Le processus ne changeant pas selon les commerçants ou les banques, il a pu plus facilement s'imposer chez les consommateurs : la communication a pu se faire de manière uniforme selon les professionnels, il n'y a pas le « brouillage de message » qui existe en France du fait de la multiplicité des processus. De même, le bouche-à-oreille et l'apprentissage mutuel entre consommateurs peuvent se faire plus facilement dans un système de paiement unique que dans un système où se juxtaposent plusieurs procédures.

Ce dispositif unique a permis la création d'un cercle vertueux au Royaume-Uni : le système unique a favorisé l'adoption massive du 3D Secure par les commerçants, laquelle a favorisé l'appropriation de la procédure par les consommateurs, et ainsi de suite.

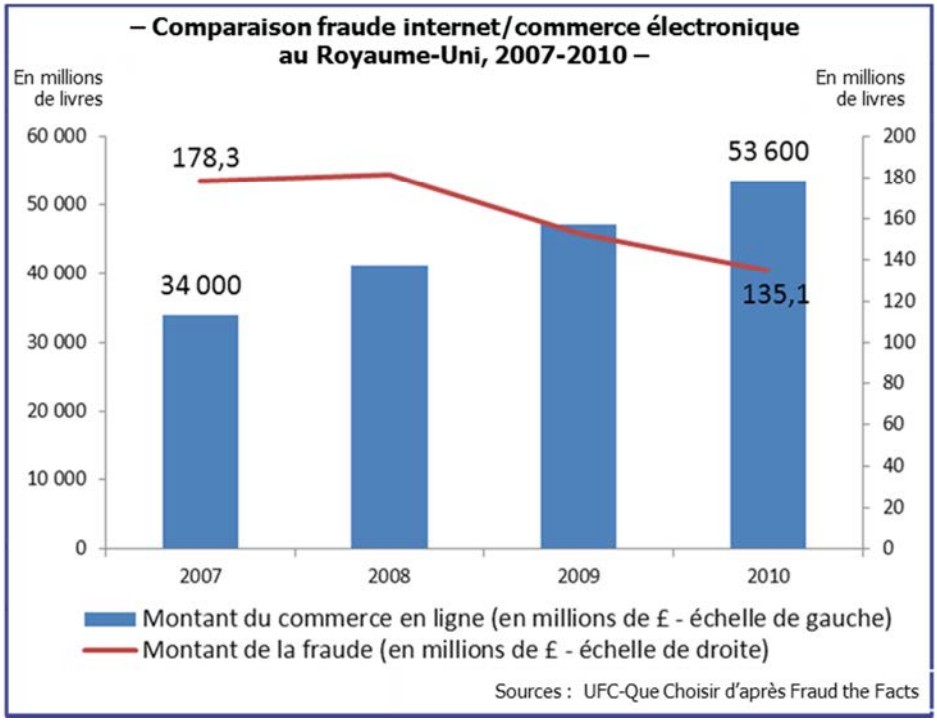
Un impact positif malgré un authentifiant fixe moins poussé qu'en France

L'adoption massive du 3D Secure par les commerçants britanniques, fruits de la concertation et de la mise en place d'un dispositif unique, a permis des résultats spectaculaires en seulement quelques années.

En 2007, en effet, le taux moyen de fraude internet (somme de la fraude internationale et de la fraude nationale) était de 0,524%. Il était alors supérieur de 15% à la fraude française. En 2010, ce taux avait diminué à 0,252%, soit une baisse de 52% de la fraude sur internet en seulement 4 ans ! A cette même date, le taux moyen de fraude internet en France était 53% plus élevé qu'au Royaume Uni.



Ce résultat est encore plus impressionnant en termes de montants. Ainsi, alors que le commerce électronique au Royaume-Uni est passé de 34 milliards de livres en 2007 à près de 54 milliards de livres en 2010, les montants fraudés ont diminué de 178,3 millions de livres en 2007 à 135 millions de livres en 2010. A titre de comparaison, le Royaume-Uni a aujourd'hui un montant total de fraude internet certes supérieur de 34% au montant français, mais pour un commerce électronique supérieur de 103% !



La réussite du système britannique, qu'illustre cette baisse de la fraude sur internet, montre bien l'importance de l'adoption généralisée par les commerçants d'un système d'authentification des paiements. Cette adoption n'est possible que par la mise en place d'une procédure unique d'authentification permettant une appropriation facile par les consommateurs, et donc une grande

limitation des abandons de paiements. Ces abandons qui ont fait du 3D Secure français, actuellement, un échec.

Cette baisse de la fraude est d'autant plus notable que le système d'authentification britannique repose actuellement sur un code confidentiel durable, dont le niveau théorique de sécurité est beaucoup moins élevé que les numéros non-rejouables en cours d'adoption dans le 3D Secure de seconde génération en France. Il semblerait ainsi que l'adoption en France d'une procédure unique, généralisée à tous les commerçants et à numéros d'authentification non-rejouables pourrait permettre de bénéficier de baisses de la fraude encore plus forte qu'au Royaume-Uni.

III – La fraude à la carte bancaire, une plaie au quotidien pour les consommateurs

Au-delà des aspects financiers déjà évoqués, une fraude à la carte bancaire sur internet si étendue a des répercussions sur les consommateurs. Afin de comprendre cet aspect, nous avons passé un appel à témoignages sur internet, formulé de la manière suivante :

« Nous recherchons des témoignages de consommateurs ayant été victimes de fraudes à la carte bancaire sur internet, dans lesquelles les données de leurs cartes ont été réutilisées à leur insu. Nous souhaiterions plus particulièrement connaître la réponse apportée par les banques aux clients dans ces situations, les procédures exigées par les établissements pour restituer les fonds et les délais qui ont été nécessaires à cette restitution des fonds ».

173 consommateurs ont répondu à notre demande. Cet écho important pour un sujet aussi complexe montre que les consommateurs se sentent concernés par cette problématique : en général, seuls les sujets internet et nouvelles technologies, qui concernent des publics par définition plus actifs sur internet, atteignent un taux de réponse aussi ou plus élevé.

Mais préalablement, rappelons que la règlementation en la matière est censée bien protéger le consommateur.

1 – En théorie, une règlementation très protectrice sur les fraudes internet

La réglementation relative à la protection du consommateur dans le domaine de la fraude à la carte bancaire est, dans sa lettre, très poussée. En effet l'article L133-19 du Code Monétaire et Financier, issu de la Directive sur les Services de Paiement (13 novembre 2007, transposée par l'Ordonnance n° 2009-866 du 15 juillet 2009) dispose qu'« *En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur [i.e la banque] supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 150 euros* ».

Cette réglementation est encore plus poussée pour les paiements sur internet, puisqu'elle précise que :

- « *Toutefois, la responsabilité du payeur n'est pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé* », c'est-à-dire du code confidentiel pour les paiements de proximité, ou des dispositifs d'authentification de 3D Secure pour les paiements en ligne. Comme nous l'avons vu, les dispositifs d'authentification du porteur ne sont utilisés que dans 11,3% des cas dans les paiements en France : par conséquent, dans 88,7% des cas, le consommateur ne verra pas sa responsabilité engagée et n'aura pas à payer la franchise de 150 euros prévue par la loi en cas de fraude à la carte bancaire sur internet.
- Deux autres passages de cet article renforcent également la protection du consommateur pour les paiements sur internet :
  - « *La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées* » ;
  - « *Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument* ».

En fait, le consommateur ne peut avoir à supporter les pertes que dans deux cas :

- En cas d'agissement frauduleux de la part du client (Alinéa III de ce même article L133-19), ce qui est bien entendu légitime ;
- En cas de négligences graves (Alinéa IV), c'est-à-dire si le client n'a pas pris les mesures raisonnables pour préserver la sécurité de ses moyens de paiement ou s'il n'a pas prévenu sa banque dans les meilleurs délais, compte tenu de ses habitudes d'utilisation de la carte, de l'existence d'une fraude. A noter que c'est à la banque de prouver l'existence d'une faute lourde de la part du client, comme l'a souligné la jurisprudence de la chambre commerciale de la Cour de cassation du 21 septembre 2010 : « *Il appartient à l'émetteur de la carte [i.e. la banque] qui se prévaut d'une faute lourde de son titulaire [i.e. le client], au sens de l'article L. 132-3 du code monétaire et financier, d'en rapporter la preuve ; que la circonstance que la carte ait été utilisée par un tiers avec composition du code confidentiel est, à elle seule, insusceptible de constituer la preuve d'une telle faute* ».

Les délais de remboursement suite à une fraude sont prévus par l'article L133-18 du code monétaire et financier : « En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée ».

Ajoutons également que ce même article complète aussi l'article L133-19 sur les aspects d'indemnisation en établissant que « *le cas échéant, [le prestataire de services de paiement du payeur] rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire* ». Par conséquent, le remboursement ne doit pas seulement porter sur les sommes détournées lors de la fraude, mais sur toutes les sommes prélevées sur le compte du fait de la fraude. Ce qui inclut par conséquent tous les frais liés à la fraude.

Au final donc, la réglementation est très favorable au consommateur : sur toutes les fraudes issues de paiements sur internet, le consommateur de bonne foi doit être remboursé par sa banque, immédiatement et pour l'intégralité des sommes liées à la fraude. Le seul cas où le client peut avoir à supporter les sommes détournées sont les cas de faute lourde, mais dans ce cas, c'est à la banque de prouver l'existence d'une faute lourde.

2 – Dans les faits, de nombreux freins au remboursement des consommateurs

Les réponses à notre appel à témoignages montrent qu'en réalité les banques n'appliquent pas à la lettre cette règlementation protectrice des consommateurs en matière de fraude sur les paiements à distance. De nombreux consommateurs nous ont ainsi fait part de blocages ou demandes issues de leurs banques qui ne sont pas prévues par la loi.

Une demande systématique de dépôt de plainte au commissariat avant tout remboursement

La quasi-totalité des banques demandent aujourd'hui à leurs clients victimes de fraude, comme préalable à tout remboursement des sommes volées, le dépôt d'une plainte auprès du commissariat ou de la gendarmerie la plus proche du domicile du client. Voici quelques verbatim de consommateurs sur ce sujet :

- « *[Ma banquière] a insisté sur le fait que je ne serai pas remboursée si je ne portais pas plainte. Or, il me semblait avoir entendu que ce n'était pas une obligation* » ;
- « *Là, mon "conseiller" ne veut rien savoir. [...]. La seule chose qu'il me répète, c'est de porter plainte. A la gendarmerie, on me dit que ce n'est pas possible* » ;

- « *Ma banque a exigé que je dépose plainte pour me rembourser. Au commissariat la personne qui m'a reçu m'a dit qu'une simple déclaration de main courante suffisait !* » ;
- « [*Le banquier] m'assure qu'il m'a fait une fleur. Qu'il pouvait exiger que je porte plainte avant de me rembourser...* » ;
- « *Le service financier de [la banque] m'a demandé de porter plainte, ce que j'ai fait* » ;
- *« Tant que la police n'acceptera pas que je porte plainte moi-même, la banque ne me remboursera pas cet argent... ».*

Cette demande est souvent faite à l'oral par le conseiller. Mais certaines banques l'affichent directement sur leurs sites internet.

– Exemple de demande de dépôt de plainte au commissariat –

Le saviez-vous ?

En cas de perte ou de vol...
Avertissez immédiatement votre centre de mise en opposition et faites une déclaration de vol à la police. Vous devez ensuite fournir à votre Caisse Crédit Mutuel les pièces justificatives suivantes :

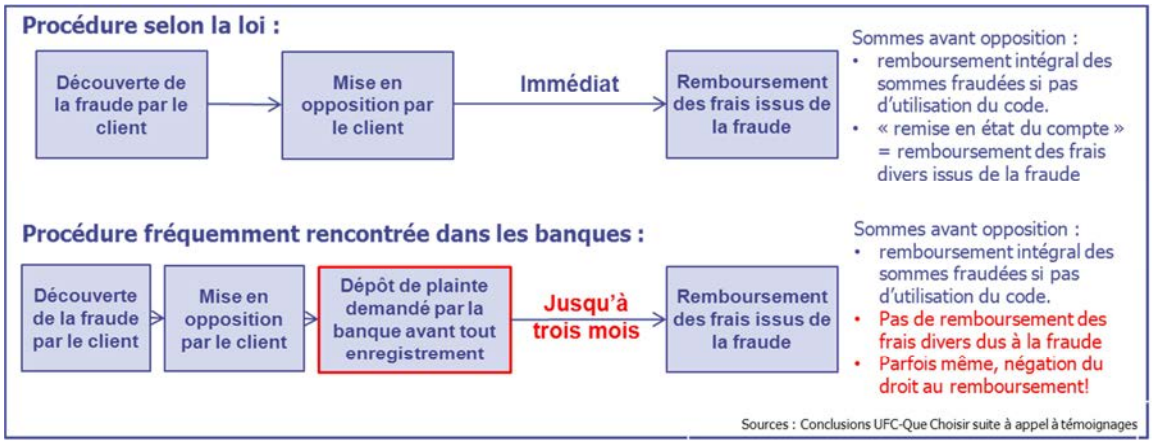
- Attestation de mise en opposition de vos cartes ou chéquiers
- Factures de réfection ou de remplacement de vos clés et serrures
- Copies de vos nouveaux papiers et des factures de remplacement
- Attestation de dépôt de plainte en cas de vol ou d'opérations frauduleuses

Sources : Site internet du Crédit Mutuel Centre Est Europe

Or dans le texte de la loi, ce dépôt de plainte n'est absolument pas nécessaire. La banque doit rembourser les sommes dérobées dès lors que le client atteste avoir été victime d'une fraude. En outre, une dépêche du Ministère de la Justice a demandé le 12 août 2011, aux procureurs généraux, d'indiquer aux officiers de police judiciaire de ne plus effectuer d'enregistrement de plaintes liées à des fraudes à la carte bancaire, car ce dépôt de plainte n'est pas nécessaire au remboursement du consommateur par la banque.

Pourquoi les banques font-elles cette demande auprès de leurs clients ? Officiellement, il s'agit de favoriser les poursuites judiciaires et de comptabiliser l'ampleur de la fraude. Cependant, toujours d'après la Chancellerie, ces poursuites seraient plus efficaces si c'étaient les banques qui déposaient plainte : « *il n'y a qu'avantage au regard de l'efficacité et de la célérité de l'enquête, à ce que la banque (...) dépose plainte* ». La prise en charge des dépôts de plainte par les banques permettrait aussi de lutter contre la criminalité en bande organisée, car elle faciliterait les recoupements de modes opératoires. Sur le fond également, on peut considérer qu'à partir du moment où la loi décrète que la banque doit rembourser le client de tous les frais issus d'une fraude à la carte bancaire, c'est bien la banque qui est victime, d'autant plus que ce sont ses systèmes de paiement, qu'elle fournit à ses client, qui ont été détournés.

Ainsi, sont totalement illégitimes des demandes émanant de banques telles que celle ci-dessous, reçue par un consommateur : « *Merci de bien vouloir déposer l'ensemble des documents dans la boîte aux lettres afin de traiter votre dossier dans les meilleurs délais : […] - le récépissé du dépôt de plainte.»*



Un délai de remboursement très allongé par rapport à ce que la loi prévoit

Comme évoqué plus haut, la loi indique que le remboursement du client des dommages créés par la fraude doit être immédiat. Or, dans la réalité, la plupart des banques mettent entre 15 jours et plus de trois mois à rembourser leurs clients : *« Les achats frauduleux ont commencé le 15 juin 2011. Je m'en suis aperçu le 1er juillet. Le service financier de [la Banque] m'a demandé de porter plainte, ce que j'ai fait […]. Le compte a été bloqué pendant deux mois. J'ai été remboursé début septembre ».*

Ce délai, déjà déraisonnable et illégal, ne prend également par en compte l'urgence pour le client d'un remboursement le plus rapide possible, en particulier quand les sommes dérobées atteignent plusieurs milliers d'euros.

Ainsi, ce message du 6 septembre : *« Ma carte bancaire a été piratée et des achats frauduleux à hauteur de 5 000 euros ont été effectués chez Ryanair en billets d'avion. Ces achats ont été effectués en Irlande entre le 25 et le 30 mai 2011. La totalité de la somme ne m'a toujours pas été restituée parce que ma banque […] prétend que les frais de taux de change doivent être remboursés par la compagnie aérienne ! »*.

Et ce message reçu le 1er septembre : *« Bonjour, j'ai pris connaissance de paiements frauduleux par internet avec mes coordonnées bancaires le 11 septembre dernier. Montant total : 3 786 euros pour un salaire moyen de 1 800 euros… Après avoir âprement combattu pour une prise en charge sérieuse du problème, je suis toujours dans l'attente d'un remboursement »*.

Tout laisse à penser que les établissements bancaires n'effectuent aucune priorisation des remboursements en fonction de la gravité et de la profondeur de la fraude. Or, le fait de priver le consommateur de centaines, voire de milliers d'euros peut être extrêmement dommageable, comme l'énonce cette consommatrice : *« Le préjudice se monte à 3 000 euros et il a fallu que j'emprunte à ma mère pour nourrir ma famille »*. En cas de découvert, le client touché peut également se voir facturer des frais d'incident de paiement aggravant sa situation financière alors qu'il n'est, depuis le départ, aucunement responsable de la fraude ni des délais de remboursement !

A noter que ces longs délais de remboursement ne sont pas liés à des contraintes techniques, de trop rares banques parvenant à rembourser leurs clients dès le lendemain de la déclaration de fraude du client auprès de la banque.

Des frais liés à la fraude mais non remboursés

Alors que la loi parle bien de « *rétabli[r] le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu* », la plupart des banques se contentent souvent de ne rembourser –avec tous les désagréments déjà évoqués– que les sommes directement volées par le paiement frauduleux.

Or la survenance d'une fraude implique souvent des frais (de recherche, de remplacement de cartes, d'opposition) directement liés à cette fraude, et qui n'auraient pas été nécessaires si le système de paiement avait été suffisamment sécurisé. Ces frais ne sont que très rarement remboursés, comme le montre ce témoignage : *« J'ai aussi appris que je n'avais pas souscrit d'assurance et il m'en coûterait 15 euros de frais de recherche pour chaque transaction frauduleuse, ce que j'ai trouvé abusif. Comme j'en ai eu 5, je dois sortir 75 euros. Bien sûr, j'ai dû souscrire cette assurance non rétroactive (environ 25 euros par an) qui, dixit le conseiller, m'exonèrera des frais de recherches si nouvel incident ».*

De même, les frais dus à la confection et l'envoi d'une nouvelle carte sont également facturés au consommateur : *« On m'a compté des frais d'opposition et de remplacement de carte »*. Ces frais sont parfois remboursés suite à la demande du client, action présentée alors comme un « geste commercial » alors qu'il s'agit bien d'un droit du client : *« Après ma réclamation au service consommateurs, la directrice de l'agence, que l'on avait toujours refusé de me passer en ligne, m'a téléphoné pour me dire qu'elle faisait un geste commercial en me remboursant ma carte mais qu'elle considérait que c'était moi qui avais acheté le billet dans la mesure où ma carte était toujours restée en ma possession […]. Pour être remboursé, il eût fallu, semble-t-il, que ma carte soit volée ou perdue. »*

Sans parler des frais des découverts issus de la fraude qui ne sont pas toujours remboursés, alors que c'est bien la banque qui est responsable des failles du système de paiements ! Par exemple, ces témoignages : *« [La Banque] m'a remboursé les sommes, mais je me bats encore pour le remboursement des frais bancaires, dus au découvert », et « Je reste cependant dans l'attente de l'extourne d'environ 300 euros de « frais d'intervention avant paiement » débités par la banque ».*

La loi évoque également que « *Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire »* pour le consommateur victime d'une fraude à la carte bancaire… Mais aucun témoignage, même positif, ne fait état d'une quelconque indemnisation par une banque pour les désagréments causés au client par une fraude sur son compte. Alors que, comme le soulignent de nombreux consommateurs, le remboursement est long, compliqué (*« Je ne sais plus quoi faire, tout le monde se renvoie la balle »*), et très stressant (*« Cela est encore très douloureux pour moi »*).

Parfois même, une négation du droit au remboursement !

La survenance d'une fraude apparaît pour certains banquiers comme une « opportunité » de vente d'une assurance des moyens de paiement, dont nous avons pourtant montré l'inutilité. Quitte à tromper le client.

En effet, certains banquiers n'hésitent pas à pratiquer la désinformation en prétendant à leurs clients que la souscription d'une assurance des moyens de paiement est le seul moyen d'être assuré du remboursement des sommes dérobées ! Ce qui constitue non seulement une non-application de la loi, mais également des agissements illicites. Par exemple ces témoignages :

« Mon ami a été victime de l'utilisation frauduleuse de sa carte bancaire […], le 18 juin lors d'un rendez-vous avec la chargée de clientèle, elle nous confirme qu'il n'a pas pris d'assurance qui couvre ce risque » ;

« *Ma banque m'indique que si je subis une fraude à ma carte bancaire sur internet je ne suis pas pris en charge… « si je ne prends pas une assurance complémentaire !! ». Et de me citer le cas d'une cliente qui s'est vu retirer des sommes « importantes » à son insu… ».*

3 – Autre conséquence : l'assurance des moyens de paiement, peu utile et surfacturée

Autre conséquence, toute aussi importante, de cette législation : l'assurance des moyens de paiement vendue massivement par les banquiers, car comprise notamment dans tous les packages bancaires qui sont souscrits par la majorité des clients, est devenue totalement inutile pour les fraudes sur internet. Les fautes lourdes démontrées par les banques, qui sont les seuls cas où les clients ne sont pas couverts pour une fraude, ne sont en effet pas ou que partiellement couvertes par les banques.

Elle n'a plus qu'une utilité pour les fraudes sur les paiements ou retrait de proximité par carte ou pour les chèques. Mais, comme nous l'avons vu au début de cette étude, les fraudes de proximité par carte sont aujourd'hui très limitées (0,012% des montants) : l'utilisation du remboursement de franchise de 150 euros n'en devient que plus rare. De même, l'utilisation des chèques décroît régulièrement, ce qui limite d'autant plus l'intérêt de l'assurance. D'autant plus que la banque doit rembourser tout chèque effectué avec une fausse signature…

En réalité, cette assurance ne sert plus aujourd'hui que pour ses services annexes : remboursement du timbre fiscal pour la réfection des papiers d'identité, remboursement des frais de refabrication de clef… Mais ces garanties, justement parce qu'elles sont annexes et parce que l'assurance des moyens de paiement est vendue « globalement » dans les packages et donc sans explication détaillée par les conseillers bancaires, sont très mal connues et donc très peu utilisées.

Par conséquent, il est totalement anormal qu'une assurance qui coûtait 22,1 euros en moyenne par an en 2004 (chiffre UFC-Que Choisir) –à une époque où elle avait son utilité– coûte désormais 24,28 euros par an (chiffres 2010 issus du Rapport de l'Observatoire des tarifs bancaires) alors que son utilité est, depuis le passage de la Directive, réduite à la portion congrue.

Rappelons également que l'hebdomadaire *Marianne* avait dévoilé, en août 2009, une note interne du Crédit Agricole datant de 2007 montrant que cette banque collectait 194,5 millions d'euros de cotisations de la part de ses clients, mais ne reversait que 8 millions d'euros à ses clients victimes de sinistres. En comptant les frais de gestion (2,9 millions d'euros), cette banque faisait donc une marge nette de 94,4%. Le même article précisait que, d'après le cabinet de conseil Xerfi, les banques françaises avait récupéré 1 milliard d'euros de cotisations sur les assurances des moyens de paiement. Par analogie avec la marge du Crédit Agricole, la marge totale des banques françaises sur cette assurance des moyens de paiement attendrait 940 millions d'euros par an. Chiffre qu'il faut désormais majorer du fait du passage de la Directive décrite ci-dessus, et de sa répercussion sur les garanties réelles fournies par ces assurances.

En conclusion, si le marché de l'assurance des moyens de paiement était aujourd'hui concurrentiel, le prix de vente de cette assurance devrait aujourd'hui être non pas de 24 euros par an, mais de moins de 2 euros par an !

IV – Conseils aux consommateurs pour éviter les fraudes à la carte bancaire sur internet

Soucieuse de jouer son rôle dans la prévention des fraudes et l'éducation des consommateurs à la fois sur les risques de fraude existants lors d'un paiement par internet et sur les moyens d'éviter ce type de fraude, l'UFC-Que Choisir a identifié quelques bonnes pratiques. Celles-ci, si elles sont respectées, n'entraîneront pas, bien sûr, un risque zéro de fraude (dans ce domaine, le risque zéro n'existe pas) mais devraient diminuer fortement les chances de faire face à ce problème.

Voici donc nos recommandations, établies en concertation avec des professionnels du secteur :

Pour éviter les fraudes :

- **Ne répondez jamais à un mail vous demandant des informations personnelles ou vos numéros de carte bancaire, même s'il semble émis par un de vos fournisseurs (banque, téléphone, internet).**
  - Ces messages peuvent vous faire la demande soit directement, soit indirectement via un lien vous dirigeant vers un site internet paraîssant appartenir à votre fournisseur ;
  - Ils peuvent vous demander soit directement vos numéros de carte bancaire, soit vos numéros de compte bancaire, mais également votre date de naissance, votre numéro de Sécurité Sociale ou le nom de jeune fille de votre mère.

  Ces messages sont vraisemblablement des tentatives de phishing (hameçonnage), visant à obtenir de votre part les informations de sécurité permettant de faire des paiements par carte bancaire sur internet. En cas de doute (par exemple, si votre message évoque des problèmes sur votre compte ou avec votre fournisseur) allez directement sur l'adresse officielle du prestataire –en tapant directement l'adresse sur votre barre d'adresse ou en passant par un moteur de recherche– pour vous connecter à votre interface de gestion de compte.
- **Effectuez régulièrement des analyses antivirus et antispyware de vos ordinateurs personnels.**
  Afin d'éviter les Spywares –ces logiciels espions qui enregistrent tout ce que vous tapez sur votre clavier ou cliquez avec votre souris, en particulier vos codes personnels– l'arme la plus efficace reste les logiciels d'antivirus et d'antispyware. Encore faut-il s'en servir régulièrement.
- **Mettez régulièrement à jour vos antivirus, antispyware, navigateurs internet, systèmes d'exploitation en particulier, et vos logiciels en général.**
  « L'innovation » dans le domaine de la fraude est sans fin, ce qui rend rapidement inefficaces les anciennes versions des programmes de protection, mais également les systèmes d'exploitation et les logiciels. Les mises à jour de ces produits permettent de corriger les failles de sécurité que les pirates informatiques peuvent utiliser pour frauder.
- **Sauf si vous en avez absolument besoin, n'utilisez jamais d'ordinateur public pour faire un achat sur internet.**
  Les ordinateurs publics –ordinateurs d'hôtels ou de cybercafés par exemple– peuvent être utilisés par plusieurs dizaines de personnes chaque jour, ce qui en fait une proie idéale pour les fraudeurs, d'autant plus que ceux-ci peuvent venir y installer eux-mêmes des logiciels espions. Ces ordinateurs sont également souvent âgés et/ou disposent de versions de logiciels assez datées et donc, peu efficaces en termes de protection de l'utilisateur. Autant d'arguments pour les utiliser au minimum.
- **Ne mentionnez jamais vos données personnelles ou vos numéros de carte bancaire dans un mail, même envoyé à un proche.**

Les mails sont beaucoup moins protégés que les sites des banques ou des commerçants : la plupart du temps les mails sont envoyés « en clair » (sans que le message soit crypté). Il est donc très facile pour un fraudeur d'intercepter un message électronique contenant des données personnelles ou de carte bancaire. A titre de comparaison, les conversations téléphoniques par téléphone portable font l'objet d'un cryptage par la carte SIM… Mais pas les conversations par téléphone fixe.

- **Si vous ne faîtes que rarement des opérations sur internet, utilisez les services de e-cartes bleues fournis par votre banque.**
  Sauf pour des achats nécessitant la carte bancaire pour pouvoir être retirés (par exemple, billets de train ou spectacles) ou pour les paiements fractionnés.
  Les e-cartes bleues sont des numéros de cartes bancaires « virtuels », à usage unique, que vous pouvez utiliser pour remplacer votre numéro de carte bancaire fixe. Ce qui empêche toute fraude sur votre carte bancaire sur internet. En revanche, du fait de son prix pouvant être relativement élevé et de son usage au coup par coup, il ne convient pas à un utilisateur intensif du paiement par internet.

Pour repérer au plus vite les fraudes :

- **Regardez régulièrement vos relevés de compte pour vérifier les paiements qui y sont passés.**
  Comme toujours, dès qu'il s'agit d'opérations bancaires, le moyen le plus simple et le plus fiable pour détecter un problème, ici une fraude à la carte bancaire sur votre compte, est de regarder régulièrement votre compte bancaire, notamment via le relevé de compte envoyé chaque mois par votre banque. Ceci permettra d'éviter que la fraude ne continue et d'éviter les objections de « manque de vigilance » de la part des banquiers.
- **Consultez très fréquemment la situation de votre compte sur l'espace personnel de votre site bancaire, qui permet une meilleure réactivité.**
  Certaines banques permettant même de voir les opérations de carte bancaire en attente de débit.
  La consultation par internet permet de voir l'état de son compte au jour le jour. C'est donc le meilleur outil pour détecter l'existence d'une fraude à la carte bancaire sur votre compte. Elle permet ainsi d'effectuer le plus rapidement possible les démarches de sécurité (opposition) sur la carte et d'entamer les démarches de remboursement facilement. De même, les banques qui affichent les opérations en attente de débit peuvent suspendre ces opérations en cas de réclamations de leurs clients.

V – Demandes de l'UFC-Que Choisir sur la sécurité de la carte bancaire sur internet

L'UFC-Que Choisir considère que l'accès au commerce en ligne est une opportunité pour le consommateur, sous réserve que celui-ci puisse jouir pleinement de tous ses droits et bénéficier de systèmes de paiements sécurisés. Dans cette optique, et pour empêcher que la fraude sur les paiements en ligne ne devienne, par son ampleur, un frein à l'accès au commerce en ligne,

L'UFC-Que Choisir demande :

1. **Pour améliorer la prévention contre la fraude :**
   - L'envoi systématique par les banques de confirmations de paiement sur internet via les espaces personnels des sites bancaires et par SMS ou email ;
   - L'obligation pour tout professionnel stockant des données de cartes bancaires de déclarer à leurs clients, quand ils surviennent, des attaques de serveurs et/ou des vols de données personnelles, bancaires ou de cartes bancaires ;
   - L'obligation pour les banques de centraliser les fraudes subies par leurs clients et de les transmettre aux services judiciaires.

2. **Pour sécuriser le système de paiement par carte bancaire sur internet :**
   - L'adoption obligatoire, au niveau français, d'un système d'authentification unique et non rejouable, mis en place en concertation entre banquiers, commerçants et représentants des consommateurs ;
   - L'ouverture d'une réflexion au niveau européen pour uniformiser ces mêmes procédures d'authentification lors des paiements par carte bancaire sur internet.

3. **Pour une réparation totale du préjudice subi par le client victime de fraude, le remboursement intégral des frais causés par les suites de la fraude (frais de découverts éventuels, remplacement de carte, recherches documentaires, etc.).**