Livre Blanc

La fraude dans le e-commerce

.com CERTISSIM
La garantie paiement des ventes

12e Édition
Juin 2014

www.fia-net-group.com

FIA-NET
39 rue Saint-Lazare, 75009 Paris

SOMMAIRE

INTRODUCTION

Le e-commerce français demeure un secteur économique prospère. Sa croissance est cinq fois supérieure à celle du commerce traditionnel.[1] En 2013, il a réalisé un chiffre d'affaires de 51,1 milliards d'euros, soit une augmentation de 13,5 % en un an.[2]

Son public s'élargit d'année en année. En 2013, le nombre d'internautes et le nombre de e-acheteurs ont crû de 5 % chacun, pour atteindre respectivement 43,2 et 33,7 millions de personnes en France.[3] Par ailleurs, plus de 80 % des e-acheteurs[2] a recours au paiement par carte bancaire pour payer en ligne.

Ce dynamisme et l'absence de présence physique de la carte bancaire au moment du paiement expose le e-commerce à un risque de fraude inévitable.
Depuis 2010, la fraude a connu de profondes mutations. Elle s'est organisée et structurée, induisant ainsi d'importants préjudices financiers pour les e-commerçants.
En 2012, le taux de fraude constaté par la Banque de France pour les paiements en ligne, par carte bancaire, était de 0,29 %.[4] Ce taux est naturellement bien inférieur pour les transactions traitées par Certissim. En projetant le taux de la Banque de France sur le marché identifié par la FEVAD, la fraude représenterait près de 150 millions d'euros de fraudes.
En 2013, les professionnels du secteur – e-commerçants, spécialistes de la lutte contre la fraude et autorités – ont su réagir et s'adapter pour revenir à un niveau de risque mieux maîtrisé.

L'objet du Livre Blanc Certissim est de dresser l'état des lieux de la fraude liée aux paiements dans le e-commerce. En détaillant ses évolutions et ses mécanismes, il donne aux professionnels comme aux particuliers les clés indispensables pour s'en prémunir ■

1- Données FEVAD – Express – Oxatis, janvier 2014
2- Données FEVAD, janvier 2014
3- Données FEVAD – Médiamétrie, janvier 2014
4- Rapport annuel de l'Observatoire de la sécurité des cartes de paiement, exercice 2012

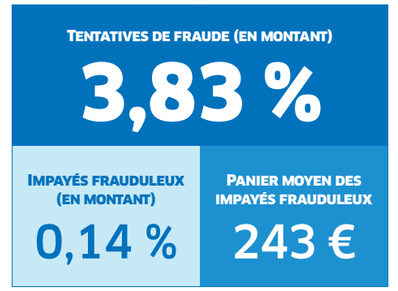
LA FRAUDE EN 2013

A. État des lieux de la fraude en 2013

Le e-commerce français demeure la cible d'une fraude importante étant donné qu'il constitue une source de biens matériels attrayante pour les fraudeurs.

En 2013, après analyse des transactions[1], Certissim observe que le taux de tentatives de fraude en valeur se stabilise à 3,83 %. Le taux de fraudes abouties en valeur (impayés frauduleux) est de 0,14 %. Une tentative de fraude sur trente se traduit par un impayé pour les e-commerçants. Le panier moyen des impayés est de 243 €, il est en recul de 18 % par rapport à 2012.

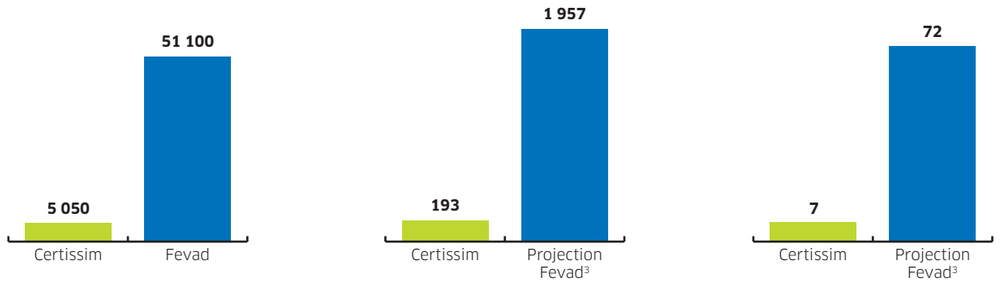
Les tentatives de fraude massives enregistrées en 2011 - 4,52 % en valeur pour un taux d'impayés de 0,22 % - ont été contrées grâce aux réévaluations des niveaux de risque menées par les acteurs du secteur. Depuis 2012, si le risque reste important, la fraude dans le e-commerce est mieux maîtrisée. Les nouveaux arbitrages adoptés depuis deux ans ont notamment permis de limiter les tentatives portant sur les paniers élevés. La fraude massive sur ces paniers aboutissait inévitablement à une augmentation significative des impayés. Le bénéfice pour les e-commerçants est donc autant quantitatif que qualitatif.



Données Certissim 2013

La projection des analyses de Certissim sur l'ensemble du e-commerce français, soit 51,1 milliards d'euros de chiffre d'affaires[2], indique que l'ensemble des tentatives de fraude se chiffrerait **à 1,9 milliard d'euros en 2013**. Les enjeux financiers sont par conséquent significatifs à l'échelle de l'économie nationale. La cybersécurité et la mutualisation des connaissances demeurent donc plus que jamais des éléments clés de la stratégie des e-commerçants.

La fraude à l'échelle du e-commerce français (en millions d'€)



1- Transactions des 900 sites marchands partenaires de Certissim
2- Données Fevad (Fédération du E-commerce et de la Vente à Distance), janvier 2014
3- Projection sur la base des taux Certissim. Ces taux sont plus élevés pour les e-marchands n'ayant pas de politique de lutte contre la fraude.

B. Évolution de la fraude depuis 2005

Selon Certissim, l'évolution du taux de tentatives de fraude et du taux d'impayés frauduleux se découpe en **quatre grandes périodes**.

• **Avant 2007 :** développement du e-commerce

La croissance de la fraude sur Internet est le pendant du développement du secteur. Les sites marchands sont confrontés à une fraude qui reste encore artisanale et opportuniste.

• **De 2007 à 2009 :** consolidation du marché

La typologie de la fraude évolue peu, même si certains secteurs, comme le tourisme, sont déjà fortement ciblés par des fraudeurs professionnels. Les outils d'analyse et de prévention du risque s'industrialisent pour répondre à la très forte croissance de l'activité du e-commerce.

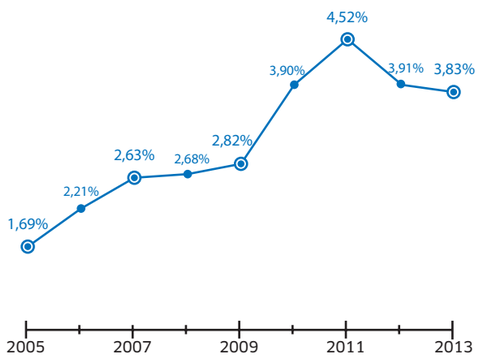
• **De 2010 à 2011 :** augmentation du risque

Le e-commerce crée de nouvelles opportunités pour les fraudeurs, tant en volume qu'en valeur. La fraude professionnelle se généralise et touche tous les secteurs du e-commerce. Certains marchands ont mis du temps à prendre la mesure de ce risque.

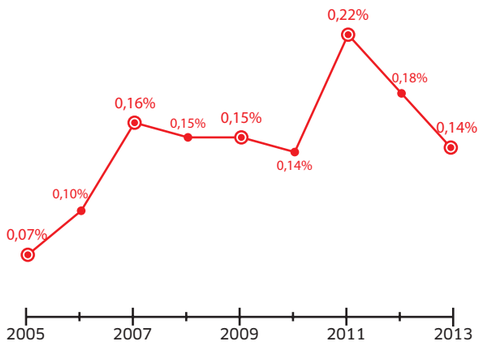
• **Depuis 2012 :** fin de « l'effet casino »[1]

Le risque de fraude est mieux maîtrisé par les e-commerçants au moyen d'un réajustement des arbitrages entre risque et opportunité de vente. Cette période marque probablement le retour à une phase de veille technologique de la part des fraudeurs.

Maîtrise de la fraude



Évolution du taux de tentatives (en montant)
pour les clients Certissim



Évolution du taux d'impayés frauduleux (en montant)
pour les clients Certissim

1- Voir définition dans le glossaire

Deux types de fraude

Certissim distingue la fraude opportuniste de la fraude professionnelle.

La fraude opportuniste est opérée par des personnes saisissant l'occasion d'effectuer des achats frauduleux pour leur propre compte ou celui de leur entourage. Il s'agit d'une fraude individuelle, non planifiée et à petite échelle, ayant pour objectif de réaliser des économies et non de générer un profit.

À l'inverse, la fraude professionnelle est mise en œuvre par des individus qui ont fait de la revente de biens frauds leur principale source de revenus. Ils sont organisés et ont généralement recours à divers réseaux criminels pour alimenter leur activité frauduleuse.

Les conséquences de cette fraude sont foncièrement différentes selon les niveaux de compétence des fraudeurs. Il y a d'une part **la fraude semi-professionnelle** se structurant sur un marché précis où les fraudeurs revendent de petites quantités de produits fraudés (exemple : la revente régulière d'une faible quantité de parfums sur une page Facebook). Le fraudeur semi-professionnel ne cherche ni à augmenter sa volumétrie, ni à se diversifier.

D'autre part, **la fraude professionnelle industrielle** a pour unique objectif de maximiser les profits. Les fraudeurs achètent et revendent frauduleusement autant de produits que possible, de l'alimentaire à l'électroménager.

Selon la typologie de fraude, le degré de risque diffère. Il est restreint dans les deux premiers cas et notable dans le dernier.

Les fraudeurs professionnels industriels suivent un processus rodé avant d'effectuer une fraude à grande échelle. Il y a une phase d'analyse, une phase de test et une phase de mise en œuvre. À chaque étape, des tentatives de fraude sont commises mais leurs objectifs divergent. La finalité de l'analyse et du test n'est pas d'acquérir frauduleusement des biens. Elles servent à identifier les e-commerçants n'ayant pas de systèmes anti-fraude et à trouver des techniques et des comportements d'achat frauduleux susceptibles de contourner ceux qui en possèdent. La phase d'analyse leur permet d'élaborer des hypothèses de contournement qu'ils tentent de vérifier, lors de la phase de test. L'objectif final étant d'appliquer ces techniques pour effectuer de véritables tentatives de fraude non détectées par les outils de lutte anti-fraude.

La notion de réitération est ce qui différencie un fraudeur opportuniste d'un fraudeur professionnel. Le premier ne donne pas suite à sa tentative lorsqu'elle est réussie alors que le second cherche à renouveler autant que possible une fraude aboutie. L'objectif est d'optimiser les gains matériels et financiers résultant de ces fraudes. Les fraudeurs professionnels sont à l'origine de « l'effet casino » et de l'augmentation du risque observés entre 2010 et 2011.

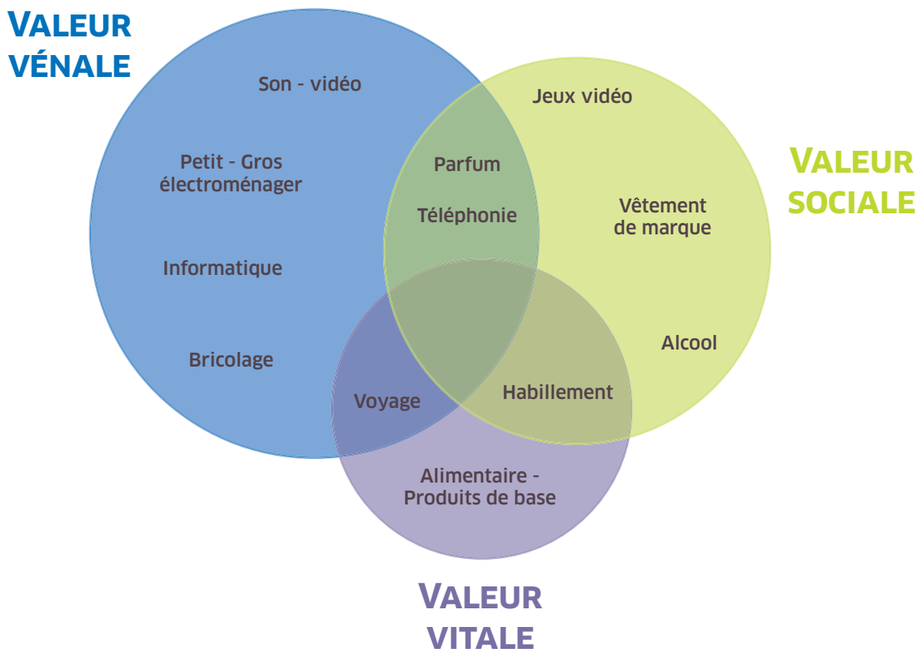
C. Analyse de la valeur dans le marché de la revente

Dans son Livre Blanc 2013, Certissim a souligné que **toute marchandise vendue sur Internet est susceptible d'être la cible d'une tentative d'achat frauduleux**. Le produit acquis frauduleusement est ensuite revendu à des particuliers sur un marché parallèle.

L'évolution du contexte socio-économique et la dimension industrielle de la fraude professionnelle expliquent en grande partie ce fait. Néanmoins, elles n'expliquent pas pourquoi certains produits sont plus ciblés que d'autres par la fraude et elles ne donnent pas les clés d'analyse du risque de fraude par produits. Évaluer précisément le risque nécessite non seulement de s'interroger sur les procédés frauduleux mais également sur les motivations d'achat de produits fraudés.

Face à une fraude opportuniste, le prix d'un produit est longtemps resté l'indicateur principal du risque de fraude. Certains produits et marques à la mode étaient également connus comme étant des cibles de choix pour les fraudeurs. Désormais, face à la fraude professionnelle, l'indicateur prix n'est plus suffisant. Ces fraudeurs choisissent les cibles de leurs fraudes en fonction de la demande de leurs acheteurs, du gain et de la facilité de revente.

Certissim distingue trois catégories de valeurs pouvant être accordées à un produit fraudé et revendu, indépendamment de son prix de vente. Pour les e-commerçants, ces valeurs sont des indicateurs permettant de déterminer l'existence d'un marché potentiel de revente et donc d'estimer le risque de fraude.



• Valeur vénale

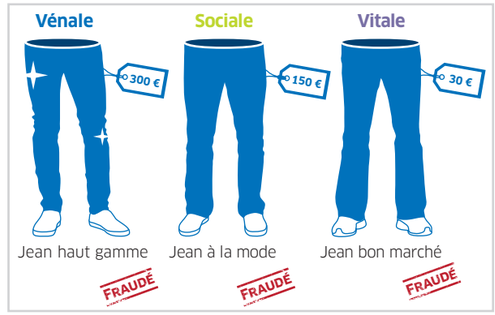
Dans ce cas de figure, la motivation est pécuniaire. L'acheteur final souhaite acquérir, sur le marché parallèle, un bien d'une gamme supérieure à celle qu'il a la capacité financière de s'acheter légalement. Il cherche à effectuer des économies mais n'a pas un besoin vital de ce produit.
Par exemple, concernant le secteur de l'électronique grand public, acheter à un fraudeur un ordinateur portable lui permettra d'en obtenir un de meilleure qualité au prix de la gamme standard.

• Valeur sociale

Les tendances et effets de mode sont à l'origine de ce type de motivation. L'acheteur final, pour des raisons d'image ou encore d'appartenance à un groupe, souhaite posséder un type de marchandise plutôt qu'un autre, sans avoir à y investir le prix magasin. La notoriété des marques ciblées est pratiquement toujours un facteur de choix.
Par exemple, à niveau qualitatif équivalent, les fraudes porteront sur une enseigne de textile prisée par les médias plutôt que sur une autre.

• Valeur vitale

Ce type de motivation est lié à un achat perçu comme une nécessité ou un besoin primaire par l'acheteur final. Cet achat est soumis à des contraintes budgétaires, ce qui l'amène à chercher les tarifs les plus bas possibles. C'est notamment un débouché pour la fraude alimentaire.



Cas d'application

Ces trois valeurs ne sont pas exclusives les unes des autres. Associer un produit à une valeur vénale, sociale ou vitale fait uniquement ressortir la valeur dominante permettant d'orienter l'analyse, le suivi et la prévention du risque. Pour les e-commerçants, évaluer le risque de fraude sur un produit à travers sa valeur consiste à déterminer un niveau en deçà duquel le produit perd tout attrait pour la revente en circuit parallèle. Ils doivent donc procéder à une analyse de l'appétence du marché de la fraude pour leur catalogue.

D. Les produits fraudés

Tous les produits proposés à la vente sur Internet sont susceptibles d'être fraudés dès lors qu'il existe un marché parallèle de revente pour chacun d'entre eux.

L'accroissement du coût de la vie a, par exemple, fait de l'alimentaire un domaine de plus en plus attrayant pour la fraude. Elle répond à une nécessité et les opportunités de revente sont élevées. Néanmoins, la fraude sur l'alimentaire comprend également une part de produits destinés à des évènements festifs (whisky, Coca-Cola, champagne) et une autre part correspondant des effets de mode.

Les secteurs traditionnellement fraudés (électroménager, informatique et parfumerie) restent parmi les cibles de choix des fraudeurs. Par ailleurs, les pièces détachées et composants informatiques constituent un marché de niche appétent et en plein essor.

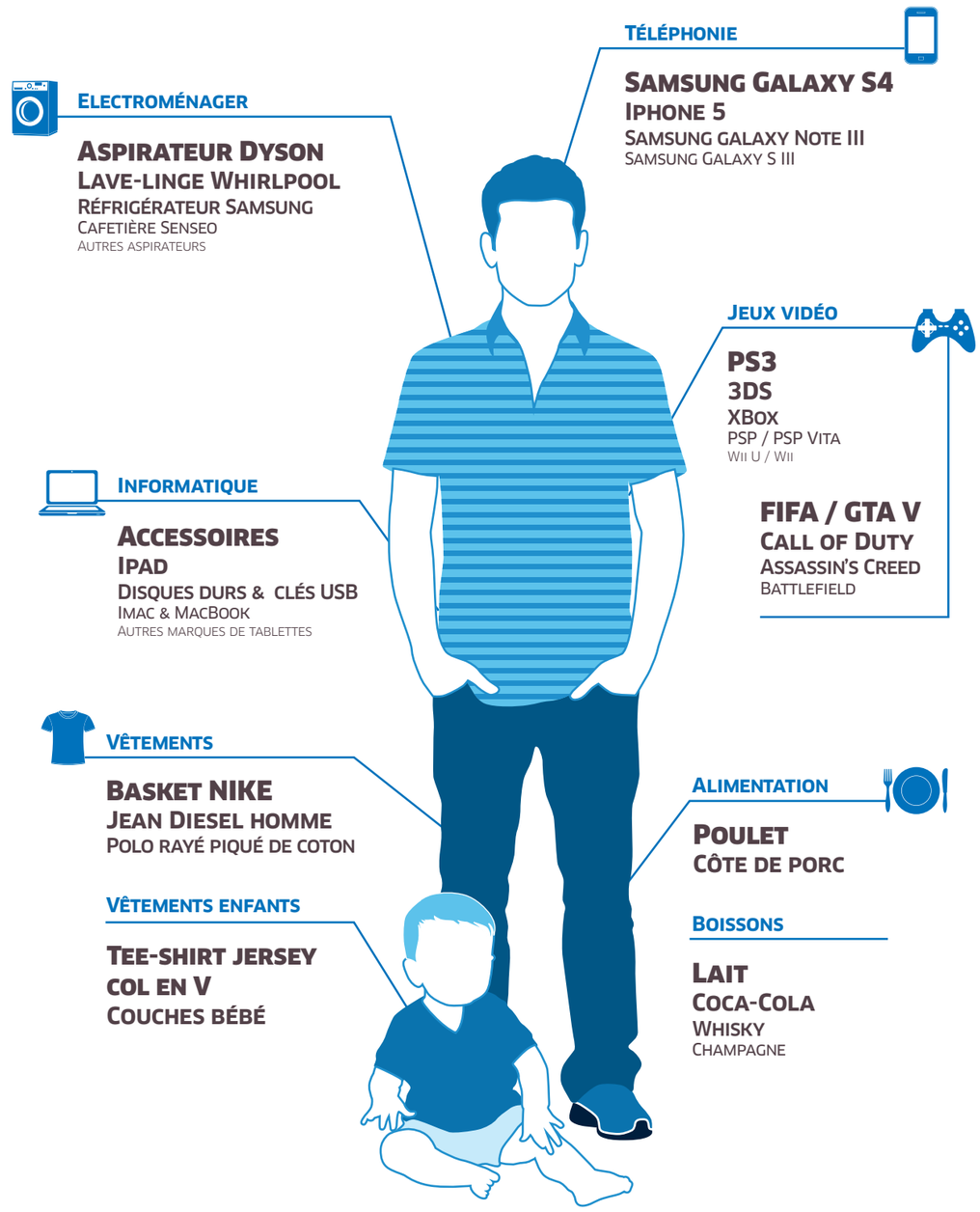
Pour certains produits, la fraude est saisonnière. Par exemple, les valises sont particulièrement fraudées du mois de mai jusqu'au mois de septembre.

La fraude s'adapte également aux nouveautés du marché car la demande est toujours plus forte lors des lancements de produits. C'est particulièrement le cas pour la téléphonie et les jeux vidéo.

En outre, la demande en biens fraudés est guidée par leur réutilisation et l'optimisation de leur usage quotidien. C'est pourquoi la console de jeux PS3 de Sony est plus demandée que la console Xbox de Microsoft car ses jeux vidéo se revendent mieux sur le marché de l'occasion. La cafetière Senseo est plus recherchée que la cafetière Nespresso en raison du coût d'achat moins élevé de ses capsules de café.

Pour chaque marchand, une analyse spécifique doit être menée pour identifier ses zones de vulnérabilité.

Top des produits fraudés en 2013



E. Répartition des fraudes à l'échelle nationale

Lors d'une commande sur Internet, le client renseigne une adresse de livraison. Cette donnée est un élément clé pour les fraudeurs car elle détermine la manière dont ils vont récupérer les marchandises achetées frauduleusement. Ils ont plusieurs options pour les réceptionner : usurper l'identité postale d'une autre personne et intercepter le colis lors de sa livraison, être livré en point relais, avoir recours à une mule, etc.

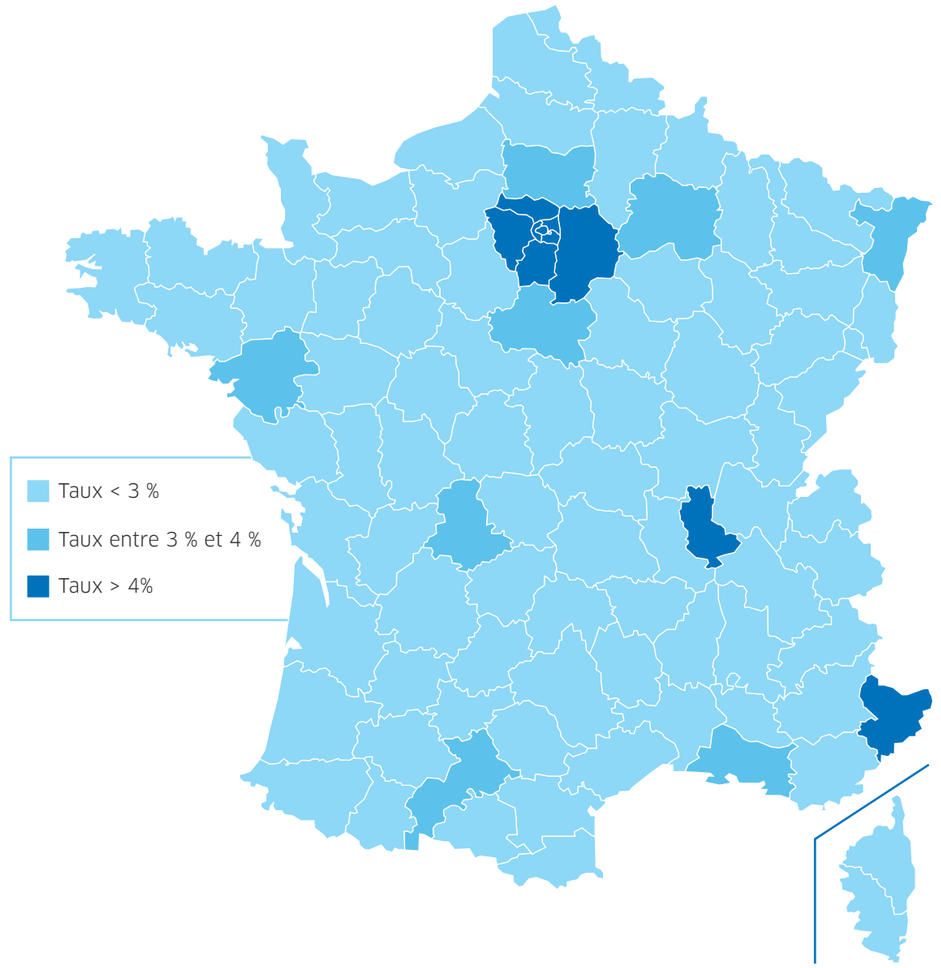
L'adresse de livraison est un des indicateurs du risque de fraude. La répartition nationale des tentatives de fraude met en évidence une concentration urbaine de ces tentatives.

Du fait de la densité de population dans les grandes agglomérations, il est plus difficile de préjuger d'une accumulation anormale de livraisons à une adresse postale utilisée frauduleusement et donc de détecter les tentatives de fraude. Ainsi, les régions Ile-de-France et Provence-Alpes-Côte d'Azur concentrent une grande partie des tentatives de fraude. Les zones urbaines permettent aux fraudeurs de mieux dissimuler leurs tentatives dans la masse des commandes et elles leur assurent un marché de revente important. Ils se concentrent donc sur ces zones à haut rendement.

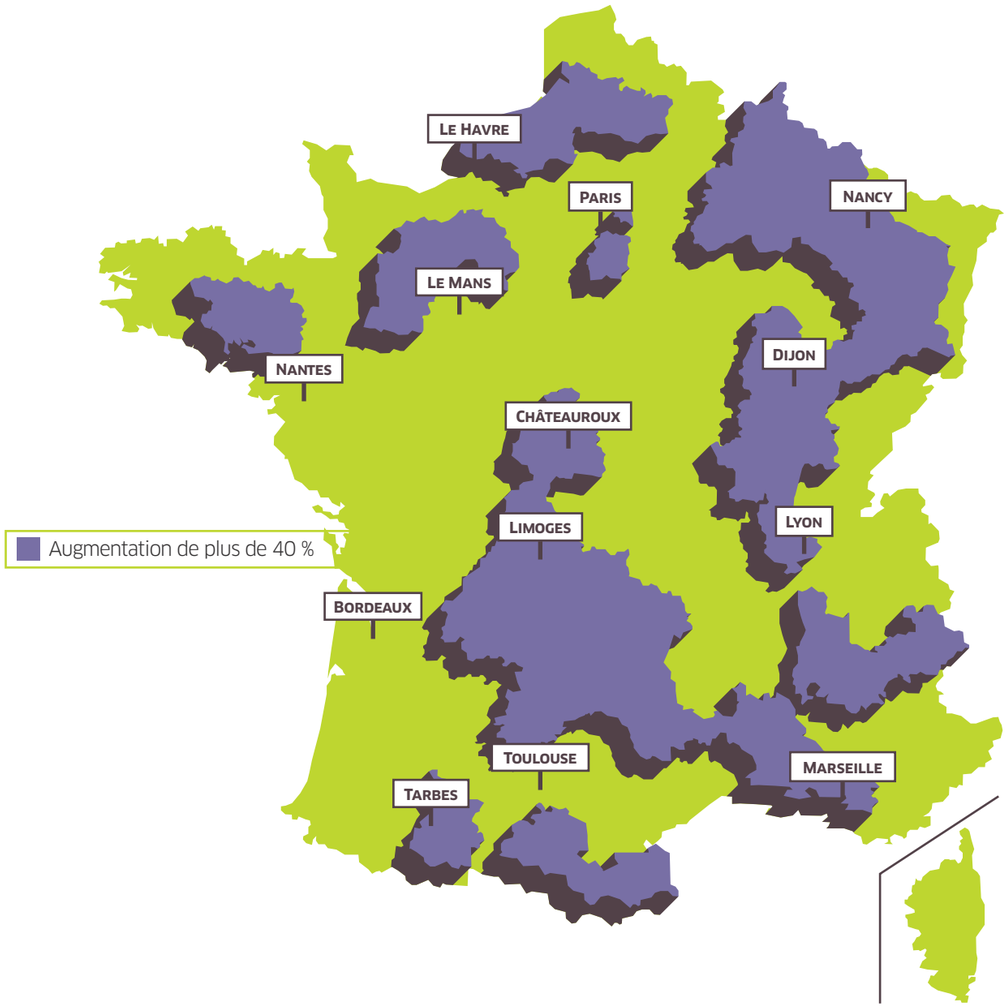
Néanmoins, s'il est plus diffus en milieu rural, le risque de fraude est présent sur l'ensemble du territoire. Aucune région n'échappe au phénomène.

N.B. : dans les régions rurales, le flux de commandes en ligne est plus ténu qu'en zone urbaine. En conséquence, les tentatives de fraude sont plus apparentes et peuvent donner l'impression d'un taux de risque plus élevé qu'il n'est en réalité.

Répartition des tentatives de fraude par lieux de livraison



Croissance des impayés pour les commandes livrées en relais colis



Entre 2012 et 2013, Certissim constate une augmentation des impayés à la suite d'une livraison en point relais. Plusieurs zones se distinguent. Elles sont choisies par les réseaux de fraudeurs professionnels selon trois principaux critères :

• **la proximité d'un ou plusieurs réseaux de transports** (routier, ferré ou naval) permettant de déplacer rapidement les marchandises fraudées d'un endroit à un autre. Par exemple, la zone s'articulant autour des villes de Nancy, Dijon et Lyon est reliée par un même axe autoroutier.

• **la proximité d'une frontière.** Elle leur permet de faire sortir les marchandises fraudées du territoire, à l'exemple de la zone identifiée autour du Havre, alimentant un trafic à destination de l'Angleterre.

• **l'existence d'un important marché de revente aux alentours.** Les grands centres urbains (Paris, Marseille, Lyon) sont des lieux d'écoulement des biens fraudés connus du fait de leur importance démographique. Les zones de livraison des commandes frauduleuses se situent systématiquement à moins de deux heures de train des grandes agglomérations françaises.

Les réseaux de fraudeurs modifient fréquemment leurs zones de livraison en relais colis pour ne pas être repérés. De plus, ils ciblent souvent des régions rurales en comptant sur une méconnaissance de leurs procédés de la part des autorités locales qui y sont peu confrontées.

Dans certains cas de figure, les zones de livraison coïncident directement avec la spécialisation des réseaux qui s'y sont installés. Les marchandises fraudées ne sont alors pas déplacées vers une autre région. Par exemple, dans les alentours de Dijon et Lyon s'est établi un réseau spécialisé dans la revente de pièces détachées informatiques.

DES PROCÉDÉS FRAUDULEUX

Depuis plusieurs années, Certissim observe une professionnalisation des méthodes de fraude dans le e-commerce. Les fraudeurs ont su s'adapter aux contrôles opérés par les acteurs de la lutte anti-fraude et recréer des profils d'acheteurs sur la base d'identités manipulées ou inventées, en utilisant de vrais numéros de cartes bancaires acquis en masse.

A. Les mécanismes de la fraude

La fraude professionnelle industrielle impactant le e-commerce est une ramification d'organisations criminelles plus vastes. Leurs activités comprennent le trafic de drogues et d'armes, la prostitution ainsi que diverses arnaques (à la loterie, à l'héritage, au virement SEPA, etc.)

1. La fraude identitaire

Le premier maillon de cette fraude est la fraude identitaire. Une identité n'est pas un tout indivisible. Elle est constituée d'une multitude d'éléments plus ou moins importants et chacune de ces informations d'ordre personnel est susceptible d'être volée à un tiers pour être utilisée à son insu sur Internet :

- **données d'état civil** : nom, prénom, date et lieu de naissance, filiation ;
- **données bancaires** : numéros de carte et de compte bancaires ;
- **coordonnées** : adresse postale, numéro de téléphone (fixe et mobile) et adresse électronique.

Cette utilisation frauduleuse des données personnelles est constitutive de l'infraction d'usurpation d'identité prévue par l'article 226-4-1 du Code Pénal, issu de la loi LOPSI 2 du 14 mars 2011 : *« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »*

D'où proviennent les données usurpées ?

Si des données personnelles sont usurpées sur Internet, elles le sont également dans le monde physique, dans la vie de tous les jours. Elles alimentent les fraudeurs en justificatifs de tous types et en identités « propres » et cohérentes.

La réutilisation de documents d'identité et l'usage de données authentiques sont en forte augmentation dans le domaine des tentatives de fraude dans le e-commerce. Deux réseaux d'approvisionnement spécialisés coexistent. Ils sont un des débouchés de filières criminelles parallèles : le vol et le piratage informatique.

a. Le vol

- À l'arrachée, cambriolage, car-jacking, etc.
- En agence de location de voitures, hôtel, agence immobilière, grâce à des malveillances ou des négligences isolées au sein de ces entreprises détenant des éléments identitaires.

Ces actes sont susceptibles de constituer des infractions d'abus de confiance ou de vol, définies par le Code Pénal aux articles 314-1 et 311-1. Ils peuvent être punis d'emprisonnement et/ou d'amendes.

b. Le piratage informatique

• Phishing[1], hacking[2], piratage de boites e-mail, etc.

Histoire vraie

En juin 2013, Madame X., résidant dans le sud-est, répond à un e-mail de la « CAF » lui demandant d'envoyer une copie de sa carte d'identité et de son RIB afin de compléter son dossier d'allocation vacances.

En août 2013, les documents envoyés sont recyclés par un réseau de fraudeurs pour l'acquisition de biens mobiliers sur Internet (meubles, quads, etc.)

Contactée, Madame X. avoue ne pas s'être méfiée de cet e-mail puisqu'il ne lui demandait pas les numéros de sa carte bancaire.

• Récupération d'informations sur les réseaux sociaux, arnaques sur les sites de vente entre particuliers.

Histoire vraie

Monsieur G., fraudeur, se sert des sites de vente entre particuliers pour usurper des identités.

Il répond aux annonces de ventes de véhicules. Face à un vendeur intéressé, il refuse de payer en espèces car il prétend avoir été victime d'une escroquerie il y a peu de temps. Il souhaite donc payer par virement bancaire. À cette fin, il demande au vendeur de lui fournir une copie de sa C.N.I., de son RIB et d'un justificatif de domicile. Bien entendu, il n'achètera pas le véhicule mais recyclera ou revendra les copies des documents obtenus.

Une fois collectés par ces différentes filières, les éléments d'identité sont revendus, notamment par le biais de forums Internet spécialisés.

Annonce de revente de cartes bancaires volées

Les fraudeurs n'ont alors plus qu'à acheter et assembler les éléments qui les intéressent pour effectuer des achats frauduleux. Afin de compléter l'identité qu'ils ont usurpée, ils peuvent également recourir au faux en achetant de faux documents.

c. Le cas particulier des détournements de comptes clients

Les Français utilisent régulièrement le même **mot de passe** sur tous les sites qu'ils fréquentent. Ces mots de passe peuvent être volés via du phishing ou simplement par déduction en fonction des informations publiées sur les réseaux sociaux. Le fraudeur accède alors très facilement à l'ensemble de leurs comptes, notamment les comptes clients sur les sites marchands.

1- Voir définition dans le glossaire
2- Voir définition dans le glossaire

Concrètement, le fraudeur réussit à usurper l'identité d'un client ayant un historique d'achat chez un e-commerçant. Après avoir récupéré le mot de passe, il se connecte au compte client à la place de celui-ci. Il modifie rapidement l'adresse e-mail et le numéro de téléphone afin de s'approprier le compte client. Il conserve et utilise ainsi la crédibilité du client pour passer des commandes avec des numéros de cartes bancaires volés. Certains éléments de facturation ou de livraison varient selon la stratégie de récupération de marchandise du fraudeur.

À la suite de la commande et de l'impayé frauduleux, le site marchand se retourne légitimement vers son client, qui devra alors prouver qu'il n'est pas à l'origine de cette commande.

Histoire vraie

Été 2013, une commande d'un appareil photo haut de gamme est passée par Mme O., habituée du e-commerce, habitant dans les Yvelines. Cette commande doit être livrée dans le sud de la France en relais colis. En période estivale, ce type de comportement d'achat est courant.

Contactée par Certissim par téléphone, Mme O. indique ne pas être à l'origine de cet achat. Après vérification, il s'avère qu'elle ne peut plus accéder à sa boîte e-mail ni à ses comptes clients habituels.

Peu de temps auparavant, elle avait fait l'acquisition de billets d'avion sur un site Internet étranger. Puisqu'elle utilise le même mot de passe pour tous ses comptes e-mails et clients, les fraudeurs n'ont eu aucun mal à y pénétrer et à commander sur Internet à sa place.

Afin de contrer ces détournements, les sites de e-commerce doivent mettre en œuvre une politique de protection des données personnelles. Ils peuvent, par exemple, supprimer l'envoi de l'identifiant et du mot de passe en clair par e-mail lors de la création d'un compte client. En effet, ces informations peuvent être facilement usurpées en cas de piratage de la boite e-mail. Ils peuvent également refuser les mots de passe trop simples (exemples : azerty, 0123456, motdepasse) et inciter leurs clients à modifier leur mot de passe régulièrement.

Dans ce contexte de développement du phishing et du piratage informatique[1], les e-commerçants doivent tenir compte de l'existence d'un risque de fraude sur les transactions de clients connus et réguliers. L'idée que ces transactions seraient moins risquées n'est plus valable.

2. La fraude indirecte

Dans le cadre du e-commerce, la fraude indirecte est la manipulation d'une personne honnête dans le but de masquer une opération frauduleuse pour le compte d'un vrai fraudeur. Elle a pour objectif l'expédition de colis à l'étranger, sans que l'intermédiaire sache qu'ils proviennent de commandes frauduleuses réalisées sur Internet. La victime devient ce qui est communément appelé **une mule**. Il existe différentes déclinaisons de cette fraude visant des types de victimes précis.

Les associations caritatives

Avec ce système, les fraudeurs ciblent principalement des seniors en recherche d'activités bénévoles. Une fois recrutés, ils sont, par exemple, amenés à recevoir une grande quantité d'ordinateurs chez eux et à attendre l'arrivée d'un conteneur qui permettra d'envoyer ces biens aux élèves d'une école d'un pays défavorisé. Sous des aspects de bénévolat, il s'agit simplement d'un trafic de marchandises achetées frauduleusement. Cette technique est souvent couplée à celle des contrats de travail. Cependant, les fraudeurs peinent à trouver des bénévoles car les particuliers préfèrent participer à une action caritative proche de chez eux.

1- Voir définition dans le glossaire

La mule amoureuse

Le fraudeur rencontre sa victime, principalement des femmes, via des sites de rencontre en ligne. Il prétend souvent exercer une profession prestigieuse, comme chirurgien, et être de nationalité étrangère mais francophone (Québec). Les photos qu'il publie, pour prouver son identité, ont été volées sur Internet (Facebook, blogs, etc.) Il peut aussi s'agir de photographies de célébrités ou de mannequins. Lorsque la relation amoureuse s'est développée, le fraudeur demande à sa victime de réceptionner des colis pour son compte et de les lui renvoyer sous un prétexte quelconque (préparation du mariage). Cette technique se développe depuis cinq à six ans. Néanmoins, elle est peu à peu délaissée par les fraudeurs car beaucoup d'émissions de télévision ont traité de ce sujet.

La mule familiale

Le fraudeur demande à une ou plusieurs personnes de sa famille de récupérer des colis pour son compte et de les lui renvoyer par la suite. Pour le fraudeur, l'avantage est d'utiliser des membres de sa famille auprès desquels il n'a pas besoin de se justifier. Il demande simplement à son entourage de lui rendre un service.

Histoire vraie

Monsieur C. reçoit régulièrement à son domicile, pour rendre service, des colis à son nom pour le compte de son cousin domicilié au Maroc. Il lui transmet les marchandises, achetées frauduleusement, par l'intermédiaire d'amis faisant la navette entre Paris et Casablanca.

Monsieur C. est avisé des fraudes à la suite d'une convocation policière. Il pensait simplement rendre service à un membre de sa famille.

Les contrats de travail

Cette escroquerie cible principalement les personnes en recherche d'emploi ou de revenus complémentaires. Les fraudeurs mettent en ligne des offres d'emploi, généralement sur des sites de petites annonces gratuites, proposant de travailler comme « manutentionnaire », « déclarant douane » ou encore « commissionnaire occulte ».

Depuis l'émergence de cette technique, les fraudeurs se sont perfectionnés et les annonces sont plus difficilement repérables. Elles ne se démarquent plus autant par le nombre de fautes d'orthographe.

De plus, les fraudeurs n'hésitent plus à usurper l'identité de grandes entreprises pour publier ces offres d'emploi. Cet acte est susceptible de constituer une infraction d'escroquerie et peut être puni d'emprisonnement et/ou d'amendes.

Dans le cadre de la signature de son « contrat de travail », la victime de l'escroquerie fournit les documents standards nécessaires (photocopie de carte d'identité, RIB, justificatif de domicile) qui serviront au réseau de fraudeurs à passer des commandes frauduleuses. Le fraudeur cache son identité lors des commandes et se sert de celle de sa victime pour ne pas être détecté par les systèmes anti-fraude des sites marchands. La victime devient une mule en étant chargée par le fraudeur de lui réexpédier les colis qu'elle réceptionne, à l'aide d'étiquettes prépayées qu'il lui envoie par e-mail. Les adresses e-mail utilisées sont de plus en plus créées volontairement par la victime et servent exclusivement aux échanges avec le fraudeur.

Dans la plupart des cas, la victime n'obtiendra jamais le salaire attendu et sera considérée comme l'unique « responsable » pour les sites marchands et les autorités, puisque le nom du fraudeur n'apparaît sur aucune opération. Il existe des cas de figure où la victime reçoit un chèque pour salaire. Souvent deux à trois fois supérieur au montant initialement prévu, il s'agit d'un chèque volé.

En 2013, le cadre de cette escroquerie s'est élargi. En sus de l'activité de réception de colis, certaines mules ouvrent désormais un compte bancaire personnel sur lequel elles reçoivent des virements. Elles sont employées en tant qu'« intermédiaire financier ». Suivant le même principe que la première activité, les sommes sont virées à l'étranger, en échange d'un pourcentage. Il peut s'agir de blanchiment d'argent. La démarche d'ouverture de compte étant volontaire et nominative, les mules en sont d'autant plus responsables pénalement.

Les fraudeurs changent souvent de victime. En effet, **« la durée de vie » moyenne d'une mule est d'environ trois semaines**. Cela correspond au seuil psychologique à partir duquel une personne commence à parler de son nouveau travail. Plus l'entourage est au courant, plus le risque que l'escroquerie soit mise au jour est grand. Il s'agit également du temps nécessaire aux différents organismes pour détecter le phénomène. Quelques cas particuliers existent où les mules « travaillent » plus longtemps et où ce rôle est alors pleinement assumé.

Entre 2012 et 2013, Certissim a constaté **une augmentation de 9,67 % du nombre de cas d'escroqueries aux « contrats de travail »**, soit une croissance de 16 % en montant.

B. Se prémunir contre le vol de données

Pour les autorités, la démocratisation d'Internet a compliqué les travaux de détection des sources d'approvisionnement en éléments d'identité ainsi qu'en coordonnées bancaires. En effet, les techniques de collecte s'étant démultipliées, la recherche d'un point de compromission[1] n'est plus aussi déterminante que par le passé.

Certissim préconise certaines bonnes pratiques afin de contrer ces techniques.

Sur Internet

- Faire attention aux mots de passe. Chaque mot de passe doit être unique et comporter *a minima* un chiffre, un caractère spécial et une majuscule. Il faut également éviter de noter ses mots de passe.

- Ne pas répondre aux e-mails de **phishing**. Pour les reconnaître, il faut regarder tant le fond que la forme des e-mails. Fautes d'orthographe, absence de personnalisation (nom, prénom), nécessité de répondre en urgence, proposition d'un gain important sont autant d'indices pour détecter un phishing. En cas de doute, il faut contacter directement l'institution concernée par téléphone et ne pas cliquer sur les liens de l'e-mail suspicieux.

Les techniques de phishing ont évolué ces dernières années. Auparavant concentrés sur la récupération de données bancaires, les auteurs de phishings cherchent désormais à récupérer tous types d'éléments personnels (état civil, coordonnées, mots de passe et réponses aux questions secrètes).

Toute tentative de phishing peut être déclarée sur : *www.internet-signalement.gouv.fr*.

Dans le monde physique

- Être vigilant quant aux documents mentionnant des données personnelles, souvent jetés à la poubelle sans être préalablement déchirés (originaux et copies de remise de chèques jetés dans les corbeilles des banques). Un fraudeur n'hésitera pas à récupérer des informations dans les ordures.

1- Lieu où des données bancaires ont été volées, identifié par les autorités par recoupement entre les fichiers d'utilisation des cartes bancaires et les dépôts de plaintes de plusieurs victimes de vol.

• Être attentif aux données personnelles et photocopies fournies lors de locations (hôtel, voiture) ou de souscriptions de contrats. Si possible, éviter d'envoyer des documents sensibles par courrier et à la fin du contrat, demander à récupérer les documents ou demander leur destruction.

• Désactiver l'option de prévisualisation des sms sur écran verrouillé sur des smartphones. En cas de vol couplé de la carte bancaire et du smartphone, le fraudeur pourra acheter en ligne même en cas d'Authentification Non Rejouable[1] puisqu'il n'aura pas besoin de déverrouiller le téléphone pour visualiser le code.

• Appliquer **un sticker sécuritaire** ou une gommette sur les trois chiffres CVV de la carte bancaire permet de limiter les risques de vol des données au moment d'un règlement en magasin.

Il arrive parfois que le consommateur perde de vue sa carte bancaire quelques instants (nécessité de reconnecter le terminal de paiement à sa base, comptoir trop haut, etc.) Ce laps de temps suffit pour noter ou retenir le code CVV, les autres numéros de la carte bancaire étant notés sur le reçu conservé par les professionnels.

Avec un sticker sécuritaire, le fraudeur ne pourra pas voir le code CVV, indispensable lors d'un achat en ligne. La tentative de vol des données n'aboutira pas et celles-ci ne seront ni revendues ni utilisées sur Internet.

Sticker sécuritaire Certissim

Histoire vraie

Madame S. va au musée avec son mari et ses deux enfants. Elle paye les places avec une carte bancaire qu'elle utilise rarement.

Quelques jours plus tard, en consultant ses comptes en ligne, elle constate le débit du musée mais également plusieurs achats en ligne qu'elle n'a pas effectués.

Ses numéros de carte bancaire ont été retenus par une personne mal intentionnée lors de cette visite au musée, et utilisés pour des achats sur Internet.

1- Voir définition dans le glossaire

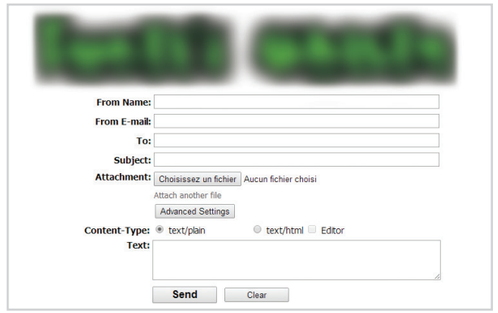
C. Les nouveaux procédés frauduleux

Alors que les systèmes de lutte contre la fraude se perfectionnent continuellement, les fraudeurs recherchent sans cesse des moyens pour les contourner. Certissim en a rencontré plusieurs en 2013.

1. Le spoofing

Certains programmes initialement destinés à réaliser des canulars sont désormais détournés de leur usage premier par les fraudeurs. Le principe est d'appeler ou d'envoyer un e-mail en affichant un numéro ou une adresse e-mail autre que le leur, qu'ils soient réels ou non. Ils espèrent ainsi contourner les systèmes anti-fraude en se faisant passer pour un client lambda.

Dans le cadre d'un appel, la supercherie peut être facilement découverte en rappelant le numéro suspect. Soit le numéro n'est pas attribué, soit il renverra sur le portable du véritable détenteur de la ligne téléphonique.



Logiciel de spoofing e-mail

Les adresses e-mails maquillées sont plus délicates à démasquer car les fraudeurs ont la possibilité d'en créer qui présentent toutes les caractéristiques d'adresses véritables et sécurisées (exemples : *barack.obama@whitehouse.gov* ou encore *jean.dupont@finances.gouv.fr*). Le danger de ce type de spoofing est que le destinataire soit en confiance, puisqu'il pense connaître l'expéditeur, et qu'il clique sur le lien présent dans l'e-mail.

Pour vérifier l'authenticité d'une adresse e-mail, il faut que l'adresse d'expédition (From) et l'adresse de réponse (Reply-To) soient identiques. Il en va de même pour l'ID du message (Message-ID) et le domaine de l'adresse d'expédition (From). Par exemple, sur Gmail, il suffit de cliquer sur le menu déroulant à côté de « Répondre » pour accéder à ces informations.

Les cas de spoofing sont en forte hausse en Angleterre, aux Etats-Unis et au Canada.

2. Les générateurs

Les fraudeurs ont besoin de renouveler régulièrement les identités utilisées pour acheter frauduleusement en ligne. Ceux qui ne souhaitent pas recourir aux filières classiques (vol, piratage ou usage de faux) font désormais appel aux générateurs.

Ces logiciels permettent de générer des identités complètes. D'autres permettent à ceux ayant recours à l'usage de faux de générer les lignes MRZ (ZLA)[1] d'une pièce d'identité.

Carte d'identité française contrefaite

1- Lignes de caractères situées dans la partie inférieure d'une carte d'identité contenant des codes destinés à vérifier sa conformité.

D. Les conséquences de la fraude

1. Pour les e-commerçants

Les conséquences de la fraude pour les e-commerçants sont invariablement liées à des **coûts financiers**. Lorsqu'il subit une fraude, un e-marchand perd non seulement la marchandise mais également les frais engendrés par son stockage, la préparation de la commande et l'expédition. De plus, la banque du e-commerçant débite systématiquement ce dernier de l'intégralité du montant de la commande indûment payé, sauf mise en œuvre d'un mécanisme de garantie. La loi précise que : « *L'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit sous peine de forclusion à moins que le prestataire de services de paiement ne lui ait pas fourni ou n'ait pas mis à sa disposition les informations relatives à cette opération de paiement. Sauf dans les cas où l'utilisateur est une personne physique agissant pour des besoins non professionnels, les parties peuvent convenir d'un délai distinct de celui prévu au présent article* » (Article L133-24 du Code monétaire et financier).

Ce ne sont pas les seules répercussions de la fraude. Les **risques d'image et de réputation** sont conséquents et ce auprès de tous les publics du e-marchand : banques, assureurs, actionnaires, clients. Ainsi, un consommateur victime d'usurpation d'identité ou de détournement de données bancaires deviendra hésitant quant à une prochaine commande en ligne. Il partagera cette déconvenue avec son entourage qui risquera, à son tour, de développer les mêmes réserves. Il pourra également la partager sur les forums Internet.

Les e-commerçants ne doivent pas hésiter à porter plainte lorsqu'ils sont victimes d'une fraude. Depuis mars 2013, le pré-dépôt de plainte en ligne leur permet de gagner du temps : *www.pre-plainte-en-ligne.gouv.fr.*

À savoir : Pour compléter le dossier, il faudra transmettre plusieurs éléments : facture, avis d'impayé, bon de commande et adresse IP.

2. Pour les particuliers

Si l'usurpation de données personnelles a obligatoirement un impact, son ampleur varie en fonction de la nature de l'usurpation.

L'usurpation des données d'une carte bancaire

Le consommateur s'en aperçoit lorsque des achats qu'il n'a pas effectués sont débités sur son compte bancaire. Le préjudice est financier et les délais de remboursement chronophages. En effet, il devra entreprendre des démarches pour obtenir la régularisation de sa situation auprès de sa banque et signaler l'opération de paiement non autorisée. Néanmoins, le préjudice s'éteint le plus souvent en quelques semaines ou quelques mois.

À savoir : le porteur de la carte n'a plus obligation de porter plainte pour être remboursé par sa banque.

L'usurpation d'identité numérique

Les aspects de l'usurpation d'identité numérique sont multiples, tout comme leurs conséquences. En cas de hacking d'une boite e-mail, tous les contacts du carnet d'adresses sont à leur tour mis en danger. Le fraudeur, en se faisant passer pour le propriétaire de la boîte e-mail, pourra leur envoyer des virus ou leur demander des informations personnelles. Les destinataires, en confiance, seront plus réceptifs.

La création de faux profils sur les réseaux sociaux est un exemple de la difficulté à maîtriser son image numérique. Ces faux profils peuvent se servir uniquement de photographies volées ou bien de la totalité des éléments d'une identité. Ils sont ensuite utilisés pour des escroqueries.

Les consommateurs doivent porter plainte au commissariat de police ou à la gendarmerie et tenter de faire fermer ou retirer les pages Internet incriminées en contactant le responsable du site hébergeant ces pages. En cas de non réponse du responsable, la CNIL peut seconder les consommateurs dans leurs démarches.

L'usurpation de documents d'identité

Dans ce cas de figure, le cheminement est plus complexe car le particulier ne s'aperçoit pas immédiatement de l'utilisation frauduleuse de son identité. Il est dans l'obligation de démontrer qu'il n'est pas à l'origine de la fraude. Tout se présente comme s'il était **en situation de « présomption de culpabilité » et doit prouver son innocence**. Il doit dans la quasi-totalité des cas faire appel à un avocat. C'est devant la justice, civile ou pénale, qu'il doit justifier de la provenance des documents d'identité utilisés à son insu. La durée du préjudice est difficilement quantifiable puisque les données sont susceptibles d'être revendues et réutilisées.

Comme le souligne Benoit Dupont dans son article « La coévolution du vol d'identité et des systèmes de paiement »[1], l'usurpation d'identité n'est pas un phénomène nouveau. Il a été transposé de la vie de tous les jours aux différentes applications rendues possibles par Internet (achat en ligne, réseaux sociaux, etc.)

1- Paru à l'automne 2010 dans la revue *Criminologie*, volume 43, numéro 2, p. 247-268.

Les nouveaux enjeux de la lutte contre la fraude

Pour les e-commerçants, les fraudes réalisées par des fraudeurs opportunistes ont un impact maîtrisable et moins important. En effet, ces derniers utilisent une carte bancaire volée mais achètent souvent sous leur propre nom et se font livrer à une adresse en lien avec leur identité réelle (travail, entourage, etc.) L'attention des e-commerçants, des systèmes de lutte anti-fraude et des autorités se porte donc avant tout sur le moyen de paiement utilisé pour détecter ce type de fraudeurs. Les e-commerçants peuvent ensuite entamer les démarches de recouvrement en réponse au préjudice subi.

En revanche, face à la fraude professionnelle, il ne s'agit plus uniquement de détecter l'utilisation d'une carte bancaire volée. Les e-commerçants et systèmes de lutte anti-fraude doivent être capables d'évaluer l'authenticité et la cohérence de l'ensemble des éléments identitaires utilisés pour acheter en ligne.
L'identification d'une utilisation frauduleuse d'un ou de plusieurs éléments identitaires engendre une probabilité plus importante de déceler une fraude bancaire. L'enjeu de cette identification est capital car, pour le e-commerçant, accepter une vente qui découle d'une fraude professionnelle signifie une perte sèche. En effet, puisqu'un ou plusieurs éléments identitaires ne correspondent à rien de réel, il n'a pas de recours face à l'impayé. Dès lors, il perd la marchandise et le montant de la vente.
Par exemple, lors de l'utilisation frauduleuse d'une adresse postale et du nom d'une personne qui n'existe pas ou qui ne réside pas à cette adresse, la lettre recommandée du e-commerçant demandant la régularisation de l'impayé lui sera retournée (NPAI).

A. Assimiler les évolutions de la fraude identitaire

L'évolution des typologies de fraudeurs et de leurs méthodes implique une modification du métier de lutte contre la fraude dans le e-commerce. Il ne consiste donc plus seulement à évaluer un risque d'usurpation d'identité bancaire. Il doit maintenant identifier les mécanismes de la fraude identitaire au sens large.

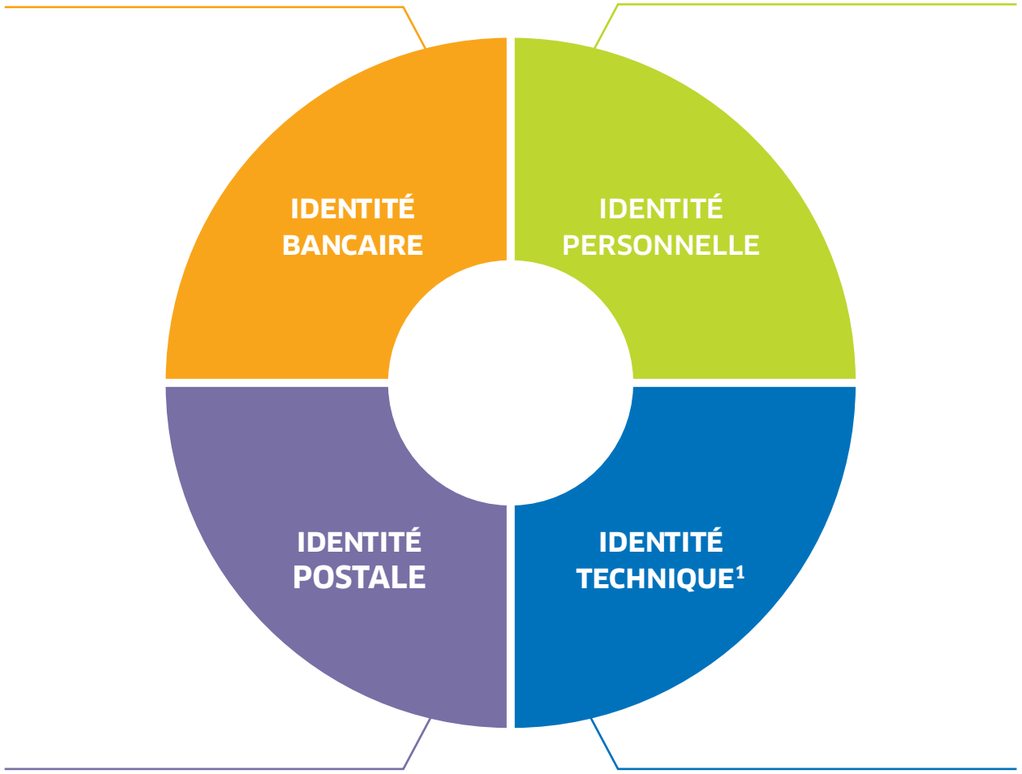
Les fraudeurs utilisent rarement l'intégralité d'une identité tierce. Ils assemblent les fragments de plusieurs identités afin d'en créer une nouvelle plus difficilement détectable. Seuls les fraudeurs professionnels ont la capacité de réunir et d'utiliser autant de ressources.

Une identité est composée de quatre parties distinctes et nécessaires à un achat en ligne : l'identité bancaire, l'identité personnelle, l'identité postale et l'identité technique. Les fraudeurs professionnels peuvent donc associer des éléments identitaires appartenant à quatre personnes différentes au maximum.

Pour l'ensemble des acteurs du e-commerce français, l'enjeu est d'avoir une vision globale de cette méthode de fraude et des risques liés afin de mutualiser les expertises et de contrer la fraude.

Il s'agit des coordonnées complètes d'un moyen de paiement. Celles d'une carte bancaire sont le type de carte (Visa, Mastercard, etc.), les nom et prénom du porteur, le numéro à 16 chiffres, la date d'expiration et le cryptogramme.

Il s'agit de l'ensemble des informations nominatives désignant une personne (nom, prénom) ainsi que ses coordonnées (téléphone et e-mail).



Il s'agit des coordonnées géographiques désignant l'adresse d'une personne physique ou morale.

Il s'agit du dispositif technique à travers lequel une commande est passée. Cela inclut le terminal de saisie ainsi que la nature et l'origine de la connexion Internet établie avec le site marchand.

1- Notion distincte de l'identité numérique (voir glossaire).

De façon à dissimuler l'utilisation frauduleuse d'un ou plusieurs éléments identitaires, les fraudeurs professionnels peuvent mettre en œuvre quatre mécanismes :

• **la falsification** est le fait de se servir d'une identité inexistante mais qui a tous les attributs et caractéristiques d'une identité réelle.
Exemple : réceptionner une commande frauduleuse à une adresse de livraison inexistante, par le biais de l'ajout d'un numéro supplémentaire dans une rue, pour récupérer des colis avec la complicité du livreur.

• **l'usurpation** est le fait d'utiliser l'identité d'une autre personne à son insu et sans son accord.
Exemple : payer une commande avec une carte bancaire volée.

• **l'anonymisation** est le fait d'employer une identité qui ne peut être associée directement ou nominativement à une personne précise.
Exemples : utiliser une adresse de livraison en point relais (anonymisation de l'identité postale), passer une commande via un cybercafé ou une borne en magasin (anonymisation de l'identité technique).

• **la compromission** est le fait d'utiliser l'identité d'une autre personne qui l'a communiquée de bonne foi mais sans compréhension de la finalité frauduleuse.
Exemple : profiter d'une mule en lui faisant signer un faux contrat de travail. Elle compromet volontairement son identité postale et personnelle, sans savoir qu'elle devient la victime d'un fraudeur.
Le rôle des systèmes de lutte contre la fraude n'est jamais d'évaluer une personne mais uniquement d'évaluer si l'un ou plusieurs des éléments renseignés lors d'une commande en ligne font l'objet d'une utilisation frauduleuse ou non.

Ainsi, savoir évaluer le risque lié à chaque type de fraude identitaire, en tenant compte des impacts sur la relation client, est un des nouveaux défis de la lutte contre la fraude dans le e-commerce.

B. Placer la lutte contre la fraude au cœur de la relation client

Réduire la fraude dans le e-commerce nécessite d'assimiler ces nouveaux paramètres. En revanche, l'optimisation de la lutte contre la fraude ne doit pas se faire au détriment de la majorité des clients honnêtes. Dans cette optique, il est essentiel pour les e-commerçants de créer un équilibre entre leur stratégie de lutte contre la fraude et de relation client.

Aujourd'hui, les divers niveaux de contrôle appliqués par les acteurs du e-commerce afin de se prémunir contre les impayés ont des conséquences plus ou moins importantes sur l'expérience d'achat.

Un contrôle strict mais efficace contre les fraudeurs peut être pénible pour les clients honnêtes obligés de se justifier sans raison apparente. Pour les e-commerçants, l'objectif d'une lutte moderne contre la fraude est de distinguer les deux populations, fraudeurs et clients honnêtes, pour maîtriser les impayés tout en transformant un maximum d'opportunités de ventes. L'évaluation de la performance d'un dispositif anti-fraude se mesure à l'aune de sa capacité à préserver la relation client.

La stratégie de lutte contre la fraude d'un e-commerçant doit être pilotée conjointement avec les autres services clés de l'entreprise : les directions financière, marketing, commerciale et client. Un pilotage et un arbitrage collectifs permettront d'ajuster au mieux les actions de chacun de ces services pour établir une harmonie entre croissance des ventes et maîtrise du risque.

Afin de préserver la relation client, les e-commerçants pourront choisir les types de contrôles à effectuer et le meilleur moment pour le faire. En effet, il faut désormais tendre vers une répartition des contrôles tout au long du parcours d'achat plutôt que d'appliquer un verrou unique au moment du paiement. Par exemple, une vérification de l'identité personnelle et technique à l'instant où le client saisit son login permet d'évaluer l'authenticité de la personne qui se connecte à un compte client sans pour autant perturber la relation client. Cette stratégie de répartition doit être couplée à une information des particuliers sur l'utilité des contrôles. Mis au fait de leur importance pour leur propre sécurité, les consommateurs comprendront mieux ces contrôles et ceux-ci ne seront plus considérés comme pénibles. Des actions ponctuelles et pertinentes seront mieux perçues par les clients honnêtes et ne nuiront plus à la relation client.

Le défi relevé en associant relation client et lutte contre la fraude permettra d'être encore plus radical vis-à-vis des fraudeurs puisque les fausses alertes, générées par les clients honnêtes, seront écartées en amont.

CONCLUSION

Les résultats du Livre Blanc Certissim 2014 démontrent que la fraude opportuniste et la fraude professionnelle continuent à coexister. Néanmoins, la fraude professionnelle prédomine. Elle a des impacts de notoriété et financiers conséquents pour les e-commerçants lorsque le risque n'est pas correctement évalué. En effet, le volume des tentatives de fraude est généralement considérable et concentré dans un court laps de temps.

En outre, les e-commerçants ne sont plus les seuls à subir les conséquences de cette fraude, les particuliers en sont également de plus en plus victimes. En effet, si les mécanismes de vol des données bancaires sont désormais connus, le grand public ne mesure pas encore la forte probabilité de vol de l'ensemble des éléments d'identité, aux conséquences plus importantes. Or, les réseaux criminels comptent sur cette ignorance pour commettre leurs délits. Dans le but de récupérer un maximum de données, ils n'hésitent pas à construire des attaques de grande envergure, qu'il s'agisse de campagnes massives de phishings ou du piratage de bases de données.

Cependant, les e-commerçants et les acteurs du secteur ne sont pas démunis face à la fraude. La mutualisation des données, l'amélioration constante des systèmes, la mise en place d'arbitrages pertinents ainsi qu'une collaboration avec les autorités permettent de la maîtriser. De plus, certains acteurs sont en mesure de leur apporter des conseils afin de mettre en place des bonnes pratiques. Désormais, l'efficacité d'une lutte moderne contre la fraude passe par une intégration au sein de la stratégie de relation client de chaque site marchand et doit comprendre des actions de prévention auprès du grand public ■

Glossaire

A.N.R.

L'Authentification Non Rejouable est un dispositif de sécurisation des paiements en ligne. Dans le cadre d'un paiement à distance, il permet de s'assurer que l'auteur du paiement et le détenteur de la carte bancaire correspondent. La méthode la plus courante est la saisie d'un code à usage unique envoyé par SMS sur téléphone mobile, par l'établissement bancaire du détenteur de la carte.

Carding

Terme désignant les différentes méthodes de piratage des cartes bancaires.

Carte bancaire

Moyen de paiement délivré par un établissement de paiement, de crédit ou de monnaie électronique comportant, le plus souvent, une puce électronique et une piste magnétique permettant d'effectuer des retraits dans les distributeurs de billets et/ou des paiements auprès des commerçants de proximité et sur Internet.

C.N.I.L.

Créée en 1978, la Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante chargée de veiller à ce que l'informatique ne porte pas atteinte aux libertés, aux droits, à l'identité humaine ou à la vie privée.

Données personnelles

Attributs propres à une personne permettant de l'identifier directement ou indirectement (nom, prénom, adresse e-mail, numéro de téléphone, date de naissance, etc.)

Effet casino

Propension des fraudeurs professionnels à réitérer une fraude réussie. Ce mécanisme est généralement répété sur plusieurs sites marchands.

Fraude

Acte réalisé en utilisant des moyens déloyaux destinés à obtenir un avantage matériel ou moral indu ou réalisé, en contravention avec la loi.

Fraude identitaire

Utilisation des coordonnées d'un individu à des fins malveillantes. On peut citer par exemple, le fait d'utiliser les coordonnées d'une personne afin d'en tirer un bénéfice commercial, économique ou monétaire, de se procurer des produits, de l'information ou d'accéder à des installations ou à des services.

Fraude de proximité

Acte de fraude ayant lieu dans le cercle familial ou professionnel.

Hacking

Voir *Piratage informatique*

Impayé

Facture non honorée à l'échéance par l'acheteur.

Impayé frauduleux

Facture non honorée à la suite du signalement, par l'utilisateur du service de paiement à son prestataire de services de paiement, d'une opération de paiement non autorisée.

Phishing

Technique de fraude consistant à imiter les e-mails de tiers de confiance – institutions officielles, entreprises – dans le but d'obtenir des renseignements personnels, des informations d'accès à des comptes clients ou des coordonnées bancaires.

Piratage informatique

Utilisation de compétences informatiques pour exploiter les failles et vulnérabilités d'un système informatique, de façon à en tirer un bénéfice financier ou pour nuire à des individus ou organisations.

Point de compromission

Endroit où des données bancaires ont été volées, identifié par les autorités par recoupement entre les fichiers d'utilisation des cartes bancaires et les recoupements de plaintes de plusieurs victimes de vol.

Skimming

Activité frauduleuse consistant à pirater des cartes bancaires, notamment depuis les distributeurs automatiques de billets. Les cartes sont ensuite dupliquées ou « clonées ».

Spoofing

Technique d'usurpation d'identité utilisée par des fraudeurs pour maquiller leurs coordonnées (e-mail ou téléphonique) réelles.

Chiffres

Livre Blanc Certissim

Depuis 2000, le Livre Blanc Certissim apporte une vision objective de la fraude sur le marché du e-commerce français. Document de référence pour les e-marchands souhaitant optimiser leur gestion de la fraude, le Livre Blanc Certissim présente les grands indicateurs de la fraude dans le e-commerce ainsi que les nouveaux enjeux de la lutte contre la fraude. L'expertise de Certissim et son implication dans la lutte contre la fraude lui permettent également de décrire les nouvelles techniques des cybercriminels.

Les données du Livre Blanc Certissim proviennent des fraudes détectées par son système ainsi que des déclarations d'incidents de paiement de ses 900 sites marchands partenaires.

FIA-NET

FIA-NET, filiale de FIA-NET Europe, est le leader français des solutions de confiance et de lutte contre la fraude dans le e-commerce. La société propose des services dédiés aux sites marchands et aux e-consommateurs. Les solutions Certissim et Sceau de Confiance FIA-NET apportent aux e-marchands et aux e-acheteurs la confiance nécessaire au développement du e-commerce.
Créée en 2000, FIA-NET compte aujourd'hui près de 250 collaborateurs et 1 700 sites marchands clients.

CONTACT

FIA-NET
39 rue Saint-Lazare - 75009 Paris
Tél : **+33 (0)1 45 23 73 73**
Fax : **+ 33 (0)1 45 23 05 96**
RCS Paris 429 121 866

POUR PLUS D'INFORMATIONS

www.fia-net-group.com
www.certissim.com

FIA-NET e-solutions