La fraude dans le e-commerce

Nadia ANTONIN, animatrice du groupe de travail « Commerce électronique » de l'Académie des Sciences commerciales

Avril 2017

En France, le commerce électronique connaît un essor rapide. Ainsi, le chiffre d'affaires du commerce électronique a progressé de 14,6 % entre 2015 et 2016 pour atteindre 72 milliards d'euros en 2016 selon les sources de la Fédération du e-commerce et de la vente à distance (FEVAD). Cela représente 33 transactions par seconde. Par ailleurs, le nombre de sites marchands actifs progresse de 12% sur un an. On estime désormais à plus de 200 000 le nombre de sites marchands en France. En dix ans, le nombre de sites a été multiplié par 10. Enfin, en 2017, la FEVAD prévoit que le commerce électronique français atteindra 80 milliards d'euros de chiffre d'affaires, grâce à une croissance supérieure à 11 %.

Mais malheureusement, en même temps que les ventes en ligne se développent, la fraude augmente de la même façon car le commerce électronique constitue entre autres une source de biens attrayante pour les fraudeurs. Ainsi, d'après une étude menée par PYMNTS.com et Forter la fraude a augmenté de 163 % en 2015. En outre, un livre blanc intitulé « *la fraude dans le e-commerce* » de Certissim publié en juin 2014 révèle que 3 % des transactions en ligne sont frauduleuses.

La fraude dans le commerce électronique peut prendre plusieurs formes.

1. Typologie des fraudes dans le e-commerce

On peut répartir les types de fraude en deux catégories : la fraude opportuniste et la fraude professionnelle

A. La fraude opportuniste

La fraude opportuniste est le fait de personnes qui saisissent l'occasion d'effectuer des achats frauduleux pour leur propre compte ou celui de leur entourage. Elle permet de réaliser des économies mais pas de profit. On peut citer comme exemple de fraude opportuniste l'utilisation de cartes bancaires de son entourage ou « trouvées » pour acheter en ligne.

Ce type de fraude ne représente qu'une faible part du panier des fraudeurs, comparée à la fraude professionnelle ou organisée.

B. La fraude organisée

La fraude organisée également appelée « fraude professionnelle » ou « fraude industrielle » représente, en valeur, la majeure partie des fraudes dont les commerçants en ligne sont victimes. Parmi la fraude organisée, on observe notamment la fraude à la mule et le détournement de compte client.

- **La fraude à la mule**

Dans le cadre du e-commerce, la fraude à la mule est la manipulation d'une personne honnête dans le but de masquer une opération frauduleuse pour le compte d'un vrai fraudeur. En d'autres termes, le véritable fraudeur va utiliser des cyber-acheteurs comme intermédiaires ou « mules » pour acheter des colis et commettre ainsi la fraude. A cet égard, on peut citer :

- ***La mule au contrat 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 ». Dans le cadre de la signature de son "contrat de travail", la victime de l'escroquerie fournit les documents standards nécessaires (photocopie carte d'identité, RIB, justificatif de domicile) qui vont servir au réseau de fraudeurs pour passer des commandes frauduleuses avec des cartes bancaires volées ou des chèques falsifiés. Les escrocs se servent de l'adresse de la victime pour cacher leur identité lors des commandes et pour ne pas être détectés par les systèmes anti-fraude des sites marchands. La victime devient alors 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. Lorsque les vendeurs se rendent compte qu'ils ne seront pas payés, ils se retournent vers les victimes de l'escroquerie grâce aux coordonnées que leur ont communiquées les fraudeurs.
- ***La mule familière*** : 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.
- ***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).

- **Le détournement de compte client**

Désormais, les auteurs d'hameçonnage ou « *phishing* » ne se contentent plus de se procurer des coordonnées bancaires. Ils cherchent à collecter tous types de données personnelles comme l'état civil, les coordonnées postales, les mots de passe, etc. afin d'utiliser une identité crédible pour commander en ligne.

Outre cette typologie, d'aucuns opèrent une distinction en fonction de la valeur des marchandises fraudés.

- ***La valeur vénale*** pour les produits haut de gamme. Dans ce cas de figure, le fraudeur souhaite acquérir un bien d'une gamme supérieure à celui qu'il pourrait s'acheter.

- ***La valeur sociale*** concernant les produits à la mode.

- ***La valeur vitale*** pour les produits bon marché destinés à satisfaire les besoins primaires et vitaux comme se nourrir ou s'habiller.

2. <u>Comment lutter contre les conséquences néfastes de la fraude pour les commerçants en ligne et les particuliers ?</u>

A. Les conséquences de la fraude pour les commerçants en ligne et les particuliers

- Pour le **commerçant en ligne**, une des conséquences néfastes de ce phénomène concerne le coût financier de la fraude : perte financière pesant fortement sur les

bénéfices, procédures judiciaires entamées par les parties lésées, etc. A ce coût financier, s'ajoutent le coût de la lutte contre la fraude ainsi qu'une atteinte à son image (préjudice d'image) et à sa réputation qui se concrétise notamment par une perte de confiance des clients.

- Le **particulier** quant à lui est victime de l'usurpation de ses données personnelles avec tous les désagréments que cela entraîne.

B. La lutte contre la fraude dans le commerce électronique

Pour les e-commerçants et les professionnels du paiement, la lutte contre la fraude sur la vente en ligne est un combat permanent dans lequel le risque zéro n'existe pas.

Qu'en est-il des dispositifs tels que 3D-Secure et les outils d'analyse du risque pour faire baisser le taux de fraude sur la vente en ligne ?

- **Le système 3D-Secure**

Créé par Visa et MasterCard et instauré depuis 2008 en France, le système 3D-Secure concerne les paiements en ligne. Il vise à sécuriser les transactions effectuées par carte bancaire sur un site e-commerce ou boutique en ligne.

Pour les commerçants, le système 3D-Secure a pour objectif de réduire le risque de paiements frauduleux et donc le montant des impayés.

Pour les particuliers, ce système apporte une protection renforcée contre l'usage frauduleux des cartes bancaires.

- **L'analyse des données, un outil stratégique pour détecter les profils des fraudeurs**

« *L'analyse des données permet de détecter des fraudes dans les ventes à* distance »
(Marie-Claude Santon - SAS)

Grâce aux Big Data et aux analyses de données, les sites de vente en ligne peuvent diminuer les risques de fraude en contrôlant plus d'informations en quasi temps réel. Pour illustrer cette affirmation, on peut prendre l'exemple du « *data mining* ».

Le « *data mining* », ensemble de méthodes scientifiques destinées à l'exploration et l'analyse de bases de données informatiques, va servir à identifier et à prédire dans ces données des profils-types, des comportements « suspects » comme ceux de mauvais payeurs ou d'acheteurs par exemple.

De même, l'intelligence artificielle, une des innovations majeures de ces dernières années, prend tout son sens avec les mégadonnées (« *Big data* ») et détient une part déterminante dans tous les domaines tels que le e-commerce. Au-delà du marketing prédictif, l'intelligence artificielle offre des nouvelles perspectives aux acteurs du Web et ses applications dans le e-commerce concerne entre autres la détection de la fraude.

3. <u>Conclusion</u>

Face aux attaques des fraudeurs de plus en plus sophistiquées et conséquentes et à une hausse massive de la fraude, on observe quelque peu un manque de sensibilisation de la part des sites

de commerce électronique concernant les risques encourus. Si ces sites ne déploient pas des technologies plus adéquates pour contrer la fraude en ligne et n'accordent pas plus d'attention à la sécurité des transactions, ils risquent de perdre la guerre contre la fraude et, donc, d'accroître les pertes financières d'une part et de compromettre la confiance et la fidélité de leurs clients d'autre part.

La nécessité de lutter contre la fraude est d'autant plus impérative que l'on risque d'assister à une migration du risque de fraude du e-commerce vers le m-commerce qui est un marché relativement nouveau avec un potentiel de développement important mais qui est également une cible de choix pour les fraudeurs. A cet égard, le cabinet d'études Gartner prévient que le succès du commerce via un mobile dépend étroitement des moyens mis en œuvre pour prévenir les risques de fraude. Dès lors, eu égard à la forte croissance des appareils mobiles, à la progression du commerce mobile et à la migration du risque de fraude vers ces appareils, l'utilisation d'outils de détection de la fraude dans des environnements mobiles est indispensable.