



### Une crise de défiance semble s'installer sur Internet. Comment rassurer les internautes et les commerçants ?

Attention, avec 45 milliards de chiffre d'affaires prévisionnel en 2013 et 31 millions de cyberacheteurs, le commerce en ligne prend une importance non négligeable. La satisfaction est au rendez-vous, les commandes sont traitées dans les temps et les produits bien réceptionnés. En revanche, le risque de fraude sur les moyens de paiement est réel. Or, d'un côté les e-commerçants souhaitent être payés et de l'autre, les internautes craignent de subir des fraudes.

### Quels dispositifs de paiement privilégier ?

Plusieurs solutions existent pour régler un achat : carte bancaire, virement, chèque, mandat cash, portefeuille virtuel, etc. L'internaute doit utiliser un moyen de paiement avec lequel il prend le moins de risque

## « Pour un recouvrement responsable »

**Dominique Viejo**, directeur général France d'**Alektum**

possible. Le moyen de paiement le plus utilisé étant la carte bancaire (80 %), privilégier les systèmes 3DSecure est une bonne stratégie car ils permettent de vérifier que l'internaute est bien le détenteur de la carte. Pour autant, cela ne règle pas le problème dans son ensemble. Que proposer aux clients qui ne détiennent pas de carte bancaire ou qui craignent de l'utiliser pour des achats en ligne ? Des solutions alternatives existent. Des portefeuilles en ligne (ou wallets), comme Paypal ou tout nouvellement Paylib, proposent des services sécurisés avec un degré d'authentification forte. Ces offres sont déclinées également via des applications mobiles afin de favoriser le m-commerce qui représente déjà un milliard d'euros de chiffre d'affaires.

Les e-marchands tentent, eux aussi, de limiter le risque. Ils disposent de 3DSecure pour sécuriser les paiements, mais cette solution trouve ses limites pour les règlements en plusieurs fois. Par ailleurs, les e-commerçants peuvent opter pour des prestataires ou des organismes bancaires qui garantissent le paiement. Toutes ces solutions représentent un coût non négligeable ; le choix dépend donc de l'activité et des modalités de paiement qu'elle nécessite.

### Comment se positionne Alektum sur son marché ?

Dans le secteur de l'e-commerce, le panier moyen est faible. La loi française ne prévoit pas de solution rapide et peu onéreuse pour permettre aux commerçants de récupérer les impayés. Alektum se positionne comme un partenaire des e-commerçants avec des services qui s'inscrivent dans le prolongement des missions du service client. Nos prestations de recouvrement responsable privilégient les solutions amiables et l'auto-résolution afin de pérenniser la relation client. Innovants, nos outils sont adaptés au traitement de très gros volumes.

En 2013, grâce à notre partenaire Buyster, nous avons ajouté une solution nouvelle via le mobile pour le paiement des dettes. Et nous nous apprêtons à proposer une solution de prélèvement automatique avec l'offre Sepalia de Docapost (filiale de La Poste) afin de gérer plus efficacement les échéanciers. Enfin, Alektum devrait intégrer la Fédération nationale de l'information d'entreprise et de la gestion de créances (Figec). Ce syndicat demande à ses adhérents de suivre une certaine déontologie et s'efforce de faire reconnaître le métier du recouvrement comme une action d'ordre publique.

prévenir les risques d'utilisation malveillante. Experian s'adresse aux banques, aux établissements financiers, aux compagnies d'assurance et aux e-commerçants qui peuvent ainsi compléter leurs offres de service de manière innovante pour rassurer leurs clients. La solution observe consciencieusement le Web, les réseaux sociaux et les flux de données pour détecter immédiatement la perte, le vol ou la révélation accidentelle d'informations personnelles. Pour chacun de ses abonnés, DataPatrol surveille notamment :

- **Informations personnelles** : nom, pseudonyme utilisateur, permis de conduire, numéro de passeport, numéro de carte d'identité.

- **Informations financières** : numéros de comptes, cartes de crédit.

- **Informations de contact** : adresse postale, e-mail, numéro de téléphone, carnet d'adresse électronique.

- **Autres données** : photos, e-mails, autres contenus du téléphone.

Si DataPatrol découvre une information personnelle d'un utilisateur, un e-mail ou un SMS lui est envoyé directement. Un service client dédié fournit une aide et des conseils adaptés pour faire face à la situation.