THE TURNING POINT*

OPTIMISER LA VALIDATION MAXIMISER LE PROFIT

*LE VIRAGE

Rapport 2013 sur la Fraude E-commerce en France

CyberSource®
the power of payment

DANS CE RAPPORT

Avec la participation de Acsel L'ASSOCIATION DE L'ÉCONOMIE NUMÉRIQUE

INTRODUCTION

Le e-commerce représente des opportunités considérables pour les entreprises françaises. Le marché intérieur du e-commerce enregistre une croissance annuelle [i] de 20 pour cent, huit utilisateurs d'Internet sur dix effectuant désormais des achats en ligne [ii]. En outre, les ventes en ligne internationales sont en plein essor (en Europe, les ventes sur Internet ont généré un chiffre d'affaires de 300 milliards d'Euros [iii] en 2012), les nouveaux terminaux connectés à Internet comme les smartphones et les tablettes donnant accès à de nouveaux canaux de vente. Selon comScore, en décembre 2012, 9,2 % des possesseurs français de smartphones ont utilisé leur téléphone pour acheter un produit ou un service, et ce chiffre augmente régulièrement [iv].

Mais cette opportunité n'est pas dénuée de risque. Pour les e-commerçants, le risque majeur est celui de la fraude.

En France, le taux de fraudes en ligne augmente régulièrement depuis 2007 et a enregistré une hausse de 20 % en 2011 [v], les fraudeurs ayant recours à des techniques de plus en plus sophistiquées, qui rendent leurs transactions plus « propres » et, par conséquent, plus difficiles à détecter.

Pour étudier les moyens dont disposent les e-commerçants français pour mieux traiter le problème de la fraude, CyberSource a analysé les réponses du panel ACSEL sur la fraude en ligne, constitué notamment de quelques-uns des principaux acteurs français, afin de recueillir leurs opinions concernant les principales pratiques de suivi et de contrôle de la fraude.

Le panel ACSEL de la fraude en ligne représente plus du tiers du marché du commerce en ligne français, la moitié d'entre eux générant un chiffre d'affaires annuel de plus de 100 millions d'euros ; les deux tiers sont présents à l'échelle internationale.

L'objectif consistait à comprendre les actions à mener pour aider les sites marchands français à mieux se protéger eux-mêmes ainsi que leurs clients honnêtes contre la fraude tout en les aidant à accepter plus de commandes provenant d'un plus grand nombre de clients, de marchés et de canaux de vente.

Selon les résultats de notre étude, certaines entreprises n'ont pas encore mis en place des mesures de contrôle et de gestion visant à appréhender et traiter globalement l'impact de la fraude. Nous formulons donc des recommandations clés ainsi que des conseils pratiques visant à aider les sites marchands à relever ce défi.

Nous tenons à remercier tout particulièrement l'équipe de l'ACSEL pour son implication et tous les e-commerçants interrogés pour le temps qu'ils ont consacré à l'étude et pour les observations et commentaires dont ils ont fait part.

Patrick Flamant

Directeur France, CyberSource

Consultez et téléchargez ce rapport à l'adresse www.cybersource.com/levirage

Source : [i] Croissance du commerce en ligne B2C, ACSEL, 2011 [ii] ComScore, Le marché du digital en France, mars 2013 [iii] EMOTA 2012 [iv] ComScore, Le marché du digital en France, mars 2013 [v] Selon l'Observatoire français de la sécurité des cartes de paiement, le niveau de fraude a atteint 0,34 % en 2011, en hausse de 20 % par rapport à 2010 [vi] Rapport CyberSource 2013 sur la Fraude e-commerce au Royaume Uni [vii] Rapports CyberSource 2013 sur la Fraude e-commerce aux États-Unis et au Royaume-Unis

01 | LE E-COMMERCE AUJOURD'HUI

EN TOILE DE FOND : LE PROFIL DES RÉPONDANTS

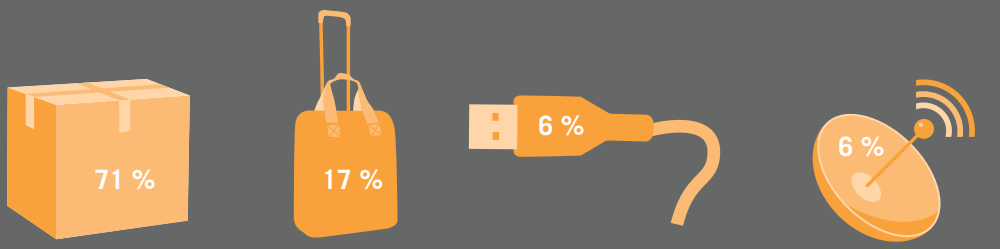
Les e-commerçants qui ont participé à notre enquête comprennent certaines des plus grandes enseignes du e-commerce français. Près de 80 % d'entre elles se consacrent au commerce en ligne depuis plus de cinq ans, 17 % d'entre elles ont entre deux et cinq ans de présence dans ce domaine. Toutes les personnes interrogées sont concernées par la lutte contre la fraude.

La moitié des e-commerçants interrogés ont enregistré, avec leurs activités en ligne, un chiffre d'affaires supérieur à 100 millions d'euros. En moyenne, les sites consultés ont généré un chiffre d'affaires annuel d'au moins 120 millions d'euros. Nous estimons que le panel de sites interrogés représente:

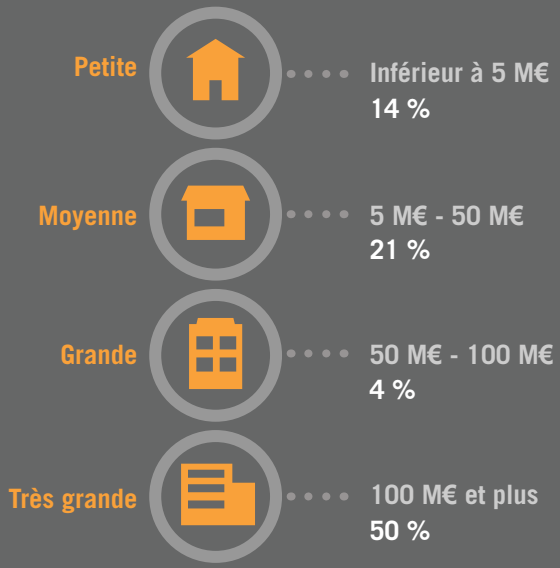
- Plus de 35 % du marché du e-commerce français en termes de volume de transactions en ligne
- Plus de 32 % du marché du e-commerce français en valeur

Rapport basée sur 48 répondants.

Répondant par secteur d'activité :



Taille des entreprises en fonction du chiffre d'affaires e-commerce

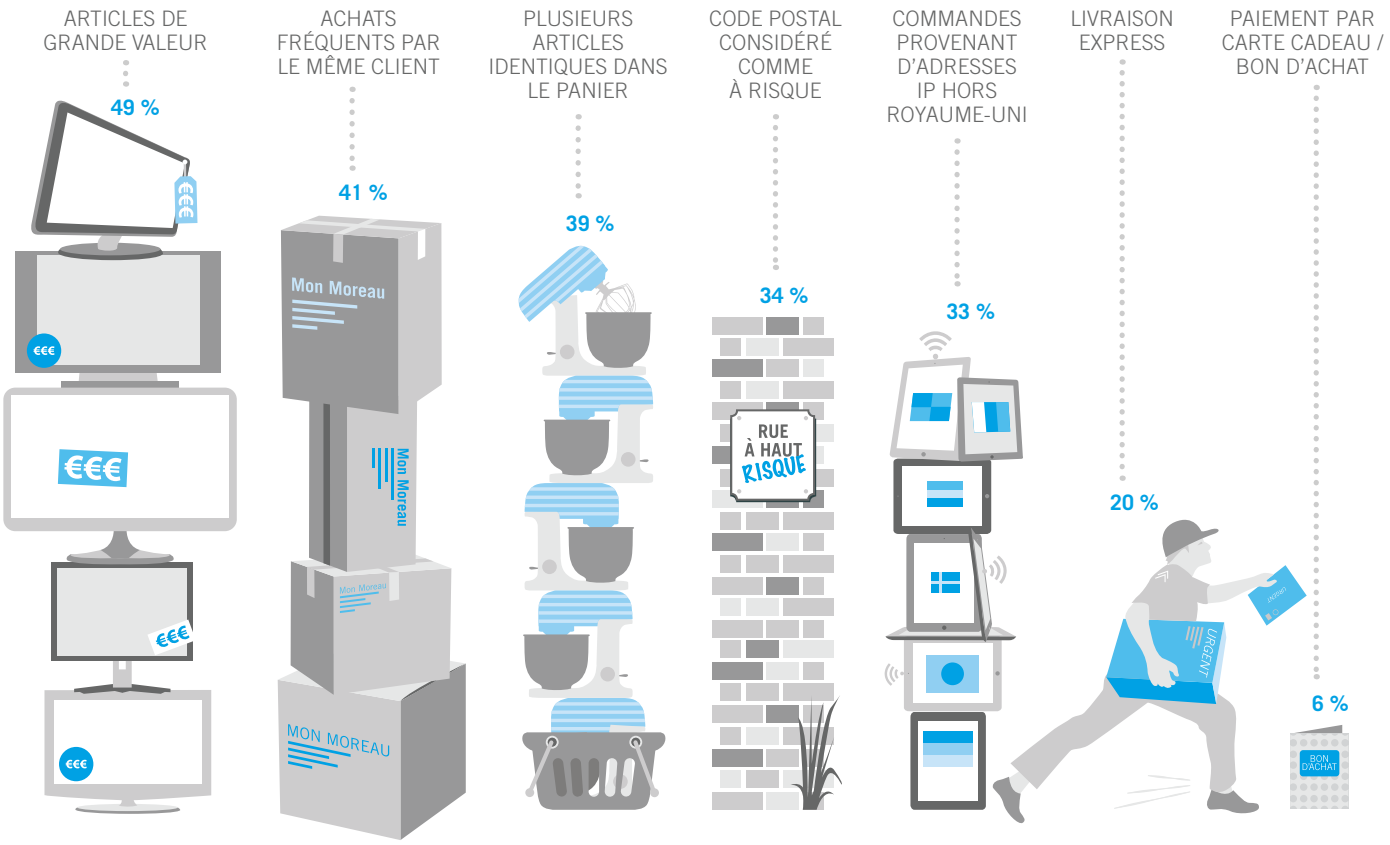


02 | PRINCIPES FONDAMENTAUX DE LA FRAUDE

EXEMPLES DE FRAUDES EN LIGNE

Face à l'émergence de techniques de fraude de plus en plus sophistiquées, les e-commerçants utilisent des outils plus perfectionnés pour déterminer le profil des comportements à risque élevé. Les indicateurs pertinents d'un comportement potentiellement frauduleux sont notamment les suivants [vi].

Graphique 1 :
INDICATEURS LES PLUS COURANTS DE TRANSACTIONS À HAUT RISQUE



Source : Rapport 2013 sur la fraude en ligne au Royaume-Uni
Légendes : articles de grande valeur, achats fréquents par le même client, grand nombre d'articles identiques dans le même panier, code postal considéré comme à risque, commandes provenant d'adresses IP hors Royaume-Uni, livraison express, paiement par carte cadeau ou bon d'achat.

L'étude réalisée par CyberSource [vii] révèle que LES RISQUES DE FRAUDE MAJEURS MENAÇANT LES SITES DE COMMERCE EN LIGNE SONT LES SUIVANTS

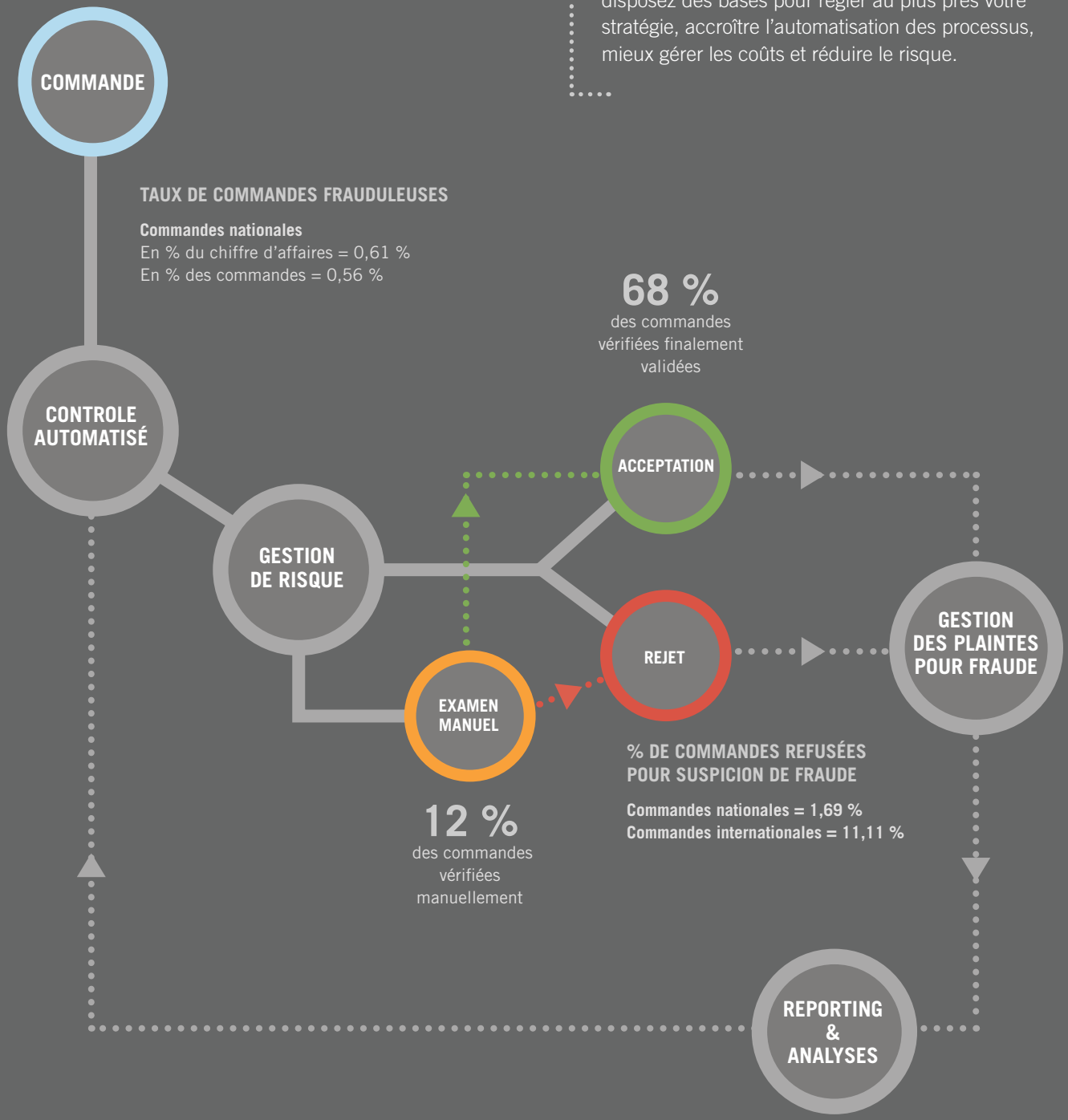
FRAUDE « PROPRE » ET FRAUDE AMICALE La fraude « propre » représente une menace croissante. Elle implique des fraudeurs aux méthodes de plus en plus sophistiquées qui fournissent des données de transaction correctes et complètes, difficiles à détecter. Le présent rapport revient plus en détail sur l'impact de la fraude « propre » dans les sections suivantes. La fraude amicale est une tendance observée parallèlement qui consiste pour le consommateur à effectuer un achat en ligne authentique avec sa carte de paiement puis à effectuer une répudiation auprès de la banque émettrice au motif qu'il n'a pas reçu les biens ou les services.

CYBER-ATTAQUES, NOTAMMENT PHISHING (HAMEÇONNAGE) ET PHARMING (DÉVOIEMENT) À DES FINS D'USURPATION D'IDENTITÉ le phishing implique l'envoi d'un message, généralement un courriel, à un utilisateur en se faisant passer pour une entreprise officielle en vue d'inciter l'utilisateur à fournir des informations personnelles qui seront utilisées à des fins d'usurpation d'identité. Le pharming exploite les vulnérabilités du système informatique hôte afin d'essayer de détourner le trafic du site internet d'une entreprise vers un faux site à l'apparence similaire, toujours à des fins d'usurpation d'identité.

Comment identifier les clients authentiques le plus tôt possible tout en maintenant le taux de fraude à un niveau acceptable ? Et comment maîtriser les dépenses induites ?

Les e-commerçants doivent envisager une solution de prévention des fraudes qui leur permette de mesurer et d'évaluer correctement les performances dans les principaux domaines de leur politique anti-fraude : détection automatique, vérification manuelle, gestion des commandes (acceptation/refus) et gestion des réclamations pour fraude.

Une fois en possession de ces données, vous disposez des bases pour régler au plus près votre stratégie, accroître l'automatisation des processus, mieux gérer les coûts et réduire le risque.



02.1 | PRINCIPES FONDAMENTAUX DE LA FRAUDE
DÉTECTION AUTOMATISÉE DE LA FRAUDE

LES SITES DE COMMERCE EN LIGNE UTILISENT EN MOYENNE CINQ OUTILS POUR LUTTER CONTRE LA FRAUDE.

De nombreux outils sont à la disposition des e-commerçants afin de les aider à repérer les fraudes éventuelles sur les commandes reçues. Les résultats obtenus par ces outils peuvent être ensuite interprétés par des systèmes automatisés à base de règles afin de déterminer si la transaction doit être acceptée, rejetée ou soumise à une vérification.

S'il est important d'adopter une approche équilibrée associant plusieurs outils de lutte contre la fraude, ces outils doivent fonctionner de concert. En outre, les e-commerçants ne doivent pas s'en remettre exclusivement aux méthodes traditionnelles pour combattre les techniques de fraude les plus récentes.

Le filtrage automatique des commandes doit exploiter les données propres à l'entreprise parallèlement aux outils tiers de prévention des fraudes (notamment la géolocalisation de l'adresse IP, les modèles de calcul de l'évaluation des fraudes, les données de plusieurs sites marchands, les vérifications de rapidité, etc.) ainsi qu'une variété de services de lutte anti-fraude proposés par les divers systèmes de paiement par carte (notamment le code/numéro de vérification de la carte, 3D Secure, etc.).

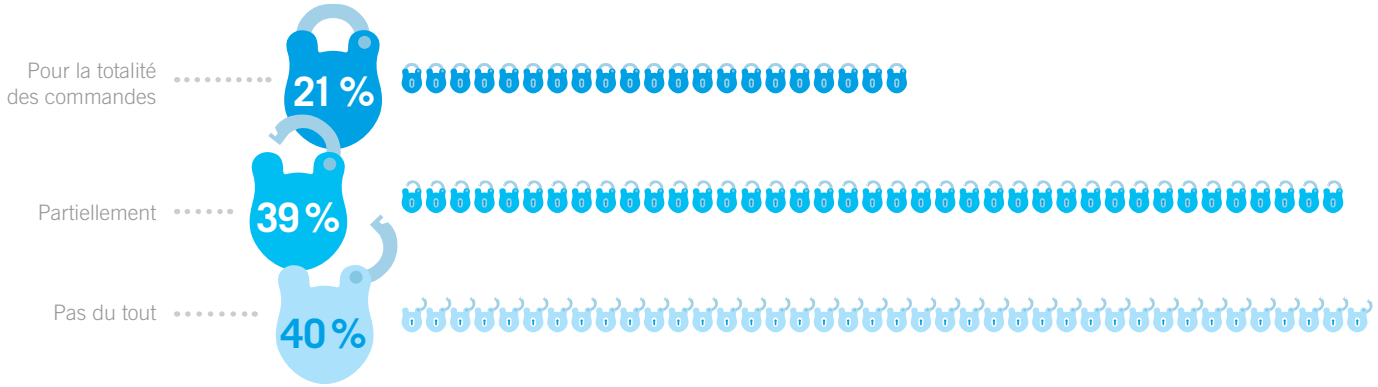
3D SECURE EN BREF

3D Secure (Verified by Visa, MasterCard SecureCode et AMEX SafeKey) offre un niveau de sécurité supplémentaire et contribue à réduire le risque de fraude en ligne. En adoptant le système 3D Secure, les e-commerçants peuvent bénéficier d'un transfert de responsabilité.

Parmi les entreprises participant à cette étude, 40 % n'utilisent pas le système 3D Secure, principalement parce qu'elles redoutent un taux élevé d'abandon de panier. Le niveau d'utilisation est beaucoup plus élevé au Royaume-Uni, même si cela tient au fait que 3D Secure est imposé par Maestro, un système de paiement largement utilisé. Cela dit, plus d'un cinquième des sites marchands français interrogés, notamment tous ceux dont le chiffre d'affaires en ligne atteint 100 millions d'euros, utilisent 3D Secure lors de chaque transaction.

La pertinence de 3D Secure est renforcé lorsqu'il est utilisé en association avec d'autres outils, et permet alors de minimiser l'impact des fraudes.

Graphique 2 :
ADOPTION DE 3D SECURE EN FRANCE



MESURES Á PRENDRE

DÉFENSE EN PROFONDEUR

- Les fraudeurs utilisent des méthodes plus sophistiquées : ne misez pas trop sur une stratégie ou sur une méthode anti-fraude spécifique. Vous devez en utiliser plusieurs pour détecter les menaces les plus récentes. L'utilisation d'outils de détection des fraudes plus sophistiqués combinée au système 3D Secure peut vous aider.
- Les sites marchands doivent tirer profit du système 3D Secure dans le cadre de leur stratégie globale de lutte contre la fraude afin de bénéficier du transfert de responsabilité.
- Demandez à votre fournisseur d'outils anti-fraude de vous expliquer comment utiliser ces outils intelligemment et veillez à ce qu'ils puissent fonctionner via une connexion unique pour le client. Des procédures de sécurité successives peuvent être néfastes pour l'expérience globale du client.

LA FRAUDE « PROPRE »

constitue la plus forte menace

Il y a quelques années, CyberSource a étudié l'impact de la fraude « propre », qui demeure un réel problème.

Nous constatons que les fraudeurs utilisent des méthodes toujours plus sophistiquées, et fournissent des informations de paiement en apparence complètes et correctes (autrement dit, les données semblent « plus propres »), ce qui complique le repérage de la fraude.

Selon les sites marchands concernés par les études réalisées en 2013 par CyberSource au Royaume-Uni et aux États-Unis, la menace de fraude « propre » représente la préoccupation majeure, avant l'usurpation d'identité, la fraude amicale, le phishing, les botnets et le pharming.

MESURES Á PRENDRE

ACCORDER LA PRIORITÉ À LA FRAUDE « PROPRE »

Le seul moyen pour s'attaquer réellement à la fraude « propre » et à la fraude amicale consiste à prendre en compte des facteurs autres que les données de paiement « classiques » et à utiliser des outils tels que l'enregistrement du compte, parallèlement à l'analyse historique et comportementale.

Nous recommandons la mise en œuvre de mesures supplémentaires permettant de mieux traiter les fraudes « propres », notamment :

- Utiliser les réseaux sociaux pour confirmer le lieu géographique d'un client, son activité au moment de passer la commande ou pour vérifier tout simplement qu'il existe.
- Vérifier l'ancienneté de l'adresse de courriel du client. Même si le nom se trouve dans l'adresse de courriel et semble authentique, si l'adresse n'a que quelques jours d'existence, elle n'a peut-être pas été créée par le titulaire de la carte.
- Procéder à une analyse régulière des données, pas uniquement à une vérification des remboursements : avez-vous constaté une augmentation du nombre de commandes adressées à un code postal donné au cours des derniers jours ou bien un intérêt accru, pouvant sembler inhabituel, pour un produit ou service spécifique ?

02.2 | PRINCIPES FONDAMENTAUX DE LA FRAUDE
CONTRÔLE MANUEL

NEUF SOCIÉTÉS SUR DIX

procèdent à un contrôle manuel des commandes, même si le nombre total de commandes contrôlées est faible

Selon notre enquête, 94 % des sites marchands français procèdent à une vérification manuelle des commandes traitées, contre 58 % au Royaume-Uni, même si le nombre global de commandes contrôlées est inférieur.

En France, le recours accru à la vérification manuelle est probablement dû à un plus grand nombre de sites interrogés spécialisés dans la vente de biens physiques. Le nombre de commandes vérifiées manuellement par entreprise est faible (les sites marchands français vérifient en moyenne une commande sur dix, taux qui ne dépasse pas 6,5 % pour les grands sites) à comparer au taux de vérification moyen de 25 % des sites marchands au Royaume-Uni. L'écart reflète probablement la taille de l'entreprise : les sites marchands les plus grands ont tendance à vérifier un nombre plus limité de commandes et le panel interrogé dans notre enquête comprenait un nombre élevé de gros sites marchands.

Il est important de souligner que plus d'un quart des sites interrogés n'a pas répondu à la question relative au taux de vérification manuelle, ce qui signifie peut-être que ce taux ne fait pas l'objet d'un suivi très étroit.

LES DEUX TIERS DES COMMANDES CONTRÔLÉES (68 %) SONT VALIDÉES

En règle générale, la moitié des commandes vérifiées devraient être acceptées. Des taux d'acceptation excessivement élevés ou faibles suggèrent que les procédures en place sont inefficaces et devraient être modifiées.

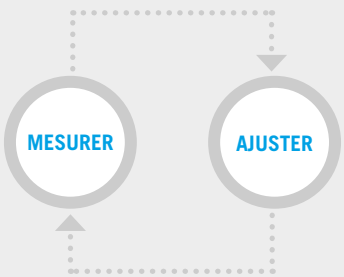
Pour les sites marchands français, le résultat est très proche de celui des entreprises basées au Royaume-Uni (71%). Ce taux élevé peut notamment s'expliquer pour les raisons suivantes :

1. Stratégies inadaptées en matière de détection automatisée des fraudes, qui impliquent un ajustement afin d'accepter un plus grand nombre de commandes « valides » plutôt que de les soumettre à un contrôle;
2. Prudence excessive des e-commerçants : certaines entreprises vérifient même les commandes légèrement suspectes, au risque de mécontenter le client en cas de rejet d'une commande authentique.

Encore une fois, un nombre relativement élevé de sites interrogés (42 %) ont indiqué qu'ils ne savaient pas combien de commandes vérifiées manuellement étaient finalement validées.

MESURES Á PRENDRE

MESURER ET OPTIMISER VOTRE CONTRÔLE



Les équipes de contrôle absorbent généralement la part la plus importante du budget consacré à la gestion de la fraude ; le contrôle et l'amélioration de leurs performances sont donc décisifs. Nous recommandons d'identifier des indicateurs de performance clés, puis d'optimiser les processus de vérification :

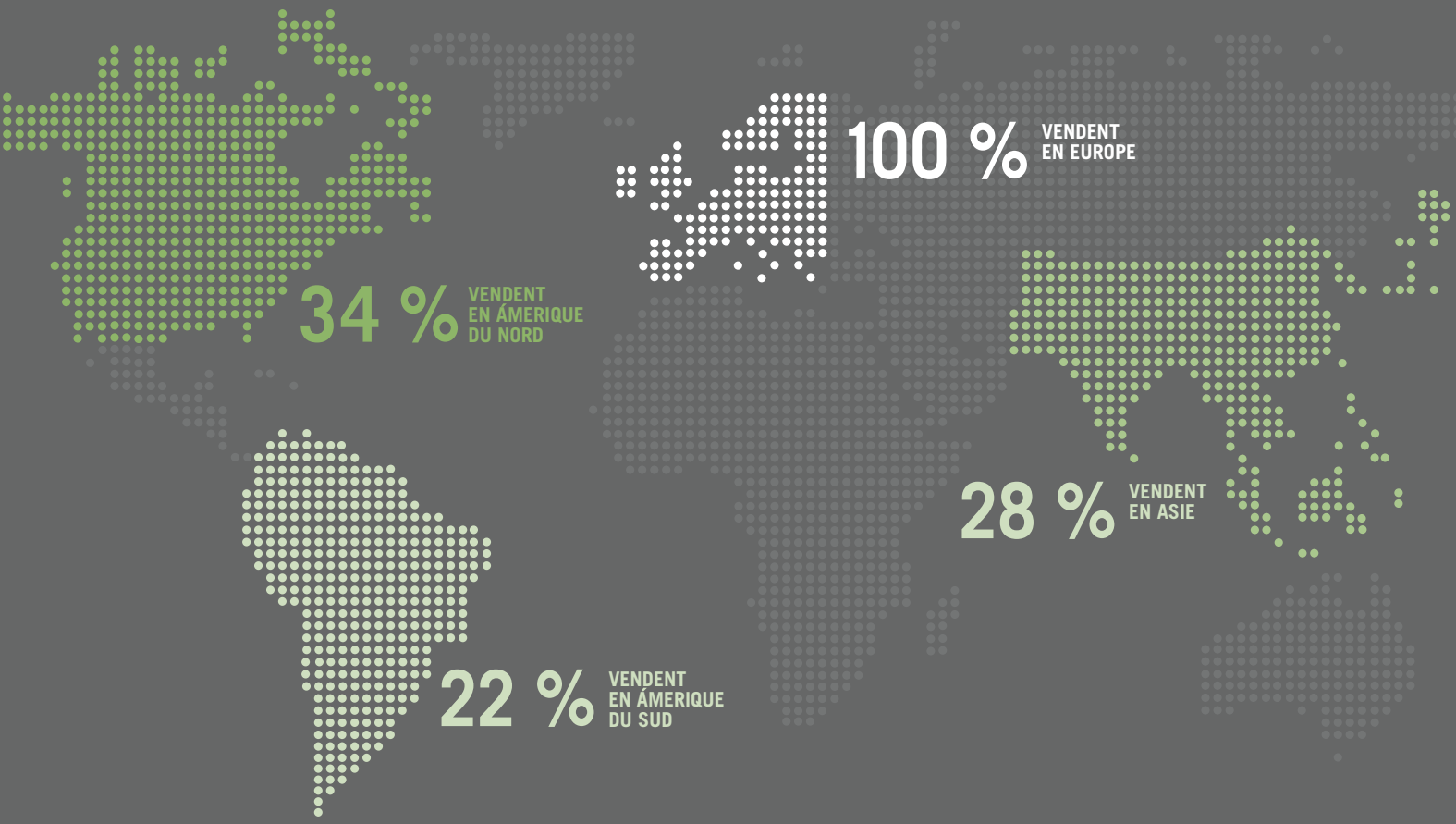
1. Trouvez un juste équilibre entre l'efficience et l'efficacité. Les paramètres à mesurer par vérificateur et de manière générale comprennent:
   - Les impayés
   - La durée des contrôles
   - Le nombre de transactions contrôlées
2. Utilisez un système de gestion des cas de fraude pour mettre en place une vérification plus structurée et collecter des indicateurs clés de performance. Mesurez et évaluez les résultats par rapport aux indicateurs clés de performance en matière de gestion de la fraude pendant une durée déterminée afin de définir des tendances et des points à améliorer.
3. Veillez à ce que vos équipes de gestion de la fraude échangent régulièrement leurs connaissances relatives aux dernières tendances et comprennent quelles sources d'informations/bases de données de validation sont les mieux adaptées aux différents marchés.

03 | L'OPPORTUNITÉ INTERNATIONALE

Étant donné le nombre élevé de grandes entreprises participant à notre étude, il n'est guère surprenant que plus des deux tiers des e-commerçants français concernés vendent à l'étranger.

Parmi les sites qui vendent hors de France :

Graphique 3:
L'OPPORTUNITÉ INTERNATIONALE



Le développement international représente une réelle opportunité de croissance pour les sites marchands français. A condition d'établir un climat de confiance, les pays BRIC offrent de réelles opportunités. L'indice du e-commerce A.T. Kearny pour 2012 a placé la Chine, le Brésil et la Russie en tête des marchés émergents qui offrent le potentiel de e-commerce le plus élevé aux sites marchands désireux de développer leurs activités.

Graphique 4

Cela pose toutefois un certain nombre de difficultés.
Selon notre étude :

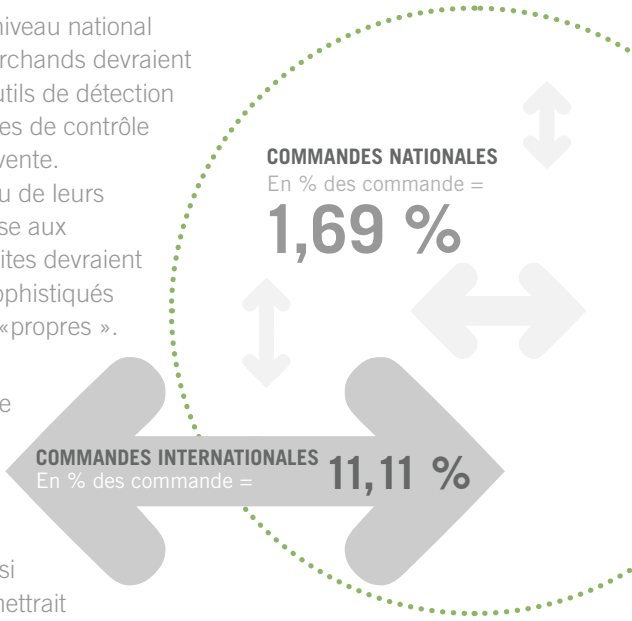
1. LES TAUX DE COMMANDES FRAUDULEUSES DES SITES MARCHANDS SONT EN GENERAL PLUS ÉLEVÉS EN CAS DE TRANSACTIONS TRANSFRONTALIÈRES

(Graphique 4)

En raison d'un échantillon limité, le taux de fraude sur les commandes internationales s'est révélé incohérent par rapport aux autres études. Le taux élevé de rejet des commandes internationales tend à soutenir l'hypothèse d'une prudence excessive des e-commerçants français.

Selon le rapport sur la fraude aux États-Unis réalisé par CyberSource en 2013, les sites marchands acceptant des commandes internationales ont fait état d'un taux de fraude deux fois plus élevé pour les commandes hors États-Unis. Les sites marchands qui vendent à l'étranger éprouvent plus de difficultés à distinguer les commandes authentiques de celles qui ne le sont pas. Il leur manque peut-être les données internationales ou les connaissances locales nécessaires à l'acceptation ou au rejet des commandes internationales.

La différence entre les taux de fraude au niveau national et international démontre que les sites marchands devraient pouvoir optimiser les capacités de leurs outils de détection automatisée des fraudes et de leurs équipes de contrôle pour chaque marché et chaque canal de vente. Garantissant ainsi une évolution en continu de leurs règles et procédures de contrôle en réponse aux menaces les plus récentes. En outre, les sites devraient envisager d'investir dans des outils plus sophistiqués permettant de mieux détecter les fraudes «propres ».



Graphique 5

2. LE POURCENTAGE DE COMMANDES REJETÉES POUR SUSPICION DE FRAUDE EST BEAUCOUP PLUS ÉLEVÉ POUR LES TRANSACTIONS TRANSNATIONALES

(Graphique 5)

Les sites marchands semblent adopter une approche excessivement prudente et il est probable qu'ils rejettent certaines commandes valides. Il importe d'optimiser les outils de détection de la fraude, non seulement par type de paiement mais aussi pour chaque marché concerné. Ceci permettrait d'améliorer l'expérience client dans son ensemble.

COUP DE PROJECTEUR SUR LA FRAUDE INTERNATIONALE

Voici un aperçu de quelques différences régionales dont les équipes de lutte contre la fraude doivent avoir connaissance :

DÉPARTEMENTS FRANÇAIS D'OUTRE-MER : la Guadeloupe dispose de son propre code pays ISO mais les cartes de paiement qui y sont délivrées sont généralement directement attribuées à la France. Autrement dit, les règles de contrôle reposant sur des discordances du numéro d'identification bancaire (BIN) doivent faire l'objet de la plus grande attention.

BRÉSIL : Il importe de mettre en place des contrôles par code postal car la fraude est régionalisée. Nous préconisons que les sites marchands enregistrent également le numéro CPF (semblable au numéro de sécurité sociale aux États-Unis) dans le cadre du processus de vérification.

CHINE : La fraude à l'intérieur du pays est limitée mais compte tenu de l'importance du marché de l'exportation, la fraude transfrontalière peut être élevée. En Chine, les banques n'ont pas mis en place des procédures permettant aux titulaires de cartes de signaler les transactions frauduleuses, la récupération de fonds peut donc s'avérer très difficile.

INDE : Il est extrêmement courant pour les consommateurs de partager des numéros de cartes de paiement lorsqu'ils font des achats en ligne, notamment sur les sites internet de voyages. Ces règles doivent être revues. 3D Secure est obligatoire pour les achats en ligne et, par conséquent, le transfert de la responsabilité peut s'appliquer.

04 | LE NOUVEAU VISAGE DU E-COMMERCE

Les consommateurs d'aujourd'hui sont plus connectés que jamais et le e-commerce moderne ouvre de nombreuses voies d'accès au marché.

Sur les sites marchands étudiés :

48 %
exploitent un site ou une application de commerce mobile

52 %
ont un canal de vente par téléphone ou par correspondance

63 %
disposent de points de vente physiques

2 %
acceptent les paiements sur automates

MESURES Á PRENDRE

TRAQUER LA FRAUDE PAR CANAL DE VENTE

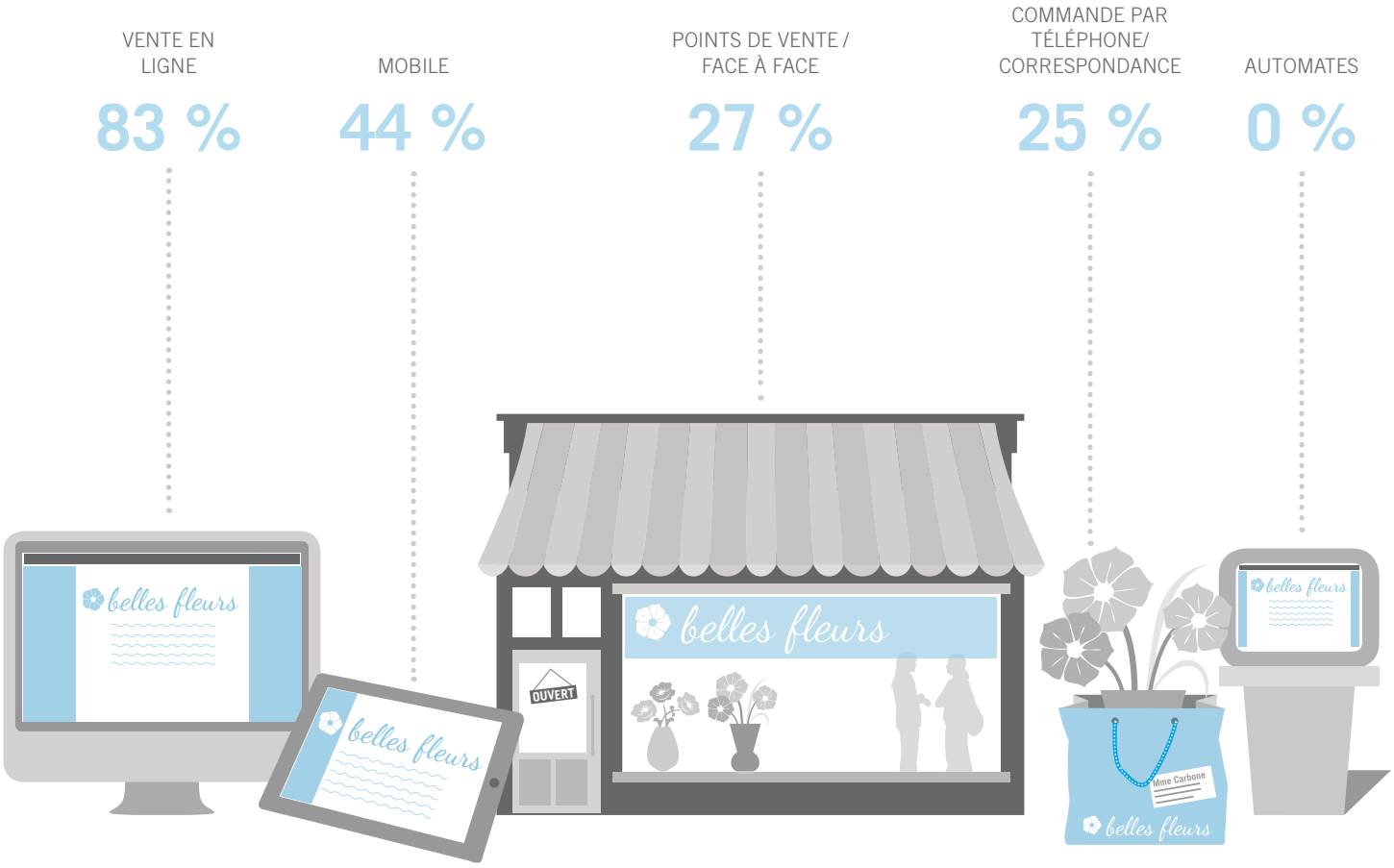
L'absence d'une surveillance spécifique pour chaque canal peut masquer les tactiques des fraudeurs ou les taux de fraudes. Face à la croissance du e-commerce, il est indispensable que les sites marchands comprennent l'impact de la fraude sur tous les multiples points de contact avec leurs clients.

Assurez-vous que vos outils de détection de la fraude soient correctement configurés pour prendre en compte les différentes caractéristiques et spécificités de chaque canal de vente, notamment les difficultés de géolocalisation de l'adresse IP sur un appareil mobile ou la probabilité accrue que les commandes à partir de ces terminaux soient passées à des heures inhabituelles de la journée.

Graphique 6 :
CANAUX DE VENTE FAISANT L'OBJET D'UN CONTRÔLE DE LA FRAUDE

Chaque canal de vente peut présenter des enjeux différents, les méthodes et tactiques des fraudeurs n'étant pas les mêmes. Toutefois un grand nombre de sites marchands interrogés ne contrôlent pas la fraude sur tous leurs canaux de vente.

Interrogés sur les canaux les plus touchés par la fraude, près de 60 % des e-commerçants ont répondu qu'il s'agissait de la vente en ligne et 31 % du canal mobile.



MESURES Á PRENDRE

CENTRALISER LA GESTION DE LA FRAUDE

Nous recommandons que les sites marchands utilisent une plate-forme centralisée pour surveiller toutes les transactions effectuées à travers leurs différents canaux de vente, Internet, téléphonie mobile et centres d'appels. Ceci vous permettra d'avoir une vue unique de l'expérience de vos clients et d'optimiser l'ensemble de leur expérience de commerce en ligne, et non uniquement pour un terminal ou un point de contact donné.

- Veillez à ce que la plate-forme choisie dispose de la flexibilité nécessaire pour contrôler les commandes des différents canaux de vente, à partir d'ensembles de règles différents ;
- Utilisez la plate-forme pour contrôler les tentatives de transactions à partir de plusieurs sources. Par exemple, si une commande est passée via votre centre d'appels ou une application mobile, il serait utile de savoir si l'acheteur a déjà été refusé par votre boutique en ligne car cela peut révéler un comportement frauduleux.

05 | CONCLUSION

Le e-commerce offre des opportunités considérables aux entreprises françaises. Mais l'expansion vers de nouveaux pays et canaux de vente risque d'exposer les e-commerçants à des techniques de fraude toujours plus sophistiquées si une gestion et un contrôle desfraudes ne sont pas mis en place et optimisés.

Les sites marchands doivent s'attacher à offrir la meilleure expérience possible aux clients, quel que soit le marché ou le canal de vente. Cette offre devrait être complétée par une solide approche de la gestion de la fraude, en adoptant les outils et les pratiques les mieux adaptés à leur 'business model.'

Nous recommandons que les entreprises se concentrent d'abord et avant tout sur une meilleure vérification automatisée de la fraude. Ceci leur permettra de limiter le recours à des procédures de contrôle manuel, qui consomment une grande quantité de ressources.

Les e-commerçants doivent s'assurer de disposer de règles optimisées leur permettant d'identifier les clients 'valides' plus rapidement et de façon plus fiable, tout en détectant et en rejetant le plus tôt possible les tactiques et les comportements frauduleux. Ceci est particulièrement important lors de l'expansion sur de nouveaux marchés ou canaux de vente, tels que les mobiles, où des pratiques frauduleuses différentes peuvent se développer.

Les sites marchands doivent également veiller à mettre en place des outils sophistiqués de capture et d'évaluation des données afin de mieux appréhender les niveaux de fraude dont ils peuvent être victimes. Ils pourraient ainsi mieux comprendre où se trouvent leurs points les plus vulnérables.

D'après notre enquête, certains sites marchands ont des doutes concernant l'efficacité réelle de leurs outils de prévention des fraudes. Nous recommandons que les entreprises déterminent leurs indicateurs clés de performance les plus importants (par exemple, le taux de fraude, de vérification, de commandes acceptées, de remboursement, etc.). Ces indicateurs devraient être suivis et contrôlés sur tous les différents marchés et canaux de vente, en veillant à enregistrer toutes les données pertinentes sur les transactions, de préférence via une plate-forme centralisée afin d'améliorer l'efficacité.

Les résultats obtenus pourront alors être utilisés pour affiner et améliorer régulièrement la stratégie de l'entreprise en matière de lutte anti-fraude pour les transactions en ligne.

Dernier point, mais non des moindres, dans le contexte actuel de tactiques frauduleuses de plus en plus sophistiquées et « propres », les e-commerçants devraient adopter une approche globale de la gestion des fraudes. Cela passe par l'introduction d'outils perfectionnés de détection, qui ne traitent pas seulement les menaces actuelles ou émergentes mais peuvent également enregistrer et consolider toutes les données requises sur les transactions, quel que soit le terminal utilisé ou le pays d'origine.

Le résultat ? Un plus grand nombre de commandes acceptées plus rapidement, une diminution des risques, une amélioration significative de l'expérience client et un développement plus rapide et plus sûr sur de nouveaux marchés et de nouveaux canaux de vente.

A PROPOS DE CYBERSOURCE

CyberSource, filiale à 100% de Visa Inc., est un spécialiste de la gestion de paiements. Plus de 400.000 marchands à travers le monde utilisent ses solutions sous les marques CyberSource et Authorize.Net pour traiter les paiements en ligne, optimiser la gestion de la fraude et simplifier la sécurité des paiements. La société a son siège à Foster City en Californie, et possède des bureaux dans le monde entier, avec des sièges régionaux à Singapour, Tokyo, Miami, Sao Paulo et Reading au Royaume Uni. CyberSource opère en Europe en accord avec Visa Europe.

Pour plus d'informations, consultez www.cybersource.fr

A PROPOS DE L'ACSEL

Présidée par Pierre Alzon, l'ACSEL, l'association de l'économie numérique, regroupe 180 sociétés représentatives de l'ensemble des acteurs du secteur. Elle a pour principal objet de décrypter l'impact des technologies émergentes, notamment en termes d'usages, de comportements et de modèles économiques.

Acsel
L'ASSOCIATION DE L'ÉCONOMIE NUMÉRIQUE

www.associationeconomienumerique.fr

Conception pinkgreencreative.co.uk

POUR TOUTE INFORMATION COMPLÉMENTAIRE

Contactez CyberSource France par téléphone au **01 7098 3220** ou par courriel à l'adresse **fr@cybersource.com**

CyberSource®
the power of payment

www.cybersource.fr