

# « La perception des porteurs de carte sur les nouveaux dispositifs d'authentification lors des paiements en ligne »

Synthèse d'Harris Interactive  
pour l'Observatoire de la sécurité des cartes de paiement



Avril 2011



Face à l'essor des transactions sur Internet et aux risques de fraude associés, l'Observatoire de la Sécurité des Cartes de Paiement a émis la recommandation en 2009 de renforcer les mesures destinées à protéger les paiements par carte bancaire à distance et de **mettre en place des solutions d'authentification renforcée**. L'objectif de ces solutions est de valider l'identité de l'acheteur sur Internet à travers le recoupement de plusieurs éléments. Sont donc apparus, depuis cette date, des systèmes comme le mot de passe statique, le code non-rejouable envoyé par SMS, le lecteur de carte de paiement, le token ou encore la carte matricielle.

Une étude qualitative réalisée en 2009 pour l'Observatoire a permis de mettre en lumière une réaction positive des acheteurs face à l'implication de leur banque dans la sécurisation de leurs paiements et face au développement de ces procédures d'authentification. L'idée était accueillie favorablement et deux principales conditions étaient apposées à leur diffusion : une appropriation aisée des différents dispositifs et un accompagnement de la part des banques. Aujourd'hui, alors que de plus en plus d'individus ont été en situation d'utiliser ces dispositifs sur différents sites marchands, l'Observatoire a souhaité réaliser **une enquête quantitative pour évaluer le degré de connaissance et d'usage de ces nouveaux dispositifs** de sécurisation des paiements en ligne, mais également **appréhender l'expérience et les jugements des utilisateurs**.

Les résultats de cette étude confirment quantitativement un certain nombre de conclusions du rapport de 2009 et mettent principalement en évidence que :

- Ces différents dispositifs d'authentification, particulièrement ceux se traduisant par la saisie d'un code unique, sont **perçus par leurs utilisateurs comme des moyens efficaces de renforcer la sécurité des paiements** en ligne ;
- **Leur usage est perçu comme relativement aisé et peu contraignant** bien que certaines difficultés soient associées à leur mise en place ou au recours à un élément physique : téléphone portable, carte matricielle... ;
- Ces dispositifs permettent de réaliser des achats en ligne en se sentant plus en sécurité : si pour une majorité des utilisateurs, cela n'est pas de nature à influencer sur leur propension à acheter en ligne, on note néanmoins pour une partie importante d'entre eux **la volonté de favoriser à l'avenir les sites présentant de tels dispositifs** ;
- Les banques apparaissent comme le meilleur interlocuteur sur ce sujet, devant les pouvoirs publics.

## 1. Notoriété et usage des nouveaux dispositifs d'authentification

**Les paiements par carte bancaire en ligne suscitent aujourd'hui peu d'inquiétude chez les cyberacheteurs**

**23% des cyberacheteurs interrogés déclarent éprouver de l'inquiétude lorsqu'ils effectuent un achat sur Internet avec leur carte bancaire**, 3% étant très inquiets et 20% plutôt inquiets. A l'inverse, 77% ne ressentent plutôt pas (55%) ou pas du tout (22%) d'inquiétude. Pour la majorité des personnes qui réalisent effectivement des achats sur Internet, cette démarche n'est donc pas associée à une prise de risque inconsidérée. Toutefois, pour une partie non négligeable d'entre eux, une légère appréhension peut subsister. Dans le détail, on constate que les femmes (29%), les cyberacheteurs appartenant aux catégories populaires (28%) ainsi que ceux dont les achats en ligne sont très occasionnels (moins de trois fois par an : 46%) sont plus susceptibles de se sentir inquiets.

En revanche, alors même que le lien n'est pas établi dans cette première question, **les personnes ayant déjà utilisé au moins un système d'authentification se montrent moins inquiètes que la moyenne** : elles ne sont que 19% tous systèmes confondus, et même 17% en cas d'utilisation d'un système d'authentification forte<sup>1</sup>, à se dire inquiètes contre 28% des personnes n'ayant jamais utilisé le moindre dispositif complémentaire.

**Une importante majorité de cyberacheteurs a connaissance de l'existence de dispositifs supplémentaires pour sécuriser les achats en ligne ...**

**Près de 8 cyberacheteurs sur 10 (79%) indiquent avoir déjà entendu parler de dispositifs supplémentaires pour sécuriser les achats sur Internet**. 58% déclarent même « voir bien ce dont il s'agit », quand 21% en ont une idée plus floue. La notoriété de ces dispositifs, dont l'existence est pourtant encore relativement récente, apparaît d'ores et déjà relativement bien établie au sein de la population des cyberacheteurs.

---

<sup>1</sup> Sont considérés comme systèmes d'authentification forte ceux nécessitant la saisie d'un code non-rejouable, à savoir le code envoyé par SMS, la carte matricielle, le token ainsi que le mini-lecteur de cartes.

La notoriété de ces dispositifs est plus élevée chez les cyberacheteurs de sexe masculin (83%) et ceux appartenant aux catégories supérieures (84%). A l'inverse, elle est un peu moins forte parmi les femmes (76%), les catégories populaires (75%) et surtout les cyberacheteurs les plus jeunes (69% des 16-24 ans). Logiquement, **plus les personnes interrogées achètent en ligne, plus elles sont susceptibles d'avoir entendu parler des nouveaux dispositifs de sécurisation des achats en ligne** et de savoir en quoi cela consiste. Ainsi, le taux de notoriété passe de 62% parmi les cyberacheteurs très occasionnels à 86% chez ceux qui effectuent au moins un achat par mois. On constate également que la quasi-totalité des personnes qui dans la suite de l'enquête vont être identifiées comme ayant déjà été confrontées à un de ces dispositifs indiquent à ce stade en avoir entendu parler (92% quel que soit le type de dispositif, 96% en cas de dispositif d'authentification forte). Environ deux-tiers des non-utilisateurs (66%) ont en également déjà entendu parler, mais seuls 37% voient bien ce dont il s'agit.

**... bien que peu affirment avoir reçu à ce sujet une information émanant de leur(s) banque(s)**

**Seuls 4 cyberacheteurs sur 10 (39%) répondent par l'affirmative** à la question « Avez-vous reçu une information de la part de votre / vos établissement(s) bancaire(s) concernant des dispositifs supplémentaires pour sécuriser les achats sur Internet ? ». Cette proportion monte à 54% parmi ceux qui ont déjà fait face à un tel dispositif, et même 64% en cas de confrontation à un dispositif d'authentification forte. Une communication est en effet nécessairement établie pour transmettre à l'acheteur « l'authentifieur » en cas de recours à la carte matricielle, le token ou le mini-lecteur de carte. En revanche, elle reste inférieure à 50% parmi les cyberacheteurs fréquents (44% lorsque l'individu réalise plusieurs achats en ligne par mois, 43% lorsqu'il en effectue en moyenne un par mois). Elle descend même à 27% parmi les cyberacheteurs âgés de 16 à 24 ans.

**Ceux qui déclarent avoir reçu une information l'ont jugé claire pour les aider à sécuriser leurs achats sur Internet à hauteur de 84%** (33% très claire et 51% plutôt claire). Seuls 15% déplorent à l'inverse son relatif manque de clarté.

## Un usage établi pour un cyberacheteur sur deux

La connaissance déclarée étant plus forte que le sentiment d'avoir été informé par sa banque, une partie de la notoriété de ces dispositifs découle sans doute d'autres canaux d'information ou d'une confrontation directe à l'un d'entre eux. En effet, **une personne sur deux achetant en ligne a déjà utilisé au moins un des six modes d'authentification testés lors de cette enquête.**

Le dispositif d'authentification le plus utilisé aujourd'hui est la **saisie d'un code unique envoyé par la banque par SMS** : 29% des cyberacheteurs disent avoir déjà utilisé ce dispositif. Viennent ensuite les deux systèmes d'authentification 'faible' : **la saisie de la date de naissance** (21%) et **le fait de devoir répondre à une question secrète** (13%). On retrouve ensuite les trois autres dispositifs d'authentification forte : **l'utilisation d'une carte matricielle** (13%), et **le mini-lecteur de carte** ou **le token** dont l'usage reste beaucoup plus confidentiel pour le moment (respectivement 3% et 2%).

Au global, **50% des cyberacheteurs ont déjà utilisé au moins un des dispositifs testés.** Si l'on restreint le champ aux **dispositifs d'authentification forte** impliquant la saisie d'un code unique généré automatiquement, la proportion est de **38%**. La moyenne du nombre de dispositifs déjà utilisés s'établit à 1,6 : cela signifie qu'une partie non négligeable des cyberacheteurs a déjà été confrontée à plusieurs dispositifs. Ainsi, 32% de ceux qui ont déjà utilisé un code reçu par SMS déclarent également avoir déjà eu à saisir leur date de naissance et 24% la réponse à une question secrète convenue au préalable avec leur banque.

**Plus sa fréquence d'achat sur Internet est élevée, plus le cyberacheteur est susceptible d'avoir déjà rencontré un tel dispositif.** Ainsi, parmi les personnes qui effectuent plusieurs achats mensuels sur la toile, près des deux-tiers (65%) déclarent avoir déjà utilisé au moins un des six dispositifs et un sur deux (51%) un dispositif non-rejouable. Dans le détail, on remarque également que les cyberacheteurs appartenant aux catégories supérieures sont un peu plus nombreux à avoir déjà utilisé un de ces dispositifs (56% contre 47% des CSP-). Cela est essentiellement dû à un usage plus répandu de la saisie de la date de naissance (29% contre 16%) mais aussi du code reçu par SMS (37% contre 27%). Si les jeunes de 25 à 34 ans sont parmi les plus nombreux à avoir déjà été confronté au code reçu sur son téléphone portable (38%), ce n'est pas le cas des 16-24 ans (20%).

## 2. Expériences et jugements concernant l'utilisation des nouveaux dispositifs d'authentification

### Des dispositifs jugés très majoritairement faciles à utiliser

L'utilisation de ces différents dispositifs d'authentification ne semble pas poser de problèmes majeurs. Certes, il s'agit ici des « early-adopters », à savoir les premiers à tester cette nouvelle technologie et majoritairement des personnes qui réalisent souvent des achats en ligne dont on peut imaginer qu'elles ont un rapport décomplexé à l'innovation technologique. Toutefois, la confrontation à ces dispositifs peut concerner tous les profils d'acheteurs – on ne peut choisir de s'y soustraire si le site le propose – et le constat d'une facilité d'utilisation est majoritairement partagé par tous, jeunes ou plus âgés, CSP + ou CSP-...

Ainsi, **seuls 8% des utilisateurs déclarent trouver au moins un des dispositifs difficiles à utiliser, 10% lorsqu'on se concentre sur les dispositifs d'authentification forte.** Ce sont les mini-lecteurs de carte et les cartes matricielles qui sont perçus comme les moins faciles à utiliser, mais la proportion de personnes qui déplorent une difficulté d'utilisation reste très faible : 11% dans les deux cas. 7% des personnes qui ont déjà été confrontées à la saisie d'un code unique par SMS jugent ce dispositif difficile à utiliser. Concernant les trois derniers dispositifs, les difficultés perçues sont très faibles (proportion inférieure ou égale à 5%). On n'observe pas une catégorie d'utilisateurs qui serait particulièrement déstabilisée.

Sur le principe, ces dispositifs ne semblent donc guère perçus comme trop compliqués, trop techniques. Qu'en est-il à l'usage ?

### Près d'un utilisateur sur cinq a néanmoins rencontré des difficultés lors de sa première utilisation d'un dispositif d'authentification forte

36% des utilisateurs d'un mini-lecteur de carte font état de difficultés lors de la première utilisation, 16% des utilisateurs d'une carte matricielle, 14% des utilisateurs d'un code reçu par SMS et 8% des utilisateurs d'un

token. **Au global, c'est donc environ un utilisateur sur cinq (19%) qui a éprouvé des difficultés lors de l'utilisation initiale d'un dispositif d'authentification forte.** Peu de difficultés sont mentionnées pour le fait de devoir répondre à une question secrète ou de saisir sa date de naissance au moment du paiement (respectivement 6% et 5% des utilisateurs). Dans le détail, on observe que les membres des catégories supérieures sont plus nombreux à avoir identifié des difficultés lors de la première utilisation d'un code unique envoyé par la banque par SMS (18% contre 14% en moyenne).

Ces difficultés **sont d'ordres multiples et peuvent intervenir à différents moments** : 27% des personnes ayant rencontré des difficultés ont eu du mal pour comprendre le mode de fonctionnement du dispositif, 26% pour y accéder, 28% pour l'activer ou procéder à l'enregistrement des données ou encore 24% au moment même de l'utiliser. 21% font également mention d'autres difficultés qui tiennent davantage à l'implication dans le dispositif d'un objet matériel : batterie de téléphone portable à plat, changement de numéro non signalé à la banque, impossibilité de retrouver chez soi la carte matricielle...

Au final, **environ un tiers des personnes qui ont fait face à de telles difficultés (31%) n'a pas pu ou su finaliser leur achat.** Ramené sur la population des utilisateurs d'au moins un dispositif (15%), cela représente donc un peu moins de 5% des utilisateurs qui ont renoncé à leur achat lors de la première confrontation à ce type de dispositif.

### **Une partie des difficultés disparaît lors des utilisations ultérieures**

Si l'on s'intéresse maintenant aux difficultés persistantes, qui se sont manifestées lors des utilisations suivantes, **la proportion de personnes ayant de nouveau fait face à des difficultés chute à 6% des utilisateurs, 7% pour les dispositifs d'authentification forte.** Dans un contexte où la majorité des utilisateurs interrogés ont bien réitéré leur usage du dispositif, on observe donc que la proportion de personnes ayant rencontré des difficultés est plus que divisée par deux entre la première utilisation et les suivantes.

Encore une fois, c'est le mini-lecteur de carte qui pose le plus de problèmes (11%) devant la carte matricielle (6%) et le code reçu par SMS (5%). La base de personnes ayant eu des difficultés lors des utilisations suivantes



est donc relativement faible dans notre échantillon et on observe comme pour la question précédente que ces difficultés correspondent plus à des difficultés matérielles ou humaines (oubli de la question secrète, numéro de téléphone non-enregistré ou incorrect, SMS reçu trop tardivement...) qu'à des problèmes ayant trait véritablement aux dispositifs. Très peu mentionnent en effet des codes invalides ou des dispositifs défectueux.

**Toutefois, lorsque les difficultés persistent, les individus ont davantage tendance à ne pas finaliser l'achat : 44%** contre 31% dans le cas de difficultés liées à la première utilisation. Cela représente un peu moins de 3% des utilisateurs.

### **Le temps supplémentaire nécessaire pour finaliser l'achat en raison de ces dispositifs n'apparaît pas comme trop gênant**

Seule **une minorité d'utilisateurs considère que le temps supplémentaire nécessaire à l'utilisation de ces nouveaux dispositifs est gênant (18% au global)**. Certes, cette proportion est plus forte lorsque les dispositifs impliquent le recours à un objet mais reste dans tous les cas inférieure à un tiers des personnes concernées, **la proportion de personnes se plaignant d'une gêne importante étant très faible (6% maximum)**. Ainsi, 29% des utilisateurs d'un token jugent le délai supplémentaire gênant. 28% des utilisateurs d'une carte matricielle et 24% des utilisateurs d'un mini-lecteur de carte établissent également ce constat. En ce qui concerne le dispositif d'authentification le plus utilisé, à savoir la saisie du code unique envoyé par SMS, seuls 16% des utilisateurs déplorent un temps supplémentaire gênant. Enfin, 12% trouvent gênant de prendre plus de temps pour répondre à une question secrète et 8% pour saisir sa date de naissance.

Dans le détail, on constate que ce sont les utilisateurs les plus jeunes, à savoir les 16-34 ans, qui sont les plus susceptibles de se déclarer gênés (21% contre 18% en moyenne pour l'ensemble des dispositifs, 22% contre 19% pour les dispositifs d'authentification forte). Les personnes qui réalisent peu d'achat en ligne conçoivent également moins ce temps supplémentaire comme gênant que ceux qui achètent plus souvent et sont donc amenées à « perdre » plus de temps (14% de ceux qui réalisent moins d'un achat par mois estiment qu'au moins un des dispositifs implique un délai gênant contre 20% de ceux qui achètent plus souvent sur Internet).

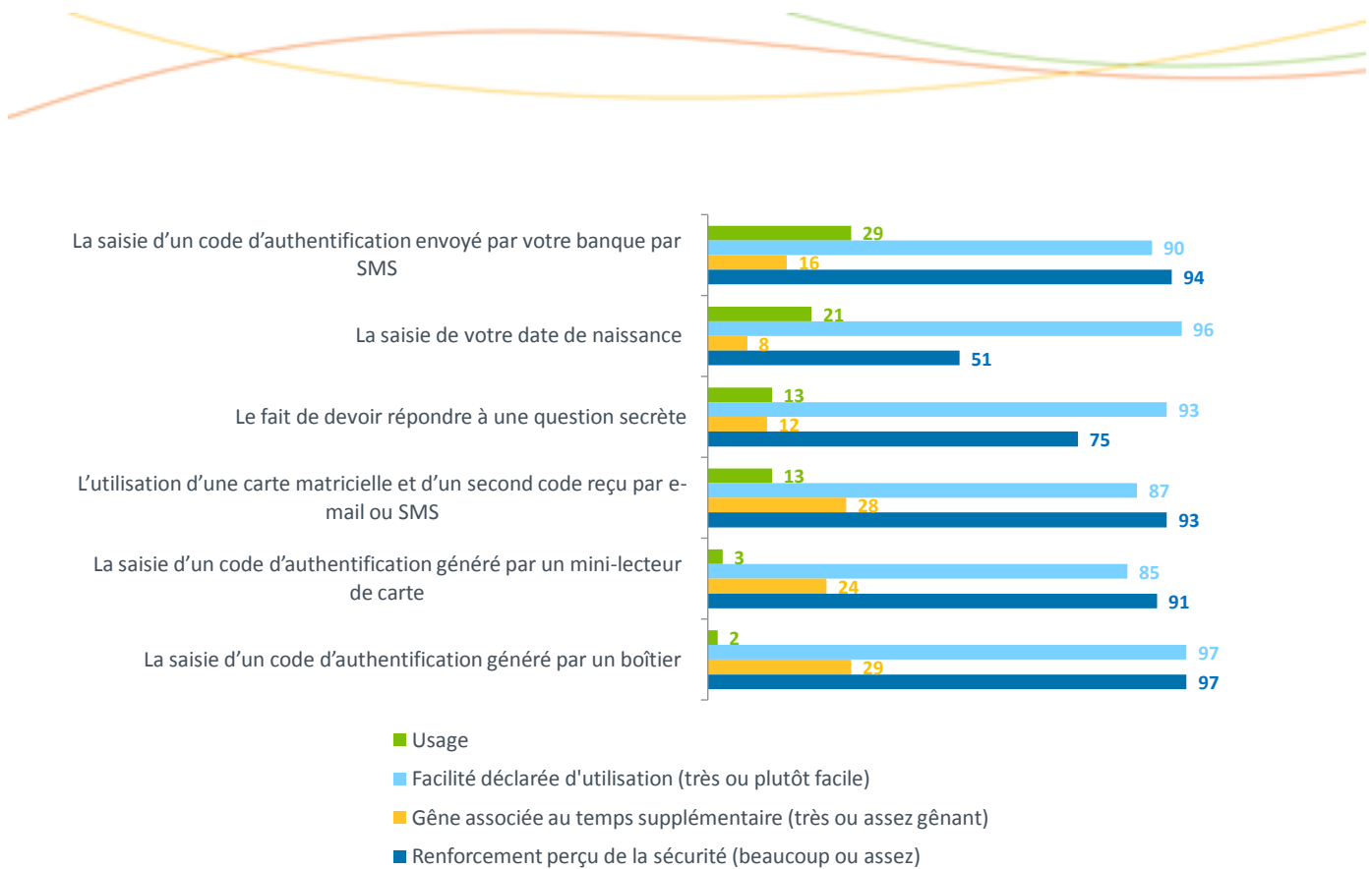
### 3. Perception du renforcement de la sécurité et souhaits concernant l'avenir des dispositifs

#### Une sécurité jugée renforcée, surtout par les dispositifs non-rejouables

Si les répondants estiment peu gênant le délai supplémentaire entraîné par ces nouveaux dispositifs, c'est sans doute parce que le rapport désagrément/sécurité est perçu comme positif. En effet, **les utilisateurs ont majoritairement le sentiment que ces dispositifs renforcent significativement la sécurité des paiements par carte bancaire sur Internet, et particulièrement les dispositifs impliquant la saisie d'un code unique.**

En première position, on trouve le dispositif d'authentification forte le moins répandu, à savoir **le token** : 97% des utilisateurs de ce dispositif estiment que cela renforce la sécurité du paiement, dont 73% beaucoup. En deuxième position, on trouve au contraire le dispositif le plus répandu, **la saisie d'un code unique reçu par SMS** : 94% des utilisateurs estiment que la sécurité est confortée par ce dispositif, dont 53% beaucoup. Viennent ensuite juste derrière **la carte matricielle** (93%, dont 55% beaucoup) et **le mini-lecteur de carte** (91%, dont 56% beaucoup). Les dispositifs d'authentification 'faibles' se traduisant par la saisie d'une information personnelle rassurent moins d'utilisateurs et les rassurent moins fortement : ainsi 75% des personnes ayant déjà dû répondre à **une question secrète** lors d'un paiement en ligne ont le sentiment que cela accroît la sécurité, et seulement 23% beaucoup. La saisie de la date de naissance ne rassure qu'un utilisateur sur deux (51%) et seulement un sur dix beaucoup (10%).

Au global, sur la base de l'ensemble des utilisateurs, **86% ont le sentiment que la sécurité est renforcée par au moins un de ces dispositifs et même 96% quand on restreint le champ aux dispositifs non-rejouables.** Ce sentiment de sécurité renforcée est majoritairement partagé par toutes les catégories de population, même s'il est un peu plus faible chez les 16-34 ans (81%) et les cyberacheteurs occasionnels (82%) dont l'inquiétude concernant les achats en ligne est plus forte à la base.



Ainsi, **76% des utilisateurs disent se sentir plus en sécurité lorsqu'ils effectuent leurs achats en ligne avec ces nouveaux dispositifs**. Cette proportion monte même à 83% parmi les personnes ayant déjà utilisé au moins un des 4 dispositifs d'authentification forte testés. Notons également que les acheteurs fréquents sont plus susceptibles de se dire plus en sécurité que les acheteurs occasionnels. En outre, ces dispositifs sont plus susceptibles de rassurer encore plus les utilisateurs pas du tout ou plutôt pas inquiets que ceux qui éprouvent de l'inquiétude lorsqu'ils réalisent un achat par carte bancaire en ligne (77% contre 71% et seulement 44% des personnes très inquiètes).

## **Pour les utilisateurs, ces dispositifs n'apparaissent pas comme un handicap pour les sites, mais au contraire comme un argument pouvant conforter les cyberacheteurs**

Ces dispositifs vont-ils favoriser ou non le développement des transactions en ligne ? **Pour près de 8 utilisateurs sur 10, cela ne va pas changer leur comportement en matière d'achats sur la Toile**, ils continueront à acheter ni plus, ni moins. En revanche, **19% déclarent que ces nouveaux dispositifs sont susceptibles de les amener à acheter davantage sur Internet**. Ce sont avant tout les utilisateurs qui achètent déjà beaucoup en ligne qui anticipent cet effet positif : 24% des personnes qui effectuent déjà au moins un achat en ligne par semaine et 23% de celles qui réalisent 2 ou 3 achats par mois. A l'inverse, seuls 2% (5% des 16-24 ans) estiment que cela aura tendance à les dissuader d'acheter en ligne, 1% déclarant qu'ils achèteront moins et 1% qu'ils n'achèteront plus du tout.

Les utilisateurs déclarent majoritairement qu'à l'avenir ils porteront attention à la présence ou non d'un tel dispositif lors de leurs achats par carte bancaire en ligne. Ainsi, **17% déclarent qu'ils feront leurs achats exclusivement sur des sites d'e-commerce présentant un tel dispositif et 54% qu'ils les favoriseront même s'ils pourront continuer à acheter sur un site n'en proposant pas**. 28% en revanche n'y feront pas particulièrement attention. Cela confirme les résultats de la question précédente : ces dispositifs ne dissuadent pas les cyberacheteurs potentiels et peuvent même apparaître comme un argument susceptible de se distinguer positivement. Dans le détail, on observe que l'attitude qui consiste à déclarer que les achats futurs se feront seulement sur les sites ainsi sécurisés concerne plutôt les catégories populaires (20%) et les acheteurs occasionnels (29% en cas de 3-4 achats par an et 38% en cas d'achats moins fréquents) ainsi que les utilisateurs de la carte matricielle, du token ou du mini-lecteur de carte (respectivement 24%, 37% et 28%). La deuxième attitude qui consiste à les favoriser sans être exclusive est davantage citée par les acheteurs très fréquents (65%). Quant à l'attitude consistant à ne pas prêter attention à ces dispositifs, elle est surtout le fait des plus jeunes (44% des 16-24 ans), des CSP + (32%), des Franciliens (33%) ou encore des personnes qui ont eu recours à la saisie de la date de naissance (32%).

Les cyberacheteurs les plus fréquents sont moins nombreux que la moyenne à envisager se restreindre aux seuls sites présentant ces dispositifs d'authentification (8% et 12% contre 29% et 38% pour les cyberacheteurs plus occasionnels).

## **Le souhait d'une généralisation de ces dispositifs et d'une communication émanant avant tout des banques**

**83% des utilisateurs d'au moins un dispositif déclarent souhaiter que ces dispositifs soient généralisés à l'ensemble des sites d'achats en ligne**, dont 54% tout à fait. On le voit, le principe est donc plutôt bien accueilli et la poursuite du développement de ces outils est attendue par les utilisateurs.

**L'hypothèse d'un déclenchement du dispositif seulement à partir d'un certain montant d'achat fait sens pour 50% des utilisateurs** (21% tout à fait et 29 plutôt), **tout comme celle d'un déclenchement conditionné à la nature de l'achat** : billet d'avion, vêtements, matériel électroménager... (20% tout à fait et 30% plutôt).

Les utilisateurs sont donc majoritairement favorables à une généralisation, mais pour une partie d'entre eux, à une généralisation avec certaines conditions restrictives. C'est particulièrement le cas des utilisateurs les plus jeunes : les 16-24 ans, qui rappelons-le sont un peu plus gênés par le temps supplémentaire nécessaire à l'utilisation de ce dispositifs, souhaitent moins une généralisation à l'ensemble des e-marchands (76% contre 83% en moyenne), mais sont plus favorables à un déclenchement en fonction de la nature de l'achat (58% contre 50% en moyenne). C'est également le cas des utilisateurs qui achètent très souvent en ligne : 75% sont pour la généralisation et 59% pour un déclenchement à partir d'un certain montant d'achat.

L'enquête était close par une question visant à identifier les acteurs perçus comme les plus pertinents pour communiquer sur ces nouveaux dispositifs. Seuls 10% expriment clairement ne pas vouloir de communication à ce sujet. Pour les autres, **ce sont avant tout les banques qui sont identifiées comme les acteurs devant prendre la parole sur ce sujet (74%)**, devant les sites commerçants (43%), les associations de consommateurs (24%) et les pouvoirs publics (16%). On le sait, en France, les citoyens attendent souvent que l'Etat ou plus largement les pouvoirs publics s'emparent des sujets. Cependant, dans ce cas, sur ce sujet technique et qui implique une relation de confiance presque interpersonnelle entre le cyberacheteur et son établissement bancaire, ce sont donc avant tout les banques qui sont sollicitées, et ce par toutes les catégories de répondants.

