

Acte de la vie citoyenne des Français, l'usage de la carte bancaire s'est répandu au point de devenir un geste courant de leur vie quotidienne.

L'une des missions du Groupement des Cartes Bancaires "CB" est d'assurer, pour le compte de ses 170 banques membres, la sécurité et la prévention des fraudes. Tous les acteurs de la vie locale sont des relais précieux de la chaîne qui, de l'État aux utilisateurs, œuvre à la sécurité des transactions par carte bancaire à puce. En cette veille de grande migration estivale, propice aux usages des cartes bancaires CB à l'étranger, nous indiquons, dans cette lettre, les précautions à prendre pour se prémunir du mieux possible contre le risque de fraude. Nous présentons aussi les conseils qui permettront aux utilisateurs de la carte, porteurs et commerçants, de se garantir efficacement contre les actes de malveillance les plus courants.

Michel Renault,
Président

CARTES CB : le plus sûr des moyens de paiement

De nombreux acteurs participent à la chaîne qui permet à la carte bancaire à puce CB de réaliser des performances record en matière de sécurité tout en assurant un nombre toujours croissant de transactions.

La puce associée à un code confidentiel est aujourd'hui l'un des systèmes les plus sûrs du monde. Adopté en France par la communauté bancaire CB dès 1992, ce choix technologique a permis de **diviser le taux de fraude par dix** en dix ans alors que, dans le même temps, il augmentait fortement dans de nombreux pays.

Vingt fois plus sûre que la carte bancaire à piste magnétique, bien plus résistante à la contrefaçon que le chèque, la carte bancaire à puce CB n'est toutefois pas infaillible. Les cas de fraude restent néanmoins extrêmement marginaux au regard du volume sans cesse croissant des transactions assurées par les cartes bancaires CB.

La lutte contre la fraude, axe prioritaire pour la communauté bancaire, est l'affaire de tous. C'est sur une **chaîne de la vigilance** que repose en effet la sûreté de ce moyen de paiement. Une chaîne dans laquelle tous les acteurs, dans leur sphère de compétence, ont un rôle à jouer :

- les **banques**, garantes de la sécurité du service à leurs clients, mobilisent leur personnel au quotidien pour contrôler la fiabilité des opérations de paiement et de retrait;
- la **communauté bancaire et le Groupement des Cartes Bancaires CB** consacrent de lourds investissements au développement de technologies toujours plus sûres;
- les **industriels** mobilisent savoir-faire hautement spécialisés et technologies de pointe pour répondre aux normes de sécurité imposées par le Groupement des Cartes Bancaires CB pour les cartes, les terminaux de paiement et les distributeurs automatiques de billets ;
- les **commerçants**, qui investissent dans des terminaux de paiement toujours plus performants ;
- l'**État**, par l'intermédiaire des services de police, de défense et de justice, œuvre au démantèlement et à la répression des réseaux frauduleux;
- enfin les **porteurs**, qui se doivent de respecter, pour un «bon usage» de la carte, des précautions élémentaires de bon sens.

Nombre de cartes bancaires CB

1992
21,071 millions

2002

45,404 millions

Nombre de distributeurs automatiques de billets

1992
17 432

2002

38 975

Nombre de transactions CB par an

1992
2 milliards

2002

5,3 milliards

Nombre de commerçants CB

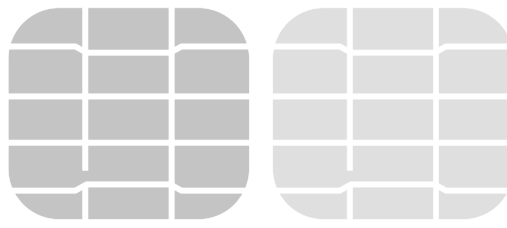
1992
767 000

2002

956 000

Le taux de fraude est divisé par dix en dix ans alors que le volume des transactions ne cesse de croître, faisant de la carte à puce le moyen de paiement préféré des Français.





Carte bancaire CB Le moyen de paiement préférés des Français⁽¹⁾

84%

des Français, en âge
d'en avoir une, détiennent
une carte CB

68%

préfèrent, lorsqu'ils
ont le choix, régler un
paiement par carte CB

98%

des détenteurs de
carte CB sont
satisfaits de ce moyen
de paiement

87%

des détenteurs
de carte CB souhaiteraient
pouvoir l'utiliser
plus souvent dans
des lieux l'acceptant
peu aujourd'hui
(professions de santé,
administrations...)

(1) Étude Sofres de septembre
2002 auprès d'un échantillon de 1 053
personnes âgées de 18 ans et plus
représentatif de la population française.

LA VIGILANCE, gage de sécurité pour tous

Aucun système de sécurité n'est infaillible. Connaître les types de fraude les plus caractéristiques, c'est aiguïser sa vigilance. Respecter quelques recommandations de bon sens, c'est se prémunir des risques les plus courants.

C'est un fait : le risque zéro n'existe pas. Les technologies les plus sûres n'empêcheront jamais le vol ou la perte d'une carte bancaire, qui génèrent, à eux seuls, plus de **50%** de la fraude. Et, de même que des escrocs tentent régulièrement de contrefaire des espèces ou de falsifier des chèques, d'autres s'emploient à la contrefaçon des cartes. Ce type de fraude est déstabilisant pour ses victimes, leur compte bancaire étant débité à leur insu, alors qu'ils sont toujours en possession de leur carte. La loi sur la sécurité quotidienne du 15 novembre 2001 protège les consommateurs contre ce genre de malversations en dégageant entièrement leur responsabilité.

Une démarche auprès de leur banque leur permet d'obtenir le remboursement intégral, rapide et sans frais, des débits frauduleux.

La communauté bancaire, les services de police et la justice collaborent étroitement pour détecter les opérations douteuses et démanteler les réseaux d'escroquerie à la carte. Mais quelque trente millions de porteurs et un million de commerçants sont également, au quotidien, les acteurs essentiels de la **chaîne de la vigilance**. L'immense majorité d'entre eux n'a jamais subi d'acte de malveillance et accorde une très grande confiance à ce moyen de paiement. À tel point qu'ils ont parfois tendance à oublier qu'une carte est aussi précieuse que des liquidités. Or, un minimum de prudence s'impose. Le respect de recommandations de bon sens suffit à **se prémunir des risques les plus courants** (cf. Dix conseils pratiques aux porteurs et aux commerçants).

Pour mieux comprendre l'intérêt et l'**efficacité de ces gestes simples de prévention**, voici les exemples actuels de fraude les plus caractéristiques :

- une copie des informations de la piste magnétique de la carte est effectuée à l'insu du porteur et encodée sur une carte vierge. Le code confidentiel est obtenu par ruse. La fausse carte ne peut être utilisée qu'à l'étranger,
- vol de la carte grâce à un piège invisible inséré dans la fente d'un distributeur automatique de billets (collet marseillais). La carte est avalée par le distributeur sans que trois codes erronés aient été composés, puis récupérée par le fraudeur. Souvent, ce dernier aura abusé le porteur, lui proposant son aide pour l'amener à composer son code confidentiel devant lui,
- une copie de certaines informations de la puce est effectuée. Ces informations sont alors intégrées dans une fausse carte à puce utilisable avec n'importe quel code confidentiel (Yescard). Elle ne peut être utilisée que pour le paiement de faibles montants, sur certains terminaux ou systèmes d'acceptation,
- les 16 numéros et la date d'expiration gravés en relief sur le recto des cartes, sont utilisés, à l'insu du porteur, pour effectuer des achats à distance.

De nouveaux développements technologiques (lire p. 4), portés par les cartes bancaires CB de dernière génération, ont pour but de limiter drastiquement les types de fraude possibles, notamment à l'étranger qui représente plus de la moitié de la fraude sur les cartes CB.



Dix conseils aux porteurs

- 1 Préserver le secret du code confidentiel : ne l'écrire nulle part, ne le communiquer à personne, ni même à sa banque, aux services de police ou d'assurance, notamment par téléphone.
- 2 Composer toujours le code confidentiel à l'abri des regards indiscrets : ne pas hésiter à le saisir tout en protégeant le clavier de son autre main, notamment sur les automates de paiement.
- 3 Ne pas se laisser distraire lors d'un retrait, y compris par des personnes proposant leur aide, en se gardant de composer son code devant elles.
- 4 Conserver sa carte en lieu sûr : strictement personnelle, elle ne doit être prêtée à personne, pas même à ses proches.
- 5 Conserver les tickets de paiement et de retrait pour faciliter la vérification des relevés bancaires.
- 6 Vérifier régulièrement ses relevés bancaires et signaler immédiatement toute anomalie à la banque.
- 7 Conserver toujours un œil sur sa carte lors d'un paiement chez un commerçant.
- 8 Mettre immédiatement la carte en opposition si elle est avalée par un distributeur sans qu'un code erroné ait été composé trois fois.
- 9 Conserver en lieu sûr les 16 numéros de la carte et sa date d'expiration pour faciliter une mise en opposition en cas de perte ou de vol.
- 10 Noter le numéro d'appel du centre d'opposition de la banque ou du serveur interbancaire, accessible 7 jours sur 7 et 24h/24 au 0892 705 705 (0,34€/minute).

Dix conseils aux commerçants

- 1 Offrir au porteur les conditions optimums de sécurité : l'emplacement du clavier doit permettre d'effectuer la saisie du code confidentiel à l'abri des regards indiscrets.
- 2 Conserver en lieu sûr, pendant un an, les factures de paiement.
- 3 Sensibiliser le personnel en contact avec la clientèle en lui rappelant, régulièrement les contrôles à effectuer sur la carte bancaire.

En cas de présentation d'une carte étrangère ou en cas de doute

- 4 Comparer, lorsqu'elle est requise, la signature apposée sur la facture à celle de la carte.
- 5 Ne pas hésiter à téléphoner au centre d'autorisation pour faire valider une transaction.
- 6 Demander un justificatif d'identité au porteur de la carte.
- 7 Vérifier la présence des dispositifs visuels de sécurité de la carte : l'absence de l'hologramme ou du filigrane, révélés par la lampe UV servant à contrôler les billets de banque, est synonyme de contrefaçon.
- 8 Vérifier que le numéro de la carte imprimé sur le « ticket commerçant » correspond bien au numéro figurant sur la carte du porteur.

En cas de vente à distance

- 9 Demander au porteur de communiquer les trois derniers chiffres du numéro figurant sur le panneau de signature, au verso de sa carte : ce dispositif de sécurité supplémentaire, appelé cryptogramme visuel, sera obligatoire au 1^{er} janvier 2004.
- 10 Préserver la confidentialité des données de la carte communiquées au téléphone par son porteur lors d'un achat à distance : leur répétition, pour vérification, doit être faite en toute discrétion.

La carte bancaire CB c'est, chaque jour⁽²⁾

21,3 millions
de transactions

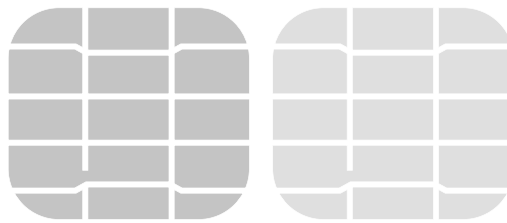
16,4 millions
de paiements

4,9 millions
de retraits

8
nouveaux distributeurs
de billets mis en service

(2) Calcul effectué sur la base de 250 jours ouvrables par an.





Les étapes de la migration EMV

1997

la communauté bancaire CB décide l'adoption de la norme de cartes à puces EMV, nouveau standard international qui succédera à la norme française actuelle.

2001

signature de l'accord fixant le calendrier d'adaptation des terminaux de paiement à la norme EMV par la communauté bancaire et les représentants du Commerce.

2002

les premières cartes bancaires EMV sont émises en France et la première transaction pilote par carte à puce EMV se déroule dans l'Hexagone.

2003

début de l'adaptation des terminaux de paiement à la norme EMV, dont la migration s'achèvera au 30 juin 2004.

2005

toutes les cartes à puce émises en France et en Europe sont à la norme EMV.

2005-2007

la norme EMV devient le nouveau standard mondial de la carte bancaire.

LA PUCE, référence européenne de la sécurité

En 2005, les cartes bancaires européennes auront adopté la puce dont la sécurité se verra renforcée par le déploiement d'innovations technologiques majeures.

La carte bancaire à puce a fait ses preuves. Sa capacité à résister à la fraude n'a pas échappé aux banques européennes qui ont décidé **de suivre l'exemple français**. Et d'ici 2005, l'ensemble des pays européens l'aura adoptée. Moteur de cette évolution majeure, la communauté bancaire française CB développe, en parallèle, des innovations technologiques qui diminueront les voies possibles de fraude.

• CARTES BANCAIRES EUROPÉENNES EMV

La généralisation de la puce en Europe contribuera à double titre au **renforcement de la lutte contre la fraude** :

- l'abandon de la piste magnétique au profit de la puce interdira l'usage, à l'échelle européenne, de fausses cartes où sont copiées les données des pistes magnétiques de vraies cartes ;
- le nouveau standard international EMV (Europay, MasterCard, Visa) renforcera la sécurité intrinsèque des puces.

Coût de cette mobilisation de la communauté bancaire européenne : 8,6 milliards d'euros. À la clé, la migration de plus de 400 millions de cartes bancaires à piste magnétique vers la puce, et une sécurité renforcée pour les porteurs, en Europe comme en France.

• PUCES À AUTHENTIFICATION DYNAMIQUE

Le mécanisme d'authentification des cartes CB par les terminaux de paiement va prochainement évoluer en Europe. Le DDA (Dynamic Data Authentication) est **un nouveau système cryptographique** qui renforce le processus d'authentification des cartes par les terminaux de paiement européens. Ces cartes à puce, dites à authentification dynamique, seront déployées à partir du dernier trimestre de l'année 2004.

• LA SÉCURISATION DES ACHATS À DISTANCE

La sécurisation des paiements à distance par carte bancaire est l'un des objectifs majeurs de la communauté bancaire CB. Aujourd'hui, ce n'est pas la puce, mais le numéro de la carte et sa date d'expiration qui sont mis en jeu dans ce type de transaction. Des dispositifs innovants sont à l'étude au niveau européen. En garantissant l'**authentification du porteur** et le recueil de son consentement pour une transaction de paiement, ces nouveaux dispositifs apporteront aux paiements à distance une sécurité comparable à celle des achats de proximité. Le Groupement des Cartes Bancaires CB pilote plusieurs groupes de travail où banques, industriels et pouvoirs publics, œuvrent à la mise au point de solutions sécurisées de paiement à distance.

Groupement des Cartes Bancaires "CB"

Groupement d'intérêt économique régi par l'ordonnance du 23 septembre 1967
tél. : 01 53 89 34 34
www.cartes-bancaires.com
communication@cartes-bancaires.com

