LA GESTION ET LA MAÎTRISE DES RISQUES DANS LE SYSTÈME CARTES BANCAIRES

GILLES GUITTON *

Avec 50 millions de cartes en circulation, 1 million de commerces et 45 000 distributeurs automatiques de billets accessibles en France, le nombre d'opérations réalisées annuellement par le système Cartes Bancaires « CB » excède 6 milliards.

Les paiements par carte - 220 Md€/an - représentent ainsi un quart de la dépense des ménages français.

Le système « CB » est le plus important d'Europe avec un volume de transactions de l'ordre de 25 % du total européen des paiements par carte, ou de 35 % dans la zone euro.

Une telle situation donne la mesure des enjeux attachés au système de paiements par cartes bancaires, tout particulièrement au plan sécuritaire.

C'est pour y répondre que le Groupement s'est doté, dès 1999, d'une structure spécifique de *risk management* afin d'analyser en profondeur les risques et de piloter la politique globale de sécurité du système.

Après une présentation succincte du système « CB », le présent article expose les caractéristiques essentielles de ses dispositifs sécuritaires et de ses mécanismes de gestion de risques avant de les resituer dans les nouvelles perspectives européennes du SEPA[1].

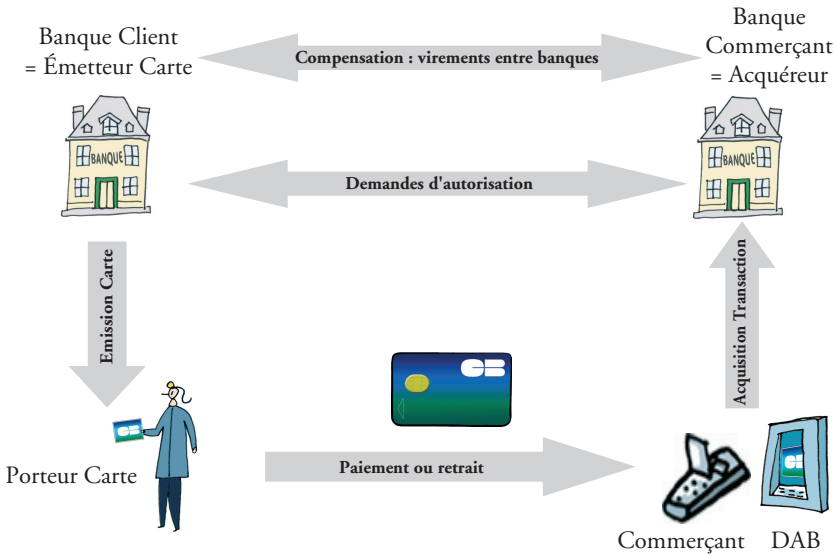
PRÉSENTATION SUCCINCTE DU SYSTEME « CB » ET DE SES ENJEUX

À l'origine (1967), le paiement par carte a été proposé par les banques françaises à leurs clients dans le but de réduire le nombre de chèques émis.

* Président du Conseil de direction du Groupement des Cartes Bancaires « CB ».

Le système de paiements par carte bancaire a été créé en 1984 par la communauté des banques opérant en France pour permettre au client d'une banque d'utiliser sa carte chez un commerçant affilié à une autre banque et de retirer de l'argent dans un distributeur automatique de billets géré par une autre banque : c'est ce que l'on appelle l'interopérabilité du paiement et du retrait par carte, fondée sur l'interbancarité.

Graphique n° 1
L'interbancarité



Source : Groupement des Cartes Bancaires « CB ».

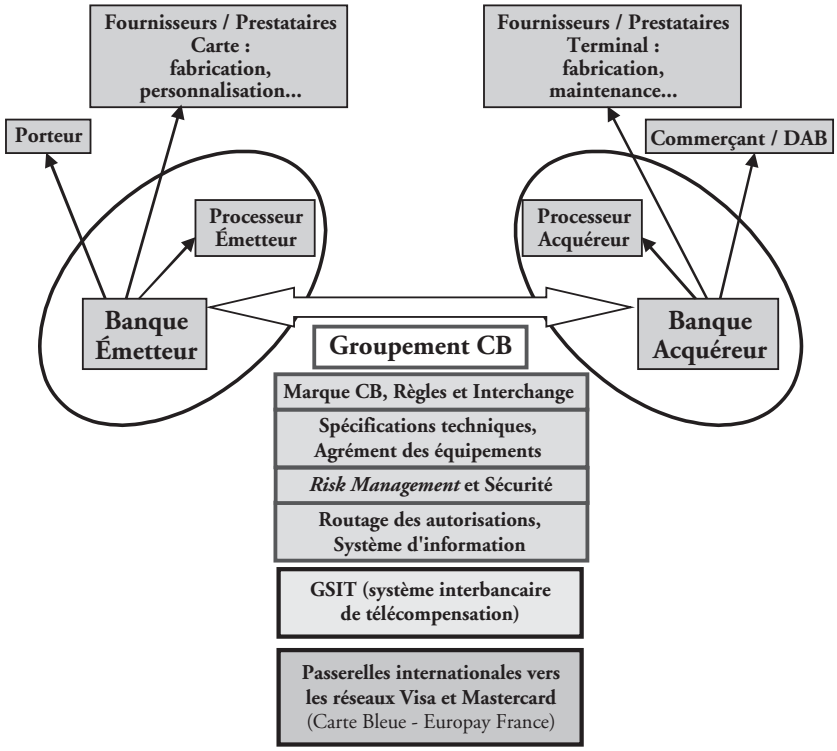
Les établissements financiers participant au système « CB » se sont ainsi regroupés au sein d'un Groupement d'intérêt économique, le Groupement des Cartes Bancaires « CB ». Sur les 146 membres que compte aujourd'hui le Groupement, 35 sont à capitaux étrangers.

Les responsabilités des différents acteurs du système « CB » sont réparties de la manière suivante :

- pour sa part, le Groupement des Cartes Bancaires « CB », outil commun à tous les membres, assure la promotion, le développement et la sécurité du système « CB ». Instance d'étude et de coopération, le Groupement établit les standards techniques d'interopérabilité, définit les règles interbancaires assurant l'équilibre économique du système et pilote la sécurité d'ensemble du dispositif ;

- les banques membres du Groupement émettent les cartes bancaires, affilient les commerçants et gèrent les distributeurs automatiques de billets. Chaque membre du Groupement développe librement sa propre politique commerciale à l'égard de ses clients, commerçants ou titulaires de cartes bancaires ;
- le Groupement pour un système interbancaire de télécompensation (GSIT) assure l'échange et la compensation de l'ensemble des opérations automatisées de moyens de paiement de masse et de petits montants, dont les opérations cartes bancaires (paiements et retraits) ;
- enfin, le GIE Carte Bleue et la société Europay France gèrent les passerelles informatiques vers les réseaux internationaux (Carte Bleue pour Visa et Europay France pour Mastercard).

Graphique n° 2
L'intérêt commun et la concurrence dans le système « CB »



Source : Groupement des Cartes Bancaires « CB ».

En créant la carte « CB », les membres du Groupement ont développé un moyen de paiement universel, économique, et sûr qui concourt au progrès économique et bénéficie à toutes les parties prenantes :
- le *porteur* apprécie la simplicité d'utilisation, l'universalité de l'instrument de paiement, et le choix offert entre débit différé, immédiat ou à crédit sur son compte courant (un « baromètre » de la Sofres montre que le niveau de satisfaction des titulaires de cartes atteint... 98 %, chiffre confirmé d'année en année) ;
- le *commerçant* bénéficie d'un paiement irrévocable, garanti, assorti d'une gestion simplifiée. Les points d'acceptation sont très variés, allant du commerce de proximité aux hyper et supermarchés, en passant par les péages d'autoroute et la télévision à péage. Les automates de paiement connaissent un essor important (distribution de carburant, RATP, SNCF, parkings). Enfin, le « décollage » des opérations de commerce électronique sur Internet constitue un axe fort de développement. Le Groupement a pris l'initiative d'instaurer une concertation permanente et approfondie avec la plupart des instances parties prenantes de la monétique :
  • Mercatel, pour les grands commerces et la distribution ;
  • Acsel et Fevad pour le paiement sur Internet ;
- le *système bancaire,* avec la carte bancaire, facilite la circulation fiduciaire via les distributeurs de billets et contribue à la baisse des coûts de gestion des opérations de paiement, tout en développant de nouveaux services ;
- les *industriels de la monétique*, regroupés dans le cadre de l'AFPC (Association des fabricants et personnalisateurs de cartes) et du « Concert » pour les industriels des terminaux et DAB, pionniers de la technologie du microprocesseur en France, ont, grâce à « CB », acquis une expérience précieuse et se sont développés de manière très importante dans le monde entier : beaucoup jouent un rôle de tout premier plan dans la conquête de nouveaux marchés de terminaux et de cartes à microprocesseur.

La quasi universalité d'acceptation des cartes, avec des modes opératoires différents et donc des niveaux de sécurité différents, exige une grande rigueur dans le développement de règles et de standards adaptés à chaque environnement. C'est là une mission essentielle du Groupement, qui s'insère dans un contexte international. Car la maîtrise des standards, tout particulièrement au plan sécuritaire, est une donnée essentielle et stratégique pour les systèmes de paiements par cartes.

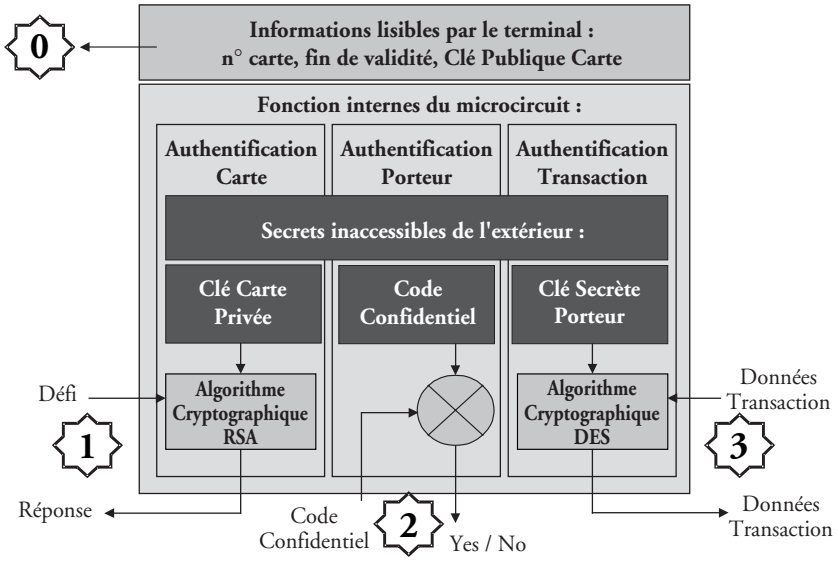
L'importance économique que revêt le système de paiements « CB » justifie l'attention qu'y portent de grandes institutions qui concourent à la cohésion et à la sécurité de ce système :

- *le Secrétariat général de la défense nationale* a ainsi classé le site de production du GIE, en « point sensible » et le réseau d'autorisations e-rsb en « infrastructure d'importance vitale ». Le Groupement « CB » a, en conséquence, pris les mesures adéquates de protection physique de son site et de contrôle d'accès à ses locaux ;
- *la Banque de France* s'assure de la sécurité des moyens de paiement et de la pertinence des normes applicables en la matière. Pour l'exercice de ces missions, la Banque de France procède aux expertises et se fait communiquer, par l'émetteur ou par toute personne intéressée, les informations utiles concernant les moyens de paiement et les terminaux ou les dispositifs techniques qui leur sont associés. Présidé par le Gouverneur de la Banque, un Observatoire de la sécurité des cartes de paiement, regroupe des parlementaires, des représentants des administrations concernées, des émetteurs de cartes de paiement et des associations de commerçants et de consommateurs. Il assure, en particulier, le suivi des mesures de sécurisation prises par les émetteurs et les commerçants, l'établissement des statistiques de la fraude et une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. L'observatoire établit chaque année un rapport d'activité remis au ministre chargé de l'économie, des finances et de l'industrie et transmis au Parlement. Le Groupement des Cartes Bancaires informe régulièrement la Banque de France des évolutions sécuritaires du Système « CB » et des dispositifs de couverture des risques mis en place ou à l'étude. Il lui transmet chaque année les statistiques de la fraude. Par ailleurs, la Banque de France participe, en tant qu'observateur, au Conseil de direction du Groupement des Cartes Bancaires ;
- *la Direction du Trésor,* au Ministère de l'Economie, des Finances et de l'Industrie, est également proche du système «CB» ;
- *les divers services spécialisés du Ministère de l'Intérieur* et notamment l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) assurent au Système « CB » le niveau de protection requis par les circonstances.

LES DISPOSITIFS SÉCURITAIRES AU CŒUR DU SYSTÈME « CB »

Les cartes « CB » sont équipées d'un microcircuit qui contribue à la sécurité de la transaction par trois mécanismes d'authentification :

Graphique n° 3
Les fonctions de la carte à microcircuit



Source : Groupement des Cartes Bancaires « CB ».

Phase 1 : en début de transaction, le terminal commence par authentifier la carte en lui lançant un défi. Seule une carte authentique peut relever le défi grâce à son premier secret.

Phase 2 : le terminal demande ensuite à la carte d'authentifier le porteur : il présente à la carte le code confidentiel que le porteur a frappé au clavier. La carte le compare avec son second secret, la vraie valeur du code confidentiel, et répond au terminal par oui ou non. La carte n'autorise que trois essais et mémorise les essais négatifs.

Phase 3 : le terminal demande à la carte de signer la transaction avec son troisième secret. Si la transaction donne lieu à une demande d'autorisation, l'émetteur vérifie cette signature en temps réel.

Par mesure de sécurité, les secrets sont différents dans chaque carte. Les « clés maîtresses » auxquelles se rattachent les secrets présents dans les cartes sont les plus importantes du système « CB ». Elles n'existent que dans des « boîtes noires » hautement sécurisées.

Le Groupement « CB » opère le réseau de routage des autorisations, dénommé e-rsb (Réseau électronique de services bancaires) qui vient d'être totalement rénové pour acheminer des flux toujours croissants, dans un environnement hautement sécurisé (cryptographie au meilleur niveau - à l'état de l'art -, architecture basée sur le protocole IP).

Le cœur du dispositif de chiffrement du réseau a, en particulier,

donné lieu à une évaluation sécuritaire par la Direction centrale de la sécurité des systèmes d'information (DCSSI).

Le réseau achemine en temps réel les « demandes » d'autorisation en provenance des terminaux de paiement et des DAB vers les « serveurs » d'autorisation des banques émettrices et retransmet les réponses de ces derniers aux terminaux/DAB « demandeurs ».

Le temps de transit, aller-retour demandes-réponses, dans le réseau est inférieur à 2 secondes.

Le réseau est connecté à la totalité des membres « CB », mais également à Visa et Mastercard pour garantir l'interopérabilité, partout dans le monde.

28 % des transactions de paiement (montant généralement supérieur à 100 €) et 100 % des transactions de retrait DAB font ainsi l'objet d'une autorisation de l'émetteur en temps réel, 24h/24.

Le réseau e-rsb voit transiter actuellement plus de 8 millions d'opérations par jour (2/3 en paiement, 1/3 en DAB) et est dimensionné pour faire face à des « pointes » horaires et journalières spectaculaires, comme les samedis de décembre en particulier, et ce dans des conditions de performance, de disponibilité et de sécurité élevées.

LES ÉVOLUTIONS TECHNOLOGIQUES, FACTEUR DE MAÎTRISE DES RISQUES

La communauté bancaire « CB », en fonction de l'évolution des typologies de fraude, fait évoluer en permanence ses référentiels techniques et sécuritaires dans le but de renforcer la sécurité du système « CB ».

À titre d'exemple, à partir de l'année 2006, la nouvelle génération de microprocesseurs qui met en œuvre un processus d'authentification « dynamique » rendra impossible les contrefaçons partielles de cartes à puce (appelées Yescard).

La maîtrise des évolutions technologiques s'articule autour de trois étapes :

- la définition de standards et de cibles de sécurité ;
- la mise en œuvre d'une méthode et d'un système d'évaluation sécuritaire ;
- un système d'agrément des produits et des processus monétiques.

Le Groupement définit des standards techniques fonctionnels et sécuritaires, pour les cartes, les ateliers de fabrication et de personnalisation, les terminaux, les distributeurs de billets.

En ce qui concerne les cartes où il s'agit tout particulièrement de protéger les secrets de la carte : code secret et clés cryptographiques, les exigences de sécurité, regroupées dans une « cible de sécurité », sont

extrêmement élevées : les cartes doivent pouvoir résister à toutes les attaques connues. Ces spécifications sont communiquées aux industriels concernés.

Le Groupement a choisi d'avoir recours à une méthode d'évaluation basée sur un standard international de sécurité : « les critères communs ». Ce processus d'évaluation s'appuie sur des laboratoires indépendants, totalement extérieurs au Groupement, dûment accrédités par la Direction centrale de la sécurité des systèmes d'information (DCSSI), sous l'égide du Secrétariat général de la défense nationale, dans le cadre du Schéma national de certification.

Le système « CB » a été un des tout premiers acteurs ayant activement contribué à l'émergence du Schéma national de certification au sein duquel se mettent maintenant en place de puissantes synergies avec d'autres types de cartes (carte nationale d'identité...) dans le cadre d'une méthode internationalement reconnue ; c'est là un élément central de la confiance dans le moyen de paiement.

En ce qui concerne les aspects fonctionnels, le Groupement dispose d'un laboratoire certifié ISO9001, où, avant de prononcer l'agrément formel des cartes et terminaux, il procède à des milliers de tests pour vérifier leur conformité aux spécifications, gage de bon fonctionnement des différents processus.

LA GESTION DES RISQUES DANS LE SYSTÈME « CB »

Les risques d'image

L'importance des opérations par carte « CB » est telle que le risque d'image et de perte de confiance est sans aucun doute le plus important. En effet, la logistique bancaire dans le domaine des moyens de paiement est centrée sur la carte et demanderait des délais et des moyens très importants pour pouvoir faire face à un report vers d'autres moyens de paiement, comme le chèque par exemple, en cas de détournement de la clientèle suite à une perte de confiance sur la carte. Ils sont intégrés dans l'analyse des risques majeurs, exposés plus loin.

Les risques opérationnels

Selon la définition du Comité de Bâle, « [...] il s'agit des risques de pertes résultant de carences ou de défauts attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs. La définition inclut le risque juridique [...] ».

En simplifiant, les risques opérationnels peuvent être classés en deux grandes familles :

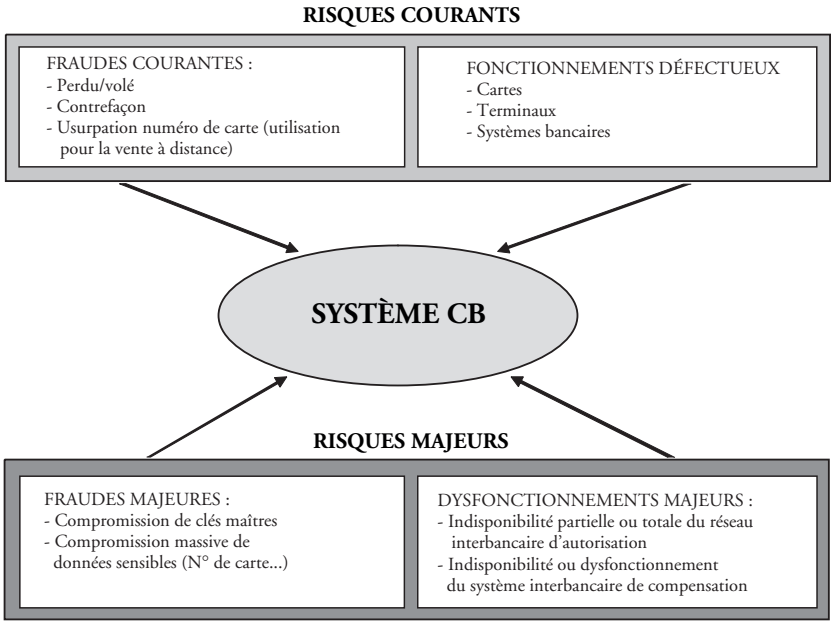
- ceux qui affectent la qualité de service offerte aux clients du système (porteurs et commerçants) ;

- ceux qui affaiblissent la sécurité du moyen du paiement et augmentent potentiellement la volumétrie de la fraude.

Dans ces deux familles, on distingue :

- *les risques courants,* inhérents à l'activité mais avec un impact limité sur le système « CB » (la fraude « courante » constatée quotidiennement et liée aux cartes perdues/volées, contrefaites, numéros utilisés sur Internet...) ;
- *les risques majeurs* (ou exceptionnels) qui ont une probabilité de survenance très faible et un impact potentiellement très fort sur le système « CB » (cassage d'une clé maître, indisponibilité du réseau d'autorisation interbancaire, compromission massive de données « carte »...). La survenance de ces risques peut porter atteinte à l'image du système « CB » et entamer la confiance des utilisateurs à l'égard de ce moyen de paiement.

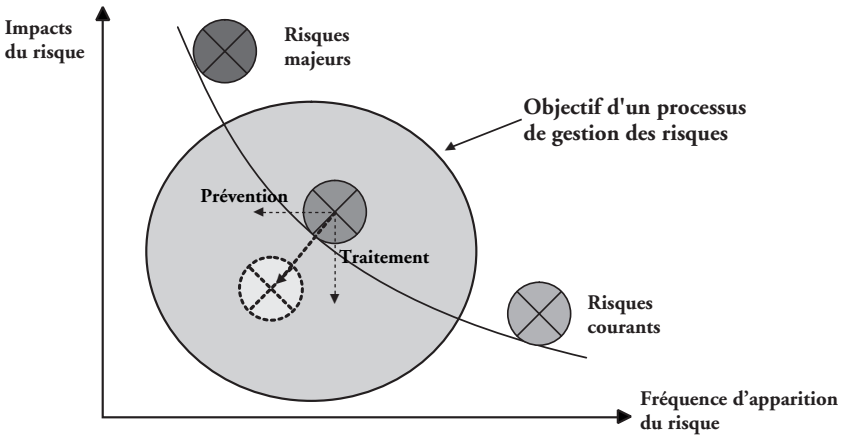
Graphique n° 4
Risques sur le Système CB



Source : Groupement des Cartes Bancaires « CB ».

Il est donc impératif de structurer une politique efficace de gestion des risques qui consiste, pour chaque risque identifié, à prendre des mesures préventives dans le but de diminuer la probabilité de survenance et à anticiper des mesures de correction afin de limiter les impacts sur le système en cas de survenance du risque.

Graphique n° 5
Processus de gestion des risques



Source : Groupement des Cartes Bancaires « CB ».

Les risques courants : la lutte contre la fraude

En aval des dispositifs proactifs techniques de sécurité tels que présentés plus haut, la lutte contre la fraude implique une coopération active des acteurs bancaires dans le système : ce n'est jamais, en effet, - et ce ne peut être - une source de compétition entre les établissements.

La très grande amplitude de l'acceptation des cartes par de multiples acteurs impose à tout établissement partie prenante du système d'informer et d'être informé sur tout incident en matière de fraude.

Quelle que soit sa taille, aucun établissement ne peut efficacement lutter seul contre la fraude.

Une composante centrale du dispositif est constituée par le Système d'information communautaire (SICB) : pour combattre la fraude efficacement, il faut la connaître.

La communauté « CB » s'est donc organisée de manière à ce que chaque émetteur de cartes déclare au SICB, l'intégralité des transactions frauduleuses sur ses cartes.

La fraude est liée à l'utilisation de cartes par un tiers qui n'est pas le porteur légitime : cartes perdues/volées/contrefaites ou dont le numéro est utilisé sur Internet et en vente à distance à l'insu du porteur et sans que celui-ci ait été dépossédé de sa carte.

Les déclarations de fraude au SICB sont très détaillées, précisant le mode opératoire exact de la transaction ainsi que les informations sur le commerce ou le distributeur de billets où a eu lieu l'opération.

Par ailleurs, le SICB enregistre les déclaratifs de fraude en France

avec les cartes des banques émettrices de cartes Visa et Mastercard à l'étranger : l'intégralité de la fraude se produisant en France est ainsi répertoriée dans cette base de données.

Le SICB consolide alors l'ensemble de ces informations et permet ainsi de faire émerger et détecter les points de concentration de fraude pour lesquels une action de surveillance et de suivi particulier va être engagée par la banque « acquéreur » qui gère le compte du commerce ou le DAB ainsi détecté.

Il existe, en outre, une équipe d'enquêteurs au GIE « CB » qui travaillent en étroite coopération avec les divers services de police et de gendarmerie. Dans certains cas (fraude récurrente, comportements manifestement frauduleux de la part de certains commerces, attaques ciblées sur des DAB...), le travail de liaison quotidienne du GIE avec la police aboutit à des interpellations et à la mise hors d'état de nuire des fraudeurs.

Le relais est ensuite pris au plan juridique : dans des affaires importantes (collusion de plusieurs commerces, réseaux de fraudeurs), le GIE coordonne les dossiers, se constitue partie civile pour le compte de ses membres, mais également pour le compte de banques étrangères non membres « CB », lorsque celles-ci sont victimes de fraude sur leurs cartes en France. À cet égard, il convient de noter que ce type d'action de la part du GIE n'a pas d'équivalent en Europe ou même dans le monde. La présence, dans les dossiers de contentieux, de l'intégralité de la fraude perpétrée par tous les types de cartes (CB, Visa, Mastercard) permet de conduire à des jugements exemplaires et à des recouvrements de fonds qui vont, dans certains cas, jusqu'à être rétrocédés aux banques étrangères non membres de « CB ».

Le durcissement de la législation en France sur la contrefaçon de moyens de paiement est aussi une conséquence positive de ces actions en justice systématiques de la part du GIE.

Par ailleurs, l'exploitation au quotidien des données du SICB permet de détecter les cartes dont l'utilisation frauduleuse est la plus importante et d'établir automatiquement des « listes noires », reprenant les numéros de ces cartes, qui seront téléchargées dans les terminaux de paiement des commerçants dans un délai de 24 heures. Cette action permet de stopper très rapidement les cartes utilisées pour des montants faibles « *off line* » (c'est-à-dire sans demande d'autorisation en temps réel).

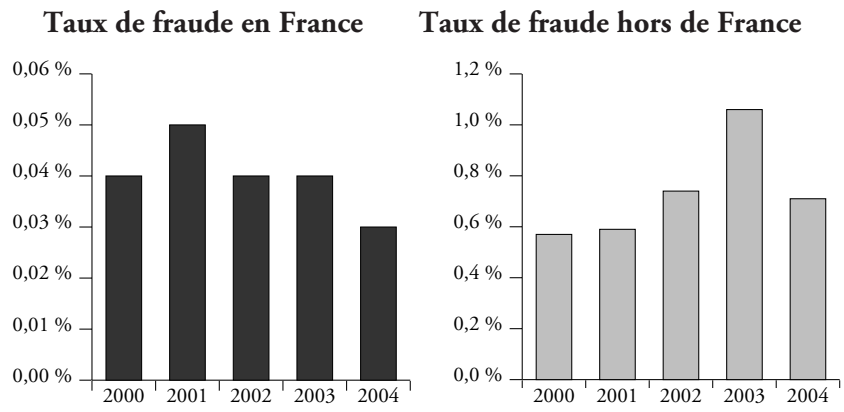
Enfin, le Système d'information produit des indicateurs globaux chiffrés sur la fraude qui permettent de suivre les évolutions des différents types d'opérations et constituent donc une base de réflexion irremplaçable pour anticiper sur les fraudeurs : définition de mesures préventives, évolutions de la composition (capacité, type de fraude...) de listes noires, détection précoce de « points de compromission »

(commerces et/ou DAB où la piste magnétique des cartes est copiée pour utilisation ultérieure à l'étranger, mises en alerte sur certains numéros de cartes...).

L'ensemble de ces actions a pour résultat un taux de fraude limité à 0,03 % du montant des paiements réalisés dans le système « CB », taux parmi les plus bas constatés dans les différents systèmes de paiements.

Ce taux est toutefois plus élevé pour l'activité hors de France :

Graphique n° 6
Taux de fraude en paiement des cartes « CB »



Source : Groupement des Cartes Bancaires « CB »

Ces graphiques démontrent la pertinence des choix technologiques sur la carte à puce effectués il y a 15 ans par la communauté « CB ». En effet, en France, en dehors des paiements en vente à distance, toutes les transactions de paiement et de retrait mettent en œuvre la « puce » des cartes « CB » ; a contrario, à l'étranger, c'est encore la piste magnétique des cartes « CB » qui est très majoritairement utilisée.

La migration vers la technologie « puce » est un facteur déterminant de réduction de la fraude. Elle est en cours en Europe, où l'on voit déjà ses premiers effets, mais elle est encore en devenir dans d'autres régions du monde, voire non décidée, comme aux États-Unis.

La gestion des risques majeurs

Pour chaque processus sensible du système, le Groupement des Cartes Bancaires identifie les évènements dont la survenance ferait dévier un processus de son objectif initial, évalue la probabilité

d'occurrence et/ou la complexité de réalisation de l'évènement, quantifie l'impact de l'événement sur le système (volumétrie de la fraude, niveau d'indisponibilité de service : impacts sur les porteurs et les commerçants, risque juridique...).

Ce travail de cartographie et d'identification et de valorisation des risques est documenté, révisé tous les ans pour tenir compte de l'évolution de l'environnement réglementaire et technique du système « CB » et de l'apparition de nouvelles menaces.

La démarche de couverture des risques majeurs s'articule selon deux axes :

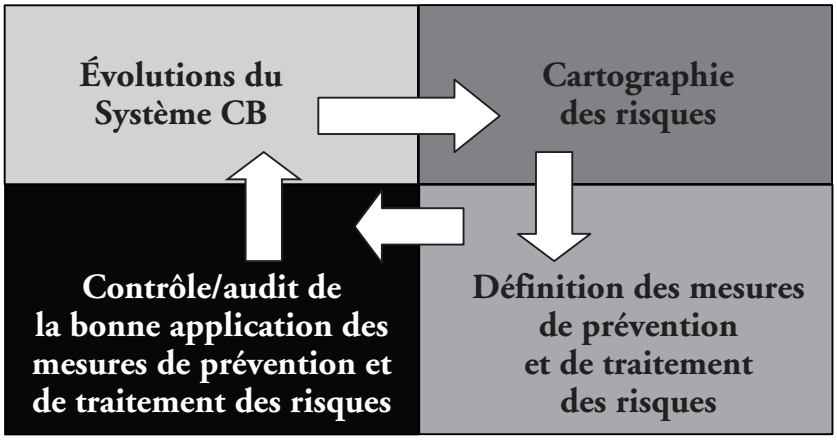
- *la prévention pour réduire la probabilité de survenance des risques majeurs*[2]. La prévention des risques majeurs s'appuie sur la définition et/ou l'évolution de règles à même de réduire l'occurrence du risque, ainsi que sur le contrôle de l'application des règles (élaboration de référentiels de contrôle et d'audit). Des audits ciblés (Inspections générales des banques, Service audit du Groupement « CB »...) permettent de contrôler la bonne application et d'apprécier l'efficacité des règles ; il existe enfin un suivi de la mise en œuvre des actions de correction ;
- *le traitement pour limiter l'impact si le risque survient effectivement.* Sur le système « CB », les impacts potentiels liés à la survenance d'un risque majeur sont estimés, il est donc possible d'apprécier les effets sur le système de telle ou telle mesure corrective. Le traitement des risques majeurs s'appuie sur les étapes suivantes :

- la détection des risques, par des capteurs et des indicateurs dont l'évolution est révélatrice de la survenance ou de l'augmentation de la probabilité d'apparition d'un risque majeur. Des procédures d'escalade sont prévues pour déclencher à bon escient la réunion d'une cellule de crise ;
- la réaction face à la survenance d'un risque nécessite l'organisation d'une cellule de crise opérationnelle. Elle prend en charge l'analyse des impacts (sur les utilisateurs du système, pertes financières, risque de détérioration de l'image du système...) ainsi que les mesures correctives envisageables (plans de secours, plans de continuité d'activités, plans de communication de crise...). Un organe de décision est chargé de valider les mesures de réactions proposées par la cellule de crise. Enfin, des mécanismes de couverture financière des risques (fonds propres en application de la Directive européenne sur l'adéquation du capital et des exigences Bâle II, assurances...) sont en place ;
- le contrôle de l'existence et de l'efficacité des mesures de traitement par l'intégration, dans les objectifs de contrôle interne ou d'audit, de la vérification de l'existence et de l'efficacité des plans de secours

qui doivent pouvoir être activés en cas de survenance d'un risque (existence a priori des moyens de réaction - tests réguliers de l'efficacité de ces plans).

En résumé, le cycle de vie d'un processus de gestion des risques s'analyse comme suit :

Graphique n° 7
Cycle de vie du processus de gestion des risques



Source : Groupement des Cartes Bancaires « CB ».

Les mécanismes de couverture des risques majeurs des différents domaines du système « CB » sont documentés dans des Plans de prévention et de secours, par exemple :
- Plan de prévention et de secours du risque majeur de compromission de clés du système ;
- Plan de prévention et de secours du risque majeur de compromission massive de données sensibles (numéros de carte, données présentes sur les pistes magnétiques des cartes...) ;
- Plan de prévention et de secours du risque majeur d'indisponibilité du réseau d'autorisation e-rsb.

Le système « CB » s'est structuré pour offrir à l'ensemble des partenaires, porteurs de cartes, commerçants et banques, un service de grande qualité et offrant un haut niveau de sécurité.

Cette réussite est notamment attestée par les résultats d'études spécifiques de la Sofres, qui, année après année, confirment une grande satisfaction des utilisateurs de cartes « CB ».

Au cœur des missions du système se trouve l'impératif de sécurité

attaché aux moyens de paiement, garant de la confiance. Cet objectif est d'autant plus stratégique que la volumétrie des opérations par carte « CB » a dépassé, en France, celle du chèque et occupe le premier rang en Europe.

La sécurité repose sur de nombreux facteurs, techniques, organisationnels et réglementaires, et nécessite la mise en place d'indicateurs pertinents et de dispositifs d'audit et de contrôle.

En ce qui concerne les aspects techniques, la sécurité doit faire appel à des technologies au meilleur niveau - à l'état de l'art - et tout particulièrement dans le domaine des microprocesseurs où les cycles industriels liés à l'apparition de nouvelles gammes de produits sont de plus en plus rapides. Il en est de même pour la définition de standards.

La sécurité nécessite, en conséquence, une forte anticipation stratégique, ce qui a amené « CB » à se doter d'une Direction du « *risk management* et de l'audit », cette démarche étant particulièrement novatrice dans le monde des systèmes de paiements.

Le système étant structurellement ouvert à l'international doit s'organiser pour gérer les risques inhérents à l'acceptation des cartes dans des environnements significativement différents et contrastés, notamment dans le monde du commerce électronique et dans les nombreux pays n'ayant pas encore migré à la technologie de la puce.

Cette diversité impose de définir des standards internationaux, permettant de garantir l'interopérabilité et un niveau de sécurité élevé, même dans des environnements différents. À cet égard, l'ouverture d'un espace européen de paiement, dont les perspectives sont tracées par l'EPC (European Payment Council) et appelé de ses vœux par la Commission européenne constitue une opportunité unique.

La maîtrise des standards est un enjeu tout à fait stratégique, afin de préserver les investissements très importants qui sont actuellement consentis dans toute l'Europe pour migrer l'ensemble des systèmes à la technologie « puce », alors que d'autres régions sur la planète, et non des moindres (États-Unis), restent à l'écart.

Le cadre général défini par l'EPC en septembre 2005 (Single Euro Payment Area Card Framework) présente les grandes lignes d'architecture de cet espace des paiements européens, pour lequel la Banque centrale européenne en tant que régulateur, veillera au niveau de sécurité.

De ce point de vue, les hauts niveaux d'exigence sécuritaire demandés et obtenus en France dans le développement de cartes à puce de plus en plus sécurisées ne devraient en aucun cas être affaiblis dans le cadre de cet espace européen.

Bien au contraire, les perspectives de développement, eu égard aux volumes en cause, doivent permettre de concilier haute sécurité, qualité

et universalité du service, avec l'impératif de confiance sur lequel repose tout moyen de paiement.

L'organisation de la sécurité et la gestion du risque, telles qu'elles ont été mises en œuvre dans le système « CB » ont produit, à cet égard, des résultats particulièrement positifs, dont on pourrait s'inspirer pour la maîtrise des risques systémiques au niveau européen.

Seront ainsi réunies les conditions d'un réel progrès économique, offrant à toutes les parties concernées un moyen de paiement spécialement performant dans toutes ses composantes.

NOTES

1. SEPA : Single Euro Paiement Area - Espace unique de paiement en euros.

2. L'estimation théorique de la probabilité de survenance d'un risque majeur est très difficile, voire le plus souvent impossible à déterminer. L'objectif se limite donc à diminuer une probabilité (inconnue) dans une proportion également non quantifiable.