# FRAUDE A LA CARTE BANCAIRE ET PAIEMENT EN LIGNE : QUELLE GARANTIE DE SECURITE ?

**Sokrou Adélaïde GAKOUE**
Docteure en Droit privé et sciences criminelles

**Citation de l'article :** A. Gakoué, « Fraude à la carte bancaire et paiement en ligne : quelle garantie de sécurité ? », D^oc Publication, Les Editions de l'Immatériel, 2017, pp. 64-74.

## Résumé

L'évolution constante du commerce, le développement des techniques de fraudes et techniques de falsification ont considérablement modifié le cadre des pratiques liées à l'utilisation de la carte bancaire. Dans le même temps, les efforts de protection techniques et juridiques du titulaire de la carte-victime de fraude, ont été identifiés et analysés. De nouvelles infractions et un renforcement de la sécurité des paiements à distance notamment sur internet ont été instaurés. En complément, le législateur a élargi le périmètre d'opposition au paiement en cas d'utilisation frauduleuse de la carte bancaire. Toutefois, une sensibilisation renforcée des porteurs de carte est nécessaire pour garantir la sécurité des paiements en ligne.

## Abstract

*The constant evolution of trade, the development of the techniques of frauds and of forgery considerably modified the frame of the practices bound to the use of bank cards. Thus, the technical and legal efforts to protection the card's holder - the victim of fraud, were identified and analyzed. New criminal sanctions and a strengthening of the safety of the remote payments especially on the Internet were established. In addition, the legislator expanded the perimeter to report and cancel a bank card in case of fraudulent activity. However, a raising awareness for the cardholders is necessary to guarantee the security of online payments.*

## Article

La carte bancaire[1] est à l'heure actuelle l'instrument de paiement le plus utilisé dans les pays développés[2] aussi bien dans le quotidien des personnes[3] que pour les paiements en ligne. Avec l'essor des nouvelles technologies et son pendant le commerce électronique, cette évidence est encore plus prononcée au point de s'imposer à nous comme le futur mode normal d'échange[4]. La virtualité totale des échanges et des paiements e-commerce n'est pas sans risque, et fait partie intégrante de ce que l'on appelle le paiement instantané ou l'*instant payment*. Conjuguant de fait la rapidité des autorisations en temps réel des cartes et la disponibilité instantanée des fonds, les paiements instantanés constituent donc des canaux de profit pour les fraudeurs[5].

Les faiblesses des systèmes actuels de paiement en ligne sont réelles[6] et préoccupantes. Les fraudes demeurent nombreuses [7]malgré les constantes améliorations techniques.

En 2016, la fraude sur l'ensemble des moyens de paiement scripturaux émis en France s'est élevée

à 800 millions d'euros, et, la carte bancaire représente la moitié de ce montant[8]. Aujourd'hui la moitié des fraudes aux cartes de paiement se fait sur internet[9].
La fraude à la carte bancaire à des conséquences économiques et sociales particulièrement importantes. Selon le FBI, les virus, les intrusions sur les réseaux et autres incidents relatifs à la sécurité coûtent chaque année 70 milliards d'euros aux entreprises américaines.
Cet état de fait nous interpelle sur l'existence de moyens de paiement adéquats et surtout sécurisés[10].
Cette exigence de sécurité est d'autant plus marquante lorsqu'il s'agit du commerce sur internet[11], paradoxalement la moins protégée et, pourtant, en plein essor.
Ainsi, il paraît essentiel d'identifier d'abord efforts de protection techniques du titulaire de la carte bancaire contre les risques de fraude en ligne (I), pour ensuite analyser les dispositions protectrices en vigueur (II) susceptibles de garantir la sécurité de paiement sur Internet.

## I. Des moyens techniques de protection diversifiés mais limités

Il existe une pluralité de risques (vulnérabilités) de dérober une carte bancaire sur internet, par exemple, un risque d'interception[12] ou de modification par un tiers non autorisé des informations échangées, d'usurpation d'identité d'un utilisateur autorisé, de sabotage ou de détournement de site Internet[13]. L'une des mesures aujourd'hui connue et pratiquée est la cryptologie[14]. Elle constitue un gage de sécurité pour l'utilisation de la carte bancaire en ligne. Pour prévenir le vol des données de carte bancaire lors des paiements en ligne, la communication des identifiants bancaires figurant sur la carte du titulaire doit s'effectuer selon un mode sécurisé : la cryptographie[15]. Les moyens de cryptologie vont permettre la vérification de la justesse et de l'authenticité des données transmises tout en garantissant la confidentialité par le chiffrement des informations.
Les protocoles d'authentification à distance doivent nécessairement être améliorés afin de prévenir les cas de fraudes, l'authentification étant l'élément essentiel tendant à préserver la sécurité des paiements par carte bancaire en ligne.
L'utilisation de la carte à microprocesseur, encore appelée « *carte à puce* » ou « *carte à mémoire* » semble être la solution la plus satisfaisante puisque sa puissance contribue à améliorer la précision de la procédure d'identification du porteur et effectue des autorisations *off line*, hors réseaux[16]. Le principal atout de ce procédé est la protection de l'ordre de paiement par le système SET (Secure Electronic Transaction)[17], appelé à remplacer, par ailleurs, le système SSL (Secure Socket Layer)[18]. Dès lors, il apparaît comme un moyen de paiement sécurisé puisqu'il procède à l'authentification de l'émetteur de l'ordre de paiement et de son bénéficiaire. Par ailleurs, sa fonction de scellement du contenu de la transaction permet d'exclure, en principe, toute possibilité de contestation du montant payé. Enfin, il a une fonction de chiffrement, gage de confidentialité des transactions financières[19].

Cependant, l'utilisation des cartes à puce dans le cadre d'Internet a conduit les banques françaises à harmoniser leur stratégie de paiement par la création d'une société nouvelle « *e-comm* ». Pour éviter l'envoi de données bancaires sur les réseaux, l'adoption du couplage d'un lecteur de carte à puce avec l'équipement d'accès à Internet s'est imposé[20].
Ce faisant, le cryptogramme visuel[21], la demande de renseignement (AVS address vérification System)[22], la carte virtuelle dynamique (e-carte bleue)[23]et le dispositif "*3D secure*"[24]protocole de sécurité renforcé des paiements en ligne par carte bancaire[25] représentent une garantie d'authentification donc de sécurité qui évite l'utilisation d'une carte bancaire à l'insu de son véritable

propriétaire. De plus, le code fourni par la banque et non par le site de commerce en ligne protège l'éventuel détournement des identifiants par intrusions informatiques. L'inconvénient majeur réside dans le fait que peu de sites de commerce en ligne sont équipés de ce mécanisme[26]. Par conséquent, les risques de fraudes subsistent.
Précisons que les commerçants non équipés de ce dispositif supportent la fraude et pas les banques[27].

## II. Le renforcement de la protection des utilisateurs des cartes bancaires comme parade à la fraude

La loi n° 2001-1062 du 15 novembre 2001 apporte deux sortes de précision. D'une part, l'article L. 132-2(abrogé), prévoyait l'irrévocabilité des paiements[28], mais aussi des exceptions prenant la forme de cas d'opposition. C'est ainsi que l'utilisation frauduleuse des données liées à l'utilisation de la carte a été instituée comme nouveau cas d'opposition. D'autre part, la loi est venue encadrer les effets civils de la contestation d'une opération de paiement réalisée « *en ligne* », telle l'irresponsabilité du titulaire d'une carte lorsque le paiement en question avait été « *effectué frauduleusement, à distance, sans utilisation physique de sa carte* »[29]. La simple contestation écrite du titulaire de la carte d'avoir effectué un paiement ou de retrait suffisait pour que les sommes contestées lui soient recréditées sur son compte par l'émetteur de la carte ou restituées, sans frais, « *au plus tard dans le délai d'un mois à compter de la réception de la contestation* ». Cette contestation devait intervenir dans un délai de 70 jours à compter de la date de l'opération contestée[30], délai pouvant être prolongé contractuellement à 120 jours au maximum[31].
Cette évolution légale a poussé les banques à prévoir des clauses[32] mettant à la charge des commerçants le remboursement des opérations en question.
En matière de paiements « *en ligne* » opérés indûment par un tiers, ce délai de 120 jours sera, d'ailleurs, plus facilement admis. En effet, dans ce cas, on peut légitimement penser que le payeur ne sera pas en mesure de constater, sous un bref délai, le détournement ainsi réalisé.
Une difficulté demeure : le « risque » de la preuve. La question de l'identité de celui qui est au clavier a nécessairement dû être envisagée pour faciliter le commerce électronique et tout ce qui l'accompagne.
La preuve de la régularité de l'autorisation pèse exclusivement sur le banquier[33]. Ce dernier devra prouver que l'ordre émane bien du payeur ou de l'utilisateur[34].
Ainsi, spécifiquement en cas de fraude, l'utilisateur de services de paiement est soumis à une obligation d'information à l'égard de son prestataire aux fins de blocage de l'instrument[35].

Selon l'article L. 133-18 du Code monétaire et financier, lorsqu'une opération de paiement non autorisé est signalée par l'utilisateur conformément aux conditions prévues à l'article L. 133-24[36] du même code le prestataire de services de paiement du payeur doit rembourser « immédiatement » à celui-ci le montant de l'opération non autorisée et, le cas échéant, rétablir le compte débité dans l'état où il se serait trouvé avant l'opération en question. Préalablement, le prestataire peut manifestement souhaiter réaliser quelques vérifications afin de s'assurer qu'il s'agit bien d'une utilisation frauduleuse à la carte bancaire d'autrui et non pas du client. Autre aspect, l'article L. 133-18 ne précise pas le délai de remboursement des sommes contestées par le prestataire tel que le prévoyait l'ancien article[37]. Le banquier n'est donc pas légalement contraint quant au temps dont il dispose pour effectuer des vérifications, comme pour démontrer le cas échéant, sur le fondement

de l'article L. 133-23 du code, que l'opération en question a bien été authentifiée et enregistrée.
Les articles L. 133-19 et L. 133-20 du code monétaire et financier prévoient, un régime spécifique à l'égard des instruments dotés d'un dispositif de sécurité personnalisé[38]notamment les cartes bancaires.
Des solutions particulières sont proposées, en la matière, selon que les opérations aient été passées avant l'« *information-opposition* » ou après cette dernière par le titulaire victime d'une utilisation frauduleuse[39]. Pour les opérations passées avant l'information, le payeur supporte les pertes liées à l'utilisation de cet instrument, jusqu'à l'information[40], dans la limite d'un plafond de 150 euros. En cas d'opérations de paiement non autorisées effectuées sans utilisation du dispositif de sécurité personnalisé, la responsabilité du payeur n'est pas retenue[41]. Cette législation est favorable à l'égard du titulaire de la carte, car sa responsabilité n'est pas retenue contrairement à un paiement contesté suite à l'utilisation frauduleuse à distance sans utilisation physique de ladite carte. Quant aux opérations passées après l'information, suite à la perte, au vol au détournement de l'instrument de paiement ou des données qui lui sont liées, le prestataire de services de paiement à l'obligation de bloquer l'instrument de paiement. En conséquence, le payeur ne supporte aucune conséquence financière découlant des utilisations postérieures à l'information de la banque, hormis s'il a commis des agissements frauduleux[42].

Depuis 2004, y compris pour des faits antérieurs à la loi de 2001, les décisions de justice tendent toujours à protéger le porteur de la carte victime d'une fraude. Ainsi la chambre commerciale affirme « *qu'en cas de paiement intervenu à distance sans utilisation physique de la carte ni saisie d'un code confidentiel (...) il résultait pour la banque l'obligation d'annuler le débit contesté* »[43].
De plus, une jurisprudence de la Cour de cassation rendue en matière de carte bancaire, précise qu'il appartient à l'émetteur de la carte qui se prévaut d'une faute lourde de son titulaire d'en apporter la preuve : le fait que la carte ait été utilisée à l'aide de la composition du code confidentiel est, à elle seule, insusceptible de constituer la preuve d'une telle faute lourde[44]. Par conséquent, la preuve de la négligence grave sera très difficile à établir pour le prestataire de services de paiement. L'exemple fourni par un arrêt du 16 octobre 2012 laisse entendre que cette preuve ne pourra être rapportée que dans des circonstances très particulières[45].
Cependant, au regard de ce qu'on pourrait qualifier d'excès ne risque-t-on pas de légitimer la négligence des utilisateurs voire d'inciter à la fraude ? Cette question reste ouverte[46].

*
* *

Malgré l'alliance des moyens techniques et juridiques protecteurs du titulaire de la carte bancaire, la fraude persiste. Le développement constant du commerce électronique et la multiplication des fraudes ont favorisé le renforcement de la sécurité des pratiques liées à l'usage de la carte bancaire. Ainsi, l'amélioration de la protection des porteurs de carte qui participe au commerce électronique en effectuant des paiements en ligne demeure une priorité législative et jurisprudentielle. Cependant, améliorer l'information des risques que peuvent encourir les cyberconsommateurs reste essentiel pour une sécurisation efficace[47] des paiements via internet et cela au profit de tous.

[1] D'un point de vue juridique, la carte bancaire entre dans la catégorie des instruments de paiement ; destinés à permettre le paiement de créanciers, et plus généralement le transfert de fonds, sans manipulation de monnaie fiduciaire

(billets et pièces). Au sens de l'art. L. 311-3 du C. mon. fin. il s'agit d'un instrument qui permet « à toute personne de transférer des fonds ».

[2] M. ROUSSILLE, La carte bancaire : reine des moyens de paiement, à la destinée juridique tortueuse. Gazette du palais-04/02/2012-n°35 page 7.

[3] En France, la carte bancaire est l'instrument de paiement le plus utilisé en termes de valeur agrégée des transactions (462,3 milliards d'euros) selon la banque de France. 43 % des paiements de détail sont réglés par carte bancaire. BANQUE DE FRANCE [2012], *Rapport annuel de l'Observatoire de la sécurité des cartes de paiement, exercice 2011*, Appendix A5, Table 2.

[4] Le commerce électronique semble atteindre un degré de développement dépassant toute prévision raisonnable. En Europe, de 14 milliards d'euros en 1999, il est passé à 95 milliards en 2000 pour atteindre en 2004, environ, 550 milliards, Vo www.men.minefi.gouv.fr

[5] O. BERNANOSE, L. ROUILLAC., Paiement instantané, fraude en temps réel ? Revue Banque n°808, disponible sur http://www.revue-banque.fr/print/risques-reglementations/article/paiement-instantane-fraude-en-temps-reel

[6] A. DANIS-FATOME, Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement : une nouvelle probatio diabolica ? Revue des contrats - 01/06/2017 - n° 02 - page 270.

[7] J STOUFFLET., Instruments de paiement et de crédit, 8e éd., 2012, LexisNexis, n° 418 ; J MOREL-MAROGER., « La répression des fraudes à la carte bancaire », Gaz. Pal. Rec. 2012, p. 1809.

[8] OBSERVATOIRE DE LA SECURITE DES MOYENS DE PAIEMENT, Premier rapport annuel de l'Observatoire de la sécurité des moyens de paiement, Paris, le 18 juillet 2017 disponible sur : https://www.banque-france.fr/sites/default/files/medias/documents/osmp_rapport_2016_-_communique_de_presse_0.pdf

[9] Z. TUMIN., Les futures techniques de paiement. *L'avenir de l'argent*, 2002.

[10] V. A VALLET., La sécurité des paiements électroniques, Mémoire DEA Contrats civils et commerciaux, 2003-2004, Université de Saint-Quentin-en-Yvelynes.

[11] Aux termes de l'article 14 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique : « Le commerce électronique est l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou services ».

[12] M. ABELS, Le commerce sur internet, moyens de paiement et risques afférents, RDAI 1998, p. 349.

[13] BANQUE DE France, La sécurité des moyens de paiement sur Internet, Bulletin de la banque de France, n° 98, Février 2002.

[14] Définition précisée à l'article 29 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

[15] L'article 29 de la Loi n°2004-575 du 21 juin 2004 dite LCEN précise que les moyens de cryptologie visent à « transformer des données, qu'il s'agisse d'information ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'inverse avec ou sans convention secrète », l'objectif étant de garantir « la sécurité du stockage ou de la transmission des données, en permettant d'assurer leur confidentialité, leur authentification, ou le contrôle de leur intégrité ».

[16] http://www.ciber-comm.m ; Groupements des cartes bancaires-Grands Dossiers (http://www.cartes-bancaires.com ; Mission pour le commerce électronique : Rapport Lorentz, http://www.finances.gouv.fr/lorentz

[17] Visa et Master-Card ont convergé vers une norme commune, SET, qui est une synthèse entre leur Secure transaction technology (STT) et le Secure electronic payment protocol (SEPP), développé notamment par Netscape, IBM et Cybercash. Cette convergence s'est réalisé au début de février 1996.

[18] C'est une application des outils cryptographiques intégrés par défaut à la quasi-totalité des logiciels de navigation. « Le système SSL crée un canal de communication sécurisé entre le serveur du vendeur et l'ordinateur du client, assurant entre eux la transmission cryptée des informations communiquées (numéro facial de la carte de crédit, date d'expiration et le nom du titulaire). Mais, si ce système présente certains avantages (coût réduit, simple d'utilisation, authentification du vendeur, cryptage asymétrique), il a l'inconvénient de ne pas vérifier l'identité du client ». J. DJOUDI, L'internet ou le défi au paiement sécurisé, Gazette du Palais - 31/03/2005 - n° 090 - page 4.

[19] M. ESPAGNON, Le paiement d'une somme d'argent sur internet, JCP éd. G, 1999. I. 131.

[20] *cf.* Lucas de Leyssac C., Lacaze X., Le paiement en ligne, JCP G 2001, I, nO 302.

[21] Composé des trois chiffres, il figure au dos d'une carte bancaire, et est exigé pour les achats effectués en ligne. Cependant, la communication de ces chiffres ne permet pas de savoir si la personne est bien le titulaire de la carte et non un usurpateur.

[22] Consiste à vérifier les coordonnées du titulaire de la carte par l'interrogation de la banque qui a émis la carte. Néanmoins cette technique pose néanmoins le problème de la confidentialité des données personnelles et de la conservation du secret bancaire.

[23] C'est un numéro de carte attribué à l'internaute par sa banque chaque fois qu'il veut régler un achat en ligne. Octroyé de manière aléatoire et à usage unique, il permet d'éviter la circulation de numéros de carte physique et surtout de rassurer les internautes ne souhaitant pas communiquer leur numéro de carte pour des transactions en ligne.

[24] Pour un label européen – certificat n° EP-S-ODS3YQ – délivré aux établissements bancaires utilisant cette technique, v. www.european-privacy-seal.eu.

[25] www.journaldunet.com

[26] En France, le taux de commerçant en ligne équipé du 3D-Secure reste encore assez faible : 43% selon le rapport de l'observatoire de la sécurité des cartes de paiement.

[27] C'est le transfert de responsabilité ou *liability shift* en anglais.
[28] Pour un cas de transmission des mentions figurant sur une carte bancaire ne valant pas ordre de paiement, Cass. com., 24 mars 2009, no 08-12.025, D. 2009, p. 1735, notre Lasserre Capdeville J., D. 2010, p. 1047, obs. Martin D. R., RD bancaire et fin. 2009, no 3, p. 47, obs. Crédot F.-J. et Samin Th., Banque et droit 2009, no 125, p. 21, obs. Bonneau Th.
[29] C. mon. fin., art. L. 132-4.
[30] C. mon. fin., art. L. 132-6 ; Cass. com., 12 nov. 2008, n$^{O}$ 07-19.324, Bull. civ. IV, n$^{O}$ 190, RD bancaire et fin. 2009, n$^{O}$ 1, p. 44, obs. Crédot F.-J. et Samin Th., RTD com. 2009, p. 186, obs. Legeais D., JCP G 2008, II, 10211, note Lasserre Capdeville J.
[31] CA Paris, 19 févr. 2009, no RG : 08/03788, M. Gueye c/ BNP Paribas.
[32] Ces clauses ont été jugées ni potestatives, ni abusives par la Cour d'appel de Paris. CA Pau, 2e ch., 8 janv. 2007, no RG : 04/02285, SARL Caves et épiceries du progrès c/ Société générale, RD bancaire et fin. 2007, no 3, p. 29, obs. Caprioli E., RJDA 2007, n°1274.
[33] Selon l'article L. 133-23 du code, lorsqu'un utilisateur de services de paiement conteste avoir autorisé une opération de paiement qui a été exécutée, sa banque à l'obligation de démontrer que l'opération a été « authentifiée, dûment enregistrée et comptabilisée, et qu'elle n'a pas été affectée d'une déficience technique ou autre ».
[34] De plus, L'alinéa 2 de l'article L. 133-23 dispose que l'utilisation de l'instrument de paiement telle qu'enregistrée par le banquier ne suffit pas nécessairement à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas « satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière ». Cette disposition tend à assurer une bonne protection du payeur.
[35] L'article L. 133-17 du Code monétaire et financier reprend la législation antérieure relativement à cette disposition.
[36] En vertu de l'article L. 133-24 du Code monétaire et financier, l'utilisateur de services de paiement qui constate l'existence, notamment par la consultation d'un relevé de compte, d'une opération de paiement non autorisée doit la signaler « sans tarder » à son prestataire de services de paiement. Dans tous les cas, ce signalement doit intervenir au plus tard dans les treize mois suivant la date de débit sous peine de forclusion. Ce dernier déroge ainsi au principe de l'article L. 110-4 du Code de commerce prévoyant un délai de prescription de cinq ans.
[37] Article L. 132-4 ancien du Code monétaire et financier précisait que « au plus dans un délai d'un mois à compter de la réception de la contestation » les sommes contestées devraient être recréditées ou restituées.
[38] Un moyen technique affecté par un prestataire de services de paiement à un utilisateur donné pour l'utilisation d'un instrument de paiement.
[39] Article L. 133-17 du Code monétaire et financier.
[40] Cette information est imposée par l'article L. 133-17.
[41] L'article L. 133-19 prévoit un certain nombre de cas dans lesquels le payeur est qualifié de totalement irresponsable et, à ce titre, se trouve pleinement déchargé du paiement des sommes débitées avant l'opposition dans la limite de 150 euros.
[42] C. mon. fin., art. L. 133- 20.
[43] Cass.Com 23 juin 2004 n °02-15147, *Banque et droit* 2004 n°97, p.83.
[44] Cass.Com 2 octobre 2007 n°05-19899, *Dalloz*, p.2604, obs. V. Avena-Robardet.
[45] Cass.com.,16 oct. 2012, n°11-19.981, Bull.civ.IV, n°183, JCPE2012, 1680, note S. Piedelièvre, D.2013, p.407, note J. Lassere Capdeville, JCPG 2012, 1202, K. Rodriguez.
[46] Voir en ce sens S. Torck, art. préc., n° 40. Voir égal. S. Piedelièvre, L'ordonnance du15juillet 2009 relative aux conditions régissant la fourniture de services et de paiement, Gaz. Pal. 2009, p. 2820.
[47] Pour la Banque de France, l'efficacité et la sécurité des moyens de paiement scripturaux sont particulièrement importantes, compte tenu de leur usage prépondérant dans les transactions économiques. BANQUE DE FRANCE, La surveillance des moyens de paiement scripturaux : objectifs et modalités de mise en œuvre, Revue de la stabilité financière, n°5, Novembre 2004.