

CARTE BANCAIRE ET SECURITE SUR INTERNET
DEBITS FRAUDULEUX A DISTANCE
LE CREDIT AGRICOLE LOIRE HAUTE LOIRE CONDAMNE A REMBOURSER
TRIBUNAL D'INSTANCE DE SAINT ETIENNE – JUGEMENT DU 24 NOVEMBRE 2011

Aux termes d'un jugement rendu le 24 novembre 2011, le tribunal d'instance de Saint Etienne condamne la Caisse Régionale Loire Haute Loire du CREDIT AGRICOLE (*la Banque*) à rembourser des débits frauduleux effectués à **distance par détournement des données de la carte bancaire**.

Les faits

Les faits relèvent de la pratique devenue relativement banale sur internet : celle du hameçonnage (*phishing*) . Fin juillet 2010, la titulaire de la carte avait, sans se rendre compte du piège qui lui avait été tendu, communiqué les données figurant en clair sur sa carte, en réponse à un message reçu par l'intermédiaire de son fournisseur d'accès habituel (Orange) à savoir : le numéro de la carte , sa date d'expiration et le cryptogramme. Précision importante : elle n'avait pas communiqué son code secret confidentiel.(PIN à 4 chiffres)

A partir des données communiquées, quatre prélèvements frauduleux avaient été effectués dans les jours suivants sur le compte joint du couple, pour un montant total supérieur à 3 000 euros. Leur compte était devenu débiteur, au-delà du découvert autorisé de 1 000 euros De plus la banque avait laissé opérer un débit postérieur à l'opposition !...

La titulaire de la carte avait suivi la procédure affichée sur le site Internet de la banque : elle avait fait opposition, porté plainte et **contesté avoir autorisé ces opérations**. Ses demandes de remboursement, fondées légalement sur les articles L.133-18 et 19 du Code Monétaire et Financier (CMF)et relayées par l'association UFC QUE CHOISIR 43, avaient été systématiquement rejetées par la banque qui lui reprochait sa **négligence**. Le couple découvrait alors que l'assurance **SECURICOMPTE** incluse dans leur bouquet de services baptisé **Compte Service Optimum**, ne couvrait pas ce type de fraude, la carte n'ayant pas été **ni perdue ni volée !....**Il n'avait pas eu alors d'autre choix que d'assigner la banque, devant le tribunal d'instance de Saint Etienne avec l'appui de l'association UFC QUE CHOISIR de la Haute Loire. Cet affrontement judiciaire voulu par la Banque paraissait d'autant plus choquant que sur son site internet elle annonçait clairement : **Les Français sont bien protégés...En France, si les paiements frauduleux ont été réalisés à distance (par correspondance ou internet par exemple).....votre responsabilité n'est pas engagée !...**

Rappel des principes de base de non responsabilité du titulaire de la carte de paiement jusqu'au 1^{er} novembre 2009

Deux situations étaient envisagées :

(a) Les opérations frauduleuses effectuées suite au vol ou à la perte de la carte :

Selon l'article L.132-3 ancien du CMF , pour ces opérations, le titulaire devait supporter la perte avant la mise en opposition, dans la limite d'un plafond de 150 euros, sauf s'il avait agi avec une **négligence constituant une faute lourde**.

Selon une jurisprudence constante, il appartenait à l'émetteur de **rapporter la preuve de la faute lourde**, la Cour de Cassation ayant même adopté une conception très restrictive de la faute lourde en jugeant que la circonstance que la carte ait été utilisée par un tiers **avec composition du code confidentiel** était, **à elle seule**, insusceptible de constituer la preuve d'une telle faute .(Cass. Com. , 2 octobre 2007 ; Civ 1, 28 mars 2008 ; et Com. 21 septembre 2010).

Cette jurisprudence était d'ailleurs en phase avec une recommandation ancienne de la Commission Européenne 97/489/CE du 30 juillet 1997.

(b) Les opérations frauduleuses effectuées à distance, sans utilisation physique de la carte :

Selon l'article L.132-4 ancien du CMF , *la responsabilité du titulaire d'une carte de paiement n'était pas engagée, si le paiement contesté avait été effectué frauduleusement , à distance, sans utilisation physique de la carte.*

Les tribunaux en déduisaient l'obligation pour l'émetteur de recréditer , le montant de toute **opération contestée** dans le délai de l'article L.132-6 (70 jours), sans qu'il puisse en être déchargé en invoquant la **négligence** du titulaire (Cour de Cassation Chambre Commerciale , 12 novembre 2008 : X...c/ BNP Paribas Guadeloupe)

La Cour d'appel d'Angers, dans deux arrêts identiques du 16 décembre 2008 (X...c / Caisse de Crédit Mutuel d'Angers) se fondait sur cet arrêt de la cour de cassation et enfonçait le clou en précisant que la banque , même en cas de **négligence** du titulaire, ne pouvait échapper aux obligations résultant de l'article L.132-4 du CMF , sauf pour elle à établir la **mauvaise foi** du titulaire **en apportant la preuve** qu'il était directement, ou indirectement le **véritable donneur d'ordre**. Il n'était pas question de faute lourde dans cette hypothèse.

La loi actuelle

Le code monétaire et financier dans sa version en vigueur depuis le 1^{er} novembre 2009, à la suite de la transposition de la directive européenne SEPA consacre le principe du droit au remboursement par les prestataires de services de paiement (PSP) dans les hypothèses de perte, vol, détournement ou **toute utilisation non autorisée** de l'instrument de paiement ou **des données qui lui sont liées** sauf **quelques exceptions limitativement spécifiées**.

L'article L.133-19 nouveau du CMF traite toujours différemment :

(a) Les opérations frauduleuses effectuées suite au vol ou à la perte de la carte :

- Avant l'**information** du banquier - le texte ne mentionne plus *l'opposition*, mais nombre de contrats porteur continuent à parler d'*opposition*- le client supporte les pertes dans la limite d'un plafond de 150 €. S'il n'y a pas eu utilisation du dispositif de sécurité personnalisé (le code confidentiel), la responsabilité du client n'est pas engagée, sauf les exceptions légales,
- Après cette information, la responsabilité du banquier est entière.

(b) Les opérations frauduleuses effectuées en détournant à l'insu du payeur, la carte ou les données qui lui sont liées ou en cas de contrefaçon :

- avant l'information du banquier, le client ne supporte aucune perte, sauf les exceptions légales,
- après l'information, la responsabilité du banquier est entière.

Les exceptions légales limitativement énumérées à l'article L.133-19 § IV du CMF, sont dorénavant communes aux cas (a) et (b); elles visent : l'agissement frauduleux du payeur et le non respect intentionnel ou par **négligence grave** des obligations du titulaire, concernant la **garde de ses dispositifs de sécurité personnalisé** et l'**information à donner sans tarder** à la banque afin que celle-ci procède au blocage de la carte.

Au surplus, lorsque l'utilisateur **nie avoir autorisé une opération de paiement**, il incombe au PSP de **prouver** que l'opération a été **authentifiée**, dûment enregistrée et comptabilisée et qu'elle n'a pas été **affectée par une déficience technique** ou autre. (Article L.133-23 du CMF) .

Le délai pour contester les débits frauduleux a été porté de 70 jours à 13 mois ,sauf pour les paiements effectués en dehors de l'Union Européenne où il est ramené à 70 jours.

La question pouvait se poser de savoir si la **négligence grave** dont la preuve incombe, comme avant, aux banquiers devait s'interpréter d'une façon moins restrictive que celle donnée à la **faute lourde** par la jurisprudence antérieure. Il n'en est rien pour le tribunal saisi de l'affaire.

Le jugement du tribunal de Saint Etienne

La décision du tribunal, rendue **plus de 16 mois après les faits** en raison des manœuvres dilatoires de la banque, et qui est, à notre connaissance, l'une des premières rendues sur la base des nouvelles dispositions du Code Monétaire et Financier, se situe dans le droit fil de la loi et de la jurisprudence antérieures. Elle est solidement motivée sous la plume d'un juge fin connaisseur du droit bancaire.

Sur le fond le juge considère que le fait de communiquer des **données qui figurent en clair sur la carte** et qui sont couramment demandées pour toute opération de paiement à distance ne peut s'analyser en une **négligence grave**. Au surplus le code confidentiel n'avait pas été communiqué !....L'aurait-il été, il n'est pas sûr que la décision eût été différente, le texte de l'article L.133-23 nouveau reprenant la formule des arrêts précités de la cour de cassation selon laquelle l'**utilisation** de l'instrument de paiement ne suffit pas nécessairement, **en tant que telle** 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, la charge de la preuve incombant au prestataire de service paiements.

La Banque , qui a fait **une interprétation erronée de la loi**, est donc condamnée à rembourser les débits frauduleux ainsi que les frais et agios consécutifs.

Les attendus sont particulièrement sévères pour la Banque, dont l'attitude particulièrement dilatoire et non conciliante est sanctionnée par des dommages et intérêts conséquents de 1200 euros et 500 euros au titre des frais non couverts par les dépens (article 700 du CPC).

- elle n'avait même pas reconnu ses propres négligences – prélèvement postérieur à l'opposition !...;
- elle avait procédé à l'inscription de l'incident au FICP de la Banque de France ;
- elle avait menacé de prononcer la déchéance du terme sur les autres engagements de ses clients.

L'action en intervention volontaire de l'association UFC QUE CHOISIR 43 est accueillie par le tribunal qui lui alloue l'euro symbolique demandé, ainsi que 500 euros au titre de l'article 700.

Des procédures d'authentification renforcée existent déjà

Le rappel à la loi ainsi adressé par le juge aux prestataires de services de paiement est clair : il leur appartient de mettre en place des verrous efficaces pour **authentifier** les ordres de paiement à distance. Des procédures **d'authentification renforcée** existent déjà, (par exemple : e-carte, numéro unique envoyé par SMS sur le portable du client , 3 D secure etc..)qui permettent des contrôles supplémentaires en complément des données liées à la carte, comme le rappelait une réponse ministérielle publiée au JOAN du 01/02/2011 (Question No 87402).

Suite et fin judiciaire

Prise d'un remords tardif ou doutant du résultat(?) , mais se souvenant enfin, que *le bon sens doit avoir un avenir au CREDIT AGRICOLE*, la Caisse Régionale de la Banque Verte n'a pas fait appel du jugement qui est donc définitif.

Restons vigilants

Bien entendu, ce jugement ne doit pas nous conduire à oublier les conseils de prudence habituels : ne mordons pas aux hameçons en ligne et n'y accrochons pas nos données de carte bancaire et jamais notre code confidentiel. Quant aux **options** censées nous couvrir contre **l'utilisation frauduleuse de nos moyens de paiement**, prenons le temps de lire les **limitations contractuelles** des options labellisées *Sécur* (exclusions, plafonds de garantie ...) avant de payer pour une garantie peau de chagrin. Attention les options ne sont pas toujours à **la carte** mais incluses d'office dans un bouquet de services indissociables. Enfin posons-nous la question de l'utilité réelle de ces assurances dans la mesure où la loi impose aux PSP, de garantir leurs clients dans la plupart des cas. Leur seul intérêt serait-il de rembourser la franchise de 150 euros ?

UFC QUE CHOISIR 43 – Jacques DELAROUÉ – 16 février 2012