CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

ATTENTION AUX FRAUDES AUX DISTRIBUTEURS! QUI EST LE RESPONSABLE?

Avez-vous jamais dû faire un retrait au distributeur et ne clôturer pas l´opération parce que la carte n´est pas lisible ou parce que le service n´est pas disponible, sans récupérer la carte? N´ayez crainte, la banque en est responsable!

di **Teresa Piccirillo**
IUS/04 - DIRITTO COMMERCIALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Sabato 28 Gennaio 2017

CamminoDiritto.it
ISSN 2421-7123

Ce n'est pas rare de faire un retrait au distributeur et ne clôturer pas l'opération parce que "la carte n'est pas lisible" ou parce que "le service n'est pas disponible", sans revoir la carte. N'ayez crainte, si vous avez communiqué l'événement rapidement, en cas de fraude, on tient la banque - maintenant en garde un instrument exposé au public qui a pour objet l'octroi d'argent - pour la responsable de l'événement. La Cour de cassation l'a récemment établi, avec l'**arrêt n. 806 du 19 janvier 2016**, en retenant que le devoir de diligence de l'**article 1176 deuxième alinéa, Code Civil,** doit être proportionné à la nature de l'activité et en particulier à la spécificité du devoir de protection d'un instrument exposé au public, ayant comme objet l'octroi d'argent. Il est évident que la manipulation du distributeur constitue une circonstance qui découle de l'absence de la carte à l'intérieur et de la soustraction et utilisation par des tiers.

1. Le Cas L'espèce en examen de la Suprême Court de Cassation a comme protagoniste un titulaire de compte courant qui s'est rendu près d'un distributeur pour effectuer un retrait et il n'a pas pu parce que la carte était "non lisible" et "le dispositif était hors service", en plus sans recevoir la restitution de la carte.

Le titulaire informait rapidement l'institut bancaire de l'événement, mais il était rassuré et invité à retourner le jour après pour le retirement de la carte. Les jours suivants, des inconnus effectuaient des retraits pour 7.000,00 euro, en allant bien au-delà du plafond journalier et - pourtant - le titulaire s'appelait au jugement de la Banque pour la réparation du préjudice subi. En cours d'instance, on produisait des vidéos par lesquelles on a attesté que le titulaire avait été escroqué par des tiers, en fait les vidéos montraient que, pendant l'opération de retrait de l'acteur, un inconnu s'était approché de lui et, sous prétexte de l'aider, il avait réussi à mémoriser le PIN et, puisque l'instrument était déjà manipulé, il avait réussi aussi à voler la carte. Le tribunal et la Cour d'appel rejetaient les demandes du titulaire, en le dotant lui seulement de la responsabilité pour la perte subie après son acte imprudent, puisqu'il avait tapé le code PIN en présence d'un inconnu. La Suprême Cour de cassation, en revanche, avec l'arrêt n. 806 du 19 janvier 2016, renversait la thèse des juges de première et deuxième instance, en soutenant la Cour d'appel pour la responsabilité exclusive du requérant pour avoir permis l'individuation du code à des tiers et n'avoir pas procédé avec l'arrêt immédiat de la carte, il n'a pas évalué en manière correcte la responsabilité contractuelle de la Banque pour ce qui concerne le **loyer de diligence de l'art. 1176** du code civil, c'est-à-dire pour le retrait bien supérieur à la limite journalière. En omettant l'exécution de cette enquête, la Cour d'appel n'a pas appliqué le paramètre de diligence spécifique mis à la charge de la banque. Selon les juristes: "à fin d'une évaluation de la responsabilité contractuelle de la banque pour l'affaire d'utilisation illicite par des tiers de la carte bancaire retenue du distributeur, face à une explicite demande de la partie, la vérification de l'adoption des mesures appropriées pour la sécurité du service par l'institut bancaire ne peut pas être omise, malgré la non-rapidité de la

CamminoDiritto.it
ISSN 2421-7123

plainte du client et les prévisions règlementaires contraires; en fait, la diligence mise à la charge du professionnel est de nature technique et elle doit être évaluée selon les risques inhérents à la sphère professionnelle à laquelle on se rapporte, en adoptant donc la figure du 'banquier prudent" (le même principe énoncé par la Cassation pour un cas similaire avec l'arrêt n. 13777/07). La Cour, donc, eu égard à ce qui précède, accueille le premier motif de recours et elle casse l'arrêt. **2. D'autres hypothèses de responsabilité de la Banque.**

Un cas similaire avait déjà été traité par la Cour Suprême de Cassation, laquelle avait établi avec l'arrêt n. 13777 du 12 juin 2007 que l'institut bancaire doit se retenir responsable de la défaillance du distributeur et du clonage éventuel de la carte par des tiers. En fait, la banque doit utiliser la plus grande diligence à l'égard de ses clients en adoptant toutes les mesures nécessaires pour éviter des manipulations, donc 'en exerçant une activité professionnelle, la banque doit exécuter toutes les obligations assumées à l'égard de ses clients avec la diligence particulièrement qualifiée du banquier prudent, non seulement pour l'exécution des contrats bancaires, mais aussi en relations aux actes ou opérations expliquées de manière objective... La banque émettrice de la carte est responsable, jusqu'à preuve du contraire, de la mise en place des moyens mécaniques, de leur aptitude et de leur fonctionnement et, cependant, des erreurs dues au dol ou à faute grave'. En dehors du classique cas de fraude consistant dans la soustraction physique de la carte et des habilitations de sécurité du client (c'est-à-dire, user ID, password et PIN), avec le développement de la technologie, ils sont augmentés les cas de criminalité "informatique" qui essaient de profiter des criticités des plateformes bancaires pour en obtenir les identifications et les codes nécessaires pendant les opérations en ligne des dispositions de paiement de la banque.

Parmi les fraudes informatiques les plus diffusées on trouve: Le soi-disant **PHISHING** , c'est - à - dire l'envoi d'un mail qui invite l'utilisateur à visiter le site des banques à travers un lien contenu dans le message du courrier électronique, qui toutefois ne conduise pas au site officiel, mais à son copie créé par le phisher. Le phisher s'approprie des identifiants d'accès de la victime cliente de la banque et il les utilise au détriment de cette dernière. Une autre technique plus complexe, c'est le **TROJAN BANKING** (il rappelle la stratégie du Cheval de Troie d'Ulysse pour entrer dans la populaire ville de l'Asie Mineure) et qui consiste dans la diffusion de virus informatiques qui extorquent les identifiants d'accès aux services bancaires en ligne. Il s'agit de cas particuliers nécessitant une évaluation pour comprendre si l'éventuel acte illicite par des tiers, au détriment de la victime, doit rentrer parmi les responsabilités de la Banque qui contrôle les soi-disant "instruments de paiement" ou la non-diligence du client, auquel on demande d'utiliser l'instrument de paiement selon les modalités prévues par le contrat et de communiquer à la banque, sans délai, sa perte ou soustraction ou utilisation non autorisée par des tiers. L'**arbitrage bancaire financier** s'est occupé de nombreuses affaires et il a adhéré à la

CamminoDiritto.it
ISSN 2421-7123

notion de "**faute grave**" de la Cour de cassation, à fin d'indiquer comme responsable la conduite de ce qui agit avec **extraordinaire et non-excusable imprudence et négligence**, en omettant non seulement la diligence du "bon père de famille", mais aussi le degré minimum de diligence observé par tout le monde, aussi par ceux qui sont "ordinairement négligés". Pour l'ABF, les comportements de faute grave dans l'utilisation des instruments de paiement - et donc des situations dans lesquelles on peut indiquer le client comme responsable de l'événement - sont par exemple: la conservation de la carte avec le PIN; le non garde du sac ou du portefeuille où se trouve la carte; le retard apporté à la dénonce de la perte, du vol ou de l'utilisation non autorisée de la carte et le non-rapide blocage de la carte (la garde diligente comprend aussi le contrôle des comptes); la non-activation des systèmes de sécurité mis à la disposition par la banque; le non-blocage de la carte après l'envoi du soi-disant sms alert; la communication des identifiants et du PIN à des tiers. Ce sont des hypothèses de négligence totale pour les astuces minimales qui sont utilisées pour éviter un événement négatif. C'est clair donc qu'il ne s'agit pas d'intérêts opposés, mais de comportements complémentaires pour la sauvegarde d'un système avancé de paiements où chaque personne doit jouer son rôle, avec responsabilité: la banque doit assurer une technologie d'opération moderne pour prévenir les agressions des tiers; le client, conscient de l'époque où nous vivons - grâce aussi à une information sur les thèmes ici rappelés qui se diffuse très facilement - doit être de plus en plus attentif en utilisant les instruments de paiement proposés comme les plus fiables par les banques qui offrent des services de paiement.
