



COLLEGIO DI BARI

composto dai signori:

(BA) DE CAROLIS	Presidente
(BA) TUCCI	Membro designato dalla Banca d'Italia
(BA) CAMILLERI	Membro designato dalla Banca d'Italia
(BA) APPIO	Membro di designazione rappresentativa degli intermediari
(BA) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ENRICO CAMILLERI

Seduta del 18/10/2018

FATTO

Il ricorrente, intestatario di una carta prepagata rilasciata dall'intermediario, riferisce di aver riscontrato una *mail* apparentemente proveniente da quest'ultimo in data 15/01/2018; al riguardo, fa presente di "*aver fornito le proprie credenziali d'accesso alle operazioni online [dell'intermediario] ad ignoti truffatori, che, a [sua] insaputa hanno disposto un bonifico [del valore di €] 255,00*".

Rappresenta quindi di aver presentato denuncia - oltre che formale richiesta di disconoscimento dell'operazione - il giorno successivo.

L'intermediario afferma che, dall'esame della documentazione versata in atti, emerge chiaramente la condotta colpevole del ricorrente, il quale ha dato credito a una comunicazione costituente un evidente caso di *phishing*.

Come più volte affermato dalla giurisprudenza dell'Arbitro, il cliente risponde del proprio comportamento quando subisce tentativi di frode del tutto evidenti come quello verificatosi nel caso di specie

Tanto premesso, rileva che, dalle verifiche effettuate, è stato possibile accertare la legittima esecuzione e sostanziale regolarità dell'operazione contestata. Produce all'uopo un'evidenza informatica, da cui si evince che la transazione è stata correttamente processata e regolarmente autenticata: in particolare, al momento dell'esecuzione della stessa, i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità; inoltre, l'operazione è stata eseguita, previa autenticazione del cliente, attraverso la digitazione manuale del PAN e l'inserimento dei codici OTP inviati tramite SMS.



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Il ricorrente chiede al Collegio di riconoscere il proprio diritto al rimborso, da parte dell'intermediario, della somma di € 255,00.

L'intermediario chiede all'Arbitro di rigettare nel merito la richiesta di rimborso; in subordine, chiede *“la decurtazione della prevista franchigia”*.

DIRITTO

La controversia di cui al ricorso in esame concerne un caso di utilizzo non autorizzato di uno strumento di pagamento, nella specie di una carta bancomat.

Osserva il Collegio essere, quella dell'impiego fraudolento di strumenti di pagamento, una tematica più volte sottoposta alla cognizione dell'ABF ed in merito alla quale si danno un quadro normativo di riferimento ed un indirizzo interpretativo dell'Arbitro assai chiari nella determinazione del criterio di contemperamento tra obblighi di diligenza nella custodia e nell'uso stesso dello strumento di pagamento, a carico del cliente, e doveri di condotta dell'intermediario consoni al parametro della diligenza professionale (art. 1176, comma 2, cod. civ.), da declinare nella specie come diligenza del *“regolato ed accorto professionista-banchiere”* (cfr. Collegio di Milano, decisione n. 1873/2014).

Ai sensi dell'articolo 7 del D.lgs 27 gennaio 2010, n. 11, l'utilizzatore abilitato all'impiego di strumenti di pagamento è tenuto a farne un uso conforme ai termini del contratto quadro (comma 1), oltre che ad adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo stesso dello strumento (comma 2); d'altra parte, il successivo articolo 10 addossa in capo al prestatore dei servizi di pagamento l'onere di provare come l'operazione eseguita, che l'utilizzatore neghi però di avere autorizzato, sia stata *“autenticata, correttamente registrata e contabilizzata”* e che non abbia subito le conseguenze di un malfunzionamento. Coerentemente con questo quadro, poi, l'articolo 12 del medesimo testo normativo, rubricato *“Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento”*, fissa sì un tetto massimo di € 150,00 all'entità della perdita che l'utilizzatore può sopportare a seguito di un utilizzo indebito dello strumento di pagamento fornitogli, conseguente a furto o smarrimento, ma facendo espressamente salvo il caso in cui il medesimo soggetto *“abbia agito con dolo o colpa grave”*.

Il criterio di bilanciamento, che chiaramente si desume dalle citate disposizioni, tra doveri di condotta professionale riposti in capo al prestatore dei servizi di pagamento, ed obblighi di diligenza comunque sussistenti in capo al cliente, risulta poi ulteriormente cristallizzato in seno alle Disposizioni della Banca d'Italia del 5.7.2011, di *“Attuazione del Titolo II del Decreto Legislativo n.11 del 27 gennaio 2010, relativo ai servizi di pagamento”*, allorché, al punto 2.2, sez. IV, si legge che *“Il rispetto degli obblighi di condotta diligente da parte dell'utilizzatore esime quest'ultimo da responsabilità per utilizzi non autorizzati dei servizi e degli strumenti di pagamento. Il mancato adempimento di tali obblighi può invece comportare la sua responsabilità per gli utilizzi non autorizzati. La violazione degli obblighi posti in capo all'utilizzatore dalla legge o dal contratto in essere con il suo prestatore di servizi di pagamento integra una condotta negligente”*

In sintonia con questo quadro normativo risulta l'indirizzo ormai consolidato, assunto dall'ABF nella materia in esame.

In una, infatti, con l'evidenziazione del regime di speciale protezione e di *favor* probatorio a beneficio degli utilizzatori, cui si collega una tendenziale estensione dell'area di rischio di impresa e di potenziale responsabilità a carico del professionista-banchiere, comunque chiamato ad un costante sforzo di adeguamento delle contromisure tecniche che possano dirsi realmente adeguate ed idonee a presidiare la sicurezza dell'impiego del sistema di pagamento offerto, non si è mancato di ribadire la concorrente rilevanza di ogni condotta



gravemente colposa dell'utilizzatore ai fini di una imputazione a suo carico delle perdite riportate a seguito di usi fraudolenti (cfr., Collegio di Coordinamento, decisione n. 3498/12, Collegio di Bari, decisione n. 5039/17; Collegio di Milano, decisione n. 10306/16, Collegio di Napoli, decisione n. 9343/16).

In connessione con ciò e volgendo l'attenzione al profilo probatorio, benché sia stato ribadito gravare comunque sul prestatore la prova (non solo dell'adozione da parte sua dei presidi di sicurezza degli strumenti di pagamento, nonché della corretta autenticazione dell'operazione contestata, bensì anche) della sussistenza di quell'elevato e abnorme grado di negligenza dell'utilizzatore, questo Arbitro – in aderenza peraltro ai principi a più riprese fissati dalla giurisprudenza di legittimità (Cass. civ., Sez. II, 18 gennaio 2010, n. 654) – ha riconosciuto ampio spazio ad elementi indiziari della sussistenza proprio di colpa grave, affermando cioè come la prova della sua sussistenza possa essere fornita pure per mezzo di presunzioni, purché queste, com'è noto, siano gravi, precise e concordanti secondo quanto dispone l'art. 2729 c.c. (cfr. Collegio di Coordinamento, decisione n. 6168/13; Collegio di Roma, decisione n. 1033/2012).

Tra le condotte ritenute pacificamente rivelatrici di una colpa grave dell'utilizzatore, vi è senz'altro la comunicazione delle proprie credenziali o comunque di altri dati sensibili inerenti l'uso dello strumento di pagamento in esito ad un fenomeno di *phishing*, noto ormai da diversi anni e che nondimeno l'ordinaria diligenza consente agevolmente di schivare.

Orbene, venendo ai fatti di causa, giusto ad una mail civetta (del 15.01.2018) ha dichiarato – anche in sede di denuncia – di aver fatto seguito il ricorrente, comunicando i propri dati sensibili relativi allo strumento di pagamento.

Per contro, l'intermediario ha allegato il *log* dell'operazione al fine di fornire evidenza del fatto che la stessa sia stata autenticata, correttamente registrata e contabilizzata. Ha altresì fornito riscontro dell'essere stata l'operazione eseguita *“con sistema dinamico di autenticazione”*, fornito *“evidenza attestante l'avvenuto enrollment della carta di pagamento di cui trattasi al sistema autorizzativo di tipo dinamico, funzionante mediante invio con sms della password dinamica sul numero di cellulare indicato”* ed infine documentato come il numero di telefono associato allo strumento risultasse coincidente con quello del ricorrente.

Ha poi, in ultimo, evidenza dell'avvenuta *“digitazione manuale del Pan ai fini dell'esecuzione”*.

Ciò posto, nel mentre può ritenersi assolto – da parte dell'intermediario – l'onere probatorio che le vigenti disposizioni ripongono a suo carico, si profila con nettezza una condizione di colpa grave a carico del ricorrente, nella veste di utilizzatore dello strumento di pagamento. Come affermato da questo stesso Collegio in analoghi precedenti *“il Collegio ritiene che nella condotta dell'utilizzatore dello strumento di pagamento siano ravvisabili, nella specie, gli estremi della colpa grave, ai sensi degli artt. 7, comma 2, e 12, comma 4, del d.lgs. 11/2010, per non aver custodito con le dovute cautele i codici di accesso allo strumento di pagamento di cui è titolare, tenuto anche conto che il fenomeno del phishing è ormai noto da diversi anni e che, adoperando l'ordinaria diligenza, il ricorrente avrebbe potuto agevolmente accorgersi che la mail pervenutagli proveniva da un indirizzo non riconducibile in alcun modo all'intermediario emittente della carta (cfr. Collegio di Bari, decisione n. 12476/17).”*

P.Q.M.

Il Collegio non accoglie il ricorso.



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS