



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - PIERFRANCESCO BARTOLOMUCCI

Seduta del 14/10/2024

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro riferendo di essere titolare di un libretto dematerializzato a cui era associata una carta libretto, i cui risparmi ivi depositati potevano essere gestiti a distanza, tramite sito internet o app, nonché tramite utilizzo della predetta carta presso gli ATM dell'odierno resistente.

Riferiva di aver ricevuto un sms, in data 23/09/2023, da un mittente riconducibile alla resistente, recante un link al quale accedeva, per poi essere indirizzato ad una pagina avente la medesima veste grafica della pagina internet ufficiale dell'odierno convenuto ed effettuava pertanto il login richiesto.

Insospettito da tale vicenda, si recava in filiale in data 25/09/2023 e, su indicazione del direttore di filiale, provvedeva alla sostituzione della carta libretto "conservando lo stesso pin per accedere all'area riservata".

Intorno alle ore 18:00 del 02/10/2023 constatava l'impossibilità di effettuare l'accesso online e pertanto tentava di avviare la procedura di sostituzione della password di accesso: nell'eseguire tale attività si avvedeva che il codice numerico a tal fine necessario fosse stato inviato ad un'utenza telefonica diversa da quella a sé intestata e notava altresì l'indicazione di un differente indirizzo mail.

Affermava che "pochi istanti dopo" avesse ricevuto una telefonata da un numero corrispondente al servizio clienti dell'intermediario con cui un interlocutore, qualificatosi come agente della Polizia Postale, gli offriva supporto per "sbloccare il sistema" e lo invitava



a recarsi presso un vicino sportello ATM. Dichiarava di aver inserito la propria carta nell'ATM e digitato il PIN, senza mai comunicarlo all'interlocutore e comunque senza mai eseguire operazioni di pagamento.

Sosteneva che, "insospettata dal prolungarsi del disservizio", si recava nuovamente presso la filiale e si avvedeva di tre operazioni in addebito rispettivamente pari ad euro 9.900,00, euro 1,00 ed euro 29.900,00 senza riuscire a risalire al beneficiario.

Soggiungeva di aver provveduto all'apertura di nuovi rapporti presso il resistente al fine di mettere in sicurezza i residui risparmi e di aver nuovamente notato, nella circostanza, una variazione non autorizzata del suo numero di cellulare e del suo indirizzo mail.

Affermava, inoltre, di aver richiesto all'intermediario il dettaglio di tutti i rapporti a sé intestati e di aver constatato che, in una diversa filiale, in data 02/10/2023, fossero stati indebitamente aperti due rapporti a suo nome (una carta di debito e un libretto di risparmio), utilizzati per trasferirvi le somme oggetto di contestazione, prima di distrarle definitivamente. Dichiarava di non essersi mai recato presso quella filiale e di non aver dunque autorizzato l'apertura di tali rapporti, attuata tramite esibizione di un documento contraffatto e di una firma palesemente apocrifia.

Censurava la condotta dell'intermediario, sia con riferimento alla mancata attivazione di alert nonostante le "operazioni eseguite superassero [...] il limite previsto dalle stesse condizioni contrattuali", sia con riferimento alla mancata adozione di un sistema di autenticazione multifattoriale.

Lamentava inoltre la negligenza dell'operatore di filiale che avesse reso possibile l'illegittima apertura di rapporti bancari.

Chiedeva, pertanto, la restituzione della complessiva somma oggetto di frode, oltre al pagamento delle spese di lite, quantificate in euro 300,00.

Si costituiva ritualmente l'intermediario convenuto, il quale faceva preliminarmente presente che l'oggetto della controversia concernesse la richiesta di rimborso della somma relativa a un'operazione di girofondi e un'operazione di ricarica a valere su un libretto dematerializzato, disposte online in data 02/10/2023.

Eccepiva che le verifiche effettuate avessero accertato la legittima esecuzione e la sostanziale regolarità delle operazioni in contestazione, autorizzate tramite codice OTP inviato sull'utenza telefonica certificata al momento dell'esecuzione delle stesse, verosimilmente modificata dal frodatore.

Dichiarava di produrre, inoltre, tutti gli accessi effettuati dal ricorrente nella propria area riservata nel periodo compreso tra il 22/09/2023 ed il 02/10/2023.

Con riferimento alla colpa grave, faceva presente che lo stesso ricorrente avesse ammesso di aver cliccato un link, nel quale aveva inserito le credenziali di accesso, peraltro proveniente da un sms di cui non allegava documentazione.

Sottolineava che il ricorrente non avesse specificato quali sarebbero state le indicazioni fornite dal truffatore una volta inserita la carta nell'ATM, ma che fosse presumibile lo stesso ad aver provveduto a modificare le impostazioni del proprio profilo inserendo la numerazione telefonica alla quale erano poi state recapitate le OTP necessarie per l'esecuzione delle operazioni.

Riteneva pertanto che la fattispecie in esame potesse essere inquadrata nell'ambito del *phishing*, reso possibile dalla condotta incauta del cliente che aveva fornito a terzi dati che era tenuta a custodire.

Inoltre, secondo l'intermediario il ricorrente non aveva allegato documentazione volta a provare la provenienza dell'sms dai canali dell'intermediario.

Riteneva infondata la richiesta di refusione delle spese di lite e chiedeva, pertanto, il rigetto integrale del ricorso.



Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale produceva una schermata recante il *link* contenuto nel messaggio ricevuto il 22/09/2023. Versava, inoltre, evidenza relativa alle telefonate ricevute da un numero riconducibile al convenuto, per cui riteneva che la truffa subita fosse inquadrabile nel novero del *id caller spoofing/vishing*.

In ogni caso, richiama l'orientamento dell'Arbitro secondo cui la prova della SCA rappresenta un *pruis* logico rispetto all'esame di eventuali profili di colpa dell'utilizzatore.

Faceva, inoltre, presente che anche la variazione dell'utenza telefonica, secondo la normativa regolante la materia, dovesse essere presidiata dall'autenticazione forte, come riconosciuto dalla giurisprudenza di questo Collegio.

Si doleva della negligenza con cui l'intermediario avesse consentito l'apertura di rapporti a sé intestati, tramite documenti contraffatti e firma apocrifa, in contrasto con il parametro della diligenza dell'accorto banchiere di cui all'art. 1176, comma 2, cod. civ.

Sosteneva, al riguardo, di essere stato vittima di furto d'identità e che, senza l'apertura di tali rapporti, la frode non si sarebbe potuta perfezionare, posto che con il libretto per cui è ricorso è possibile trasferire denaro solo verso altri rapporti intestati allo stesso titolare.

Riteneva che il limite massimo giornaliero che si può trasferire tramite girofondi sia pari ad euro 15.000,00 e che, dunque, fosse perlomeno da rimborsare la minor somma di euro 24.800,00, "se pur volessimo pensare per assurdo che la resistente sia esente da responsabilità".

Insisteva, pertanto, per l'accoglimento delle conclusioni già rassegnate.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale riferiva che il *link* prodotto dal ricorrente non risultasse a sé riconducibile. Allo stesso modo sosteneva che il numero da cui lo stesso avesse dichiarato di essere stato contattato "risulterebbe appartenente ai servizi di firma digitale e non di contro dei servizi finanziari dell'Istituto".

Contestava la doglianza relativa al superamento dei limiti massimi giornalieri, in quanto affermava che non vi fosse limite per l'operazione in contestazione.

Per il resto si riportava a quanto precedentemente dedotto e concluso ed insisteva per il rigetto dell'avverso ricorso.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di due operazioni on-line, successivamente disconosciute.

La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- *Payment Services Directive 2*).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *strong customer authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa *de qua* prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione,



con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Quanto al caso di specie, le operazioni disconosciute consistono in due pagamenti per il complessivo importo di euro 39.801,00 (oltre ad euro 1,00 di commissione su una di esse) effettuate in data 02/10/2023.

L'intermediario afferma che le operazioni contestate siano state eseguite con autenticazione dell'utente in modalità SCA, tramite l'utilizzo di codici OTP (fattore di possesso) inviati "sul numero certificato inserito al momento della effettuazione delle stesse"; afferma, inoltre, che il numero sia stato "presumibilmente inserito dal frodatore in occasione della vicenda".

Dalle deduzioni dell'odierno resistente, nonché dalla documentazione versata in atti, non risulta tuttavia descritto né tantomeno indicato alcun riferimento relativo al secondo fattore di autenticazione richiesto.

Emerge inoltre *per tabulas* che i messaggi risultano inviati al numero di cellulare che l'intermediario stesso ipotizza essere stato variato dal frodatore, non essendo coincidente con quello del ricorrente, riportato in denuncia.

Il Collegio deve rammentare che nell'ipotesi in cui l'operatività disconosciuta sia stata preceduta dalla modifica del numero di cellulare certificato associato all'*home banking*, perfezionatasi attraverso l'inserimento di un codice OTP inviato all'utenza telefonica del frodatore (e non a quella del cliente, precedentemente registrata), il sistema non può essere considerato conforme alla SCA, secondo quanto stabilito all'art. 4, comma 30, della PSD2 (qualcosa che solo l'utilizzatore possiede) e che, secondo l'orientamento dell'EBA, il fattore di possesso non è dato dal messaggio in sé, ma dalla SIM card associata al relativo numero di telefono impostato dal cliente (Q&A EBA 2018_4039).

Del resto, lo stesso orientamento condiviso dai Collegi territoriali ha precisato che la variazione dell'utenza telefonica destinataria delle OTP dispositive è un'operazione rilevante ai fini della sicurezza e, come tale, richiede un'autenticazione forte attraverso due o più elementi classificati, in base alle regole stabilite dall'EBA, nelle categorie della conoscenza, del possesso e dell'inerenza (cfr., *ex multis*, Coll. Bari, dec. n. 15211/2022; 15958/2022).

Nel caso di specie l'intermediario non fornisce indicazioni in merito ai fattori richiesti per la modifica del numero di telefono, né produce i relativi log, limitandosi ad affermare che presumibilmente vi avesse provveduto tramite ATM il ricorrente, assecondando le richieste del frodatore.

Si osserva, inoltre, che non constano neppure evidenze relative ai fattori di autenticazione relativi alla fase di autorizzazione delle operazioni.

Di contro, emerge documentalmente (secondo quanto dedotto anche dal ricorrente) che l'operazione di girofondi di euro 29.900,00, sia stata disposta oltre il limite di operatività previsto, contrattualmente fissato ad euro 15.000,00 giornalieri.

Sul punto, il Collegio di Coordinamento ha chiarito che il controvalore dell'operazione con la quale viene superato il c.d. plafond deve essere interamente restituito al cliente in quanto, una volta disconosciuto il pagamento, esso difetta del consenso dell'utilizzatore dello strumento (cfr. Coll. coord., dec. n. 15784/2018; Coll. Bari, dec. n. 12581/2020).

Il Collegio deve pure rilevare che la frode in questione sia stata realizzata anche attraverso l'apertura, da parte del truffatore, di nuovi rapporti formalmente intestati al ricorrente presso una diversa filiale dell'intermediario convenuto; essa è stata realizzata nella stessa giornata di esecuzione delle operazioni contestate (02/10/2023) tramite esibizione di un documento



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

contraffatto e l'apposizione di firme apocriefe. Sul punto, l'intermediario non ha mosso contestazioni.

In base alle risultanze documentali e alle deduzioni dell'intermediario deve quindi ritenersi che parte resistente – oltre ad aver tenuto una condotta palesemente contraria ai canoni della diligenza professionale del *bonus argentarius* – non abbia neppure fornito, nello specifico, la prova dell'autenticazione e della formale regolarità delle operazioni contestate; il mancato assolvimento di tale onere probatorio rende superflua l'analisi relativa ai profili di colpa grave del ricorrente, rispetto alla quale la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

La domanda restitutoria avanzata dal ricorrente deve, quindi, trovare accoglimento.

Di contro, non può essere accolta la domanda di rifusione delle spese di assistenza difensiva, a sostegno della quale il ricorrente non ha prodotto alcun elemento documentale di supporto.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 39.801,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI