

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) GENOVESE	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore LORENZA BULLO

Seduta del 16/09/2025

FATTO

Parte ricorrente espone quanto segue:

- in data 27/02/2025, alle ore 19:17, riceveva un SMS da un numero criptato riconducibile all'odierna resistente che gli comunicava un tentativo di accesso nel suo internet banking;
- contattava il numero in calce al messaggio e il presunto operatore della banca lo informava di un'azione sospetta sul suo conto corrente, azione bloccata dalla banca, e che, per essere annullata, richiedeva l'effettuazione di alcune procedure indicate dall'operatore stesso;
- si rendeva conto di avere eseguito un bonifico di € 3.300,00 a favore di un soggetto sconosciuto; contattava quindi la banca e bloccava le carte, ma non riusciva a bloccare il bonifico;
- i malfattori hanno hackerato i sistemi di sicurezza della banca che si deve ritenere responsabile per una non adeguata gestione della sicurezza informatica dei propri sistemi;
- avendo segnalato immediatamente l'accaduto, la banca avrebbe potuto sospendere l'autorizzazione dell'addebito.

Parte ricorrente chiede pertanto all'Arbitro di condannare l'intermediario convenuto al rimborso della somma fraudolentemente sottratta dagli ignoti malfattori, per un totale complessivo chiesto a rimborso di euro 3.300,00 oltre al risarcimento dei danni morali e materiali subiti.

L'intermediario resiste alla pretesa contro deducendo quanto segue:

- il ricorrente stesso ha espressamente dichiarato di avere seguito le istruzioni impartite dall'operatore e di aver disposto il bonifico tramite APP installata sul suo *device*, successivamente autorizzato tramite *PIN, seppure a seguito di un raggio;
- il cliente ha fornito i codici personali di accesso all'APP violando il sistema di sicurezza della banca;
- *la truffa si è potuta realizzare solo grazie al contributo causale decisivo del ricorrente che ha dimostrato una "colpevole credulità"*;
- i dati di contatto dei correntisti possono essere recuperati dai truffatori in svariati modi, senza bisogno di violare la sicurezza della banca la quale non ha neanche la possibilità di anticipare un eventuale abuso dei propri recapiti telefonici; dunque non si rileva alcuna responsabilità in capo all'intermediario;
- sono state attivate diverse campagne di sensibilizzazione in tema di frodi attraverso i principali canali di comunicazione, tra i quali la pagina web della banca;
- il cliente non ha comunicato anomalie sul telefono o sulla sim; quindi, non sono ravvisabili intrusioni informatiche;
- l'operazione oggetto di contestazione è stata eseguita in conformità con il d.lgs. 11/2010, ossia tramite un *sistema di autenticazione forte*;
- si ravvisa la colpa grave del cliente il quale ha fornito i codici personali ed ha contribuito al perfezionamento della truffa ai suoi danni.

L'intermediario conclude pertanto per il rigetto del ricorso, in quanto infondato.

DIRITTO

Parte ricorrente contesta l'esecuzione fraudolenta di un bonifico di euro 3.300,00 di cui chiede il rimborso; detto bonifico risulta eseguito in data 27/2/2025 tramite APP; parte ricorrente non contesta le commissioni del bonifico pari a euro 0,31. In ordine all'orario di esecuzione dell'operazione contestata, dai log prodotti dall'intermediario, risulta che il bonifico sia stato eseguito alle ore 19:28 e non alle ore 20:00 come invece dichiarato nel modulo di disconoscimento.

Parte ricorrente dichiara di avere immediatamente contattato l'intermediario in data 27/02/2025 per tentare di revocare l'operazione; il bonifico risultava comunque irrevocabile in quanto la richiesta di revoca era stata formulata dopo l'orario del *cut-off* del giorno di disposizione del bonifico.

Dalle dichiarazioni confessorie rese dal cliente in sede di denuncia sembra pacifico che il bonifico di euro 3.300,00 sia *stato eseguito personalmente dal ricorrente* tramite la app installata sul suo telefono, sia pure a seguito di una truffa perpetrata in suo danno. In particolare, il ricorrente dichiara che il sedicente operatore *"mi faceva eseguire un bonifico bancario al fine di procedere al blocco del conto corrente"*, dunque *"eseguivo su sua indicazione un bonifico"*.

Secondo l'orientamento dell'ABF, affinché un'operazione possa dirsi *non autorizzata* e, dunque, possa trovare applicazione la relativa disciplina di diritto speciale approntata dal D. Lgs. n. 11/2010 come modificato dal D.lgs. n. 218/2017 di attuazione della Direttiva 2015/2366/EU (c.d. PSD 2), *deve difettare il requisito del "consenso del pagatore"* di cui all'art. 5 del medesimo decreto.

Al riguardo il Collegio si richiama all'orientamento condiviso dai Collegi secondo il quale, se *l'operazione è eseguita per intero dal pagatore* (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione, come peraltro accaduto nel caso in esame stando alle stesse dichiarazioni del ricorrente), *deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD*.

In questi casi, non è pertanto configurabile una responsabilità oggettiva del PSP.

In tali casi, infatti, secondo l'ABF “ *per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggirio subito dal terzo ignoto, l'intermediario non poteva che considerare autorizzati i pagamenti effettuati personalmente dal titolare dello strumento di pagamento, non avendo alcuna possibilità di accorgersi della truffa perpetrata ai danni del cliente. Non potendosi configurare come non autorizzate le operazioni compiute personalmente dal ricorrente, sia pure sulla base del vizio di volontà sopra descritto, non sussistono i presupposti previsti dalla normativa sopra richiamata per un rimborso della somma a favore del medesimo*” (ex multis, Collegio di Milano, decisione n. 3280/2023).

I Collegi ABF, dunque, nell'ipotesi di operazioni disposte ed autorizzate personalmente dal titolare dello strumento di pagamento, come accaduto nel caso in esame, sebbene sulla base di un consenso viziato dagli artifizii e raggiri posti in essere da un truffatore anche per mezzo di sms o chiamate “civetta” apparentemente provenienti dall'intermediario resistente, fuoriescono dal campo di applicazione del regime di protezione previsto dal D. Lgs. 11/2010 sopra citato; di conseguenza, *non sussiste l'onere per l'intermediario di dare prova della corretta autenticazione con doppio fattore SCA* e non vi è luogo al rimborso previsto invece dal Dlgs 1172010 per le *operazioni non autorizzate* (ex multis Collegio di Bologna, n. 2290/2023).

Va tuttavia precisato che, secondo gli orientamenti più recenti condivisi dei Collegi ABF (v. Collegio di Milano decisioni 4567/2022 e n. 2281/2024; Collegio di Napoli, decisione n. 329/2024; Collegio di Bologna n. 1730/2024, Collegio di Roma, decisione n. 1655/2025) *quando l'operazione sia eseguita per intero dal pagatore se a distanza come nel caso in esame ovvero personalmente dal pagatore stesso in presenza allo sportello*, pur trattandosi di operazione autorizzata potrebbe comunque venire in rilievo *una responsabilità concorrente del PSP*, sulla base delle evidenze disponibili e *secondo le norme di diritto comune* (quali la violazione da parte dell'intermediario dei doveri informativi, di correttezza e di protezione del cliente, derivanti dagli artt. 1176 comma 2 c.c., 1375 c.c.), *quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:*

- a)** mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- b)** mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto *esponendo le richieste del frodatore*;
- c)** mancato rilievo di indizi di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Sulla eventuale responsabilità del prestatore di servizi di pagamento per il pregiudizio subito dal cliente in conseguenza del compimento *di pagamenti da lui autorizzati verso terzi al di fuori dell'art. 11 d.lgs. n.*

11/2010 si è espresso anche il Collegio di Coordinamento n. 8671/2024 il quale ha ribadito che i danni subiti dal cliente per i pagamenti da lui "autorizzati" (in quanto tali sottratti al perimetro di operatività della normativa di cui al Dlgs 1172010) possano, in astratto, essere risarciti ai sensi dell'art. 1218 c.c., *qualora sia dimostrata la negligenza dell'intermediario nell'adempimento di obblighi contrattuali*.

Per quanto concerne infine la quantificazione del rimborso da riconoscere all'utente nelle ipotesi testé sopra citate di eventuale *responsabilità concorrente del PSP secondo le norme di diritto comune*, secondo la posizione unanime dei Collegi ABF, la valutazione della responsabilità del PSP deve essere formulata in un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto: la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti.

Ciò premesso in termini di diritto, venendo al caso in esame, il Collegio rileva quanto segue:

in primo luogo, risulta incontestato tra le parti, come emerge dalle loro dichiarazioni e dalla denuncia del ricorrente, che il bonifico oggetto di ricorso è stato eseguito personalmente dalla parte ricorrente tramite app installata sul telefono del ricorrente sia quanto a inserimento dei dati sia quanto ad autenticazione; *in secondo luogo*, parte ricorrente lamenta una condotta negligente dell'intermediario per non aver il medesimo approntato misure di sicurezza atte a impedire il verificarsi della truffa, realizzatasi grazie all'uso da parte dei truffatori di utenze telefoniche riconducibili alla banca nonché grazie alla conoscenza delle generalità e dei dati bancari del ricorrente.

Al riguardo il Collegio rileva quanto segue: la truffa subita dalla parte ricorrente è riconducibile allo schema truffaldino del c.d. *social hacking*..

Dalla denuncia in atti risulta che il ricorrente abbia ricevuto un SMS da un numero riferibile alla resistente alle ore 19:17 del 27/02/2025 che lo informava di operazioni anomale sul suo conto corrente e lo invitava a chiamare il numero di telefono (cellulare) riportato in calce al messaggio. Il ricorrente chiamava tale numero alle 19:30 ed eseguiva "*procedure che non ricordo con precisione*", tra le quali un bonifico bancario in teoria destinato a "*bloccare il conto corrente*"; la durata della telefonata con il sedicente operatore della Banca è durata "*all'incirca due ore*", come dichiarato dal ricorrente in denuncia; trattasi un tempo sufficientemente lungo affinché una persona di media diligenza si riprenda dall'effetto sorpresa e si accorga della truffa in corso..

Parte ricorrente allega in atti gli SMS truffaldini da cui ha preso avvio la truffa, messaggi con riguardo ai quali il Collegio osserva che:

- dalle schermate *non emerge il numero di telefono del mittente del sms*, mentre in denuncia il ricorrente afferma di essere stato contattato da un numero riferibile alla resistente;
- emergono delle incongruenze grammaticali, in quanto nel primo SMS il mittente si riferisce al cliente in modo informale "*se non sei tu chiama*", mentre nel secondo SMS si utilizza la terza persona "*La invitiamo*";
- il numero di telefono indicato nel messaggio come numero da contattare per bloccare l'attività anomala sul conto corrente è *un'utenza cellulare non riconducibile all'odierna resistente*.

Preso atto di quanto sopra, ad avviso del Collegio, l'intermediario eccepisce, fondatamente la colpa grave del ricorrente, il quale per sua stessa ammissione ha eseguito le istruzioni dei truffatori, fornendo i suoi codici personali ed inserendo e disponendo egli stesso l'operazione di pagamento sulla app installata nel suo telefono, contribuendo in maniera decisiva al perfezionamento della truffa che non è stata subitanea, essendo durata all'incirca due ore la telefonata con il truffatore.

Il presente *Collegio*, attenendosi ai principi del citato Collegio di Coordinamento n.8671/2024, richiamate le proprie precedenti decisioni n. 3082/2025 e n. 1748/2025 in materia *social hacking*, ha comunque valutato anche la condotta complessiva dell'intermediario, alla luce degli obblighi di protezione previsti dal d.lgs. n. 11/2010 e tenuto conto delle regole generali del codice civile in materia di obbligazioni, nonché della disciplina del mandato. Al riguardo, ad avviso del presente Collegio, risultano correttamente adempiuti da parte dell'intermediario, gli obblighi di sicurezza e di protezione della sfera della controparte desumibili dall'art. 8 del decreto citato e, più in generale, dal contenuto del contratto di prestazione di servizi di pagamento, non constando alcuna anomalia, né negligenza nella condotta dell'intermediario. Per contro l'operazione disconosciuta, alla luce dei rilievi sopra svolti, appare connotata da profili di grave imprudenza da parte dell'istante, La frode in esame non presenta infatti un carattere talmente sofisticato da non poter essere sventata da un utente mediamente diligente; a ciò si aggiunga che nel caso in esame non sono integrati gli indicatori di anomalia di cui al DM 112/2007 e non risultano depositati in atti i massimali applicabili al contratto di cui è causa.

Conclusivamente, alla luce del fatto come sopra complessivamente ricostruito, ad avviso del presente Collegio, nel caso in esame non emerge dunque alcun apporto causale alla frode da parte dell'intermediario dal momento che l'ordine di pagamento è stato effettuato personalmente e interamente dal cliente tramite app installata sul proprio telefono (operazione autorizzata) e gli artifici e raggiri posti in essere dai truffatori non erano in nulla conformi alla prassi degli intermediari bancari.

La domanda di rimborso della somma bonificata a terzi a seguito della truffa in oggetto non può dunque essere accolta.

Non ravvisandosi alcun profilo di responsabilità in capo all'intermediario convenuto in ordine alla truffa subita, va peraltro respinta anche la connessa domanda risarcitoria avanzata dall'istante, domanda quest'ultima peraltro sfornita di idoneo supporto probatorio.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE