

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore CARMELA ROBUSTELLA

Seduta del 28/01/2026

FATTO

Il ricorrente, titolare di conto corrente intrattenuto con la resistente, riferisce che in data 10/04/2025 alle ore 17:29 riceveva una telefonata, proveniente dal numero ufficiale della banca, da parte di sedicente operatore che lo informava di un presunto accesso fraudolento al conto corrente dall'estero. Rappresenta che il finto operatore lo invitava ad installare una app sul telefono al fine di bloccare l'attacco in corso e di aver seguito le sue indicazioni, confidando nella veridicità della segnalazione. A tal punto, la conversazione si interrompeva e sul display del suo telefono compariva una schermata che lo invitava a non interagire con il dispositivo poiché era in corso l'analisi di sicurezza. Afferma che dopo aver ricevuto una ulteriore chiamata dal finto operatore per rassicurarlo in merito al buon esito del blocco, tentava di richiamarlo al medesimo numero, ma rispondeva un diverso operatore, dal quale apprendeva di essere stato vittima di una frode. Riferisce di essersi collegato al conto dal pc e di aver effettivamente riscontrato un saldo inferiore di € 8.700,00, pur non risultando movimenti in uscita. Precisa di non aver ricevuto alcuna risposta al riguardo dal servizio clienti e di essersi recato, il giorno seguente, presso una filiale, ove apprendeva che era stato predisposto dal suo conto un bonifico verso

l'estero e che lo stesso era stato posto in "quarantena" poiché relativo ad un conto business e, pertanto, necessitava la ratifica da parte della sede centrale dell'intermediario.

Evidenzia di aver successivamente sporto denuncia e di averla consegnata in filiale, ove gli veniva nuovamente assicurato il mancato perfezionamento del bonifico fraudolento.

Soggiunge di essersi nuovamente recato in banca in data 14/04/2023 e di aver ricevuto, anche in tale occasione, rassicurazione sulla mancata contabilizzazione del bonifico, come confermato anche dall'estratto conto effettuato il medesimo giorno da sportello.

Lamenta che, nonostante ciò, nel pomeriggio del 14/04/2025 la resistente ha eseguito il bonifico in favore di un terzo ignoto, senza alcuna comunicazione e a distanza di quattro giorni dalla frode, tempestivamente comunicata.

Ritiene dunque che la responsabilità dell'accaduto sia ascrivibile alla banca secondo quanto previsto dal d.lgs n. 11/2010, nonché per violazione dell'obbligo di diligenza professionale.

In particolare, sottolinea di aver segnalato subito la non paternità dell'operazione e che la resistente avrebbe dovuto bloccare il bonifico prima della sua contabilizzazione, avvenuta a distanza di 4 giorni. Osserva peraltro che nel contratto è indicato quale orario limite di ricezione dei bonifici in uscita le ore 17:00, mentre il bonifico in questione è stato posto in essere dopo le ore 17:29, dunque in data successiva a quella contrattualizzata.

Rileva altresì il carattere anomalo dell'operazione contestata, non avendo mai eseguito bonifici così rilevanti e di tale importo.

Contesta poi la mancata previsione da parte della resistente di un limite giornaliero e mensile con riguardo ai bonifici, ritenendo che si tratti di una negligenza imputabile alla banca in quanto attinente alla sicurezza dello strumento di pagamento che ha offerto.

Lamenta altresì la responsabilità della banca per illecito trattamento dei dati personali ex art. 2050 c.c. Chiede pertanto la restituzione della somma indebitamente sottratta.

Costitutosi ritualmente, l'intermediario fa preliminarmente presente che il ricorrente chiede il rimborso di un bonifico disposto online tramite canale business way il 10/04/2025, addebitato sul conto corrente n. *47.

Chiarisce che tale tipo di conto prevede, in fase di contrattualizzazione, la nomina di un soggetto "supervisore", modificabile nel tempo, al quale vengono consegnate, in busta chiusa, le credenziali di accesso alla postazione da supervisore e, separatamente, le credenziali, per poter disporre le operazioni ai singoli soggetti "firmatari", nominati dal supervisore.

Ciò posto, rappresenta che l'accesso al servizio avviene con Strong Customer Authentication (SCA), ossia attraverso l'inserimento di codice utente, codice postazione, password e codice OTP ricevuto tramite token fisico; per l'esecuzione dell'operazione dispositiva, l'utente deve inserire il pin/psw firmatario (riportato all'interno della busta ritirata in agenzia e personalizzata al primo accesso) ed il codice OTP monouso che riceve tramite token fisico.

Afferma che questa modalità di autenticazione a due fattori risponde alla normativa europea (c.d. PSD2) e costituisce un presidio tale da garantire la sicurezza delle transazioni effettuate attraverso l'home banking, come riconosciuto anche dal consolidato orientamento dell'Arbitro Bancario Finanziario.

Quanto al caso di specie, fa presente che le operazioni contestate sono state autenticate, registrate e contabilizzate correttamente e non hanno subito alcun malfunzionamento delle procedure necessarie per la loro esecuzione.

Evidenzia che dal 29/03/2025 al 17/04/2025 tutte le attività sono state effettuate con il codice utente n. *585 riconducibile al ricorrente, nonché dalla medesima postazione *194 e dallo stesso utente *075.

Ritiene dunque di aver dimostrato l'utilizzo di un sistema di autenticazione forte.

Rileva che non sussiste in capo all'intermediario un obbligo di monitoraggio (cita ex multis Collegio di Milano, decisione n. 6732/2025).

Ad ogni modo, fa presente che non vi erano elementi tali da poter essere letti o percepiti dal personale di agenzia come sintomatici di una possibile frode in corso, ai danni del correntista.

Precisa, inoltre, che per i clienti non consumatori non è prevista alcuna limitazione di importo per l'inserimento di bonifici ordinari.

Quanto alla condotta del cliente, osserva che in sede di denuncia il ricorrente ha confessato di aver scaricato l'applicazione indicata dal sedicente operatore e di aver seguito le istruzioni da questi ricevute, contendendo così l'accesso al suo dispositivo da parte di un terzo.

Quanto al canale di provenienza della chiamata, coincidente con quello della banca, segnala che non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display. Fa presente, infatti, che è possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi con modalità nota da tempo. Rileva che sul tema è intervenuta anche l'AGCOM con la delibera n.12/23/CIR, invitando gli operatori telefonici ad inibire questa funzionalità.

Fa presente di allertare da tempo la clientela a riporre la massima cautela nell'utilizzo dei canali telematici, mediante pubblicazione di avvisi specifici nella pagina di accesso al portale della banca, nell'app e sugli schermi degli ATM.

Osserva di essersi attivata per il recall, appena ricevuta notizia del disconoscimento.

Quanto all'asserita violazione dell'art. 2050 c.c., sostiene che nel caso di specie non vi sia stata alcuna violazione dei sistemi bancari, né alcun indizio di partecipazione della banca nella frode subita dal ricorrente. Eccepisce poi l'incompetenza per materia dell'Arbitro con riguardo alla asserita violazione dell'art. 32 GDPR.

Infine, fa presente di aver offerto al ricorrente il 50% della somma richiesta in restituzione e che questi non l'ha accettata, proponendo un accordo di rimborso dell'80%.

Chiede, pertanto, di rigettare il ricorso.

In sede di repliche, il ricorrente ribadisce che l'operazione oggetto di ricorso è stata disposta il 10/04/2025, mentre il relativo addebito è avvenuto soltanto in data 14/04/2025, dunque quattro giorni dopo. Osserva che un bonifico, anche internazionale, non richiede quattro giorni per la sua emissione e che in tale lasso temporale la resistente avrebbe potuto bloccare l'operazione fraudolenta.

Precisa di aver tempestivamente sporto querela e di essersi recato personalmente in filiale per denunciare l'accaduto, chiedendo la sospensione del bonifico.

Rileva poi che il bonifico in questione presentava anomalie, quali l'ingente importo, la destinazione estera e l'assoluta estraneità del beneficiario.

Lamenta dunque che l'intermediario non ha impedito un pagamento anomalo, nonostante le reiterate segnalazioni del cliente ed ha persino fornito a quest'ultimo rassicurazioni ingannevoli, assicurandogli che il bonifico non sarebbe partito e che il conto era sotto controllo.

Ritiene di non aver mai disposto né autorizzato alcun bonifico, ribadendo di essere stato vittima di una frode perpetrata da terzi ignoti e che, dunque, l'operazione non può qualificarsi come autorizzata. In particolare, sostiene che l'impiego di sistemi OTP non equivale a dimostrazione di volontà dispositiva, né può assolvere la banca dall'onere di dimostrare che l'operazione non sia stata frutto di un accesso fraudolento.

Afferma di aver custodito con diligenza le proprie credenziali e di non averle mai comunicate a terzi.

Evidenzia infine di non aver mai ricevuto alcuna informativa sulle frodi telematiche e sulle “regole comportamentali” da parte dell’intermediario.

Insiste per l’accoglimento del ricorso.

DIRITTO

Il presente ricorso verte sulla richiesta di rimborso di operazione di bonifico ordinario di € 8.700,00 effettuata il 10/04/2025 dal conto corrente business del ricorrente.

Il Collegio ritiene opportuno esaminare, preliminarmente, la questione - rilevabile d’ufficio -della qualificazione del ricorrente in termini di “consumatore”, ai fini della regolare costituzione del collegio. A riguardo, si osserva, infatti, che il ricorrente, nel modulo del ricorso, si qualifica come consumatore; non di meno, dall’esame del complessivo corredo documentale in atti, emerge che l’operazione contestata è stata disposta da un conto aziendale. In particolare, l’intermediario afferma che il ricorrente è una ditta individuale e il ricorrente non ha contestato tale circostanza.

Nel rammentare che l’art. 3 del Codice del Consumo (d.lgs. n. 206/2005) definisce il “consumatore o utente” come “la persona fisica che agisce per scopi estranei all’attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta”, il Collegio ha pertanto provveduto a modificare la qualifica del ricorrente in “non consumatore”

Venendo al merito del ricorso, come si diceva, la domanda proposta dal ricorrente è relativa all’accertamento del proprio diritto alla restituzione del controvalore di un’operazione on-line, successivamente disconosciuta.

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.

Quanto al caso di specie, l’operazione disconosciuta consiste in un bonifico ordinario di € 8.700,00 effettuata il 10/04/2025 dal conto corrente business del ricorrente.

Nella denuncia del 11/04/2025 e in sede di integrazione del 23/04/2025, il ricorrente ricostruisce le modalità della frode in modo analogo al ricorso.

In particolare, dichiara che:

- alle ore 17:29 del 10/04/2025 riceveva una telefonata apparentemente dalla resistente e un sedicente operatore le comunicava che era in corso un tentativo di accesso anomalo al conto dall’estero;

- su indicazione dell'operatore installava sul telefono una app con uno scudo giallo, dopodiché appariva sul telefono la scritta "analisi di sicurezza" che lo invitava a non interagire con il dispositivo;
- conclusa la telefonata con il sedicente operatore, chiamava il numero verde 06**** e una operatrice della banca lo informava di essere stato vittima di una frode;
- telefonava all'assistenza clienti per i conti aziendali, ma il numero risultava inattivo a partire dalle 18:30;
- accedeva all'homebanking tramite pc e non rilevava alcuna operazione, ma il saldo disponibile era inferiore rispetto al saldo contabile di € 8.700,00;
- il giorno seguente si recava presso la banca ove gli veniva comunicato che era in corso una disposizione di bonifico verso l'estero, denominata T3 cumulo che bloccava;
- nonostante le rassicurazioni in merito all'intervenuto blocco, il 14/04/2025 veniva eseguito il bonifico.

L'intermediario, dal canto suo, ha in primo luogo premesso che il ricorrente è titolare di un servizio di home banking di tipo business, descrivendone il funzionamento, successivamente ha proceduto a chiarire la modalità di accesso al servizio di home banking, distinguendo una fase di autenticazione al conto online, che prevede l'inserimento di elementi statici quali codice utente, codice postazione e password e di un elemento dinamico (codice OTP ricevuto via token fisico) e un'altra fase di autorizzazione, nella quale l'utente, in caso di operazione dispositiva, deve inserire il pin/psw firmatario (riportato all'interno della busta ritirata in agenzia e personalizzata al primo accesso) e il codice OTP monouso generato da token fisico.

A supporto, produce la seguente evidenza informatica, relativa alla giornata in cui è stata disposta l'operazione disconosciuta, ad un giorno precedente (29/03/2025) e a due giorni successivi (14 e 17/04/2025).

Da tale log si evince che:

- il bonifico è stato disposto dallo stesso utente (*075), dalla stessa postazione (*194) e tramite il medesimo "serial token" (*775) utilizzati anche nel giorno antecedente e nei giorni successivi alla frode;
- l'inserimento del codice OTP in fase di autorizzazione del bonifico.

Ebbene, proprio dall'esame della documentazione allegata, non sembra potersi evincere il secondo fattore utilizzato per l'autorizzazione del bonifico (pin/psw firmatario), né i fattori di autenticazione utilizzati nella fase di LOGIN per l'accesso all'home banking.

Si osserva, inoltre, che in presenza di analoghe evidenze, i Collegi territoriali non hanno ritenuto raggiunta la prova dell'autenticazione forte in ordine al sistema di autenticazione utilizzato dall'intermediario, con riguardo alla fase di login (cfr. infra Collegio di Milano, decisione n. 5156/2025, Collegio di Napoli, decisione n. 8379/2024).

Sul punto il Collegio rammenta, in primo luogo, che, secondo il consolidato orientamento dell'Arbitro, la mancata prova dell'autenticazione comporta che la responsabilità dell'utilizzo fraudolento gravi integralmente sull'intermediario (v. per tutte Collegio di Bari, decisioni n. 2434/2025 e n. 802/2024 e Collegio di Torino, decisione n. 3772/2024).

Per completezza il Collegio richiama, inoltre, l'orientamento condiviso dai Collegi, secondo il quale ai fini della prova della SCA possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché

consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. Inoltre, anche eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

Nel caso di specie, il ricorrente confessa di aver scaricato sul proprio telefono una app su indicazione del finto operatore, ma nega di aver fornito a terzi le proprie credenziali. Il Collegio, pertanto, ritiene che le dichiarazioni rese dal ricorrente non consentano di sopperire alle carenze probatorie dell'intermediario.

La descritta mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili alla ricorrente. La prova di autenticazione – al cui onere l'intermediario non ha assolto – rappresenta, infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente (cfr. Collegio di Bari, decisioni nn. 1924/2024 e 802/2024).

Alla luce di quanto precede il ricorso va integralmente accolto.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 8.700,00.

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