## 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) CIPRIANI | Membro di designazione rappresentativa degli intermediari |
| (BA) ROBUSTELLA | Membro di designazione rappresentativa dei clienti |

Relatore CARMELA ROBUSTELLA

Seduta del 25/11/2024

## FATTO

Parte ricorrente, in qualità di titolare di ditta individuale, riferisce di aver constatato la presenza sul proprio estratto conto di due ordini di bonifico non autorizzati per € 10.000,00 ed € 800,00, posti in essere *"mediante uso indebito delle […] credenziali"*.
Ritiene che l'intermediario sia responsabile per il danno subito e, dunque, sia obbligato alla restituzione di quanto indebitamente sottrattogli.
Costituitosi, l'intermediario eccepisce preliminarmente l'inammissibilità del ricorso per carenza di preventivo reclamo. In particolare, afferma che la missiva del 21/03/2024 avente ad oggetto *"diffida ad adempiere seguito esito mediazione obbligatoria"* non contiene una specifica contestazione all'operato della banca e non presenta, dunque, le caratteristiche tipiche del reclamo (cita a supporto, Collegio di Bari, decisione n. 6376/24).
Nel merito, afferma che sia l'accesso al conto, sia le operazioni di pagamento, prevedono un sistema di autenticazione basato sul codice utente, sulla password segreta e, infine, su un servizio che consente l'autenticazione via telefono cellulare, tramite chiamata al numero verde dall'utenza univocamente associata al cliente e la contestuale comunicazione di un codice "*usa e getta*" generato per ogni operazione richiesta tramite internet banking.
Richiama, al riguardo, l'art. 8 del contratto quadro ed afferma che, in data 28/12/2022 alle ore 10:39 veniva effettuata l'attività di accesso; alle ore 10:46 veniva impartito il primo ordine di bonifico; in data 29/12/2022 alle ore 16:56 veniva eseguito nuovamente l'accesso; alle ore 16:59 veniva impartito il secondo ordine di bonifico. Dichiara che tutte le operazioni menzionate risultano autorizzate secondo la modalità sopra descritta e che i sistemi

informatici non hanno rilevato anomalie o malfunzionamenti nelle giornate in cui si è consumata la truffa in questione.
Precisa che le richieste di recall, tempestivamente inoltrate a seguito della segnalazione del cliente, avevano esito negativo per "*fondi insufficienti*".
Con riferimento alla colpa grave fa presente che parte ricorrente non ha fornito elementi utili a ricostruire la vicenda ed ha allegato copia di due delle tre denunce sporte, omettendo quella in cui dichiarava di aver ricevuto delle mail e delle telefonate sospette nei giorni antecedenti gli addebiti contestati. Fa presente che non risultano nemmeno prodotte evidenze documentali relative al registro delle telefonate o ai messaggi ricevuti.
Pertanto ritiene che la truffa occorsa sia inquadrabile nello schema del tradizionale phishing e che, verosimilmente, il ricorrente abbia dato seguito ad un link ricevuto ed abbia in questo modo comunicato le credenziali di sicurezza necessarie per accedere ai servizi online e disporre le operazioni di cui è ricorso. Ritiene altresì possibile, in alternativa, che il ricorrente stesso abbia potuto porre in essere tutti i passaggi necessari per autorizzare i bonifici.
Richiama la decisione del Collegio di Bari n. 917/24 che ha presunto la colpa grave del cliente dalla mancanza di sufficienti allegazioni in ordine alle caratteristiche della truffa subita e cita l'ordinanza della Corte di Cassazione n. 7214/23 in cui si afferma che, una volta provata la SCA, la condotta del cliente che comunichi i propri codici di sicurezza a terzi esonera la banca dall'obbligo di risarcire il relativo danno. Chiede:

- in via principale che il ricorso sia dichiarato inammissibile per carenza di idoneo reclamo;
- nel merito il rigetto;
- in via subordinata l'applicazione di un concorso di colpa ex art. 1227 c.c.

Il ricorrente, in sede di controdeduzioni, contesta l'eccezione in rito sollevata dalla resistente.
Nel merito ritiene che la materia de qua segua, per il riparto dell'onere probatorio, quanto sancito dall'art. 1218 c.c. che dispensa il creditore dall'allegazione della prova dell'inadempimento.
Ritiene che il sistema di autenticazione adottato dall'intermediario non garantisca la tutela della clientela a fronte di truffe come quella verificatasi nel caso di specie.
Si duole, inoltre, dell'assenza di sistemi di rilevazione e monitoraggio anche in considerazione del lasso temporale intercorrente tra la prima operazione dispositiva del 28/12/2022 e la seconda del 30/12/2022.
Nelle controrepliche, l'intermediario ribadisce integralmente quanto già dedotto ed eccepito.
Fa presente che, anche a voler considerare reclamo la prima diffida ad adempiere ricevuta il 01/02/2023, risulterebbe ampiamente decorso il termine di 12 mesi previsto dalle Disposizioni ABF per l'invio del ricorso.
Soggiunge nel merito, con riferimento al servizio di alert, di adottare un sistema di per sé idoneo a consentire alla clientela di avere sempre la possibilità di verificare e controllare quanto avviene sul proprio conto corrente, in particolare per quanto concerne l'operatività online tramite Internet banking. Ritiene tuttavia che sia onere dei clienti di prendere visione della messaggistica inviata dalla Banca "ovvero verificare con frequenza il proprio estratto conto e relativa movimentazione".

## DIRITTO

Il Collegio deve preliminarmente respingere l'eccezione pregiudiziale sollevata dall'intermediario per carenza di preventivo reclamo. In particolare l'intermediario ritiene che la diffida ad adempiere del 21/03/2024 inviata dalla ricorrente non contenga una specifica contestazione al suo operato, né l'indicazione delle operazioni oggetto di disconoscimento e non possa pertanto considerarsi reclamo ai fini del procedimento ABF.

Il Collegio rammenta, a tal proposito, che le vigenti Disposizioni ABF (Sez. I, par. 3) descrivono il reclamo come "ogni atto con cui un cliente chiaramente identificabile contesta in forma scritta (es., lettera, fax, e-mail) all'intermediario un suo comportamento anche omissivo" e che secondo l'orientamento dei Collegi il reclamo è un atto in forma scritta, riferibile a un cliente chiaramente identificabile, che non richiede l'utilizzo di formule sacramentali o di modelli imposti dalla legge. Può, infatti, presentarsi con una lettera, un fax o una email, purché risulti espressamente e con chiarezza la contestazione mossa all'intermediario. Ciò in quanto funzione del reclamo è quella di consentire all'intermediario, in sede di riscontro, di comprendere la doglianza mossa dal cliente e di giungere ad una composizione della controversia insorta già nella sua fase iniziale, prima che si instauri un vero e proprio contenzioso (cfr. ex multis Collegio di Bari, decisione n. 778/23).
Nel caso in esame, dalla documentazione presente in atti emerge che il ricorrente aveva presentato una prima diffida ad adempiere in data 01/02/2023, riscontrata nel merito dall'intermediario, il quale aveva negato il rimborso specificando che le operazioni disconosciute erano state poste in essere previa SCA. In data 24/04/2023 il ricorrente aveva presentato istanza di mediazione all'organismo incaricato della relativa procedura, conclusasi con esito negativo, non essendo la banca intervenuta nella procedura di mediazione. In data 21/03/2024 il ricorrente presentava una seconda diffida ad adempiere, nuovamente riscontrata nel merito dall'ufficio reclami dell'intermediario.
Da tale documentazione si evince l'indicazione delle operazioni contestate, con specificazione delle date di effettuazione delle stesse e dei relativi importi; anche dal tenore del riscontro fornito, viene in rilievo che la banca ha trattato la soprariportata comunicazione come una richiesta di restituzione.
Alla luce di tali risultanze documentali il Collegio ritiene che la diffida presentata dalla ricorrente il 21/03/20024 integri gli estremi del reclamo, come previsto dalla vigente disciplina procedimentale richiamata.
Passando quindi all'esame del merito, la fattispecie all'esame del Collegio concerne il disconoscimento di due bonifici di importo pari ad € 10.000,00 ed € 800,00.
Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. Inoltre, le operazioni contestate sono state eseguite successivamente all'entrata in vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).
La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento

eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7." (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente". Ai sensi del successivo art. 12, co. 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve inoltre ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione. Infine, si deve rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema […]. Neanche l'apparentemente corretta autenticazione dell'operazione è sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa fin troppo notoriamente quella […] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014; nonché Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

Tale orientamento ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, in tema di onere probatorio a carico del debitore professionale, nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, "in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio […]; infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere" (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777; in senso conforme, cfr., più di recente, Cass., 12.4.2018, n. 9158).
Tanto premesso in termini generali, rileva il Collegio che, nel caso di specie, il ricorrente disconosce due operazioni di bonifico di importo pari ad € 10.000,00 ed € 800,00.
Sul piano della regolarità formale delle operazioni di pagamento, l'intermediario afferma che l'operatività contestata è stata eseguita tramite il servizio internet banking, dotato di un sistema di autenticazione forte che prevede per il suo utilizzo:

- L'inserimento delle credenziali di accesso (codice utente e password di conoscenza esclusiva del cliente).
- L'inserimento di un codice "*usa e getta*", generato dal sistema della banca solo a seguito di una telefonata al numero verde, proveniente dall'utenza univocamente associata al cliente.

Più nel dettaglio, dichiara che tale presidio di sicurezza prevede "*la chiamata di sicurezza al Numero Verde dedicato della Banca con il proprio telefono cellulare certificato presso la Banca e [la digitazione] sulla tastiera del telefono chiamante del codice "usa e getta" che compare sulla schermata*".
A sostegno delle proprie deduzioni, parte resistente produce documentazione (non corredata da legenda esplicativa) riguardante i log relativi agli accessi all'app, registrati in data 28/12/2022 alle ore 10:39 per l'esecuzione del primo bonifico (che sarebbe successivamente avvenuta alle 10:46:56) e in data 29/12/2022 alle ore 16:56 per l'esecuzione del secondo bonifico (che sarebbe successivamente avvenuta alle 16:59:54).
In corrispondenza della colonna "*ID*" è presente il codice identificativo ***4-04 riconducibile al profilo utente del ricorrente.
In merito ai fattori di autenticazione richiesti, la voce "*DropCall*" in corrispondenza di ogni operazione riportata potrebbe indicare la telefonata al numero verde; la voce "*OK Esito positivo – Validaz."* in corrispondenza della colonna "*Esito Descr*" potrebbe invece rappresentare il buon esito delle operazioni in questione.
Il Collegio constata, tuttavia, che dall'esame della documentazione allegata non sembra evincersi il previo inserimento della password (fattore di conoscenza) e la digitazione del codice "usa e getta" da parte dell'utenza univocamente associata al cliente e generato dal sistema informatico della banca (fattore di possesso).
Si rileva, inoltre, che lo stesso intermediario, in sede di controdeduzioni, non sembra chiarire se tali operazioni siano state poste in essere direttamente dal device del ricorrente ovvero previo *enrollment* di nuovo dispositivo (quello del truffatore) associato alla sua utenza, né i log allegati sembrano dirimere tale circostanza. Il Collegio rammenta che, in fattispecie analoghe, dinanzi ad una ricostruzione del caso dal quale non v'è alcuna certezza su quale app sia stata utilizzata per l'esecuzione dell'operazione contestata, questo Arbitro ha ritenuto che difettasse la prova circa la regolare autenticazione delle operazioni contestate (cfr. Coll. Bari, dec. n. 12233/2022). Conformemente a tale orientamento, dunque, anche nel caso di specie deve ritenersi che emerga il medesimo difetto di prova che – alla luce del quadro normativo sopra richiamato – evidenzia un profilo di responsabilità imputabile in via esclusiva sull'intermediario.

Ad ogni modo – anche laddove si volesse ritenere che la transazione sia stata eseguita con l'app installata sul device del terzo – il Collegio constata che anche nelle schermate allegate relative alla fase di esecuzione dei due bonifici non sembrano riscontrabili i fattori di autenticazione richiesti per la loro esecuzione (i.e. password = fattore di conoscenza; telefonata al numero verde dall'utenza univocamente associata al cliente e digitazione di codice usa e getta "che compare sulla schermata" = fattore di possesso). La mancata prova dell'autenticazione comporta che la responsabilità dell'utilizzo fraudolento gravi integralmente sull'intermediario, senza che si proceda alla valutazione della colpa grave dell'utente (cfr. Collegio di Bari, dec. nn. 5054/22 e 1917/22). Di conseguenza la domanda sul punto avanzata dal ricorrente deve essere accolta.

**P.Q.M.**

**Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 10.800,00.**
**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