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) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore - NICOLA CIPRIANI

Seduta del 28/09/2023

FATTO

A. Il ricorrente si rivolge all'Arbitro affermando di essere titolare di conto corrente presso l'intermediario convenuto, con associazione del servizio di internet banking con massimali per le funzioni dispositive pari ad € 5.000 giornalieri ed € 25.000 mensili. Ciò premesso, il ricorrente illustra che, in data 06.09.2022, riceveva un sms da "infobanca" contenente un link che lo indirizzava ad una pagina internet, all'interno della quale inseriva il proprio codice utente. Successivamente, il ricorrente veniva contattato telefonicamente da un sedicente operatore dell'intermediario, il quale lo informava che il servizio di internet banking era in fase di aggiornamento e che, pertanto, non avrebbe potuto utilizzarlo nei giorni seguenti. Nei giorni successivi, il ricorrente riceveva ulteriori telefonate dal sedicente operatore, il quale lo rassicurava che il servizio sarebbe stato ripristinato "nell'arco di un paio di giorni". Dopo aver contattato il numero verde della resistente per chiedere informazioni in merito alla riattivazione del suddetto servizio, il ricorrente si avvedeva della presenza a sistema di un numero di cellulare e di un indirizzo email diversi rispetto a quelli comunicati in sede di sottoscrizione del contratto nonché di n. 8 operazioni di pagamento non autorizzate, costituite da sei bonifici e due prelievi cardless, per un totale di € 54.952,30. Sul punto, il ricorrente lamenta in primis il superamento dei limiti di plafond contrattualmente previsti e, in ogni caso, il mancato monitoraggio di operazioni anomale sia con riferimento all'importo ("€ 10.000 circa cadauna"), sia con riferimento alla frequenza ("un bonifico al giorno nell'arco di 7 giorni"). Pertanto, egli chiede la "restituzione dell'importo complessivo di € 54.952,30, maggiorata delle spese e commissioni di addebito e recall delle operazioni oggetto di truffa, nonché le spese per la presentazione del presente ricorso".

B. Costituitosi, l'intermediario fa preliminarmente presente che uno dei bonifici in contestazione, eseguito in data 12.09.2022, è stato riaccreditato al cliente in data 26/09/2022 a seguito di recall. Pertanto, l'intermediario chiede di rideterminare l'importo della controversia al netto dell'importo di € 2.000,00 relativo al citato bonifico.
Con riguardo ai limiti operativi concernenti le disposizioni di bonifico, l'intermediario precisa che i limiti di plafond originariamente previsti in contratto e menzionati in sede di ricorso sono stati elevati ad € 10.000 giornalieri ed € 50.000 mensili e che di tale modifica il ricorrente è stato debitamente informato mediante una "notifica pop up con presa visione obbligatoria", letta in data 27.11.2017 alle ore 06:42 PM. Inoltre, l'intermediario illustra le modalità: a) di accesso all'home banking (sia tramite app sia tramite pc); b) di disposizione di un bonifico tramite i predetti canali; c) di esecuzione dell'enrollment di un token software su nuovo device; c) di modifica dei dati personali a sistema. Con riferimento ai prelievi cardless, il resistente precisa che gli stessi consentono di effettuare prelevamenti presso ATM senza utilizzo della carta, con plafond di € 5.000 giornalieri ed € 25.000 mensili; sul punto, l'intermediario riporta i passaggi funzionali all'esecuzione di tali operazioni. Nel merito, l'intermediario rileva che il ricorrente ha fornito i dati necessari ai truffatori, dal momento che i medesimi non avrebbero potuto installare l'app senza la divulgazione della OTP. Effettuato l'accesso alla piattaforma, gli stessi procedevano anche alla modifica dei recapiti e-mail e numero di cellulare e il ricorrente ignorava in maniera negligente la comunicazione relativa alle predette modifiche. Invero, solo successivamente, il ricorrente comunicava di essere stato vittima di truffa e veniva così richiesta procedura di recall dei bonifici, conclusa tuttavia con esito negativo ad eccezione di quella relativa al bonifico di € 2.000,00 del 12/09/2022. Pertanto, l'intermediario chiede il rigetto del ricorso.
C. In sede di repliche, il ricorrente ridetermina l'importo complessivo del quale chiede il rimborso in € 52.952,30, in considerazione dell'esito positivo del recall del bonifico del 12.09.2022 di € 2.000. In ogni caso, il ricorrente rileva che, qualora fosse accertata la sua esclusiva responsabilità per la realizzazione della truffa a suo danno, l'intermediario deve essere tenuto perlomeno alla restituzione di € 27.952,30, pari alla differenza fra la somma complessiva fraudolentemente sottratta ed il massimale mensile di € 25.000,00.

DIRITTO

1. La controversia concerne una vicenda di utilizzo non autorizzato di uno strumento di pagamento (artt. 9 ss. d.lgs. 27 gennaio 2010, n. 11), nella specie consistente in n. 7 operazioni non autorizzate, di cui n. 2 prelievi cardless e 5 disposizioni di bonifico.
2. Il Collegio rileva innanzi tutto che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, 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 nuove 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).
3. 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 comma 2 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). Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, sí che la violazione di uno di essi 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 è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia 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 necessariamente 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 è 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. Da ultimo, cfr. Coll. Coord., decisione n. 22745/2019, 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).

L'orientamento di questo Arbitro ha trovato ripetuto riscontro nella giurisprudenza della Corte di cassazione, la quale ha avuto modo di chiarire che la disciplina speciale in materia di strumenti di pagamento ha esplicitato un 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., 3.2.2017, n. 2950; in senso conforme, più di recente, Cass., 12.4.2018, n. 9158; Cass., 26 novembre 2020, n. 26916, anche per l'importante statuizione, secondo cui "al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento - prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente - la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo").

4. Svolto questo doveroso inquadramento della disciplina, nel venire all'esame del caso oggi sottoposto all'attenzione del Collegio, si deve rilevare che, nella specie, l'intermediario, nell'affermare di fare uso della autenticazione "forte", ha fornito informazioni non univoche.

In particolare, l'intermediario eccepisce che le operazioni contestate, impartite a mezzo internet banking, sono state validate attraverso un sistema di autenticazione forte a due fattori. Più precisamente, il resistente afferma che: 1) per l'accesso tramite App, è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e delle credenziali statiche, mentre per l'accesso tramite browser/pc è necessario l'utilizzo congiunto della user id-password e del codice OTP generato dal Token Software, previa digitazione del PIN); 2) per la disposizione di un bonifico a mezzo App è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e del codice PIN, mentre per la disposizione di un bonifico a mezzo browser/pc è necessario l'utilizzo congiunto della lettura a video, tramite App, del QR code riferito alla singola operazione e del codice OTP generato dal Token Software, previa digitazione del PIN; 3) per quanto attiene l'enrollment del Token Software su un nuovo device è indispensabile l'utilizzo congiunto della userid-password e del codice OTP, inviato a mezzo e-mail; 4) per la modifica dei dati personali a mezzo App, è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e del codice PIN.

Ciò premesso, dall'esame dei log e dell'annessa legenda esplicativa, è possibile rinvenire l'autorizzazione del 06/09/2023 relativa alle operazioni di modifica dei dati personali (ore 12:24 e 14:39) e alla predisposizione dei bonifici disconosciuti, con i relativi login. Al contrario, non risulta presente in atti alcun riferimento all'operazione di enrollment del Token Software sul device dei truffatori, nonché alcuna indicazione su quali siano stati i fattori di sicurezza richiesti, sia in fase di login, sia nella successiva fase di autorizzazione delle

operazioni di bonifico e prelievo cardless. In altre parole, dalla documentazione prodotta dall'intermediario, non è possibile individuare i fattori di sicurezza utilizzati per l'attivazione del Token Software e per la successiva modifica dei recapiti intestati al ricorrente.

5. Tanto premesso, questo Collegio – ribadendo quanto già affermato in alcuni precedenti relativi a fattispecie analoghe (cfr. Collegio di Bari, Collegio di Bari, decisione n. 9425/2022) – ritiene che l'intermediario non abbia assolto l'onere probatorio relativo alla prova dell'autenticazione delle operazioni. In particolare, se è vero che dalle evidenze in atti risulta l'utilizzo della SCA nella fase esecutiva, non altrettanto può dirsi per quella di installazione dell'applicazione, rispetto alla quale non constano tracciature informatiche attestanti le modalità con le quali è stata effettuata la relativa configurazione sul device del terzo, né risulta presente documentazione relativa all'invio/ricezione degli SMS contenenti la OTP necessaria per configurare il codice *****id.

6. Con riferimento alla richiesta di rimborso delle commissioni pagate per l'esecuzione dei bonifici oggetto di disconoscimento e per le richieste di recall, il Collegio osserva che, dalla documentazione in atti (cfr., "lista movimenti al 16.09.2022", allegata al ricorso), si evince che l'importo commissionale complessivamente sostenuto è pari ad € 74,90, di cui € 56,90 addebitati a titolo di "commissioni su bonifici" ed € 18,00 addebitati a titolo di "commissione recall". Sul punto, l'intermediario non ha mosso specifiche contestazioni.

Pertanto, il Collegio ritiene che, anche sotto questo profilo, la domanda del ricorrente sia meritevole di accoglimento.

7. L'accoglimento della domanda nei termini sopra illustrati comporta l'assorbimento di ogni questione relativa al superamento dei massimali.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 53.027,00.

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