Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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 LUCA DI NELLA

Seduta del 16/09/2025

FATTO

La parte ricorrente espone, allega e chiede nel ricorso quanto segue.

- È titolare del conto corrente n. ***677 in essere presso l'intermediario convenuto, oltre che di altri conti corrente accesi presso gli intermediari B* e N*.
- Il 04.10.2024, alle ore 17:30 circa, riceveva una telefonata da un numero sconosciuto e si trovava ad interloquire con un sedicente operatore dell'intermediario N*, il quale gli riferiva in merito alla necessità di predisporre un aggiornamento all'applicazione per il rilascio di un certificato di sicurezza.
- Seguiva le istruzioni ricevute e scaricava l'App.
- Mentre compariva sul dispositivo mobile una schermata integralmente bianca recante la dicitura "N*** Aggiornamento in corso", il sedicente operatore chiedeva un paio di volte di poggiare sullo schermo l'impronta digitale.
- A un certo punto la telefonata veniva interrotta e il cellulare risultava completamente spento e resettato.
- Contattava immediatamente l'intermediario convenuto nonché gli altri due intermediari che disponevano il blocco dei rispettivi conti.
- Apprendeva poi che, durante la conversazione, i malviventi erano riusciti a controllare da remoto il device e avevano effettuato operazioni dai conti radicati presso gli intermediari B* e N* nonché dal conto acceso l'intermediario convenuto, dove erano stati eseguiti due pagamenti, rispettivamente di € 1.956,81 ed € 978,40, a mezzo della carta di debito tokenizzata.
- Date le sue particolari condizioni fisiche, rileva di essere incorso in un legittimo affidamento su quanto comunicato dall'interlocutore in merito ad asseriti messaggi precedentemente ricevuti e non letti.
- Afferma di non aver ricevuto SMS alert in merito alle operazioni disconosciute.
- Parte ricorrente chiede il rimborso di € 2.935,21, oltre interessi legali dalla domanda al saldo.

Nelle controdeduzioni l'intermediario espone, allega e chiede quanto segue.

- Le operazioni disconosciute dalla parte ricorrente sono state correttamente autorizzate mediante l'utilizzo delle credenziali statiche e dinamiche in suo possesso, con autenticazione forte a due fattori, e registrate e contabilizzate senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

- Gli accessi e le operazioni sono stati registrati da abituale dispositivo usato anche per gli accessi passati e futuri, mediante riconoscimento biometrico.
- Si avvale dell'art. 10 del Regolamento delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte del cliente, qualora non siano trascorsi 180 giorni dall'ultima volta che lo stesso ha avuto accesso con il doppio fattore.
- Nessuna "anomalia" è stata riscontrata dal proprio motore antifrode, che non poteva assolutamente essere a conoscenza della presunta intromissione di terzi nello smartphone della ricorrente tramite malware.
- Si tratta di una frode condotta mediante *vishing*, nella quale si individua una colpa grave della ricorrente, la quale con una media diligenza avrebbe potuto e dovuto smascherare ed evitare la truffa.
- L'intermediario chiede il rigetto del ricorso per tutti i motivi in fatto e in diritto sopra esposti.

In sede di repliche alle controdeduzioni parte ricorrente afferma quanto segue.

- La decisione n. 9591/24 del Collegio di Bologna ha chiarito che l'art. 10 Reg. UE 2018/389, significativamente rubricato "Informazioni sui conti di pagamento", dispone l'esenzione per la SCA, ma solo ed esclusivamente per l'accesso al conto a fini informativi, non certo anche per quell'accesso che avvenga al fine dell'esecuzione di disposizioni di pagamento.
- Qualora l'utilizzatore desideri compiere altre e differenti azioni da quelle elencate dall'art. 10, l'intermediario è tenuto a chiedere sempre la SCA, mentre ciò non è avvenuto nel caso di specie.
- Inoltre, non risultava attivo l'sms alert.

In sede di controrepliche l'intermediario afferma quanto segue.

- Nonostante si avvalga dell'art. 10 del Reg. delegato (UE) 2018/389 relativamente all'accesso informativo del saldo e delle ultime operazioni eseguite, tutti gli accessi sono avvenuti dal dispositivo abituale del cliente e tutte le operazioni che hanno portato all'esecuzione dei pagamenti disconosciuti nonché le stesse operazioni di pagamento online sono avvenute con autenticazione forte a doppio fattore.
- Nello specifico, la generazione del "CVV dinamico" della Carta di debito è stata eseguita con: accesso tramite Riconoscimento Biometrico (primo fattore – inerenza) e utilizzo della Conferma con Token (secondo fattore – possesso).
- I due pagamenti online sono stati entrambi eseguiti tramite inserimento del "CVV dinamico" generato ed autorizzazione con Conferma con Token.

DIRITTO

Nella presente vicenda parte ricorrente lamenta di essere stata vittima di una truffa perpetrata tramite una telefonata e un malware scaricato sul proprio device su indicazione del malvivente che poteva così controllarlo a distanza e disporre due pagamenti online con la carta di debito. L'attrice chiede il rimborso

dell'importo complessivo di € 2.935,21 in quanto dette operazioni sarebbero state disposte senza la SCA. A fini della decisione occorre valutare la condotta delle parti alla luce della PSD2 e del d.lgs. n. 11/2010.

Nella denuncia sporta all'autorità competente e nella sua integrazione parte ricorrente dichiara che il 4.10.2024, alle ore 17:30 circa, riceveva una telefonata da un numero sconosciuto. Si trovava così ad interloquire con un sedicente operatore dell'intermediario N*, il quale gli riferiva di dover eseguire degli aggiornamenti all'applicazione "N**" per il rilascio di un certificato necessario, in quanto aveva ignorato dei messaggi. Pertanto, le faceva scaricare un'App denominata "Certificato N**" con la quale le compariva una schermata integralmente bianca recante la dicitura "N*** Aggiornamento in corso". Nel corso della chiamata il sedicente operatore le chiedeva un paio di volte di poggiare sullo schermo l'impronta palmare a mo' di sblocco. Tuttavia, dopo essersi accorta che c'era qualcosa di strano, non riusciva più ad utilizzare il cellulare in quanto era completamente bloccato. Dopodiché, senza alcun saluto dell'interlocutore, si ritrovava con il telefono spento e ripristinato ai dati di fabbrica. Da un controllo successivo presso gli intermediari B* e N* apprendeva che, durante la conversazione, i malviventi erano riusciti a controllare da remoto il device e avevano effettuato alle ore 18:00 un bonifico di € 3.300,00 dal conto acceso presso B* a quello radicato presso N* e da quest'ultimo tre pagamenti online di € 0,10 (18:03), € 1.956,81 (18:04) ed € 1.318,27 (18:07) a favore di c****.com. L'importo complessivo della movimentazione è di € 3.300,00, per il quale l'intermediario B* ha attivato autonomamente la procedura di rimborso. In sede di integrazione della denuncia forniva il dettaglio di altri due bonifici disconosciuti di € 1.956,81 ed € 978,40.

Dalla documentazione in atti emerge che le operazioni disconosciute sono n. 2 pagamenti online per un importo complessivo di € 2.935,21, disposte tramite carta di debito. Il Collegio rileva altresì che con nell'ambito della medesima truffa è stato effettuato, alle ore 18:00, un bonifico istantaneo di € 3.300,00 addebitato sul conto radicato presso l'intermediario B* e accreditato sul conto in capo alla medesima ricorrente acceso presso l'intermediario N*, dal quale poi sono stati effettuati i n. 3 bonifici disconosciuti indicati in denuncia. Le operazioni oggetto del presente ricorso possono essere così sintetizzate:

DATA	ORA	TIPOLOGIA	IMPORTO
04/10/24	18:14	Pagamento online con carta	€ 1.956,81
04/10/24	18:18	Pagamento online con carta	€ 978,40

Secondo la disciplina posta dalla PSD2, è innanzi tutto onere dell'intermediario provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ex art. 10 d.lgs. n. 11/2010: in caso di mancanza della prova l'intermediario sopporta, in ogni caso, integralmente le conseguenze delle operazioni disconosciute. Qualora venga invece fornita la suddetta prova, occorre valutare se alla parte ricorrente sia imputabile una condotta connotata da dolo o colpa grave in violazione agli obblighi sui di lei gravanti in forza dell'art. 7, essendo altrimenti il rischio di operazioni fraudolente a carico dell'intermediario ai sensi dell'art. 12 d.lgs. n. 11/2010. La prova dei fatti a carico dell'utilizzatore dello strumento di pagamento è posta sull'intermediario dall'art. 10 d.lgs. n. 11/2010. In proposito, va

richiamato l'orientamento assunto dal Collegio di Coordinamento con la decisione n. 3947/2014, secondo la quale è comunque richiesto un quid pluris rispetto alla semplice dotazione del microchip per dimostrare la colpa grave o il dolo del cliente, gravando altrimenti l'allocazione legislativa della responsabilità in capo all'intermediario.

Il Collegio rileva che l'intermediario illustra quanto segue sulla base degli allegati versati in atti. Come risulta dai log, tutti gli accessi e le operazioni (log area riservata righe da 40 a 33) sono stati registrati da abituale dispositivo (Samsung Galaxy A71) usato anche per gli accessi passati e futuri (colonna K) mediante Riconoscimento Biometrico [Medio de autentificación (colonna G)]". Per l'accesso all'area personale, l'intermediario si avvale dell'art. 10 del Reg. delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte del cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso con doppio fattore: il 23/09/2024 (cfr. log righe 42 e 41) la ricorrente aveva fatto accesso con autenticazione forte tramite inserimento di username e password nonché OTP ricevuta sul numero di cellulare (349***) univocamente associato al suo conto. Gli accessi all'area personale della ricorrente delle ore 17:53:50 e 18:08:15 (log righe 40 e 39) venivano eseguiti con riconoscimento biometrico. Alle 18:11:38 (log riga 38), è stata registrata la generazione di un CVV dinamico della carta grazie all'accesso mediante Riconoscimento Biometrico [Medio de autentificación (colonna G)] e alla Conferma con Token [Tipo de firma (colonna H)]. Alle ore 18:14 e alle ore 18:18 venivano eseguiti i due pagamenti, rispettivamente di € 1.956,81 ed € 978,40 con l'inserimento del CVV dinamico appena generato (fattore di inerenza) o autorizzazione mediante Conferma con Token (fattore di possesso).

Ciò posto, dalle stesse dichiarazioni dell'intermediario emerge che l'accesso all'home banking prodromico all'effettuazione delle operazioni disconosciute è avvenuto avvalendosi dell'esenzione dalla SCA di cui all'art. 10 del Regolamento delegato UE 2018/389. Al riguardo, il Collegio ricorda quanto ha chiarito l'EBA in proposito: qualora l'intermediario decida di non adottare l'autenticazione forte applicando un'esenzione alla SCA normativamente prevista, nel caso in cui le operazioni siano state disconosciute dal cliente, resta ferma la sua responsabilità (fatta salva la frode dell'utilizzatore) per le perdite patrimoniali subite dal cliente stesso (cfr. EBA Q&A 2018-4042).

Il Collegio inoltre rileva che, oltre a quanto sopra richiamato in merito alla responsabilità in caso di esenzione, l'art. 10 del Regolamento Delegato dispone "sì l'esenzione per la SCA, ma solo ed esclusivamente per l'accesso al conto a fini informativi, non certo anche per quell'accesso che avvenga al fine dell'esecuzione di disposizioni di pagamento, come nel caso in esame (v., Collegio di Bologna, n. 11657/2024 e n. 9591/2024). Il Collegio ritiene pertanto che sull'intermediario debba inequivocabilmente gravare la responsabilità per le operazioni fraudolente, essendo la prima fase di autenticazione forte prodromica e necessaria al fine dell'esecuzione delle stesse.

Sulla rimborsabilità degli interessi legali, questi vengono riconosciuti dal Collegio dal reclamo al saldo su puntuale richiesta della ricorrente, come nel caso in esame (cfr. Collegio di coordinamento n. 5304/2013).

Alla luce di quanto sopra esposto il Collegio ritiene il ricorso meritevole di accoglimento e riconosce il diritto della parte ricorrente a ottenere dall'intermediario la somma di € 2.935,21, oltre interessi legali dal reclamo al saldo.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 2.935,00 (duemilanovecentotrentacinque/00), oltre interessi legali dalla data del reclamo.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
CHIARA TENELLA SILLANI