

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore ELEONORA MIRABELLI

Seduta del 03/03/2026

FATTO

La ricorrente, anche per mezzo della documentazione allegata al ricorso, riferisce di essere titolare della carta n. 5333***1203 e che, in data 16/10/2025 è stata vittima di una truffa realizzata tramite chiamata e SMS. In particolare, alle ore 16:00 circa del 16/10/2025, riceveva una telefonata dall'utenza n. 347***098, a cui non rispondeva e, dopo un minuto, riceveva un SMS dal cellulare n. 344***140 in cui veniva avvisata della scadenza della sua carta e del blocco della spedizione della nuova carta, laddove non avesse risposto alla chiamata entro le ore 19:00. Successivamente, alle ore 16:12, riceveva una nuova telefonata dall'utenza n. 347***098, durante la quale un sedicente operatore le rappresentava la necessità di comunicare tramite SMS il codice PIN della carta in suo possesso al fine di attivare la nuova carta; dunque, immediatamente, inviava un SMS al cellulare n. 344***140 riportante il PIN e contestualmente riceveva un SMS riportante il nuovo codice segreto; le operazioni avvenivano nel corso della telefonata e il truffatore comunicava altresì che, se il PIN fosse risultato esatto, la nuova carta sarebbe arrivata presso la sua residenza in data 20/10/2025. Una volta compresa la truffa, si recava immediatamente presso l'ufficio dell'intermediario e visionava l'estratto conto della sua vecchia carta, ove risultava un'operazione non autorizzata di € 3.998,04 con causale "rimborso per rinnovo carta scaduta del 16/10/2025". Secondo l'operatore della banca, i frodatori avevano spostato la somma dalla vecchia alla nuova carta di cui non era in possesso e non conosceva gli estremi; contattava quindi immediatamente il numero verde ufficiale dell'intermediario (n. 800***322) e richiedeva alle ore 17:20 del 16/10/2025 il blocco della carta; tuttavia, l'operatore del servizio clienti riferiva che il blocco non era

necessario in quanto il saldo risultava pari a zero. La carta però risultava attiva e, in data 21/10/2025, veniva eseguito fraudolentemente un prelievo ATM di € 380,00. Lamenta quindi la ricorrente che la banca ha omesso di bloccare tempestivamente la carta, permettendo l'esecuzione del prelievo ATM e violando i propri obblighi e che, in data 21/10/2025, l'intermediario comunicava l'attivazione della procedura di rimborso pari a € 2.185,50, corrispondente al 50% dell'importo complessivo contestato in quanto lo stesso affermava la corretta autorizzazione delle operazioni mediante inserimento del PIN e la sua parziale responsabilità. Conclude dunque la ricorrente chiedendo a codesto Arbitro adito la condanna della Banca al rimborso della somma di euro 2.192,54 corrispondente al 50% restante dell'importo non ancora restituito.

L'intermediario, in sede di controdeduzioni, dichiara di aver provveduto a rimborsare il 50% delle operazioni contestate, riaccreditando la somma di € 2.185,50 sulla carta della cliente e che l'importo totale indicato nel ricorso differisce dal totale effettivamente sottratto alla ricorrente, che corrisponde a € 4.371,00. Rileva la Banca che la truffa è avvenuta mediante tecniche di *social engineering* e *boxing* e che la ricorrente assecondava le richieste avanzate dall'interlocutore e rispondeva a un SMS proveniente da un'utenza telefonica privata comunicando al sedicente operatore il codice PIN, il quale rimane invariato in tutti i casi di sostituzione della carta, consentendo il verificarsi delle transazioni fraudolente in quanto lo stesso risulta necessario al fine di attivare il nuovo strumento di pagamento e la tecnologia Emv, con cui è stata processata la carta, non consente la diretta lettura del codice segreto. Rileva inoltre che la carta è stata attivata presso ATM a seguito del corretto inserimento del PIN e che la ricorrente non ha correttamente gestito l'operazione di consegna della carta in quanto la posta ordinaria, con cui vengono inviate le carte rinnovate, può incorrere nel rischio di furti e accessi non autorizzati. Segnala poi che l'autorizzazione delle operazioni è avvenuta mediante lettura del CHIP e inserimento del vecchio PIN, in assenza di precedenti tentativi di digitazione e che sussiste una sostanziale coincidenza temporale fra il momento del furto e quello del prelievo quindi la comunicazione del PIN è avvenuta poco prima rispetto al prelievo contestato, posto che l'SMS fraudolento è stato ricevuto dalla cliente alle ore 15:14, mentre la prima operazione contestata è stata autorizzata alle ore 15:52 e che il blocco della carta è avvenuto alle ore 09:50 del 21/10/2025, nonché successivamente alle operazioni contestate. L'intermediario afferma di mettere a disposizione dei propri clienti il servizio di SMS *Alert*, il quale può essere attivato gratuitamente e *di default* all'interno dell'app e che parte ricorrente ha violato gli obblighi contrattuali concernenti la segretezza dei codici e delle credenziali, i quali non devono essere condivisi con terzi; sussiste dunque la colpevolezza in capo alla ricorrente, la quale avrebbe potuto evitare la truffa mediante la diligenza media. Tra l'altro, la Banca interloquisce con i propri clienti solo tramite canali ufficiali e non richiede mai la comunicazione di dati inerenti agli strumenti di pagamento e che ha realizzato molteplici campagne informative in ordine alla sicurezza delle operazioni di pagamento e ai principali schemi di frode. Conclude dunque l'intermediario chiedendo il rigetto del ricorso in quanto infondato in fatto ed in diritto.

In sede di repliche, la ricorrente afferma che l'utilizzo del PIN non costituisce prova dell'autorizzazione del cliente, quando la credenziale è stata carpirata mediante tecniche di *social engineering* e che il sedicente operatore l'ha indotta in errore, ottenendo fraudolentemente il codice PIN; non ha infatti mai voluto autorizzare le operazioni di pagamento e non sussiste la sua colpa grave in ragione della compromissione della capacità di autodeterminazione e che la mancata disposizione del blocco da parte dell'intermediario integra una grave violazione dei propri obblighi e infine che il parziale rimborso riconosciuto dall'intermediario costituisce un implicito riconoscimento della propria responsabilità.

DIRITTO

Le operazioni contestate consistono in n. 11 ricariche e n. 4 prelievi ATM eseguiti in data 16/10/2025 e 20/10/2025 per un totale di € 4.371,00. A tali transazioni si aggiunge n. 1 ricarica di € 3.998,04 eseguita alle ore 16:22 del 16/10/2025. Tale importo risulta negli accrediti e sembrerebbe costituire una provvista atta a consentire l'esecuzione delle successive operazioni fraudolente.

Nel reclamo e nelle controdeduzioni, l'intermediario afferma di aver attivato la procedura di parziale rimborso in favore della ricorrente, in ragione del riconoscimento della paritaria responsabilità tra le parti. Sul punto, l'importo oggetto di rimborso è pari a € 2.185,50, nonché al 50% della somma contestata, ed è stato riconosciuto dalla ricorrente in sede di ricorso e controrepliche.

Il Collegio rileva che le operazioni contestate sono state poste in essere 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), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Per consolidato orientamento dei Collegi ABF, a fronte del disconoscimento delle operazioni da parte del cliente, è onere dell'intermediario provare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata, ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010 che così statuisce: *“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”*. In mancanza di tale prova, dunque, l'intermediario sopporta – in ogni caso – integralmente le conseguenze delle operazioni disconosciute.

Con riguardo alla modalità di autenticazione delle operazioni, l'art. 10 bis del medesimo D.Lgs. n. 11/2010 prevede: *“Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, 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”*. L'art. 1, lettera q bis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in *“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”*. Sul punto, è intervenuta l'EBA con la *“Opinion”* del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27.11.2017), nella quale sono stati passati in rassegna alcuni dei più comuni sistemi di autenticazione predisposti dagli intermediari per valutare se possano o meno annoverarsi tra i presidi di autenticazione forte.

Occorre dunque verificare se, nel caso di specie, le operazioni contestate siano state autenticate mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. *“autenticazione forte”*.

Pur avendo l'intermediario dedotto di aver adottato un sistema a due fattori per la protezione dei suoi clienti, non risultano chiare e complete evidenze che tale sistema di autorizzazione sia stato conformemente applicato anche nel caso di specie.

L'intermediario infatti non fornisce evidenza documentale con riferimento alla modalità di autenticazione dell'operazione di ricarica della carta, operazione che è risultata necessaria al fine di attivare la stessa ed effettuare le successive operazioni fraudolente oggetto di ricorso.

Tenuto conto della specifica distribuzione dell'onere probatorio imposta dalla normativa di settore, si deve porre a carico esclusivo dell'intermediario le conseguenze della truffa perpetrata ai danni della ricorrente, indipendentemente da qualsivoglia profilo di colpa da parte di quest'ultimo (cfr. fra le tante, Collegio di Bari n. 35/2023 *"la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente; la prova dell'autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente"*).

Si riporta a questo riguardo una recente pronuncia (Collegio Milano 15341/2022) nella quale si legge: *"Dato il fallimento della prova dell'adozione di un sistema di autenticazione forte, diviene irrilevante accertare se siano fondate le controdeduzioni dell'intermediario tese a dimostrare la colpa grave del cliente (che sarebbe stato vittima di un tipo di frode facilmente evitabile con una diligenza media) nell'adempimento degli obblighi di cui all'art. 7 del d.lgs. 27.1.2010, n. 11. Per escludere la responsabilità dell'intermediario, infatti, sarebbe necessario provare che il cliente ha agito in modo fraudolento (art. 12 2-bis del citato decreto legislativo). Pertanto, sempre richiamato l'art. 12 2-bis del d.lgs. 27.1.2010, n. 11 ("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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente"), la responsabilità per l'esecuzione fraudolenta del bonifico grava sull'intermediario. La domanda del cliente, dunque, merita pieno accoglimento"*.

Difettando, dunque, la prova dell'intermediario resistente circa le modalità di autenticazione dell'operazione relativa alla ricarica della carta, operazione necessaria per costituire la provvista atta a consentire l'esecuzione delle successive operazioni fraudolente, il Collegio ritiene che la domanda presentata dalla parte ricorrente meriti accoglimento.

Per quanto attiene invece la domanda formulata da parte ricorrente relativa all'accertamento da parte di codesto Arbitro della condotta negligente dell'intermediario, si ritiene che la stessa non debba essere esaminata in quanto assorbita dall'accoglimento delle domande precedenti.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 2.193,00 (duemilacentonovantatré/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