Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 20/01/2026

FATTO

Con ricorso depositato il 15.10.2025, la parte ricorrente ha contestato l'addebito di tre operazioni di pagamento effettuate sul proprio conto corrente, rispettivamente di € 1.295,00, € 1.036,00 ed € 518,00, per un importo totale di € 2.849,00, affermando di non averle mai disposte né autorizzate.

In particolare, rappresenta di aver ricevuto in data 08.09.2025, intorno alle ore 18:00, un messaggio tramite l'applicazione del circuito dei pagamenti dell'intermediario, nel quale le veniva richiesto di contattare un numero telefonico per il blocco della carta. Ha contattato il numero indicato e ha interloquito con un soggetto qualificatosi come operatore, il quale le ha fornito indicazioni per bloccare presunti pagamenti non autorizzati. Dichiara di non aver digitato codici né comunicato dati sensibili e di aver ricevuto, nel contempo, un SMS proveniente dal gruppo cui appartiene l'intermediario, con cui le

veniva comunicato il blocco della carta e dell'applicazione bancaria per motivi di sicurezza. Sulla base di tali circostanze, la ricorrente ha affermato di essere stata vittima di una truffa di tipo *smishing*.

L'intermediario resistente, costituendosi nel procedimento, ha ricostruito i fatti evidenziando che la ricorrente è titolare di rapporto di conto corrente sul quale è operativa una carta di pagamento. In data 8.08.2025, mediante l'utilizzo di tale carta, sono state effettuate tre operazioni di pagamento su un sito di commercio elettronico, per l'importo complessivo contestato. A seguito della denuncia presentata il giorno successivo 09.09.2025, l'intermediario aveva inizialmente ripristinato il saldo del conto, riservandosi di effettuare ulteriori verifiche, a seguito delle quali aveva comunicato l'esito negativo del disconoscimento e riaddebitato le somme.

Secondo quanto dedotto dall'intermediario, le operazioni risultano autorizzate mediante il corretto utilizzo delle credenziali personali della ricorrente, attraverso una procedura conforme ai requisiti della *strong customer authentication*, che prevede l'impiego congiunto di fattori statici e dinamici. L'intermediario ha inoltre evidenziato che le modalità della truffa descritte non sono in alcun modo riconducibili ai propri servizi, né per l'asserito SMS ricevuto, di cui contesta la mancata produzione, né per il numero indicato nel messaggio. Nonostante nel ricorso si affermi che "*non veniva digitato alcun codice né forniti dati sensibili*", la ricostruzione dei fatti e la documentazione prodotta dalla banca provano che le operazioni fraudolente sono state rese possibili solo grazie all'inserimento delle credenziali in possesso della cliente.

Rileva infine che, in occasione delle operazioni contestate, erano stati inviati alla ricorrente specifici messaggi di *alert*, dal contenuto chiaro e inequivocabile, relativi all'autorizzazione dei singoli pagamenti, che non avevano determinato alcuna reazione impeditiva da parte della stessa.

Conclude chiedendo di dichiarare inaccoglibile il ricorso e, in denegata ipotesi che il Collegio ritenga di ravvisare profili di responsabilità in capo all'intermediario, di definire la ripartizione fra le parti del danno in misura proporzionale alle rispettive effettive responsabilità ed in particolare ai sensi dell'art. 1227, 1 e 2 comma c.c., con applicazione della franchigia di € 50,00 contemplata dalla normativa in materia di servizi di pagamento.

DIRITTO

Le operazioni contestate rientrano nell'ambito di applicazione del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13.01.2018) del D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno e alla disciplina in materia di *strong customer authentication* (SCA).

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave in capo all'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Nel caso di specie, le operazioni oggetto di controversia consistono in tre pagamenti *on line* effettuati con carta per l'importo complessivo di € 2.849,00 eseguiti in data 08.09.2025 rispettivamente alle ore 17:27 per € 1.295,00, alle ore 17:30 per € 1.036,00 e alle ore 17:32 per € 518,00.

L'intermediario ha prodotto evidenze idonee a dimostrare che dette operazioni sono state correttamente registrate, contabilizzate e autorizzate mediante procedura di *strong customer authentication*. Risulta infatti che il *device* con codice univoco abitualmente impiegato dalla cliente, anche nei mesi precedenti alla truffa, è stato utilizzato per autorizzare da APP le operazioni di pagamento e che ciascuna autorizzazione è avvenuta mediante validazione del codice OTP generato dalla APP previa digitazione del PIN.

Tali elementi consentono di ritenere raggiunta la prova dell'autenticazione in senso tecnico, presupposto logico necessario per procedere alla valutazione della condotta dell'utilizzatore ai fini dell'accertamento della colpa grave (cfr. cit. Collegio di Coordinamento, decisione n. 22745/2019).

Sotto tale profilo, rileva che la ricorrente non ha prodotto evidenza dell'SMS civetta pur asseritamente riferito non direttamente all'intermediario, ma al circuito dei pagamenti di cui si serve quest'ultimo. Anche in relazione alla successiva chiamata, la cliente non produce evidenza. Tuttavia nel ricorso, indica di aver contattato il numero 02***357, come richiestole nel messaggio, che, sulla base delle verifiche svolte, non è riferibile all'intermediario resistente.

Secondo l'orientamento consolidato dei Collegi, una volta accertata la sussistenza della *strong customer authentication,* le mancate allegazioni e produzioni documentali dell'utente sulle concrete modalità della frode, possono essere valorizzate, per fondare il convincimento circa la colpa grave dell'utente, come nel caso di specie, in cui le dette omissioni non consentono di stabilire se vi sia stato un legittimo affidamento circa la genuinità delle comunicazioni ricevute.

Ciò nondimeno, anche in presenza di una colpa grave del cliente, il Collegio è chiamato a valutare anche la condotta dell'intermediario alla luce dell'operatività concretamente posta in essere e degli obblighi di controllo e monitoraggio gravanti sul prestatore dei servizi di pagamento.

Come noto, la necessità che gli intermediari operanti nel settore si dotino di sistemi di monitoraggio capaci di intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.dd. sospette si evince dalle indicazioni contenute nel D.M. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento").

In particolare, l'art. 8 del D.M. 112/2007 identifica i casi di frode che vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento. Sebbene detta normativa si riferisca alle operazioni effettuate con carta fisica, essa è stata ritenuta applicabile dalla giurisprudenza ABF anche alle operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche online) in ragione dell'unicità della *ratio*. Per completezza, occorre ricordare che anche l'art. 2 del Regolamento Delegato (UE) n. 2018/389 impone agli intermediari di predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente, sebbene l'EBA abbia precisato che non è comunque richiesto un monitoraggio delle operazioni in tempo reale (si veda la Q&A EBA relativa alla *Question* ID 2018_4090).

Nel caso in esame, sulla base delle evidenze in atti, risulta integrato l'indice di anomalia espressamente previsto dal D.M. 112/2007, art. 8, lett. a), punto 2, che individua quale fattispecie rilevante, ai fini del monitoraggio delle frodi, la presenza di tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle ventiquattro ore presso un medesimo punto vendita.

Le tre operazioni contestate risultano effettuate in un arco temporale estremamente ristretto e presentano una progressione decrescente degli importi, collocandosi nel contesto di una sequenza tipica di operazioni fraudolente di test e consolidamento.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

La presenza di notifiche *push*, pur rilevante ai fini della prova dell'autenticazione, non esaurisce l'obbligo dell'intermediario di presidiare il rischio di frode in presenza di segnali di anomalia, dovendo tali sistemi di allerta essere letti in combinazione con i presidi interni di monitoraggio delle transazioni, come richiesto dal d.lgs. n. 11/2010, nonché dai principi di diligenza qualificata di cui all'art. 1176, comma 2, cod. civ..

Secondo l'orientamento costante dei Collegi, le previsioni del D.M. n. 112/2007 non hanno valore precettivo diretto in materia di disconoscimento delle operazioni di pagamento, né determinano automaticamente l'obbligo di rimborso di un numero predeterminato di transazioni. Esse costituiscono tuttavia un parametro qualificato per la formulazione di un giudizio in concreto sulla diligenza tecnica dell'intermediario e sull'adeguatezza dei presidi di prevenzione delle frodi.

In tale prospettiva, mentre per le prime due operazioni l'intermediario ha fornito un quadro complessivo idoneo a sostenere la riconducibilità delle stesse alla sfera di controllo dell'utilizzatore, per l'ultima operazione permangono profili di criticità connessi alla gestione degli indici di anomalia, che impediscono di ritenere integralmente assolto l'onere di presidio gravante sul prestatore di servizi di pagamento.

Ne consegue che, limitatamente alla terza operazione, di importo pari a € 518,00, il ricorso deve essere accolto. Il Collegio rileva, infine, che non è applicabile la c.d. "franchigia" di € 50,00, richiesta espressamente in via subordinata dall'intermediario "*in quanto la stessa è prevista in ipotesi di 'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n.11/2010)*" (Collegio di Coordinamento, decisione n. 22745 del 10 ottobre 2019).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 518,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE