

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) DELL'ANNA MISURALE

Seduta del 29/01/2026

FATTO

il cliente espone quanto segue:

- è correntista presso il primo intermediario e titolare di carta di credito emessa dal secondo intermediario;
- ha ricevuto, in data 24.07.2024, un SMS apparentemente riconducibile al secondo intermediario, e ha cliccato sul link ivi indicato;
- ha inserito le credenziali sull'apparente portale che riportava tutte le caratteristiche e peculiarità del portale "genuino";
- si è avveduto che, nell'intervallo temporale compreso tra il 26.07.2024 e il 22.08.2024, terzi ignoti avevano eseguito, con addebito sulla sua carta di credito, n. 65 operazioni per il complessivo importo di € 2.207,66;
- ha disconosciuto le operazioni compiute fraudolentemente da terzi ignoti e ha ricevuto dal secondo intermediario un rimborso, per il complessivo importo di € 344,83, relativamente a n. 5 delle n. 65 operazioni eseguite dai terzi truffatori;
- di aver depositato denuncia-querela;
- ha chiesto il rimborso integrale presentando reclamo ad entrambi gli intermediari, senza esito positivo;
- contesta il rigetto della domanda di rimborso, sussistendo la responsabilità contrattuale o, comunque, da "contatto sociale" degli intermediari convenuti, che sono tenuti a predisporre qualsiasi mezzo idoneo onde evitare il verificarsi di eventi pregiudizievoli quale quello occorso;
- non sussiste alcun elemento di colpa grave a carico del cliente;
- il tipo di operatività fraudolenta integra i presupposti di cui all'art. 8 del D.M. n. 112/2007, a fronte della sussistenza di un indice di anomalia, ossia la sussistenza di "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento".

Chiede, pertanto, la restituzione di € 1.862,83, o la diversa somma che l'Arbitro riterrà di giustizia, oltre al rimborso della somma versata per la presentazione del ricorso e le spese legali, da liquidarsi in via equitativa.

Il primo intermediario eccepisce il proprio difetto di legittimazione passiva, affermando che la carta di credito oggetto di utilizzo fraudolento è emessa dal secondo intermediario; assume di essere mero collocatore dello strumento di pagamento ed evidenzia che le previsioni contrattuali individuano il secondo intermediario quale soggetto tenuto a riscontrare i reclami e a rimborsare le operazioni non autorizzate.

Chiede, pertanto, dichiararsi l'inammissibilità del ricorso e comunque rigettarlo nel merito.

Il secondo intermediario afferma quanto segue:

- il cliente è stato vittima di un attacco di tipo smishing, nel corso del quale ha volontariamente inserito – all'interno di un link contenuto in un SMS fraudolento – le proprie credenziali di accesso e i codici OTP ricevuti sul proprio telefono cellulare. È evidente che tali condotte configurano una grave violazione degli obblighi di custodia degli strumenti di sicurezza;
- il link contenuto nel messaggio non è in alcun modo riconducibile all'intermediario,
- il caso rientra quindi nella categoria dei tentativi di truffa in materia di servizi di pagamento realizzati con modalità telematiche che si svolgono secondo uno schema tipico e ampiamente noto;
- i pagamenti e-commerce contestati e non rimborsati sono stati convalidati con riconoscimento biometrico precedentemente registrato su device abilitato, che invece rappresenta l'elemento di possesso. In questo modo si rispetta la condizione di verifica di almeno due fattori;
- il ricorrente non ha ritenuto di tutelarsi nemmeno attraverso un altro dei sistemi di controllo offerti, il servizio "Spending Control", che consente di personalizzare la spendibilità della carta in relazione alla zona geografica e alla categoria merceologica degli esercenti o, persino, mettendola "in pausa" fino a 48 ore;
- nel merito degli indici di anomalia richiamati da parte ricorrente, si osserva che anche nel caso in cui si siano verificati indici di anomalia di cui al DM n. 112/2007, ciò non comporta automaticamente che per le operazioni successive al verificarsi della circostanza l'intermediario debba essere tenuto alla restituzione totale delle somme, ma deve essere valutata, in concreto e caso per caso, la colpa specifica del ricorrente;
- inoltre, come ricavabile anche dagli estratti conto allegati da parte ricorrente, le transazioni contestate sono intervallate da transazioni genuine compiute dal titolare della carta;
- un ulteriore elemento che denota la condotta negligente del ricorrente è rappresentato dalla segnalazione tardiva delle anomalie riscontrate, come già evidenziato dalla giurisprudenza di riferimento. Il ricorrente, infatti, aveva la possibilità di monitorare costantemente le operazioni effettuate con la carta, sia tramite l'app dedicata sia accedendo al portale titolari. Inoltre, era stato regolarmente informato via e-mail della pubblicazione dell'estratto conto online del mese di luglio, ma non si è premurato ad accedere alla propria area riservata per prenderne visione. Tale accesso è avvenuto solo in data 24 agosto, contestualmente alla richiesta di blocco della carta, ovvero con un mese di ritardo rispetto all'invio dei messaggi contenenti i codici OTP e alla prima operazione poi disconosciuta;
- appare evidente che un controllo tempestivo dei movimenti registrati sulla carta avrebbe potuto limitare significativamente l'entità del danno, che invece è aumentato proprio a causa dell'inerzia del ricorrente.

Chiede, pertanto, il rigetto del ricorso.

Il cliente, richiamati i propri scritti, contesta l'eccezione di carenza di legittimazione attiva sollevata dal primo intermediario, posto che il rapporto relativo alla carta di credito si pone "a valle" di un ordinario rapporto di conto corrente "a monte". Osserva che le pattuizioni negoziali efficaci tra le parti non prevedevano alcuna indicazione dell'intermediario responsabile per la prova di autenticazione ed esecuzione delle operazioni di pagamento o per la loro inesatta esecuzione, né alcuna indicazione circa il soggetto cui inviare i reclami.

Il primo intermediario insiste nell'eccezione di carenza di legittimazione passiva, evidenziando, in particolare, che il contratto *inter partes* individua specificamente il secondo intermediario quale soggetto emittente della carta di credito.

Il secondo intermediario non ha presentato controrepliche.

DIRITTO

La questione sottoposta all'esame del Collegio riguarda il disconoscimento di n. 65 operazioni, per un importo complessivo di € 2.207,66 eseguite tramite carta di credito nel periodo dal 26 luglio al 22 agosto 2024.

Il secondo intermediario ha già pacificamente rimborsato € 344,83, relativamente a n. 5 delle n. 65 operazioni disconosciute.

Occorre in primo luogo esaminare l'eccezione di difetto di legittimazione passiva, sollevata dal primo intermediario sul rilievo di essere soltanto collocatore della carta oggetto del ricorso, emessa e gestita dal secondo intermediario.

Secondo l'orientamento condiviso dai Collegi territoriali, in via generale – in ragione del rapporto contrattuale instaurato tra l'utente e il collocatore dello strumento di pagamento – sussiste la legittimazione passiva di quest'ultimo, con conseguente onere della prova sull'autenticazione delle operazioni contestate.

Fa eccezione l'ipotesi in cui il PSP sia "mero" collocatore della carta: per accertare questo profilo si ha riguardo alla documentazione agli atti (a titolo esemplificativo, se la denominazione e il marchio dello strumento sono riconducibili esclusivamente all'emittente, si tratta di "mero" collocatore; se le previsioni contrattuali affidano al collocatore il ruolo di riscontro all'utenza in caso di reclami, ovvero se il collocatore ha risposto al reclamo dell'utente senza segnalargli l'eventuale difetto di legittimazione passiva, non si tratta di "mero" collocatore).

Al riguardo, si osserva quanto segue.

In atti è prodotto il contratto *inter partes* relativo alla carta di credito che riporta il logo indicante la precedente denominazione del secondo intermediario oggi convenuto.

L'art. 1 delle condizioni generali individua espressamente il secondo intermediario (nella sua precedente denominazione) quale emittente della carta, mentre il ruolo del primo intermediario è unicamente quello di banca incaricata di inoltrare la richiesta di emissione della carta.

L'art. 5 prevede che la carta è rilasciata dall'emittente. L'art. 13 del contratto individua, inoltre, l'emittente quale soggetto cui comunicare lo smarrimento, la sottrazione o la falsificazione della carta.

Il primo intermediario compare esclusivamente nel modulo di richiesta della carta emessa dal secondo intermediario, coerentemente con quanto previsto dalle citate condizioni generali.

Infine, il regolamento della carta di credito attualmente vigente prevede che il titolare debba trasmettere i reclami al secondo intermediario, ossia all'emittente della carta.

Nel caso di specie, il cliente ha presentato reclamo nei confronti di entrambi gli intermediari, ma il primo intermediario si è limitato, nel riscontrarlo, ad evidenziare il suo ruolo di "mero collocatore" senza rispondere nel merito.

Il secondo intermediario ha, invece, risposto nel merito al reclamo, procedendo altresì al rimborso di determinate operazioni.

Da tutto quanto sopra esposto si ricava che il cliente non avrebbe dovuto presentare il ricorso anche nei confronti del primo intermediario perché mero collocatore della carta.

Si procederà dunque ad esaminare la domanda esclusivamente con riferimento al secondo intermediario (d'ora in avanti semplicemente intermediario).

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate.

Deve, dunque, procedersi ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010. Più in generale, le fonti normative applicabili alla fattispecie 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 è richiesta l'autenticazione forte (SCA) 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.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ciò premesso, per quanto attiene al primo profilo sopra individuato, vale a dire l'onere di provare la SCA, l'intermediario produce documentazione dalla quale si ricava la sussistenza dell'autenticazione forte per ogni fase delle operazioni.

Con riferimento alla fase di *enrollment*, l'intermediario ha prodotto evidenze dalle quali si trae che l'utenza telefonica destinataria dell'SMS corrisponde a quella indicata dal cliente nel modulo di ricorso; risulta effettuata l'attività "FINALIZE_LOGIN", mediante accesso da app ("CANALE = APP"); in base alla legenda, "FINALIZE_LOGIN" indica l'*"accesso all'area personale e contestuale certificazione del nuovo dispositivo"*; è presente il valore "AUTH_METHOD: OTP", che indica l'autenticazione mediante *"password statica + OTP sms"*; è presente la dicitura "ESITO_SCA": 000, autenticazione forte avvenuta correttamente con SMS OTP o con riconoscimento biometrico; l'invio di un SMS OTP recante il testo: *"ATTENZIONE. Non comunicare mai a terzi questo codice: se lo chiedono è una frode. Usa *** per confermare l'installazione di ** * sul nuovo dispositivo"*.

Si tratta di evidenze che, secondo il più recente orientamento dei Collegi, possono essere valutate ai fini di verificare l'assolvimento dell'onere della prova della SCA, ciò in quanto a tal fine rilevano (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese o ammesso dal cliente con dichiarazioni confessorie che assumono il valore di prova legale ai sensi dell'art. 2730 c.c.

In adesione a tale orientamento, il Collegio di Milano, nelle sue più recenti decisioni in presenza di evidenze informatiche analoghe a quelle rilevanti nel caso di specie ha valorizzato la formulazione dei log prodotti dall'intermediario e, dandone una lettura congiunta con la legenda

esplicativa, ha ritenuto provato l'inserimento della password e, conseguentemente, la SCA (cfr. Collegio di Milano, decisione n. 6153/2025).

In particolare, quanto all'evidenza dell'inserimento della password in fase di accesso, essa risulta dal valore AUTH_METHOD=OTP che, secondo la legenda, indicherebbe che è stato richiesto l'inserimento della password, oltre all'OTP SMS (di cui è presente evidenza in atti). Risulterebbero quindi utilizzati un fattore di conoscenza (la password) e un fattore di possesso (l'OTP sms).

Inoltre, dalla documentazione può trarsi prova della SCA anche con riferimento all'attivazione della biometria sul *device* utilizzato per disporre le operazioni disconosciute.

L'intermediario afferma che il cliente ha presumibilmente comunicato al truffatore il codice OTP SMS necessario per autorizzare l'attivazione della funzionalità di riconoscimento biometrico sul nuovo dispositivo certificato.

Al riguardo, produce evidenze dalle quali si ricava:

- l'attivazione della funzionalità di riconoscimento biometrico ("REGISTRAZIONE_BIOMETRIA") effettuata mediante app ("CANALE = APP");
- l'attivazione della biometria sul nuovo dispositivo avvenuta nella medesima sessione in cui è avvenuta l'attività di "FINALIZE_LOGIN" (campi di "SESSION_ID");
- l'invio di un SMS OTP sull'utenza telefonica del cliente, recante il testo: *"ATTENZIONE. Non comunicare a terzi questo codice: se dovessero chiedertelo, è un tentativo di frode. Usa *** per accedere al servizio *** che hai richiesto"*;
- è presente il campo AUTH_METHOD: SMS, ossia "richiesto OTP";
- l'"ESITO SCA" riporta l'indicazione "SMS con OTP successivo ad accesso con SCA (password statica + SMS con OTP), nel caso di specie nella medesima SESSION_ID del FINALIZE_LOGIN".

Risulta quindi che il riconoscimento biometrico è stato attivato con l'OTP SMS inviato sull'utenza telefonica del cliente (elemento di possesso), secondo quanto indicato nella legenda esplicativa, nella medesima sessione in cui era stato effettuato l'accesso dal nuovo dispositivo.

Si sottolinea che l'EBA ritiene "riutilizzabile" il primo fattore (nella specie costituito dalla password), purché l'azione avvenga, come nel caso di specie, nell'ambito della medesima sessione (Q&A EBA 2018_4141).

Infine, per quanto attiene all'autenticazione forte con riferimento alle operazioni disconosciute, l'intermediario osserva che i pagamenti e-commerce contestati e non rimborsati sono stati convalidati con riconoscimento biometrico, strumento di verifica del cliente tramite un elemento di inerenza (impronta digitale o scansione del viso) precedentemente registrato su device abilitato, che invece rappresenta l'elemento di possesso.

Tale ricostruzione è provata attraverso documentazione dalla quale si ricava che i pagamenti richiesti sono stati autorizzati mediante il ricorso a un elemento di possesso (il dispositivo certificato con le modalità descritte nei log) e a un elemento di inerenza (la biometria).

Si deve, dunque, passare alla verifica della colpa grave del cliente.

Ebbene, il cliente riferisce di aver ricevuto, in data 24.07.2024, un SMS apparentemente riconducibile all'intermediario. Dichiara espressamente di aver cliccato sul link ivi indicato e di aver inserito le credenziali sul portale che si è aperto, apparentemente uguale a quello "genuino".

Il messaggio è stato prodotto in atti, sì che è possibile ricavare che è inserito in una chat la cui denominazione corrisponde a quella dell'intermediario (sebbene non ci siano altri messaggi genuini) e contiene un link con la denominazione dell'intermediario; la schermata relativa al portale cui il link consentiva di accedere non è invece in atti.

Il messaggio non contiene errori grossolani, ma è privo di punteggiatura.

Deve dunque concludersi che il cliente sia stato vittima di uno *spoofing* seppure non sofisticato. Secondo l'orientamento condiviso dei Collegi, deve ritenersi che allo stato, nonostante la maggiore diffusione di campagne informative sul tema, lo *spoofing* conservi ancora il carattere di insidiosità, inducendo il cliente ad abbassare la sua soglia di attenzione.

Il cliente, tuttavia, non riferisce ulteriori connotati della truffa, limitandosi ad affermare che tra il 26/07/2024 e il 22/08/2024 ignoti eseguivano n. 65 operazioni di pagamento.

Vi è dunque, a fronte dell'insidiosità del messaggio ricevuto dal cliente, una grave negligenza da parte di quest'ultimo che ha omesso di monitorare il proprio conto tanto più che, in ogni caso, il messaggio civetta, comunicandogli la necessità di confermare i propri dati, lo avrebbe dovuto comunque allarmare in ordine alla regolare funzionalità della carta. Ove avesse diligentemente e prudentemente controllato il proprio conto (le cui risultanze egli poteva verificare anche tramite App) avrebbe potuto procedere ben prima al blocco della carta evitando il protrarsi dell'attività truffaldina. Per ben un mese sul conto del cliente sono state invece eseguite operazioni senza che egli se ne accorgesse, sebbene le stesse fossero intervallate da operazioni genuine che testimoniano da parte sua l'utilizzo dello strumento di pagamento.

Deve infine tenersi conto che una parte di quanto richiesto è stato già rimborsato dall'intermediario.

Per tutto quanto esposto, la domanda volta ad ottenere ulteriori somme a titolo di restituzione non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE