

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) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 21/04/2026

FATTO

Il ricorrente, titolare di una carta di debito emessa dall'intermediario resistente, ha adito questo Arbitro per ottenere il rimborso di un'operazione di pagamento *online* effettuata in data 15/12/2025, per l'importo di € 585,77, che egli asserisce di non aver mai autorizzato. Nello specifico, il ricorrente espone di aver riscontrato tale addebito e di aver immediatamente provveduto a bloccare la carta e a sporgere denuncia presso le competenti Autorità in data 16/12/2025. Sostiene che l'operazione sia stata eseguita senza l'applicazione di un sistema di autenticazione forte del cliente (c.d. *Strong Customer Authentication* - SCA), quale l'inserimento di un codice OTP o la conferma tramite l'App della banca. L'intermediario si è costituito in giudizio chiedendo il rigetto del ricorso. A sostegno della propria difesa, la Banca ha evidenziato che l'operazione contestata, originariamente di 673,00 USD, è stata regolarmente autenticata. In particolare, produce i log informatici dai quali risulterebbe che: (i) alle ore 20:46:54 del 15/12/2025, è stata inviata una notifica *PUSH* sul dispositivo smartphone del ricorrente, univocamente associato alla sua utenza; (ii) la notifica risulta correttamente consegnata al dispositivo del cliente; (iii) alle ore 20:46:59, l'operazione è stata confermata mediante validazione della notifica *PUSH* tramite l'inserimento del fattore biometrico ("*TOUCH*"), ovvero l'impronta digitale del cliente. L'intermediario conclude che l'operazione è stata autorizzata mediante l'utilizzo di due fattori di autenticazione indipendenti (possesso dello *smartphone* e inerenza del dato biometrico), in piena conformità con la normativa PSD2. Sottolinea, inoltre, la genericità delle allegazioni del ricorrente, il

quale si è limitato a disconoscere l'operazione senza fornire alcun elemento utile a ricostruire la dinamica della presunta frode (es. *smishing*, *phishing*, furto del dispositivo).

Nelle proprie repliche, il ricorrente ha contestato la valenza probatoria dei log prodotti, sostenendo che essi dimostrerebbero al più l'invio tecnico di una comunicazione, ma non il suo consenso effettivo e consapevole. Insiste quindi per l'accoglimento del ricorso.

La banca, in sede di controreplica, ha confermato la correttezza della propria ricostruzione. Insiste quindi per il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio attiene alla responsabilità dell'intermediario per un'operazione di pagamento disconosciuta dal cliente e alla corretta ripartizione dell'onere probatorio ai sensi del D.Lgs. 27 gennaio 2010, n. 11, di attuazione della Direttiva sui servizi di pagamento (PSD2).

I precedenti di questo Arbitro sono costanti nell'affermare che l'onere probatorio a carico della banca si articola in due fasi logicamente successive: in primo luogo, la prova della corretta autenticazione dell'operazione tramite un sistema di Autenticazione Forte del Cliente (SCA); in secondo luogo, qualora la prima prova sia stata fornita, la dimostrazione, anche tramite presunzioni, della colpa grave dell'utente.

Nel caso di specie, il Collegio ritiene che l'intermediario abbia assolto al primo onere probatorio. Dalla documentazione prodotta (in particolare, i log informatici), emerge in modo chiaro e univoco che l'operazione è stata autorizzata attraverso un sistema che soddisfa i requisiti della SCA. Infatti, la procedura ha previsto l'impiego combinato di due fattori appartenenti a categorie diverse: il "possesso" dello *smartphone* del ricorrente, certificato e associato alla sua utenza, sul quale è pervenuta la notifica *PUSH*; e l'"inerenza", rappresentata dal dato biometrico (impronta digitale) utilizzato per validare la notifica e autorizzare il pagamento.

Le contestazioni del ricorrente, secondo cui i log non proverebbero il suo "consenso effettivo", appaiono generiche e non idonee a inficiare la solidità delle evidenze tecniche fornite dalla banca. Tali evidenze non si limitano a registrare l'invio di una comunicazione, ma tracciano l'intera sequenza: invio della notifica, consegna al dispositivo corretto e, soprattutto, la specifica azione di conferma che ha sbloccato l'esecuzione del pagamento. L'intermediario ha quindi dimostrato che l'operazione è stata autenticata secondo le procedure di sicurezza previste.

Una volta assolta la prova della corretta autenticazione, occorre valutare se il ricorrente abbia agito con colpa grave, contribuendo in maniera determinante al verificarsi dell'evento dannoso. Secondo l'orientamento consolidato di questo Arbitro, in presenza di un'operazione autorizzata con SCA e in assenza di malfunzionamenti del sistema, si presume la colpa grave dell'utente, qualora quest'ultimo non fornisca elementi concreti e verosimili su come la frode si sia potuta perfezionare nonostante i presidi di sicurezza (es. tramite tecniche di ingegneria sociale particolarmente sofisticate, c.d. "*smishing*" o "*vishing*", che abbiano indotto in errore un utente mediamente diligente).

Nel caso in esame, il ricorrente si è limitato a un disconoscimento generico dell'operazione, senza allegare alcuna circostanza specifica. Non ha riferito di aver ricevuto messaggi o telefonate sospette, di aver cliccato su *link* fraudolenti, di aver subito il furto o la compromissione del proprio *smartphone*,

né ha fornito alcun altro dettaglio che possa far ipotizzare una truffa complessa. Tale silenzio processuale, a fronte di una prova robusta di corretta autenticazione da parte della banca, non può che essere interpretato a sfavore del ricorrente stesso.

L'autorizzazione di un'operazione tramite l'uso combinato di un dispositivo personale e di un dato biometrico unico come l'impronta digitale implica necessariamente un coinvolgimento attivo del titolare dello strumento. In assenza di allegazioni specifiche che suggeriscano una dinamica fraudolenta idonea a superare tali barriere di sicurezza senza la cooperazione, seppur inconsapevole, dell'utente, la conclusione più logica e probabile è che il ricorrente abbia, con grave negligenza, autorizzato egli stesso l'operazione, magari indotto in errore da terzi, o abbia custodito con insufficiente diligenza il proprio dispositivo e le relative modalità di sblocco.

Pertanto, in applicazione dei principi richiamati, avendo l'intermediario fornito piena prova della corretta autenticazione dell'operazione tramite SCA e non avendo il ricorrente offerto alcun elemento idoneo a circostanziare la truffa subita, mettendo così l'intermediario nella condizione di fornire la prova della colpa grave, la domanda di rimborso non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE