COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CORNO

Seduta del 05/06/2025

FATTO

Il ricorrente è titolare di rapporto di conto corrente con l'intermediario interveniente nonché di una carta di pagamento *464. In data 10 febbraio 2024, mentre si trovava alle casse di un supermercato, il ricorrente subiva il furto del proprio cellulare, tessera sanitaria, € 100,00 in contanti e carta di debito n. *464, che erano custodite dalla propria moglie.
Si avvedeva che erano state effettuate tre operazioni non autorizzate tra le ore 10:03 e le ore 10:47 nelle vicinanze del luogo del furto. Presentava denuncia alle Autorità in data 10 febbraio 2024, poi integrata in data 12 febbraio e 14 febbraio. Provvedeva inoltre al disconoscimento delle operazioni presso l'intermediario e presentava reclamo in data 2 aprile 2024, che veniva riscontrato negativamente.
Con ricorso all'ABF in data 16 febbraio 2025, il ricorrente chiede la restituzione dell'importo di operazioni non autorizzate per € 3.732,90. Afferma che il PIN non era presente nella refurtiva né in forma cartacea né camuffato in alcun modo nel cellulare.

Con le controdeduzioni l'intermediario chiede il rigetto del ricorso. Afferma che gli accertamenti hanno evidenziato che le operazioni disconosciute risultano regolarmente portate a termine con la carta originale e con l'ausilio del codice PIN. Contrariamente a quanto dichiarato dal cliente, in un tale breve frangente non sarebbe stata possibile una clonazione della carta o l'estrazione dalla stessa del PIN. Richiama in merito una

consulenza scientifica commissionata al Politecnico di Torino dal Consorzio Bancomat. Alla luce di ciò, è possibile ragionevolmente ritenere che chi ha sottratto la carta ha trovato, su di essa o almeno vicino ad essa, indicazioni o riferimenti idonei a consentire l'individuazione del PIN.

Con le repliche il ricorrente precisa che all'uscita dal supermercato, alla richiesta di restituzione della propria carta, lui e la moglie si sono accorti del furto, avvenuto per sottrazione dalla tasca esterna del cappotto in cui, nella custodia del cellulare, erano riposti la carta e dei contanti. Non avendo più un telefono con cui bloccare la carta, ne hanno chiesto uno in prestito ma nella premura della situazione hanno bloccato la carta sbagliata.
Successivamente la moglie e la figlia sono andate a sporgere denuncia mentre lui tornava a casa dove si rendeva conto dell'errore nel blocco e provvedeva a bloccare la carta corretta. In merito alla cessione della carta di debito alla moglie, riferisce di averla ceduta in quanto, non trovando parcheggio fuori dal supermercato, rimaneva in macchina con la figlia mentre la moglie entrava per effettuare gli acquisti. Alla consegna della carta, comunicava verbalmente alla moglie il codice PIN, che non era presente nella refurtiva in quanto lo ha memorizzato e non lo conserva neanche in casa. Il cliente ipotizza una sottrazione di PIN durante un prelievo precedente al furto e lamenta i presidi di sicurezza della banca, risultati lacunosi.

Con le controrepliche l'intermediario afferma che il ricorrente avrebbe dovuto essere più cauto, conferma le argomentazioni e le allegazioni fornite in merito alla responsabilità del cliente e della moglie per aver conservato congiuntamente la carta e il codice PIN, tenuto conto che le n. 3 operazioni disconosciute sono avvenute a distanza di pochi minuti dall'evento furtivo. Da ultimo richiede l'applicazione della franchigia di legge.

DIRITTO

Oggetto del ricorso è la richiesta del ricorrente del rimborso di operazioni di pagamento non autorizzate ed eseguite in data 10 febbraio 2024 per complessivi € 3.732,90 di cui: prelievo ATM di € 1.500,00 alle ore 10:03, pagamenti POS per € 1.441,90 alle ore 10:30 ed € 791,00 alle ore 10:47.
Le operazioni di pagamento contestate rientrano nell'ambito applicativo del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218. Poiché il ricorrente, quale utente di servizi di pagamento, ha negato di aver autorizzato le operazioni di pagamento eseguite, è onere dell'intermediario, ai sensi dell'art. 10 del medesimo D.Lgs., quale prestatore di servizi di pagamento, provare che tale 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 altri inconvenienti.
Ai sensi dell'art. 10bis del ricordato D.Lgs., i prestatori di servizi di pagamento sono tenuti ad applicare modalità di autenticazione forte del cliente (SCA *strong customer authentication*) 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. Nel caso di avvio di un'operazione di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico. L'autenticazione forte (SCA) è richiesta sia nella fase di *(i)* accesso al conto / *enrollment*

dell'app / registrazione della carta sul *wallet*, sia nella fase di *(ii)* esecuzione delle singole operazioni; e 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. Alla luce del disconoscimento delle operazioni da parte del cliente, è altresì onere dell'intermediario di fornire prova della frode, del dolo o della colpa grave dell'utente.
Nel caso di specie, il Collegio rileva quanto segue relativamente alla prova fornita dall'intermediario con riguardo all'autenticazione, corretta registrazione e contabilizzazione delle operazioni di pagamento disconosciute dal cliente.
L'intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate. In particolare, afferma che le operazioni risultano autorizzate mediante lettura del microchip della carta e corretto inserimento del relativo codice PIN.

Dalle evidenze prodotte risulta quanto segue.
Per quanto riguarda le operazioni di pagamento POS, il codice External Auth Id evidenzia le caratteristiche dell'operazione effettuata e codificata. In particolare:

- 6° codice 1, indica presenza fisica della carta;
- 7° codice L indica tecnologia contactless, codice 5 indica tecnologia microchip;
- 8° codice 1, indica digitazione codice PIN.

Per quanto riguarda i prelievi ATM, il codice External Auth Id evidenzia le caratteristiche dell'operazione effettuata e codificata con numero 000000500000. In particolare, in tale codice il campo:

- 7° codice 5 significa ICC Integrated Circuit Card, ovvero operazione effettuata con tecnologia microchip;
- Evidenzia che qualsiasi operazione di prelievo presso uno sportello ATM su circuito nazionale (codice CIR = N) può concludersi solo ed esclusivamente a seguito di inserimento del codice personale PIN;
- La correttezza dell'operazione è segnalata dal codice Auth.Response il quale, se valorizzato: 00 Approved, indica che l'operazione è stata approvata con il corretto e necessario inserimento del PIN (sarebbe stata valorizzata 01 in presenza di anomalie). Ne consegue che la prova può dirsi certamente raggiunta per le operazioni di cui ai punti *(i)* e *(iii)* che precedono.

Alla luce di quanto precede, le operazioni di pagamento POS risultano autenticate mediante i fattori del possesso (la carta) e della conoscenza (il codice PIN).
Quanto all'operazione di prelievo ATM, in casi analoghi, in cui – pur in assenza di evidenza specifica della avvenuta digitazione del PIN – il giornale di fondo riportava la dicitura "Anomalia: 00", questo Collegio ha ritenuto documentata la digitazione del PIN sulla base della mancata rilevazione di anomalie (cfr. decisioni n. 3531/2022 n. 1208/2023); ciò in quanto, se il PIN non fosse stato inserito o fosse stato digitato in modo errato, il sistema avrebbe rilevato un'anomalia.
Ne consegue che l'intermediario ha assolto al proprio onere probatorio della corretta autenticazione, registrazione e contabilizzazione in merito alle operazioni disconosciute e che sono rilevabili malfunzionamenti delle procedure necessarie o altri inconvenienti.

Quanto alla valutazione della condotta dell'utilizzatore, la quale è idonea ad escludere il diritto alla restituzione delle somme disconosciute solo qualora sia connotata da colpa grave, assume rilevanza centrale il disposto del nuovo art. 12, co. 2-ter e s., d. lgs. n. 11/2010., il quale prevede che "*Il pagatore non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano*

essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento, o se la perdita è stata causata da atti o omissioni di dipendente, agenti o succursali del prestatore di servizi di pagamento o dell'ente cui sono state esternalizzate le attività. Negli altri casi, salvo che abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Dalla normativa dinanzi richiamata si desume quindi che ciò che consente di escludere il rimborso della perdita subita è la colpa grave o il dolo dell'utilizzatore, in mancanza dei quali questi ha diritto al rimborso dell'operazione disconosciuta.

Dalle circostanze di fatto del caso in esame, emerge che il cliente afferma di avere subìto il furto alle ore 10.00 circa; la prima operazione disconosciuta è stata eseguita alle ore 10.03, ossia a distanza di circa 5 minuti dal furto. Al riguardo, si rappresenta che i Collegi ritengono che la valutazione della brevità del lasso temporale tra sottrazione della carta e primo utilizzo fraudolento debba essere effettuata caso per caso, alla luce degli ulteriori elementi di fatto risultanti dalle deduzioni e allegazioni delle parti.
Quanto al fatto che la carta era in possesso della moglie del ricorrente al momento del furto, i Collegi sono unanimi nel ritenere che non assume generalmente rilevanza, quale indice della colpa grave del cliente, l'affidamento dello strumento di pagamento a terzi, poiché la valutazione della gravità o meno dell'inadempimento all'obbligo di custodia e di utilizzo personale dello strumento di pagamento deve essere condotta avuto riguardo alle circostanze del caso concreto, e in particolare agli elementi di fatto della frode e all'efficienza causale rispetto al pregiudizio subito dal cliente. In questa situazione, a titolo esemplificativo, potrebbe escludersi la colpa grave in ipotesi di affidamento della carta a un prossimo congiunto o al coniuge.
Nel caso di specie l'insieme delle circostanze del fatto induce a ritenere sussistente un addebito di colpa grave in capo al ricorrente.

D'altro canto, non risulta superato il plafond di spesa della carta di pagamento né ha rilevanza l'attivazione o meno del servizio di SMS *alert* considerato che, essendo state effettuate più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, la ricezione dell'*alert* non potrebbe limitare, in concreto, il pregiudizio dell'utente.
Il Collegio non accoglie quindi il ricorso del cliente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA