

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CESARE

Seduta del 09/09/2025

FATTO

Il cliente lamenta che alle ore 12:44 del 11 marzo 2025 riceveva una chiamata apparentemente riferibile all'intermediario in quanto originata dal numero di telefono della filiale. L'interlocutore si presentava come operatore dell'ufficio antifrode e gli comunicava il codice titolare e relativo PIN di accesso, dimostrando apparentemente di essere un operatore della banca. Durante la telefonata riceveva sul proprio cellulare un SMS da parte dell'istituto di credito, di cui il sedicente operatore chiedeva conferma di ricezione. Il cliente leggeva il contenuto del messaggio, circostanza che faceva ritenere al ricorrente che il truffatore avesse accesso al suo dispositivo e potesse vedere i messaggi in arrivo nonché il loro contenuto.

Il sedicente operatore chiedeva quindi conferma del numero presente nell'SMS pervenuto dall'intermediario, che il ricorrente forniva, per poi richiedere i CVV delle due carte di debito collegate al conto per procedere al loro presunto blocco. A questo punto, consapevole di non dover fornire alcun dato relativo alle carte, il cliente chiudeva la telefonata e contattava immediatamente il numero verde dell'intermediario, apprendendo che erano già stati effettuati quattro prelievi dal suo conto per un valore complessivo di € 1.480,00.

Il ricorrente bloccava conto corrente e le carte di debito e presentava denuncia presso le Autorità in data 12 marzo 2025, presentando successivamente modulo di disconoscimento

delle operazioni all'intermediario in data 25 marzo 2025, che veniva riscontrato negativamente.

Le quattro operazioni contestate risultano essere state eseguite in rapida successione il 11 marzo 2025 alle ore 12:41:02 per € 150,00, alle 12:41:37 per € 490,00, alle 12:42:09 per € 490,00 e alle 12:42:53 per € 350,00, tutte presso il medesimo punto vendita utilizzando la carta di debito in modalità contactless tramite digital wallet. Dal punto di vista tecnico, l'esecuzione delle operazioni fraudolente era stata preceduta dall'enrollment di un nuovo dispositivo Android in sostituzione del dispositivo abitualmente utilizzato dal cliente, costituito da un dispositivo iOS, nonché dalla successiva tokenizzazione della carta sul wallet digitale del nuovo dispositivo.

Chiede la restituzione di € 1.480,00.

L'intermediario afferma che il ricorrente è rimasto vittima di una truffa telematica concretizzatasi con le tecniche del *vishing*, che esula dalla responsabilità della banca. Sostiene che le quattro operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali, senza che siano stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici. L'intermediario evidenzia che ha allertato il cliente inoltrando notifiche push per ogni pagamento effettuato e conclude rappresentando che emerge la colpa grave del cliente nell'inserimento delle credenziali.

Conclude per il rigetto del ricorso.

DIRITTO

Il caso sottoposto all'esame riguarda operazioni di pagamento con carta di debito in modalità contactless tramite digital wallet disconosciute dal cliente a seguito di truffa telefonica, con richiesta di rimborso ai sensi della normativa sui servizi di pagamento. La disciplina applicabile è costituita dal Decreto Legislativo 27 gennaio 2010, n. 11, come modificato dal D. Lgs. n. 218/17 di attuazione della Direttiva PSD II, entrato in vigore il 13 gennaio 2018.

L'articolo 10 del decreto stabilisce il regime di responsabilità per le operazioni di pagamento non autorizzate, ponendo a carico del prestatore di servizi di pagamento specifici oneri probatori che devono necessariamente essere assolti con riguardo ad entrambi i profili dell'autenticazione dell'operazione e della sussistenza di frode, dolo o colpa grave dell'utilizzatore, da ritenersi necessari e complementari secondo quanto chiarito dal Collegio di Coordinamento nella decisione n. 22745 del 10 ottobre 2019.

Nel caso in esame l'intermediario ha fornito evidenza dell'autenticazione forte tanto per la fase di enrollment del nuovo dispositivo quanto per l'esecuzione delle operazioni contestate, dimostrando che l'enrollment è risultato correttamente autenticato tramite PIN quale fattore di conoscenza e tramite codice OTP inviato via SMS quale fattore di possesso, mentre le operazioni di pagamento sono state autenticate mediante la lettura del chip della carta di debito caricata su digital wallet in modalità contactless quale elemento di possesso e tramite l'inserimento del codice di sblocco del dispositivo utilizzato come elemento di conoscenza (Collegio di Coordinamento n. 9559/2024 che ha stabilito come nell'autenticazione di operazioni di pagamento tramite digital wallet il codice di sblocco del dispositivo utilizzato possa valere come secondo fattore rilevante ai fini della SCA purché esso sia stato in via preventiva associato univocamente all'utente mediante uso nella fase di tokenizzazione dello strumento all'interno del wallet con procedura conforme a SCA).

Occorre valutare la colpa grave dell'utilizzatore alla luce delle specifiche circostanze del caso concreto.

Secondo l'orientamento consolidato dei Collegi territoriali, nelle contestazioni di utilizzi fraudolenti online, a fronte di un sistema di autenticazione conforme ai requisiti dell'autenticazione forte, si deve ritenere che l'utilizzatore dello strumento di pagamento abbia contribuito in maniera determinante alla frode subita laddove non si rinvenivano elementi per ritenere che lo stesso abbia fatto legittimo affidamento sulla genuinità dei contatti ricevuti con i truffatori.

Da un lato il cliente ha cooperato con i truffatori fornendo le credenziali necessarie per l'enrollment del nuovo dispositivo e l'accesso ai servizi bancari e ha ricevuto un SMS con contenuto parlante che chiedeva di non cedere il codice, circostanze che secondo la giurisprudenza ABF costituiscono normalmente indice di colpa grave. Inoltre il cliente si è rifiutato di fornire i codici CVV richiesti evidenziando di aver percepito il rischio di una anomalia nel contatto telefonico.

Ulteriore elemento in grado di fondare la colpa del cliente è costituito dalla mancata produzione del registro chiamate da parte del ricorrente, circostanza che secondo l'orientamento unanime dei Collegi comporta normalmente il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto se sia configurabile un legittimo affidamento dell'utente circa la genuinità della telefonata ricevuta.

Dagli elementi sopra richiamati si può dedurre la colpa grave del ricorrente, che esclude il rimborso.

Dalle evidenze agli atti risulta tuttavia la sussistenza di indizi di anomalia di cui al D.M. 112/2007, specificatamente quello relativo a tre o più richieste di autorizzazione sulla stessa carta effettuate nelle ventiquattro ore presso un medesimo punto vendita, essendo state effettuate quattro operazioni di pagamento con la stessa carta di debito in un arco temporale di soli due minuti presso il medesimo esercizio commerciale, configurando un'operatività manifestamente anomala che avrebbe dovuto essere intercettata dai sistemi antifrode dell'intermediario.

Secondo l'orientamento consolidato dei Collegi, una volta accertata la colpa grave del cliente in presenza di indizi di frode la ripartizione della responsabilità con il prestatore dei servizi di pagamento deve essere determinata caso per caso in relazione alle circostanze di fatto, in quanto le previsioni del D.M. 112/2007 rappresentano un parametro per la formulazione di un giudizio in concreto della negligenza tecnica dell'intermediario.

L'indice di anomalia rilevato prevede che in presenza di tre o più richieste di autorizzazione sulla stessa carta presso un medesimo punto vendita nelle ventiquattro ore si configuri una fattispecie di frode da segnalare.

Nel caso di specie, dovendo ritenere lecite le prime due operazioni, in linea con i parametri del D.M. 112/2007, le ulteriori operazioni risultano anomale e avrebbero dovuto essere intercettate dai sistemi antifrode dell'intermediario.

Considerando che le prime due operazioni (€ 150,00 e € 490,00 per complessivi € 640,00) rientrano nei parametri di normalità, mentre le successive due operazioni (€ 490,00 e € 350,00 per complessivi € 840,00) configurano un'anomalia che avrebbe dovuto comportare il blocco dei pagamenti, l'intermediario è tenuto al rimborso di queste ultime, ferma restando la responsabilità del cliente per le prime due operazioni eseguite prima che si configurasse l'indice di frode.

Il ricorso va accolto quindi parzialmente.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 840,00.



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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

Firmato digitalmente da
ANDREA TINA