

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore CATERINA LUCARELLI

Seduta del 15/12/2025

FATTO

Titolare della carta di credito n. ***2455 emessa dall'intermediario, il ricorrente in data 19/5/2025 riceveva sul proprio cellulare un SMS contenente l'avviso di mancata consegna di un pacco per assenza di una informazione sull'indirizzo di destinazione; selezionando il link richiamato nel messaggio accedeva ad un portale simile a quello dell'intermediario convenuto. Dopo l'inserimento del dato mancante, veniva richiesta la corresponsione della somma di euro 0,27 per sbloccare la consegna; il ricorrente effettuava il pagamento con la propria carta di credito, ma la transazione pareva non andare a buon fine. Per questo motivo, dava seguito all'ulteriore richiesta di inserimento di due codici autorizzativi notificati sul proprio smartphone e, solo successivamente, si accorgeva di aver involontariamente autorizzato due pagamenti, rispettivamente di euro 408,27 e 409,31. Scoperta la frode, provvedeva al blocco della carta e segnalava l'accaduto alla banca. L'intermediario riscontrava la comunicazione di disconoscimento delle operazioni affermando di non poter dar corso al relativo rimborso. Pertanto la parte istante inoltra ricorso all'ABF per domandare la rifusione integrale dell'ammanto subito pari 817,58 euro per le due operazioni.

Convenuto ritualmente, l'intermediario deduce l'infondatezza del ricorso evidenziando, in primo luogo, come non risulti applicabile la disciplina di tutela delineata nell'art. 5 del D.Lgs. 11/2010, poiché le transazioni contestate sono state disposte ed autorizzate direttamente dal cliente, ancorché con

volontà traviata dal raggiro subito. In ogni caso, anche nella denegata ipotesi in cui il Collegio ritenesse applicabile la disciplina in questione, la parte resistente afferma che dovrebbe confermarsi la reiezione delle istanze avverse per diverse ragioni: i) le transazioni contestate risultano correttamente disposte ed autorizzate con doppio fattore SCA, rappresentato dall'inserimento del codice OTP dinamico ricevuto via SMS sul cellulare del ricorrente (elemento di possesso) e dalla valorizzazione corretta del codice segreto statico, impostato e conosciuto solo dall'utente (elemento di conoscenza); ii) risulta evidente la colpa grave dell'odierno attore, il quale ammette di aver personalmente inserito i codici OTP ricevuti sul proprio cellulare sul sito internet truffaldino per autorizzare operazioni di pagamento il cui ammontare avrebbe dovuto essere di 0,27 euro; iii) il ricorrente non ha prestato attenzione al testo degli SMS di trasmissione dei medesimi codici, contenente la descrizione dell'operazione che si stava per autorizzare; iv) il ricorrente non ha dato rilievo agli avvisi informativi predisposti dall'intermediario e volti a rendere edotta la clientela sulle modalità operative delle truffe informatiche ed in particolare su quelle realizzate mediante phishing e smshing. La parte resistente, quindi, conclude domandando all'ABF la reiezione del ricorso o, in via subordinata, che la valutazione dell'entità del risarcimento tenga conto del concorso colposo del creditore ex art. 1127 c. 1 cod. civ.

DIRITTO

1. Questo Collegio richiama la disciplina in materia e rileva che le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
2. Il ricorrente disconosce due operazioni di pagamento online dell'importo complessivo di euro 817,58 disposte in data 19/5/2025 con la propria carta di credito n. ***2455, come risulta da denuncia e modulo di disconoscimento, riscontrate dall'intermediario resistente che allega le evidenze informatiche circa le operazioni in parola, con i loro orari di esecuzione.
3. Non risultano allegate evidenze relative al blocco dello strumento, ma il ricorrente afferma in denuncia di averlo disposto dopo essersi avveduto della truffa.
4. In merito all'autenticazione delle operazioni, il Collegio richiama l'art. 10, dlgs. 11/2010) in base al quale è onere dell'intermediario provare che le operazioni siano state autenticate, correttamente registrate e contabilizzate; in mancanza di questa prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute. Sul punto, l'intermediario afferma l'inapplicabilità della disciplina di tutela definita dal D.Lgs. 11/2010 alla fattispecie in esame, difettando il requisito della mancanza di consenso dell'utilizzatore dello strumento di pagamento, poiché le operazioni contestate sarebbero state asseritamente disposte ed autenticate direttamente dal medesimo, come appare ammesso dal ricorrente in denuncia. Tuttavia, il cliente, nel modulo del ricorso, ammette l'esecuzione diretta di uno solo dei pagamenti in questione. Questo Collegio, quindi, in linea con il costante orientamento del sistema ABF, distingue tra operazioni eseguite per intero dal pagatore, ed operazioni autorizzate con l'intervento parziale del pagatore, come in questo caso.

Secondo l'orientamento condiviso dai Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Per questo il Collegio procede con la disamina della prova della Strong Customer Authentication (SCA) con riferimento ad entrambe le transazioni disconosciute. Sul punto, la parte resistente deduce la corretta autenticazione mediante doppio fattore SCA delle transazioni contestate ed individua i fattori utilizzati, versando agli atti i log informatici relativi. Per il Collegio quindi esiste prova: i) dell'elemento di possesso, ovvero l'inserimento dell'OTP ricevuto via SMS sul device associato allo strumento di pagamento (i.e. numero di cellulare a cui sono stati inviati gli SMS coincide con quello del ricorrente, come indicato in denuncia); ii) dell'elemento di conoscenza, ovvero l'inserimento del codice segreto personale K***.

5. A questo punto il Collegio richiama la decisione n. 22745/2019 del Collegio di Coordinamento, che ha enunciato il seguente principio di diritto: "la previsione di cui all'art. 10, comma 2, del d.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente". Sul punto, la parte resistente inferisce la condotta gravemente colposa del ricorrente da una serie di argomenti, sostenuti dalla narrativa dei fatti presentata in denuncia dal ricorrente e dalle evidenze documentali prodotte dall'intermediario. Innanzitutto, l'intermediario censura la mancata produzione di copia dell'SMS civetta, da cui ha tratto origine la truffa. Su questo punto il Collegio richiama l'orientamento condiviso dei Collegi per cui la mancata allegazione, da parte del cliente, del messaggio civetta, determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e sia pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio (cfr. ex multis Collegio di Bologna, decisione n. 11920 del 26.8.2022). In secondo luogo, la parte resistente evidenzia come il cliente ammetta di aver disposto direttamente le transazioni contestate ed inserito i codici autorizzativi, sia pure nella convinzione di effettuare un pagamento per diverso importo e finalità, non prestando attenzione alla chiara descrizione delle operazioni da autorizzare che accompagnava i codici inopinatamente inseriti. Sul punto, quindi, questo Collegio, in linea con l'orientamento analogo assunto dai Collegi territoriali ABF su casi comparabili, conclude che la colpa grave del ricorrente sussista (Collegio di Torino, decisione n. 3516/2023; Collegio di Milano, decisione n. 4567/2022).

6. Non assumono rilevanza per il Collegio, ulteriori elementi di valutazione quali gli indicatori di anomalia ex DM del 2007, né la presenza di presiti quali i sistemi di alert di cui non si fa menzione nel ricorso.

7. Tutto considerato, sulla base dei punti che precedono, in linea con l'orientamento del sistema ABF espresso in decisioni su casi analoghi, questo Collegio conclude che il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE