

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

La parte ricorrente, in sede di ricorso, ha affermato che gli è stato hackerato lo smartphone con all'interno l'applicazione dell'intermediario, grazie alla quale sono state effettuate operazioni sul suo conto da lei mai autorizzate. Dopo aver esposto denuncia ed effettuato il disconoscimento delle operazioni, l'intermediario ha negato il rimborso di tali somme, in quanto ritiene che il ricorrente non abbia custodito adeguatamente i codici d'accesso al conto. Per questo, il cliente inoltra ricorso all'ABF chiedendo di "recuperare la somma totale di € 3.659,35 oppure parte di essa".

Convenuto ritualmente, l'intermediario, in sede di controdeduzioni, dichiara: i) che il bonifico di euro 1.350,00 è stato disposto a favore del ricorrente su un altro conto di un altro intermediario e quindi non sussiste alcuna perdita né responsabilità; ii) che per accedere ai servizi online della banca è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice Titolare (password statica) il codice PIN (password statica) e il codice O-Key (OTP - password dinamica) e per autorizzare le operazioni dispositive è necessario il codice dinamico, OTP. Precisando che le operazioni disconosciute dal cliente sono state eseguite dopo essere state "autenticate, correttamente registrate e contabilizzate" e non hanno "subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconvenienti", eccepisce che, rispetto alla giurisprudenza e l'orientamento dei collegi, esiste una colpa grave dell'utente. L'intermediario chiede quindi all'ABF il

rigetto del ricorso, o nella denegata ipotesi che si ravvisino sue responsabilità per l'accaduto che sia applicata la franchigia di 50 euro contemplata dalla normativa in materia.

In replica, parte ricorrente sostiene: i) di non aver ricevuto notifiche di autorizzazione delle operazioni; ii) che i 1.350,00 spostati sull'altro conto sono comunque da rimborsare perché anch'esso svuotato; iii) di non ritenere corretto che l'intermediario autorizzi immediatamente operazioni di bonifico istantaneo e creazione e utilizzo di carte virtuali subito dopo una richiesta di cambio di geolocalizzazione.

In sede di controrepliche l'intermediario ribadisce: i) di aver inviato notifiche PUSH per ogni operazione svolta; ii) che, se il conto su cui sono stati disposti i 1.350,00 con altro intermediario è stato poi svuotato, la domanda di rimborso dovrà essere disposta nei confronti di quest'ultimo; iii) che, circa il cambio di geolocalizzazione, la contestazione non è verificabile, è stata sollevata solamente con le repliche e senza allegare prove; iv) che il bonifico istantaneo è immediatamente addebitato sul conto dell'ordinante e accreditato sul conto del beneficiario, senza possibilità di revocare l'operazione.

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. La controversia ha ad oggetto la richiesta di rimborso dell'importo di euro € 3.659,35 relativo a diverse transazioni on line eseguite con due distinte carte di pagamento, e ad un'operazione di bonifico istantaneo. In dettaglio, questo Collegio rileva che dal Modulo di disconoscimento prodotto dal ricorrente risultano contestate, oltre al suddetto bonifico, n. 6 operazioni svolte per pagamenti on-line con la carta ***3778 e n.2 operazioni svolte per pagamenti on-line con la carta ***2123. Parte ricorrente allega poi copia di due Estratti conto preliminari, entrambi relativi al periodo 01.08.2025 fino al 31.08.2025, senza indicare specificamente le operazioni disconosciute. Il Collegio presta attenzione al contenuto dei due Estratti conto preliminari e nota che, da un attento confronto degli importi, non si individuano dei valori riconducibili a quanto riportato dal ricorrente nel Modulo di disconoscimento. Dall'altro lato, l'intermediario resistente nelle controdeduzioni riporta i log -che per il Collegio saranno rilevanti nei punti successivi- ma per operazioni che coincidono, per importo e tempi, solo con quelle due disconosciute dal ricorrente rispetto alla carta ***2123. Per quanto riguarda il bonifico verso l'altro conto intestato al ricorrente (dal ricorrente ritenuto prodromico ad ulteriori pagamenti disconosciuti), non risultano chiariti né provati i pagamenti disconosciuti effettuati da tale conto.

3. Sul blocco degli strumento di pagamento, il Collegio peraltro prende atto che parte ricorrente, in sede di denuncia, dichiara di aver chiesto il blocco delle carte in data 24/08/2025 non appena presa consapevolezza delle operazioni fraudolente, ovvero nel pomeriggio di questo giorno, mentre già dalla notte precedente del "24.08.2025, verso le 01/02, coricandomi (...)" si era avveduto di un funzionamento anomalo del suo cellulare dove era caricata la APP della sua banca, da cui sono state disposte poi le operazioni disconosciute.

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. Questo Collegio analizza innanzitutto l'autenticazione delle operazioni di pagamento on line identificate da parte resistente all'interno delle controdeduzioni, che coincidono con quanto disconosciuto dal ricorrente per numerosità e tempi di esecuzione. L'intermediario dichiara e prova documentalmente che l'accesso all'app è avvenuto con l'immissione di un Codice OTP generato in app (elemento di possesso) previo inserimento del User e PIN (elemento di conoscenza). Viene prodotta evidenza documentale che il ricorrente (codice utente ***48) numero di telefono certificato **57, si connette solitamente da APP usando uno smartphone di tipo Android identificato con il codice univoco "****66" che è lo stesso utilizzato per autorizzare l'operatività disconosciuta. L'intermediario documenta producendo i log che, dopo l'accesso in APP, vengono disposte nove operazioni (compreso il bonifico), autenticate in maniera analoga e validate con codice OTP previa digitazione del PIN. Per quanto concerne il bonifico istantaneo di € 1.350,00 indirizzato presso l'altro conto del ricorrente, l'intermediario prova con log l'accesso in App eseguito mediante l'inserimento delle credenziali statiche note unicamente al ricorrente (User e PIN), e la credenziale dinamica rappresentata dal codice univoco OTP generato dal device "****366" (del cliente), previa validazione del PIN. L'operazione dispositiva è avvenuta poi con autenticazione provata dall'intermediario da allegazione documentale.

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, mentre in base alla narrazione del ricorrente, le operazioni fraudolente sarebbero scaturite da episodi di hacking del telefono, la parte resistente inferisce la condotta gravemente colposa del ricorrente, sostenendo che questi si sia limitato ad affermare che crede che il suo telefono sia stato hackerato, e a disconoscere le operazioni in argomento, senza fornire ulteriori elementi o prove. Su tale circostanza, ha dunque richiamato casi analoghi a quello qui in esame, ove l'orientamento unanime dei Collegi è nel senso di riconoscere la colpa grave in capo al cliente (ad esempio la decisione n. 2640/23 del Collegio di Bologna). L'intermediario aggiunge inoltre di ritenere che il ricorrente non abbia custodito adeguatamente le proprie credenziali, perché in caso contrario, i malfattori non avrebbero potuto eseguire le operazioni. Tutte queste argomentazioni portano questo Collegio a concludere che, in linea con un orientamento analogo assunto dai Collegi territoriali ABF su casi comparabili, 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 l'utilità di presidi quali i sistemi di alert visto che la resistente evidenzia che gli sms delle notifiche push riportavano già i dati delle operazioni che si andavano ad autorizzare.

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