

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MAURILIO DANGELO

Seduta del 26/01/2026

FATTO

Con ricorso del 26/09/2025 (preceduto da rituale reclamo negativamente riscontrato dall'intermediario), la parte ricorrente ha affermato che, in data 08/05/2025 (*rectius* 18/05/2025, n.d.r), le arrivava un sms che le comunicava una disposizione dalla sua carta di € 5.500 verso *.com. Non avendo eseguito la disposizione, provvedeva a bloccare la carta comunicando l'accaduto alla banca, intimandole di non effettuare l'operazione.

In virtù dell'avvenuta esecuzione delle operazioni (per un totale di € 5.527,39), provvedeva alla relativa contestazione che, tuttavia, veniva respinta dall'intermediario poiché risultavano effettuate mediante autenticazione forte.

L'istante, ad ogni buon conto, presentava la denuncia.

Concludeva, domandando il rimborso della somma di € 5.527,39.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rappresentato che parte ricorrente non fornisce elementi concreti utili a provare che le operazioni siano state realmente fraudolente, limitandosi a disconoscere le operazioni e a contestare genericamente un non meglio definito illecito patito.

Ha precisato di ritenere che il ricorrente possa essere stato vittima di una delle pratiche fraudolente comunemente riconducibili a fenomeni di “phishing” o “vishing”, avendo verosimilmente comunicato le proprie credenziali a soggetti terzi.

Pertanto, risulta che il ricorrente abbia ricevuto due codici OTP tramite SMS sul proprio dispositivo telefonico e che, mediante l’inserimento di tali codici nell’apposita procedura, sia stato consentito l’accesso al conto, rendendo così possibile l’esecuzione delle operazioni di pagamento contestate.

Inoltre, solo una delle operazioni non è stata eseguita tramite autenticazione forte e quindi il ricorrente ha ottenuto il relativo rimborso, in data 22/05/2025, per un ammontare di € 3,99;

Invero, le altre due operazioni sono state eseguite tramite autenticazione “challenge” ovvero in Strong Customer Authentication.

Nel rilevare che il ricorrente ha ricevuto puntuale informativa di esecuzione operazione, c.d. M*, per le transazioni eseguite, ha specificato che le transazioni oggetto di contestazione risultano essere state autorizzate mediante il dispositivo che il ricorrente ha autorizzato e che questo non è stato smarrito, sottratto o utilizzato da terzi

Gli SMS contenenti i codici OTP sono giunti sul numero di telefono *078, che appartiene al ricorrente e che viene riportato anche nella denuncia

In tale contesto, ritiene che il ricorrente fosse consapevole degli SMS ricevuti e della vicenda in corso di svolgimento, posto anche che gli SMS autenticazione avvisavano il cliente di non comunicare a nessuno i propri codici.

Ha richiamato, poi, le condizioni contrattuali sottoscritte, ove l’articolo rubricato “Estraneità di [nome intermediario] ai rapporti sottostanti al trasferimento di denaro” viene enunciata l’estraneità ai rapporti e alle controversie relative ai beni e/o servizi acquistati;

In conclusione, le operazioni di pagamento sono state autenticate, correttamente registrate e contabilizzate e che non si è verificata alcuna intromissione informatica nei sistemi esecutivi.

Ha, pertanto, concluso per il rigetto del ricorso.

DIRITTO

Come noto, l’utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell’entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 correlata alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Sul punto si rammenta che, secondo la posizione consolidata dell’ABF, la disciplina sopra citata prevede un regime probatorio di favore per l’utente di strumenti e servizi di pagamento, essendo *“ispirata al principio del “rischio d’impresa”, e cioè all’idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente “pericolose”, che interessano un’ampia moltitudine di consumatori o utenti, sull’impresa, in quanto quest’ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla*

massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi" (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 (*infra* riportato) prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

- A. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti.
Nello specifico, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;
- B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Le operazioni contestate consistono in n. 1 transazione online, eseguita in data 18/05/2025 alle ore 11:39, dell'importo di € 5.500,00 e n. 1 transazione online, eseguita in data 18/05/2025 alle ore 11:41, dell'importo di € 27,39.

È stata altresì effettuata un'operazione dell'importo di € 3,99, già rimborsata dall'intermediario.

In ordine al sistema adottato dall'intermediario alla luce della SCA ed alla prova di autenticazione ed esecuzione delle operazioni di pagamento, l'intermediario ha riferito che l'operazione contestata è stata autenticata tramite autenticazione forte, previo enrollment di un nuovo dispositivo e comunicazione al malfattore dei necessari codici autorizzativi da parte del cliente.

Sulla prova della corretta autenticazione delle operazioni contestate, l'intermediario ha evidenziato che in data 18/05/2025 veniva avviato, a seguito dell'inserimento della password, un accesso eseguito alle ore 11:36:16.

L'inserimento corretto della password ha dato esito ok ma, rilevando il sistema un dispositivo mobile differente da quello utilizzato in precedenza dal Ricorrente, ha dato avvio ad un ulteriore step di autenticazione, ovvero il secondo Step.

Il sistema ha dunque avviato un controllo in Strong Customer Authentication: avendo inserito correttamente la password (quale fattore di conoscenza) per poter completare l'accesso in applicazione è quindi obbligatorio eseguire il secondo step di sicurezza. L'esecutore è obbligato ad inserire il codice dinamico OTP di 6 cifre ricevuto tramite SMS al riferimento cellulare presente in anagrafica cliente (quale fattore di possesso) e posseduto quindi del titolare carta.

L'intermediario ha poi affermato (comprovandolo con le evidenze allegate in atti) che il sistema di sicurezza prevede che nel caso in cui il nuovo dispositivo mobile da cui si è fatto accesso venga utilizzato per movimentare la liquidità depositata, questo dovrà essere obbligatoriamente autorizzato dal titolare carta con un'ulteriore OTP, correttamente inserita e verificata.

Quanto alla disposizione delle operazioni, l'intermediario ha rappresentato che le operazioni contestate dal Ricorrente sono state eseguite mediante i fattori di sicurezza stabiliti dalla Strong Customer Authentication (SCA): invero, tramite la notifica push autorizzativa giunta sullo smartphone a quel momento collegato all'account e ove l'applicazione H* è in uso, e tramite un'azione volontaria ("tap") eseguita sulla medesima notifica, il Ricorrente disponente si è "loggato" con i propri riferimenti

personali identificativi, autorizzando di conseguenza le operazioni poste in essere tramite la digitazione della password (tipo autenticazione _password).

Alla notifica push sopra illustrata corrisponde la relativa autorizzazione ovvero il Ricorrente dopo aver “tappato” sulla notifica ricevuta ha provveduto ad autorizzare le transazioni.

Il Collegio rileva che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie analoghe, l'ABF ha ritenuto provata l'autenticazione delle operazioni contestate e compliant con la SCA il sistema di pagamento adottato dall'intermediario resistente, tenuto conto dell'utilizzo dei seguenti fattori di autenticazione: i) per l'accesso all'app e contestuale enrollment: elemento di conoscenza, dato dalla password; elemento di possesso consistito nell'OTP inviato tramite SMS al numero di cellulare del cliente certificato in anagrafica; per le singole operazioni: elemento di possesso, dato dalla notifica push in app; elemento di conoscenza, dato dalla password.

A fronte di evidenze documentali di questo tenore deve giudicarsi dimostrata la corretta contabilizzazione, registrazione e autenticazione delle operazioni disconosciute, lungo tutto l'iter del loro compimento, ai sensi e per gli effetti dell'art. 10 D.Lgs. n. 11/2010.

In ordine, poi, agli utilizzi fraudolenti, l'istante non ha indicato le circostanze di fatto della frode subita, limitandosi a disconoscere le operazioni e a contestare genericamente un non meglio definito illecito patito.

Orbene, il Collegio rileva che, a differenza delle ipotesi di furto o smarrimento dello strumento di pagamento, rispetto ai quali la mancata autorizzazione dell'operazione di pagamento sarebbe legalmente presunta, nel caso di contestazioni di utilizzi fraudolenti on line di strumenti di pagamento le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo, qualora: l'intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute; il sistema di pagamento risulti conforme alla Strong Customer Authentication (SCA); non risultino indici di anomalia delle operazioni e/o ulteriori elementi (in tal senso, si veda Collegio di Torino, decisione n. 11710/2021). Parimenti, anche nella vicenda in esame l'intermediario ha dimostrato, mediante le schermate prodotte in atti, che le operazioni risultano autorizzate con inserimento sia delle credenziali di accesso statiche, sia di quelle dinamiche, conformemente alla disciplina dei sistemi di autenticazione “forte” sopra richiamata. A fronte di tale prova, la domanda di parte ricorrente si rivela pertanto carente sotto il profilo delle allegazioni, risolvendosi nel semplice, formale disconoscimento delle operazioni, senza alcuna concreta ed ulteriore contestualizzazione fattuale, così da impedire la successiva indagine sull'assolvimento dell'onere della prova della colpa grave da parte dell'intermediario.

Alla luce di quanto sopra, valutato che il ricorrente non ha fornito minimi elementi utili alla ricostruzione della vicenda, limitandosi a disconoscere genericamente delle operazioni e tenuto conto che un mero disconoscimento non può valere, senza opportuna contestualizzazione fattuale, a radicare la speciale responsabilità dell'intermediario, il ricorso non può essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE