

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 D'ANGELO

Seduta del 26/01/2026

FATTO

Con ricorso del 21 ottobre 2025 la parte ricorrente ha affermato che, alle ore 14:56 del 25/03/2025, è stata contattata dal n. +39 015**011 corrispondente a quello dell'intermediario, a cui rispondeva un soggetto asseritamente appartenente all'ufficio prevenzioni frodi, il quale la informava di un tentativo di prelievo fraudolento in corso tramite la sua carta di credito. Nella circostanza, il sedicente operatore (che conosceva i suoi dati sensibili e un pregresso tentativo di frode subito nel 2016) la invitava a bloccare l'operazione non autorizzata e la induceva in modo fraudolento ad effettuare n. 3 operazioni da € 500,00 ciascuna, rispettivamente alle ore 15:04, 15:05 e 15:08.

Terminata la telefonata, alle ore 15:12 contattava a sua volta e tramite altro cellulare il n. +39 015**011 (da cui aveva ricevuto la telefonata) e interloquiva con l'assistenza clienti carte dell'intermediario. L'operatrice effettuava dei controlli e le comunicava che era stata vittima di truffa telefonica, provvedendo poi al blocco della carta di credito e a inviare tramite e-mail il modulo disputa.

Nel riferito contesto, compilava e inviava tramite e-mail il modulo datato 28/03/2025, a cui rispondeva l'intermediario con esito negativo in data 16/04/2025.

Rilevava che, al di là della possibile scarsa cautela che aveva comportato il raggio e la truffa telefonica, l'intermediario non avesse bloccato immediatamente il pagamento.

Inoltre, controllando il proprio cellulare, riscontrava un SMS inviato alle ore 15:06 proveniente dal n. 320***123 e contenente il riferimento all'antifrode carte dell'intermediario.

Concludeva domandando il rimborso di 1500 euro.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rappresentato che durante la conversazione telefonica con l'operatrice del servizio di assistenza, il ricorrente ha ammesso di aver ricevuto le notifiche autorizzative sul cellulare e di averle confermate. Inoltre, il parte ricorrente ha confermato di aver personalmente dato il consenso all'esecuzione delle operazioni, con la conseguenza che il d.lgs. 11/2010 non trova applicazione e non è possibile disporre il rimborso.

Ha chiarito che ciascun pagamento è stato autorizzato mediante corretta autenticazione tramite utilizzo del *device* certificato su cui è stata trasmessa la notifica PUSH contenente i dati di riferimento dell'operazione e del fattore biometrico.

Il ricorrente, rispetto a ciascuna operazione, ha ricevuto sulla propria utenza telefonica n. +39 347***700 gli SMS concernenti gli esiti delle autorizzazioni.

Pertanto, ha rilevato che è intervenuto il servizio antifrode della banca, negando il tentativo di n. 2 transazioni delle ore 15:06.

In pari orario, poi, ha inviato al ricorrente un SMS al fine di richiedere conferma del pagamento, a cui il ricorrente ha risposto "SI" alle ore 15:07, consentendo la prosecuzione dell'operatività della carta e l'esecuzione del terzo pagamento contestato. Ha precisato che l'utenza telefonica del ricorrente coincide con quella indicata nel modulo per la presentazione del ricorso e nella sua anagrafica.

Sussiste, quindi, la colpa grave del ricorrente poiché quest'ultimo ha ignorato gli *alert* ricevuti dalla banca, dando seguito alle richieste contraddittorie del sedicente operatore, il quale riferiva la necessità di stornare tentativi di prelievo negli Stati Uniti da € 250,00 ciascuno e al contempo induceva il ricorrente ad autorizzare pagamenti da € 500,00.

L'operatrice del servizio clienti, contattata dal ricorrente, non potendo revocare le operazioni di pagamento, ha disposto il blocco della carta per contraffazione alle ore 15:21 del 25/03/2025.

Oltretutto, il ricorrente non ha fornito alcuna prova della telefonata asseritamente proveniente dal n. 015***011 né risultano chiamate in uscita nei confronti dell'istante, il quale ha contattato l'intermediario dal diverso recapito telefonico n. +39 331***955.

In tale direzione, considerando il comportamento imprudente (in distonia con le stesse campagne informative avviate dall'intermediario), parte resistente ha richiesto 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:

- 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;
- il comportamento gravemente colposo (o fraudolento o doloso) dell’utilizzatore (anche per presunzioni).

Con riferimento alla normativa applicabile, non trova accoglimento l’eccezione sollevata dall’intermediario, il quale sostiene che non verrebbe in rilievo quanto disposto dal D.lgs. 11/2010, con riguardo alle conseguenze sul piano giuridico del difetto di autorizzazione, in quanto il ricorrente avrebbe ammesso di aver personalmente dato il consenso all’esecuzione delle operazioni contestate (ma non anche di averle interamente disposte).

In ordine alle operazioni contestate, le medesime consistono in n. 3 operazioni di *e-commerce* – eseguite in data 25/03/2025 rispettivamente alle ore 15:04, 15:05 e 15:08 – da € 500,00 ciascuna per un totale di € 1.500,00.

Parte ricorrente, in merito alle operazioni contestate, ha allegato il reclamo e il modulo di contestazione di operazioni effettuate con carte.

In ordine al sistema adottato dall’intermediario ed alla prova di autenticazione ed esecuzione delle operazioni di pagamento, l’intermediario ha riferito che le operazioni contestate sono state correttamente autenticate tramite *device* sul quale è stata trasmessa la notifica PUSH contenente i dati di riferimento dell’operazione da autorizzare (fattore di possesso) ed elemento biometrico (fattore di inerenza).

Con riferimento alle operazioni andate a buon fine, l’intermediario rileva che alle ore 15:03, 15:04 e 15:07 del 25/03/2025, risultano avviate le operazioni contestate-

Alle ore 15:03, 15:04 e 15:08 del 25/03/2025, il ricorrente ha ricevuto sul proprio *device* le notifiche PUSH (ed il *device* ha riconosciuto l’elemento biometrico).

Ai medesimi orari, il ricorrente ha ricevuto sulla propria utenza telefonica gli SMS che riferivano l’esito autorizzato delle singole operazioni.

Sulla prova della corretta autenticazione delle operazioni contestate, l’intermediario ha prodotto – con le rispettive legende – i log concernenti: le notifiche PUSH per l’autorizzazione dei pagamenti, i dettagli delle operazioni di pagamenti ed il riconoscimento dell’elemento biometrico.

Nella circostanza, occorre segnalare che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie della specie, l’ABF ha ritenuto provata

l'autenticazione delle operazioni contestate e *compliant* con la SCA il sistema di pagamento adottato dal PSP, tenuto conto dell'utilizzo dei fattori di autenticazione in disamina.

Dalla documentazione agli atti sembra che le operazioni contestate siano scaturite da un fenomeno di *Caller ID spoofing* (spoofing applicato alla chiamata) realizzato ai danni di parte ricorrente.

Nella denuncia, il ricorrente afferma di essere stato contattato dal n. +39 015***011 apparentemente riconducibile all'intermediario e di aver interloquito con un sedicente operatore appartenente all'ufficio prevenzioni frodi, il quale conosceva i suoi dati sensibili e lo invitava a bloccare la sua carta di credito. L'interlocutore lo induceva altresì ad autorizzare n. 3 pagamenti da € 500,00 ciascuno rispettivamente delle ore 15:04, 15:05 e 15:08.

Successivamente, il ricorrente contattava lo stesso numero a cui rispondeva la vera banca, che provvedeva a bloccare il bancomat.

Sebbene l'intermediario non abbia contestato la riferibilità ai suoi contatti del numero indicato in denuncia, limitandosi ad affermare come non risultino chiamate in uscita dal numero della banca verso il cellulare del cliente, il ricorrente non ha allegato il registro chiamate a riprova della telefonata ricevuta dal numero apparentemente riconducibile all'intermediario.

Per completezza, si osserva che nel caso di specie risultano n. 5 richieste di autorizzazione sulla stessa carta di pagamento effettuate tra le ore 15:04 e le ore 15:08 del 25/03/2025 con riferimento al medesimo esercente che opera online, di cui solo n. 3 andate a buon fine, in quanto n. 2 richiesta di pagamento alle ore 15:06 sono state bloccate dall'intermediario in ragione del sistema antifrode adottato. Ad ogni buon conto, non sussiste un obbligo di monitoraggio delle operazioni sospette a carico dell'intermediario.

Appare, in proposito, dirimente che parte ricorrente, nel contestare l'operazione, non ha peraltro versato in atti prova della ricezione della chiamata.

Codesto Collegio di Torino, in plurime occasioni (cfr. decisione n. 6054 del 06/03/2021; decisione n. 10578/2021; decisione n. 10870/2021), ha accolto ricorsi di vittime di *spoofing* sulla base della particolare insidiosità della tecnica così messa in atto, e sulla base della considerazione che le conseguenze di tali tipi di aggressione debbano essere fatte ricadere nel rischio di impresa dei prestatori di servizi di pagamento. Tuttavia, in merito alla valutazione della colpa grave, per orientamento condiviso dei Collegi si è ritenuto che la mancata allegazione, da parte del cliente, della chiamata ricevuta, determini il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto se vi sia un legittimo affidamento dell'utente circa la genuinità del messaggio.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE