

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) COCCIA	Membro di designazione rappresentativa dei clienti

Relatore GIUSEPPE SPENNACCHIO

Seduta del 23/02/2026

FATTO

Il ricorrente nel proprio ricorso sostiene che:

- in data 2 ottobre 2025, alle ore 15:45, accedeva all'*home banking* ed eseguiva un bonifico a titolo di acconto al fine di bloccare l'acquisto di un ciclomotore;
 - dopo circa 10 minuti riceveva una chiamata da un numero riportante la dicitura dell'intermediario durante la quale l'interlocutore l'avvertiva di aver verificato anomalie, in quanto aveva riscontrato che l'importo era stato destinato ad un conto fraudolento, e richiedeva le sue *password*;
 - non forniva le *password* richieste e così l'interlocutore gli comunicava l'invio di codici, tramite sms, volti ad attivare la procedura di impostazione di una nuova *password* in sostituzione del cliente;
 - chiudeva la telefonata senza aver disposto alcuna operazione e provvedeva a contattare immediatamente l'intermediario, chiedendo il blocco;
 - il lasso temporale intercorso tra l'estorsione dei dati e la richiesta di blocco contattando l'intermediario era pari a circa 3/4 minuti;
 - constatava che era stata comunque prelevata indebitamente la somma di €. 9.880,00 mediante l'esecuzione di due bonifici fraudolenti di €. 4.980,00 ed €. 4.900,00;
- Pertanto, chiede il rimborso dell'importo di €. 9.880,00.
L'intermediario, nel contestare l'avversa pretesa, afferma che:

- le operazioni di pagamento del 2 ottobre 2025 sono state autorizzate dal *device* del truffatore, a seguito di una pratica di *phishing/vishing*, in quanto il ricorrente ha seguito le istruzioni impartite telefonicamente dal sedicente operatore;
- l'installazione della nuova *app* sul *device* del truffatore è potuta avvenire esclusivamente con la comunicazione all'interlocutore, da parte del ricorrente, come dallo stesso riferito, dei codici di sicurezza inviati tramite sms, consentendo l'accesso al proprio *account*;
- le operazioni di pagamento sono state correttamente contabilizzate, registrate ed autenticate in assenza di intromissioni informatiche nei sistemi esecutivi;
- il cliente ha ignorato il nuovo presidio introdotto dall'intermediario, che consente la verifica tempestiva dell'identità dell'operatore a partire dall'anno 2024 e che viene presentato nella prima schermata, una volta eseguito l'accesso al proprio *internet banking*;
- ha attuato molteplici campagne di sensibilizzazione della clientela, tramite differenti canali di contatto, contro le frodi, concernenti il presidio di sicurezza, la pratica di *phishing* e la segretezza dei codici autorizzativi, che non vengono richiesti dall'istituto di credito;
- in data 17 settembre 2025, nonché circa n. 15 giorni precedenti l'evento, il cliente ha ricevuto sul proprio *device* una notifica *push*, in cui gli veniva comunicato di prestare attenzione alle chiamate ricevute ed al presidio specifico presente in *app*;
- negli sms genuini inoltrati al cliente, l'avviso di non comunicare a nessuno i codici è riportato in stampatello al fine di evidenziare la finalità e rilevanza in termini di messa in sicurezza del conto;
- in data 2 ottobre 2025, alle ore 15:54, sono state registrate una comunicazione e-mail ed una notifica *push* sul *device* precedentemente in uso con cui si avvertiva il ricorrente dell'installazione di una nuova *app* su un altro dispositivo;
- il cliente, che non fornisce evidenze circa le chiamate ricevute dalla banca, non è intervenuto tempestivamente, proseguendo la conversazione telefonica con il sedicente operatore fino alle ore 15:59;
- la richiesta di richiamo dei bonifici, attivata una volta informato della circostanza, ha avuto esito negativo, non avendo la controparte fornito alcun riscontro;
- la frode posta in essere in data 2 ottobre 2025 non presenta gli elementi sintomatici di rischio ex art. 8, D.M. n. 112/2007.

In sede di replica il ricorrente precisa che:

- l'intermediario non ha fornito la prova dell'adozione di tutte le misure idonee ad evitare che sul telefono, al momento della ricezione della telefonata, comparisse la dicitura "assistenza" del medesimo;
- i codici forniti per l'installazione dell'*app* al frodatore, inviati tramite sms ove figurava la grafica riconducibile ai messaggi genuini inviati dall'intermediario, dovevano essere volti a bloccare definitivamente l'operazione fraudolenta in corso;
- mediante i messaggi ricevuti, avvenivano la variazione della sua *password* e l'installazione dell'*app* sul *device* del truffatore e, una volta compresa la situazione, provvedeva a chiudere la telefonata.

DIRITTO

In ragione della data delle operazioni contestate trova applicazione il d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218, entrato in vigore in data 13 gennaio 2018, di attuazione della direttiva 2015/2366/UE relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al

regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. 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.

In particolare, l'art. 10, d.lgs. n. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento, una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare, innanzitutto, l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la loro esecuzione o di altri inconvenienti. 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 dell'utente.

In secondo luogo, il PSP è tenuto a dimostrare il comportamento gravemente colposo dell'utilizzatore.

Il ricorso ha ad oggetto n. 2 operazioni contestate, consistenti in n. 2 bonifici tramite *home banking* dell'importo, rispettivamente, di €. 4.980,00 ed €. 4.900,00, per un totale di €. 9.880,00, eseguiti tra le ore 15:58 e le ore 15:59 del 2 ottobre 2025. Parte ricorrente, in merito alle operazioni contestate, ha allegato il modulo di contestazione delle stesse.

Nella denuncia depositata in atti vengono riportati gli eventi del 2 ottobre 2025, relativi alle operazioni fraudolente oggetto di ricorso. Alla luce di quanto riferito dalle parti, la truffa risulta essersi articolata mediante *enrollment*, da parte del truffatore, dell'app sul proprio *device* e successiva esecuzione delle operazioni contestate.

L'intermediario ha riferito che le operazioni contestate sono state correttamente eseguite tramite l'inserimento della *password*, dopo aver effettuato l'accesso in app. Sulla prova della corretta autenticazione delle operazioni contestate, ha prodotto, con le rispettive legende, i *log* concernenti l'accesso all'*internet banking*, l'associazione di un nuovo dispositivo all'*account* e l'autenticazione delle transazioni.

L'intermediario afferma che, alle ore 15:52 del 2 ottobre 2025, veniva eseguito in app un accesso dal nuovo dispositivo mediante inserimento della *password* (fattore di conoscenza). Sul punto, allega i *log* in cui figura il corretto inserimento della *password*.

In ragione del nuovo *device* rilevato, l'intermediario ha dato avvio alle ore 15:52 ad un controllo e ad un secondo passaggio di autenticazione, che consiste nell'inserimento del codice dinamico OTP di 6 cifre inviato tramite sms al cellulare del cliente presente in anagrafica. Ha allegato l'sms ricevuto dal ricorrente al proprio cellulare contenente il codice, in cui era precisato di non comunicarlo a nessuno e che gli operatori non lo richiedono mai.

Con riferimento al numero telefonico associato al ricorrente, la banca dichiara che quest'ultimo lo ha indicato al momento della registrazione e che risulta altresì dal contratto.

Anche a seguito delle controdeduzioni dell'intermediario, in cui emerge la prodromica installazione dell'app sul *device* del truffatore, il cliente nulla dice a riguardo. Con riferimento a tale operazione, l'intermediario afferma che la fase di *enrollment* dell'app sul dispositivo è stata autenticata tramite PIN ed invio di sms OTP sul recapito telefonico registrato sull'anagrafica del cliente.

Nelle controdeduzioni ha dettagliato i passaggi necessari per procedere all'installazione della nuova app sul *device* ed ha allegato le relative evidenze con riferimento al caso di specie, fornendo altresì prova della notifica *alert* inviata al

ricorrente circa l'*enrollment* dell'app. L'intermediario afferma, infatti, che il cliente ha attivato la nuova app in data 2 ottobre 2025 (i.e.: lo stesso giorno dell'esecuzione dei bonifici fraudolenti), su di uno *smartphone* iPhone 17.2.

Con specifico riferimento all'esecuzione delle operazioni contestate del 2 ottobre 2025, l'intermediario afferma e fornisce prova che esse sono state correttamente autenticate tramite elementi di conoscenza (il cliente ha autorizzato le operazioni digitando la *password* che solo egli conosce) e di possesso.

Il ricorrente, dal canto suo, non ha fornito nessuna prova a sostegno di quanto riferito in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento. Nella denuncia e nel ricorso, rappresenta solo di aver ricevuto una telefonata da un numero riferibile all'intermediario, di aver comunicato all'interlocutore i codici bancari e di essersi, quindi, accorto dell'utilizzo fraudolento.

Indica, in particolare, nel ricorso che:

- in data 2 ottobre 2025, alle ore 15 circa, navigando su una piattaforma di *e-commerce*, notava un annuncio e decideva di contattare il venditore, tramite la chat dell'applicativo, al fine di acquistare un ciclomotore;
- verificava che il fornitore gli forniva il cellulare appartenente al figlio, con il quale interloquiva telefonicamente, accordandosi sul versamento di €. 60,00 a titolo di acconto, allo scopo di bloccare l'acquisto del prodotto;
- contattato da un cellulare, riportante la dicitura dell'intermediario, da cui chiamava un sedicente operatore, gli forniva i codici necessari ad impostare un nuovo pin;
- tuttavia, dopo aver effettuato l'accesso al conto, notava n. 2 bonifici istantanei da lui non disposti.

Secondo l'orientamento condiviso tra i Collegi, in aderenza al dato normativo è necessario e sufficiente, ai fini dell'applicazione della PSD2, che il cliente neghi di aver autorizzato la transazione: il Collegio può valutare la mancata allegazione dei fatti ovvero del registro chiamate o dell'sms civetta, tra i vari elementi, per formare il proprio convincimento circa la colpa grave del ricorrente solo una volta verificata la sussistenza della SCA. Fermo quanto sopra, secondo l'orientamento dei Collegi nelle contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento in cui l'intermediario ha offerto la prova dell'autenticazione delle transazioni sconosciute, il sistema di pagamento risulta conforme alla *Strong Customer Authentication* e non risultano indizi di anomalia delle operazioni e/o ulteriori elementi, le mancate allegazioni del cliente o le mancate produzioni documentali sulle circostanze di fatto della frode che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del cliente medesimo.

Più in particolare, i Collegi sono unanimi nel ritenere che la mancata allegazione, da parte del cliente, del messaggio civetta o del registro chiamate debba determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti. Per tali ragioni, nel caso di specie, la pretesa del ricorrente non può essere accolta.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE