

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 21/04/2026

FATTO

La parte ricorrente espone al Collegio di essere stata vittima di una sofisticata operazione di *spoofing*. In particolare, in data 24/03/2025, riceveva un messaggio fraudolento all'interno della medesima chat utilizzata per le comunicazioni ufficiali dell'intermediario, il quale la invitava a contattare un numero telefonico per bloccare un presunto addebito sospetto di € 1.980,00.

A seguito del contatto, un sedicente addetto dell'ufficio antifrode forniva istruzioni per diverse operazioni di sicurezza, protrattesi fino al giorno successivo. Solo al termine di tali interlocuzioni, parte ricorrente riscontrava l'esecuzione di un bonifico non autorizzato di € 48.720,01, operazione mai consapevolmente disposta né riconosciuta.

Parte ricorrente riferisce di essersi attivata tempestivamente presentando denuncia-querela in data 26/03/2025 e inoltrando reclamo formale con disconoscimento in data 11/06/2025, ricevendone riscontro negativo il giorno seguente. Tramite un'associazione di tutela dei consumatori, richiedeva quindi la restituzione integrale delle somme sottratte.

A sostegno della domanda, si deduce l'assenza di dolo o colpa grave, rivendicando una condotta diligente e conforme agli obblighi normativi. Contestualmente, si contesta all'intermediario una carenza nei presidi di controllo e nei doveri di protezione, per aver consentito un'operazione di importo eccezionalmente elevato e incongruo rispetto alla normale operatività del conto senza attivare blocchi cautelativi. Secondo la tesi della parte ricorrente, l'affidamento incolpevole ingenerato dalla modalità

del contatto e le falle nei sistemi di sicurezza dell'intermediario fondano il diritto al rimborso integrale della somma.

Per questi motivi parte ricorrente chiede l'integrare rimborso delle somme indebitamente sottratte pari a complessivi € 48.721,00.

L'intermediario, contro deduce chiedendo il rigetto del ricorso ritenendolo infondato, in quanto l'operazione contestata sarebbe riconducibile alla condotta della parte ricorrente e non a un utilizzo indebito imputabile all'istituto. Viene evidenziato che la parte ricorrente è stata vittima di un fenomeno di *spoofing* ampiamente segnalato alla clientela, precisando che l'identità del mittente non garantisce l'effettiva provenienza della comunicazione dalle utenze ufficiali.

Secondo l'intermediario, il bonifico è stato correttamente eseguito, registrato e contabilizzato, essendo stato disposto tramite *home banking* con l'inserimento dei fattori di autenticazione previsti dalla *Strong Customer Authentication*. Si contesta alla parte ricorrente una condotta gravemente negligente per aver seguito le istruzioni di un sedicente operatore e aver disposto personalmente il bonifico senza effettuare verifiche tramite i canali ufficiali, nonostante gli *alert* di sicurezza forniti. Le verifiche interne non hanno fatto emergere anomalie o accessi non autorizzati, confermando che l'operazione è stata eseguita dal dispositivo abituale della parte ricorrente e correttamente tracciata nei sistemi informativi. Per questi motivi l'intermediario chiede il rigetto del ricorso in quanto infondato in fatto ed in diritto.

Parte ricorrente, richiamati i propri scritti, replica di essere stata vittima di un bonifico non autorizzato tempestivamente disconosciuto, sottolineando che nella denuncia non vi è alcuna ammissione di autorizzazione né di inserimento consapevole delle credenziali. Viene contestato all'intermediario di non aver fornito prove idonee a dimostrare il dolo o la colpa grave, né la tardività del disconoscimento. Secondo la parte ricorrente, i log applicativi e la documentazione tecnica depositata attestano solo la regolarità formale del processo informatico (Strong Customer Authentication), ma non provano chi abbia materialmente disposto l'operazione; tali documenti, essendo unilaterali e autoprodotti, sono ritenuti inidonei a dimostrare un consenso valido. Si contesta infine la carenza di diligenza professionale dell'intermediario ex art. 1176, comma 2, c.c., poiché l'importo di € 48.721,00, prossimo all'intera giacenza del conto, era oggettivamente anomalo. Tale circostanza avrebbe dovuto imporre l'attivazione di controlli informativi o un blocco cautelativo della transazione, verifiche che non risultano effettuate.

L'intermediario non ha depositato repliche.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo € 48.720,00 + € 1,00 per commissione, sottratta a seguito di un'operazione di bonifico fraudolenta eseguita in data 24/03/2025, alle ore 15:35. In particolare, parte ricorrente ha dato credito alle istruzioni fornite dal truffatore, il quale indicava la necessità di eseguire due operazioni per bloccare la transazione sospetta segnalata.

L'operazione contestata è disciplinata dal D.lgs. 27/01/2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori: a) è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni; inoltre la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse; b) è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert. Peraltro secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), 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. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.lgs. 11/2010.

L'intermediario sostiene che l'operazione sia stata interamente eseguita dalla parte ricorrente, configurando l'inapplicabilità della disciplina PSD2 e che appare inverosimile che parte ricorrente si sia avveduta della truffa solo due giorni dopo tramite l'app, visti i molteplici accessi effettuati sia il giorno dell'evento che quello successivo.

Al riguardo, si osserva che, come rilevato dall'intermediario, parte ricorrente non dichiara né nel ricorso né in denuncia di aver eseguito personalmente l'operazione, ragion per cui il Collegio procede all'esame della SCA.

Con riferimento al sistema di autenticazione forte dell'intermediario per le azioni antecedenti l'esecuzione dell'operazione contestata, il Collegio constata che dalle evidenze prodotte, corredate di legenda esplicativa, si ricava che l'autenticazione è correttamente avvenuta tramite l'applicazione di mobile token del PSP sullo smartphone, sbloccata con codice PIN, che genera un codice che ha il valore dei due fattori della SCA congiunti ("conoscenza" del PIN e "possesso" dello smartphone). Con riferimento a questa fase può quindi ritenersi provata la SCA (cfr. Collegio di Milano, decisione n. 5321/2025).

Quanto invece al sistema di autenticazione forte, con riguardo all'esecuzione dell'operazione contestata di € 48.720,00, il Collegio constata che alle evidenze prodotte risulta che: un fattore di autenticazione è dato dalla validazione della notifica push ricevuta sul device, con conseguente generazione del codice OTP transazionale c.d. silente (elemento di possesso); l'altro fattore di autenticazione è dato dall'utilizzo del PIN (elemento di conoscenza) per la validazione della push; risulta, inoltre, evidenza dell'OTP transazionale silente, generatosi a seguito del suo inserimento. Anche con riferimento a questa fase può quindi ritenersi provata la SCA (cfr. Collegio di Milano, decisione n. 5321/2025).

Il Collegio, ritenuta provata la SCA, in relazione a tutti i singoli passaggi esaminati, procede a verificare se parte ricorrente abbia agito con colpa grave e se vi sia stato un concorso di colpa da parte dell'intermediario.

Parte ricorrente riferisce di aver ricevuto, in data 24/03/2025, un messaggio relativo a un'operazione sospetta con l'invito a contattare l'assistenza a un numero indicato. Contattato tale recapito, un sedicente operatore dell'intermediario la istruiva sull'esigenza di compiere due operazioni tramite l'App di home banking per salvaguardare il conto. In sede di denuncia, parte ricorrente dichiara di aver aperto l'applicativo seguendo istruzioni di cui non comprendeva appieno la finalità.

Dall'analisi delle evidenze prodotte in merito all'SMS civetta, emerge quanto segue: (i) il messaggio fraudolento pare collocato in un'e-mail senza un mittente individuabile e, pur contenendo un riferimento all'intermediario, nella medesima chat non compaiono messaggi genuini; (ii) il testo non presenta errori grammaticali, ma il numero di telefono indicato non è riconducibile all'intermediario; (iii) parte ricorrente non ha inoltre fornito il registro delle chiamate effettuate; (iv) parte ricorrente dichiara di aver rilevato la truffa solo il 26/03/2025 tramite App, circostanza contestata dall'intermediario in ragione dei molteplici accessi che risultano effettuati già il giorno precedente.

In merito al recall, l'intermediario dichiara di averlo esperito senza successo, ma non risulta documentazione agli atti. Dalle evidenze in atti risulta inoltre sia l'invio dell'SMS alert che della notifica push in data e ora coerenti con quanto riferito dalla parte ricorrente.

La parte ricorrente sottolinea, infine, come dato l'importo rilevante, l'intermediario avrebbe dovuto adottare misure di intervento più incisive. Tuttavia, parte ricorrente non produce documentazione relativa alla propria abituale operatività. In merito al dedotto esaurimento del plafond, l'intermediario osserva che il saldo del conto corrente era in realtà ancora elevato e che la causale "pagamento immobile" non presentava anomalie, ribadendo inoltre l'insussistenza di un proprio dovere di monitoraggio.

Per questi motivi il Collegio, ritenuta provata la SCA da parte dell'intermediario e ritenuta la sussistenza di una colpa grave in capo alla parte ricorrente, ritiene che il ricorso non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE