

## COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore BARTOLOMEO GRIPPO

Seduta del 28/01/2025

### FATTO

Parte ricorrente afferma che in data 26/03/2024 alle ore 16:00 circa riceveva un SMS che lo informava di un problema di accesso al proprio conto corrente, invitandolo a contattare il n. \*18 per effettuare un aggiornamento della sicurezza.

Il messaggio SMS era inserito nel canale ufficiale dell'intermediario convenuto; ricercava su internet il numero telefonico indicato nell'SMS riscontrando la riferibilità del numero ad una filiale dell'intermediario; convinto quindi dalla bontà del messaggio chiamava il predetto numero e l'interlocutore, qualificatosi come funzionario dell'intermediario, lo informava di alcuni malfunzionamenti del sistema bancario e indicava, pertanto, la necessità di aggiornamento e messa in sicurezza attraverso un link inviato sul proprio cellulare.

Non totalmente convinto decideva di non ottemperare alla richiesta. Successivamente riceveva diverse telefonate dal n. \*60 e l'interlocutore confermava l'esigenza di svolgere verifiche e mettere in sicurezza il suo conto personale. Confidando nella bontà della chiamata, in quanto proveniente dal numero unico di assistenza dell'intermediario, dando seguito alle indicazioni del sedicente operatore, cliccava sul link inviato via SMS.

Durante la telefonata mai inseriva, digitava o forniva all'interlocutore i dati, lo user o la password del suo conto corrente. L'interlocutore riferiva di aver riscontrato alcuni movimenti anomali esteri sul suo conto personale e dopo aver terminato la procedura

chiedeva di procedere alle verifiche di corretta funzionalità del conto e dell'APP, mediante l'esecuzione di un minimale bonifico di prova.

Mediante un conto detenuto presso altro intermediario effettuava un bonifico dell'importo di € 5,00 a favore del conto detenuto presso l'intermediario resistente; il cellulare tornava operativo e la telefonata con l'operatore terminava.

Il 27/03/2024, recatosi alla propria filiale per una programmata operazione bancaria, riscontrava che erano stati effettuati n. 3 bonifici, uno istantaneo e due ordinari, per un totale di € 47.583,28, mai autorizzati.

Controllando anche l'altro conto personale presso intermediario terzo, veniva a conoscenza di ulteriori n. 4 bonifici per un totale di € 100.320,00.

L'importo complessivo dei n. 3 pagamenti risulta oltre i limiti previsti di somma bonifico giornaliera da APP, pari a € 15.000,00, oltre il limite orario e, oltretutto, azzerava la liquidità e la giacenza del conto del ricorrente.

L'intermediario avrebbe dovuto accorgersi della situazione anomala e, almeno, bloccare i due bonifici ordinari. Non sono stati inviati OTP né alcuna comunicazione di inserimento, richiesta di autorizzazione e conferma di esecuzione dei bonifici.

Ha diritto al risarcimento anche della perdita di € 100.320,00, subita sul conto corrente aperto presso intermediario terzo, quale danno consequenziale e collegato in modo unitario e diretto con l'evento di accesso da parte di terzi sul suo conto detenuto presso l'intermediario convenuto.

Parte ricorrente - esperita senza successo la fase del reclamo - chiede il rimborso della somma di € 147.903,28, oltre interessi, rivalutazione e spese di assistenza tecnica.

L'intermediario, con le controdeduzioni, precisa preliminarmente che il *petitum* del ricorso deve considerarsi ridotto ad € 45.893,50 (commissioni incluse), mentre per le ulteriori n. 4 operazioni, come previsto dalla normativa PSD2, il ricorrente dovrà indirizzare la domanda all'intermediario che ha registrato l'addebito.

Il ricorrente, intestatario del conto corrente n.\*92, al quale è collegato il servizio di home banking, ha contattato il n. \*18 non riconducibile ai propri canali ed anzi l'esito delle verifiche del numero sul web, a differenza di quanto affermato dal cliente, evidenzia che si tratta di una utenza truffaldina.

Il ricorrente non produce l'SMS "civetta" e il messaggio contenente il link, ammette di aver seguito le istruzioni ricevute al telefono da persona a lui sconosciuta che lo ha guidato nello svolgimento di una procedura che definisce molto complessa, durata ore, al termine del quale il suo *device* si riavviava.

E' plausibile ritenere che il truffatore gli abbia fatto scaricare un'APP attraverso la quale ha assunto il controllo del suo strumento di pagamento; per accedere al link è plausibile che il ricorrente abbia dovuto digitare le proprie credenziali di sicurezza, rendendole così note al terzo; infine, inducendolo ad eseguire il bonifico di € 5,00 dall'altro conto corrente ha potuto carpire le credenziali di sicurezza anche di quest'ultimo. Se al termine della telefonata il cliente avesse controllato immediatamente il suo conto corrente per verificare che effettivamente non vi fossero bonifici anomali o meglio avesse chiamato il servizio clienti per verificare la regolarità delle operazioni eseguite, sarebbe venuto a conoscenza della frode e avrebbe potuto consentire il blocco delle operazioni.

Per quanto attiene ai limiti di importo giornalieri dei bonifici l'importo di € 15.000,00 a cui fa riferimento il ricorrente riguarda solo i bonifici istantanei, mentre per quelli ordinari il limite giornaliero è di € 50.000,00; le operazioni sono state correttamente autenticate, registrate e contabilizzate senza alcun malfunzionamento dei sistemi operativi.

L'intermediario chiede, pertanto, di respingere il ricorso perché infondato.

Parte ricorrente, in sede di repliche, afferma che: l'intermediario produce i risultati della stessa ricerca web effettuata il 26/03/2024 quando ormai la truffa era stata scoperta dalla pubblica utenza; nella medesima pagina web si evince, infatti, come le segnalazioni di truffa sono iniziate dal pomeriggio del 26/03/2024, dopo l'evento in esame; in ogni caso non ha mai fornito o digitato le proprie credenziali e/o il PIN per eseguire le operazioni contestate.

## DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.

Preliminarmente il Collegio rileva che il ricorrente chiede che l'intermediario sia tenuto a risarcire non soltanto le operazioni eseguite dal conto intrattenuto presso di lui, bensì anche le perdite subite mediante operazioni truffaldine eseguite dal suo conto corrente aperto presso un intermediario terzo (non convenuto) pari ad € 100.320,00; tale domanda risarcitoria è da respingere sia alla luce dell'art. 11 del D.lgs. 11/2010 sia in quanto il ricorrente non ha dato prova alcuna che il comportamento della banca resistente gli abbia cagionato tale danno, non sussistendo pertanto neppure i presupposti perché esso sia liquidato equitativamente.

Nel merito le operazioni validamente contestate da parte ricorrente (n. 3 disposizioni di bonifico del 26/03/2024 dalle ore 16:33 alle ore 16:43 per un importo complessivo di € 45.893,50) rientrano nell'ambito di applicazione della disciplina del D.lgs. 27/01/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD2).

La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.

Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.

La normativa mostra un chiaro *favor probatorio* nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.

Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia.

In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, 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.

Con riferimento alla *strong customer authentication* (cosiddetta SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-bis del D.lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (cfr. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente: 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Nel caso di specie, sotto il primo profilo, l'intermediario non ha prodotto una completa documentazione relativa alla registrazione, contabilizzazione e autenticazione delle operazioni disconosciute.

In particolare, in merito all'inserimento del PIN (elemento di conoscenza) nella fase di login/accesso all'area riservata si evidenzia che l'utilizzo del PIN risulta dalla descrizione attività utente e dalle dichiarazioni dell'intermediario. Risulta, inoltre, evidenza dell'OTP silente, generatosi a seguito della validazione della push, ma la colonna esito operazione non è, tuttavia, valorizzata con "Y".

Anche con riferimento all'esecuzione delle operazioni contestate non vi è evidenza dell'effettivo inserimento del relativo codice PIN.

Il Collegio ricorda che è onere dell'intermediario provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D.lgs. 11/2010). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute (cfr. Collegio di Coordinamento, decisione n. 22745 del 10 ottobre 2019).

Secondo gli orientamenti condivisi dei Collegi, infatti, la prova della corretta autenticazione/contabilizzazione/registrazione delle operazioni, in aderenza al dato normativo, rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente.

Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma già arrotondata di € 45.894,00, pari all'ammontare delle tre operazioni disconosciute.

Il Collegio, infine, accoglie la domanda di parte ricorrente relativa al riconoscimento dei soli interessi legali dalla data del reclamo (cfr. Collegio di Coordinamento, decisione n. 5304/13) non avendo il ricorrente provato il maggior danno ex art. 1224, co. 2, c.c. e non accoglie la richiesta di rimborso delle spese di assistenza legale, non ricorrendo le condizioni già indicate dal Collegio di Coordinamento (decisione n. 6174/2016).

### **PER QUESTI MOTIVI**

**Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 45.894,00, oltre interessi legali dal reclamo al saldo.**

**Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.**

**IL PRESIDENTE**

Firmato digitalmente da  
ANDREA TINA