

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore SERGIO IMBURGIA

Seduta del 26/02/2026

FATTO

Con ricorso, preceduto da formale reclamo, la ricorrente – titolare di un conto corrente presso l'intermediario – espone di essere stata vittima di una truffa posta in essere da terzi ai suoi danni e chiede la restituzione della somma di € 29.800,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da sconosciuti.

Con riferimento alle modalità della truffa, riferisce di essere stata contattata, in data 11/7/2025, sulla propria utenza fissa, da un sedicente operatore dell'intermediario che la chiamava dal n. 02****471 per informarla di alcuni accessi anomali sul conto e di alcune operazioni di bonifico. Il sedicente operatore, ottenuta dalla correntista la conferma di non avere effettuato le disposizioni in corso, anticipava alla ricorrente che sarebbe stata ricontattata per le dovute verifiche.

La cliente veniva quindi nuovamente contattata dal medesimo interlocutore sulla propria utenza mobile e veniva invitata ad eseguire alcune istruzioni per bloccare i sedicenti tentativi di accesso al conto e revocare alcune operazioni di bonifico.

Allarmata dal tono incalzante dell'interlocutore, stante il fatto che l'utenza dalla quale veniva contattata era riferibile all'intermediario, accettava l'assistenza dell'operatore, che effettuava quindi l'accesso a distanza al conto corrente tramite l'app "TeamViewer". Nel corso delle operazioni, riceveva due diversi SMS che riportavano la dicitura "Bonifico di Euro 14.900,00 annullato con successo", circostanza questa che la rassicurava; di tal che lasciava che l'operatore proseguisse con le sedicenti operazioni di sicurezza.

Solo successivamente, verificando la movimentazione del rapporto, si avvedeva che erano stati effettuati dal proprio conto due bonifici di euro 14.900,00 ciascuno in favore di soggetto sconosciuto e di ammontare eccedente il saldo attivo del conto, e ciò ancorché dalla Banca non le fosse mai pervenuta alcuna notifica delle avvenute disposizioni di pagamento.

Resasi conto della truffa subita la cliente chiedeva il blocco del suo Home Banking, denunciava i fatti, disconosceva formalmente le operazioni contestate e chiedeva alla banca il rimborso delle somme oggetto dei bonifici contestati, ricevendo, in ultimo, riscontro negativo.

La ricorrente sostiene di essere rimasta vittima di una truffa sofisticata realizzata mediante tecniche di spoofing e vishing, mediante le quali i truffatori l'hanno indotta a collaborare nella presunta ed asserita messa in sicurezza del proprio home banking. Evidenzia che tali tecniche sono idonee a trarre in inganno anche un utente avveduto e che in assenza di adeguati presidi di sicurezza – nel caso di specie insussistenti o comunque inefficaci – la responsabilità dell'accaduto non può che ricadere sull'intermediario, non potendosi configurare la sussistenza di qualsiasi profilo di colpa, tanto meno grave, a carico della cliente.

Evidenzia inoltre di non avere ricevuto alcuna notifica o alert dalla banca e precisa di non avere mai dichiarato di avere effettuato personalmente i bonifici contestati.

Tali ragioni hanno indotto la ricorrente ad adire l'ABF chiedendo all'arbitro di dichiarare l'intermediario tenuto all'integrale rimborso della somma di € 29.800,00 corrispondente all'importo delle operazioni disconosciute.

Nelle controdeduzioni l'intermediario eccepisce preliminarmente che, dalle stesse dichiarazioni rese dalla ricorrente in sede di denuncia, risulta che i bonifici sono stati eseguiti personalmente dalla cliente dal proprio computer; per tale ragione la fattispecie non rientra nell'ambito applicativo del D. Lgs 11/2010. Produce comunque le tracciate informatiche attestanti la corretta autenticazione delle operazioni, autorizzate mediante OTP inviati via SMS alla utenza certificata della cliente.

Dall'analisi di dette tracciate emergerebbe – secondo il resistente – le operazioni sono state effettuate dal dispositivo della ricorrente, la quale, con imprudenza, avrebbe installato sul proprio PC il software Team Viewer, consentendo così l'accesso ai frodatori, vanificando le misure di sicurezza predisposte dall'intermediario.

La banca inoltre evidenzia di avere condotto un'ampia campagna informativa sui rischi inerenti alle frodi informatiche nonché sulle cautele da adottare e contesta che nel caso di specie la truffa asseritamente subita dalla ricorrente possa inquadrarsi nell'ambito dello spoofing e ciò in quanto né il numero telefonico né i messaggi ricevuti, recanti il mittente "info", sono riconducibili all'intermediario convenuto. Rileva, infine, l'esistenza di un bonifico disposto un mese prima in favore del medesimo beneficiario e non sconosciuto, nonché l'infondatezza dell'assunto secondo cui il conto era privo di fondi, trattandosi di conto collegato ad un "conto salvadanaio" che svincola automaticamente le somme necessarie al momento dell'operazione.

Chiede quindi il rigetto del ricorso.

Parte ricorrente, in sede di repliche, afferma che: non ha mai effettuato personalmente i due bonifici contestati né ha mai prestato alcun consenso, neppure viziato, all'operazione; è stata vittima di una sofisticata operazione fraudolenta; in tema di responsabilità, spetta all'intermediario fornire la prova della colpa grave della cliente, nel caso di specie insussistente; i truffatori conoscevano i dati anagrafici della correntista, le sue utenze telefoniche e la sua qualità di correntista, circostanza questa che depone per l'esistenza di una falla nei sistemi di sicurezza della banca; in ogni caso la sottrazione dei codici del correntista costituisce una eventualità rientrante nel rischio di impresa con la conseguenza che la banca per liberarsi dalla propria responsabilità, deve provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento.

La ricorrente osserva inoltre che le tracciature prodotte dalla banca costituiscono un mero documento interno all'intermediario e dimostrano soltanto la generazione e l'invio ma non la ricezione dell'OTP né che sia stata la cliente ad utilizzare il codice autorizzativi dei bonifici. Precisa inoltre che gli unici SMS ricevuti erano messaggi fraudolenti relativi a presunti "annullamenti" e sottolinea la mancanza di tempestivi sistemi di allerta da parte della banca. Quanto al precedente bonifico verso il medesimo beneficiario, conferma l'esecuzione, in data 11/6/2025, di un bonifico istantaneo di euro 20,00. Conclude quindi che dall'intera vicenda risulta palese la responsabilità dell'intermediario.

Nelle controrepliche il convenuto deduce che: le tracciature informatiche depositate in sede di controrepliche riportano nel foglio SMS i tre messaggi ricevuti sull'utenza certificata della ricorrente, contenenti proprio i codici OTP necessari per autorizzare il login e i bonifici disposti via browser; l'indirizzo IP dal quale risultano disposti i bonifici, risulta essere il medesimo utilizzato in precedenza per disporre diverse altre operazioni, non sconosciute; la documentazione allegata, diversamente da quanto sostenuto da controparte, prova senza ombra di dubbio come la ricorrente abbia ricevuto i messaggi sms aventi ad oggetto i codici OTP sulla propria utenza certificata e li abbia poi inseriti.

Rileva inoltre che i Collegi territoriali dell'ABF ritengono provata la colpa grave dell'utente laddove, come nel caso di specie, risulti documentata sia la inattendibilità dei "messaggio civetta", sia la ricezione da parte del ricorrente di sms dell'intermediario il cui contenuto indicava in modo dettagliato e inequivocabile il tipo di operazione che il cliente era in procinto di autorizzare. Rileva inoltre che la cliente è incorsa in colpa grave non soltanto per avere scaricato sul proprio computer il programma che ha verosimilmente consentito ai truffatori di controllare l'operatività da remoto ma per avere anche lasciato trascorre il lungo lasso di tempo intercorrente tra la prima e la seconda chiamata (40 minuti circa) senza contattare il proprio consulente bancario.

Ribadisce quindi che le operazioni fraudolente siano state rese possibili solo dal comportamento gravemente colposo della ricorrente.

DIRITTO

Parte ricorrente chiede la restituzione della somma di € 29.800,00 corrispondente all'importo di due bonifici istantanei sconosciuti, ciascuno di € 14.900,00, asseritamente eseguiti fraudolentemente da terzi in data 11/7/2025.

Le operazioni sconosciute rientrano nell'ambito applicativo del d.lgs. n. 11/2010, come modificato dal d.lgs. n.218/2017 – in vigore dal 13/1/2018 – che ha recepito la nuova Direttiva sui servizi di pagamento nel mercato interno-2015/2366/UE (c.d. PSD2). Devono in particolare essere richiamati gli artt.7, 10 e 12 del citato decreto che, con l'obiettivo dichiarato di tutelare il cliente, allocano in via tendenziale sull'intermediario il rischio di utilizzazione fraudolenta degli strumenti di pagamento.

In particolare, l'articolo 7 impone che il primo utilizzi siffatti strumenti conformemente alle prescrizioni contrattuali, in modo diligente, adottando le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo.

Relativamente all'articolo 10 vengono in rilievo le disposizioni previste nei commi 1 e 2.

L'art. 10, comma 1, stabilisce infatti che qualora l'utente di servizi di pagamento neghi di avere autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, "è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata".

Il successivo comma 2, dello stesso art. 10 aggiunge tuttavia che la prova dell'autenticazione e della regolarità formale dell'operazione fornita "non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7", e che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di

disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

L'articolo 12, comma 2 bis, infine, stabilisce che il pagatore – fatta salvo il caso in cui abbia agito in modo fraudolento – “non sopporta alcuna perdita se il prestatore di servizio di pagamento non esige una autenticazione forte del cliente”. Tale tipologia di autenticazione (c.d. SCA) viene declinata nell'art. 1, lettera q), e trova la sua regolamentazione nell'articolo 10 bis del D. Lgs n. 11/2010, negli artt. 97 e 98 della PDS2, 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.

In base a tali disposizioni, come applicate da questo Arbitro (da ultimo, ABF Collegio di Coordinamento n. 22745 del 10 ottobre 2019), due sono i passaggi ineludibili in materia.

In primo luogo, è l'intermediario a dover provare, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza che le operazioni disconosciute siano state autenticate con un c.d. “sistema di autenticazione forte” (strong customer authentication o SCA).

Secondariamente, 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 tale contesto e con riguardo al caso di specie è possibile rilevare, quanto al primo aspetto, che l'intermediario ha esibito una completa e dettagliata documentazione, ritenuta attendibile dai Collegi territoriali dell'ABF in fattispecie analoghe a quella in esame, dalla quale emerge la corretta esecuzione di tutte le fasi della procedura di autenticazione.

In particolare la fase di accesso all'Home Banking è avvenuta con digitazione delle credenziali personali note solamente alla ricorrente, valevoli quali elemento di conoscenza, e utilizzo di codice OTP inviato mediante notifica push indirizzata all'utenza certificata della cliente. Le operazioni dispositive risultano poi disposte all'interno della stessa sessione di accesso ora analizzata mediante riutilizzo del fattore di conoscenza ed impiego del codice OTP inviato alla cliente come innanzi già precisato. Alla luce di quanto sopra, il Collegio ritiene assolto l'onere probatorio in ordine all'adozione delle prescrizioni dettate dalla normativa in tema di SCA.

Una volta autenticate, le operazioni dispositive risultano eseguite secondo l'operatività propria della tipologia di conto di titolarità della cliente (conto M^{***}) che, come chiarito dall'intermediario, consente di accantonare parte del saldo creditore accedente rispetto all'importo prefissato in sede di sottoscrizione e dal quale, all'occorrenza, le somme del cliente vengono automaticamente rese disponibili con valuta pari a quella della disposizione (ricostruzione questa coerente con le risultanze del foglio informativo “salvadanaio” pubblicato sul sito dell'intermediario e non contestata dalla ricorrente in sede di repliche). Provata, così, la corretta autenticazione dell'operazione disconosciuta, è possibile passare ad esaminare il profilo soggettivo della condotta dell'utilizzatore dello strumento di pagamento.

Al riguardo il Collegio osserva che la cliente, se pur in buona fede, ha seguito tutte le indicazioni del truffatore, laddove l'utilizzo di una media diligenza avrebbe evitato il perpetrarsi della condotta delittuosa. Infatti, molti dei tentativi di truffa posti in essere in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento - a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione - a tenere una condotta suggerita dallo stesso truffatore solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza (Cfr. Collegio di Milano 12572/22).

La diffusione del fenomeno è tale che i Collegi ABF ritengono che l'impiego di una media diligenza sia ormai sufficiente a scongiurare il pericolo e ad impedire la truffa e che in fattispecie analoghe a quella oggi in esame il cliente debba ritenersi vittima di una colpevole credulità. (Cfr. Collegio di Palermo decisione n. 20936/2022; Collegio di Torino 3625/23).

Peraltro, con riferimento alla fattispecie in disamina, osserva il Collegio che gli sms ricevuti risultano inseriti in una chat non riconducibile all'intermediario (intestata "INFO") e presentano evidenti anomalie formali - errori nella denominazione dell'intermediario, assenza di punteggiature e non corretta formattazione degli importi – idonee a far legittimamente dubitare della loro autenticità. Inoltre la ricorrente, su indicazione del sedicente operatore, ha scaricato l'applicazione "Team Viewer", consentendo l'accesso al proprio dispositivo e la piena operatività da remoto al truffatore.

La colpa grave della ricorrente deve quindi ritenersi sussistente.

Va in ultimo rilevato che, ad avviso del Collegio, in relazione all'accaduto non emergono profili di responsabilità a carico dell'intermediario. Risulta infatti provata, mediante specifiche allegazioni, l'attivazione del servizio di sms alert per le operazioni contestate e non emergono indici di anomalia. Solo nelle repliche il ricorrente ha sostenuto che gli importi sarebbero anomali rispetto alla consueta movimentazione del conto, senza tuttavia produrre estratti conto idonei a comprovare detta circostanza.

Per quanto sopra esposto il Collegio ritiene che non sussistano i presupposti per l'accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE