

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) SANTARELLI

Seduta del 10/03/2026

FATTO

Parte ricorrente agisce in relazione ad un addebito di € 7.499,00 eseguita il 2 ottobre 2024 di cui chiede il rimborso integrale, ovvero, in subordine, nei limiti di cui all'art. 12, comma terzo del D. lgs 11/2010. Questi i fatti descritti a sostegno della propria domanda. In data 01/10/2024 riceveva una chiamata da un numero corrispondente a quello ufficiale dell'intermediario. L'interlocutore, qualificandosi come operatore antifrode della banca, la informava che ignoti aveva effettuato un accesso al suo conto corrente e disposto dei bonifici da lei non autorizzati. Il sedicente operatore si rendeva disponibile ad aiutarla nell'operazione di annullamento delle operazioni dicendole che

sarebbe entrato nel suo computer come 'assistente esterno'. Effettuato l'accesso al conto riscontrava un giroconto non autorizzato di circa € 6.000,00 dal proprio conto deposito al conto corrente e, sotto forte pressione emotiva, fidandosi dell'apparente identità del suo interlocutore, effettuava l'accesso al proprio *home banking* e, condiviso lo schermo con il presunto operatore tramite un sistema di assistenza remota, autorizzava tramite app più operazioni nella convinzione che si trattasse della procedura necessaria ad annullare i bonifici fraudolenti: l'interlocutore eseguiva, così, diversi bonifici istantanei apparentemente respinti dalla banca. Il giorno successivo (02/10/2024) veniva contattata nuovamente dal presunto operatore per completare l'annullamento delle operazioni residue e così veniva così eseguito un bonifico ordinario di € 7.499,00 che veniva bloccato temporaneamente dalla banca che, per provvedere alla sua esecuzione, le chiedeva tramite e-mail un documento di identità. Ritenendo di agire ancora sotto la guida del servizio antifrode, inviava copia del proprio documento confermando l'operazione. A seguito della denuncia presentata presso le competenti Autorità emergeva che i fondi trasferiti erano stati ritirati in contanti presso lo sportello dell'intermediario terzo. Ne conseguiva che il recall non sortiva effetti. Secondo parte ricorrente l'intermediario avrebbe dovuto: (i) attivare immediatamente le misure di protezione e di monitoraggio delle transazioni caratterizzate da elementi di assoluta anomalia (importi elevati; accessi da dispositivi diversi o con sessioni condivise tramite software di controllo, causali incompatibili con l'uso tipico del conto; ripetute operazioni in tempi ravvicinati); (ii) rispettare l'obbligo di diligenza qualificata, bloccando preventivamente lo strumento di pagamento in presenza di operazioni non in linea con il proprio ordinario comportamento di spesa; (iii) accertare l'effettiva riconducibilità della disposizione alla sua volontà. Parte ricorrente contesta inoltre che/di: (iv) essere stata indotta con artifizi e raggiri a credere che le operazioni servissero a bloccare i bonifici fraudolenti; pertanto, il suo comportamento non configura colpa grave; (v) i Collegi Abf hanno più volte affermato che anche in presenza di SCA la frode non può gravare sul cliente se questi è stato vittima di un inganno sofisticato, basato sul c.d. "spoofing"; (vi) nel caso di specie, anche adottando l'ordinaria diligenza, non avrebbe potuto rilevare la frode in atto, visto l'utilizzo dei canali ufficiali della banca da parte dei malviventi; (vii) anche i messaggi ricevuti apparivano per provenienza, forma e contenuto attendibili e legittimi; (viii) la normativa pone in capo al prestatore di servizi di pagamento l'onere di provare che l'operazione disconosciuta dall'utente sia stata autenticata, correttamente registrata e contabilizzata: (ix) mancando la prova della conformità alla SCA, i pagamenti devono essere rimborsati dalla banca; (x) la banca aveva confermato, con SMS, di aver provveduto al rimborso: ciononostante, l'accredito non veniva realizzato. In conclusione, parte ricorrente sottolinea che i bonifici disconosciuti pur risultando da lei apparentemente confermati sono stati in realtà predisposti dai malfattori.

L'intermediario chiede il rigetto del ricorso per le seguenti ragioni: (a) parte ricorrente ha di fatto riconosciuto di aver autorizzato la disposizione di bonifico contestata, seppur nella convinzione di ottenerne lo storno; (b) senza la inconsapevole e colpevole collaborazione della cliente, non avrebbe potuto essere compiuta alcuna frode; (c) la fattispecie, dunque, non può essere ricondotta nell'alveo della normativa delle operazioni di pagamento non autorizzate; (d) il bonifico disconosciuto è stato autenticato, senza anomalie, con doppio fattore di autenticazione, dal dispositivo utilizzato usualmente da parte ricorrente con la sua collaborazione attiva ed inserimento di tutti i codici richiesti; (e) ciò nonostante la banca ha rilevato come sospetta la disposizione effettuata, sospendendone l'esecuzione in attesa della conferma poi inviata da parte ricorrente; (f) in presenza di tale conferma, la banca non poteva rilevare alcuna anomalia; (g) la banca ha tempestivamente eseguito la richiesta di *recall*, pur senza esito; (h) il fatto che il

truffatore abbia utilizzato tecniche di *social engineering* non elide le responsabilità di parte ricorrente che ha consentito la consumazione della frode, violando il dovere di tenere un comportamento idoneo a garantire la sicurezza dei dispositivi personalizzati; (i) con riferimento alle chiamate apparentemente riconducibili alla banca, è risaputa l'esistenza di applicazione che permettono di far visualizzare un *caller id* diverso da quello effettivo; (j) gli sms di cui la cliente produce evidenza presentano in ogni caso indici di inattendibilità che avrebbero dovuto indurre la ricorrente a non porvi alcun affidamento; (k) la colpa grave della cliente si ricava inoltre dall'aver consentito al truffatore di accedere da remoto al proprio PC e dal non aver preso contatto immediatamente con la banca, avendo consentito, addirittura il giorno successivo, il perpetrarsi della truffa in proprio danno; (l) sono state poste in essere campagne di sensibilizzazione della clientela volte a fornire strumenti per poter riconoscere la frode.

Parte ricorrente ha replicato per evidenziare quanto segue: (i) l'impostazione dell'intermediario, secondo il quale la mera correttezza dell'autenticazione e la collaborazione di parte ricorrente sarebbero sufficienti a qualificare l'operazione come autorizzata, contrasta con il dato normativo e con la giurisprudenza più recente; (ii) parte ricorrente non ha mai inteso disporre un pagamento a favore di terzi, ma è stata indotta tramite *spoofing* e manipolazione psicologica a credere che le operazioni fossero necessarie per annullare i bonifici fraudolenti; (iii) neppure ha mai comunicato a terzi codici di accesso, OTP o credenziali dispositive: il truffatore era già in possesso dei dati identificativi, cosa che ha reso il raggiro particolarmente credibile; (iv) l'autenticazione è stata eseguita personalmente dalla ricorrente, prima dell'attivazione della condivisione dello schermo, senza che vi fosse alcuna richiesta di codici da parte dell'interlocutore; (v) la chiamata appariva provenire dal numero ufficiale dell'intermediario ed è proseguita su più canali (email ed sms); (vi) contrariamente a quanto afferma l'intermediario in merito all'assenza di anomalie, l'operazione è del tutto incompatibile con il profilo storico della cliente, ha una causale incoerente ed è stata realizzata a seguito di una sequenza ravvicinata di tentativi ed è stato usato un software di controllo remoto; (vii) l'intermediario si contraddice nell'affermare, per un verso, l'assenza di anomalie e, per altro verso, nel riconoscere di aver individuato profili di rischio non solo nell'ultima operazione ma anche in quelle precedenti effettuate in data 01/10/2025; (viii) l'operazione è stata disposta operativamente da pc, utilizzando in modalità di condivisione dello schermo: il dispositivo non era mai stato impiegato in precedenza per la disposizione di bonifici; (ix) la sospensione preventiva dell'operazione dimostra che l'anomalia fosse percepibile e che il rischio di frode fosse concreto; (x) non può ritenersi indice di colpa grave l'aver concesso la condivisione dello schermo, essendo questa stata richiesta da un soggetto che si qualificava come operatore della banca ed essendo la cliente in uno stato di agitazione emotiva; (xi) parte ricorrente ha ricevuto esclusivamente comunicazioni automatiche standard, prive di qualsiasi riferimento a sospette frodi: tali comunicazioni hanno rafforzato la tesi del sedicente operatore antifrode, inducendola a ritenere che le operazioni fossero effettivamente in fase di blocco da parte dell'intermediario; (xii) le operazioni sospette, nel loro complesso, ammontavano ad una cifra superiore alla giacenza del conto, circostanza che avrebbe chiesto un intervento immediato e proattivo della banca che non ha allertato la cliente.

L'intermediario ha a sua volta replicato per richiamare le difese già svolte e sottolineare che: (a) parte ricorrente nulla aggiunge rispetto a quanto già precedentemente riferito; (b) l'intermediario ha documentalmente provato la corretta autorizzazione ed autenticazione della disposizione oggetto di contestazione; (c) la chiamata riconducibile all'intermediario è una pratica diffusa e nota; (d) parte ricorrente non riferisce di aver utilizzato la funzione di verifica della chiamata in app che, se usata, avrebbe fornito un riscontro alla stessa in merito al fatto che non fosse realmente al

telefono con la banca; (e) parte ricorrente ha concesso al truffatore di entrare nel pc e di visualizzare il proprio conto e i propri dati, in aperta violazione ai doveri di custodia; (f) parte ricorrente ha dato seguito alle richieste del truffatore, compresa quella di inviare i propri documenti d'identità, nonostante l'intervento dell'intermediario che, a differenza di quanto sostiene controparte, ha posto in essere le azioni di sospensione di bonifico e di richiesta di documentazione integrativa; (g) parte ricorrente ha dato credito a sms contenenti indici di inattendibilità e di provenienza non certa; (h) secondo le decisioni dell'ABF non sussiste un obbligo di monitoraggio preventivo delle operazioni in capo all'intermediario.

DIRITTO

Materia del contendere è un bonifico di € 7.499,00 effettuato il 2/10/2024 alle ore 09.43. Dalla denuncia presentata in data 3/10/2024 si apprende lo svolgimento della truffa che ha impegnato due diversi giorni, anche se oggetto di disconoscimento è solo l'operazione effettuata il secondo giorno. Si riferisce, infatti, nella denuncia che parte ricorrente ha ricevuto in data 01/10/2024 (e quindi il giorno precedente quello in cui è stata effettuata l'operazione oggetto del contendere) una prima telefonata dal numero 02****89 da parte di un soggetto che si presentava come operatore dell'intermediario convenuto e che la allertava in relazione ad un accesso anomalo al suo conto con conseguente effettuazione di bonifici. Quindi, tale sedicente operatore la induceva ad accedere all'applicazione della banca per aiutarla *“ad annullare i pagamenti” “entrando come assistente esterno nel [suo] computer”*. Effettuato l'accesso, parte ricorrente notava *“una movimentazione del ... denaro dal ... conto deposito al ... conto corrente ... per la somma di circa 6.000 euro”*. Si apprende, poi, che parte ricorrente *“seguiva”* le indicazioni del truffatore che le *“chiedeva di fornirgli un codice per entrare all'interno del [suo] pc”* e che, pertanto, effettuato l'accesso, *“mostrava da remoto diverse schermate con iban e nominativi di bonifici”* a favore di soggetti sconosciuti, dandole ad intendere *“di aver[li] annullat[i]”* inviando SMS di conferma. Si riferisce, poi, che il 02/10/2024 parte ricorrente riceveva dal medesimo soggetto una seconda telefonata con cui le veniva segnalato *“di non riuscire ad annullare l'ultimo bonifico”* e quindi la invitava a *“confermare la disdetta di questo pagamento”*. E a tal fine parte ricorrente alle 10:02 inviava all'intermediario, sempre seguendo le istruzioni del truffatore, *“una mail con un documento di riconoscimento valido e una foto”*. In sintesi, questa la sequenza dei fatti:

- in data 01/10/2025 parte ricorrente ha consentito l'accesso esterno nel pc al truffatore, credendo di procedere ad annullare certi pagamenti, non oggetto del presente procedimento;
- in data 02/10/2025, parte ricorrente riceveva una nuova chiamata dal truffatore che le chiedeva di *“confermare la disdetta”* in quanto non riusciva *“ad annullare l'ultimo bonifico”*;
- in pari data, parte ricorrente inviava una mail con il proprio documento di riconoscimento per ottenere lo sblocco del bonifico oggi contestato, che i sistemi antifrode dell'intermediario avevano bloccato.

Alla luce di questa narrazione non può affermarsi *tout court* che l'operazione oggetto del contendere sia stata effettuata interamente e personalmente da parte ricorrente, anche se questa la ha successivamente convalidata, sia pure tratta in inganno dal truffatore con ben note tecniche di *social engineering*.

Venendo, quindi, alla prova dell'autenticazione forte del bonifico disconosciuto, appare pacifico (anche alla luce della narrazione di cui sopra) che detta operazione è stata eseguita dal *device* di parte ricorrente che, nella documentazione prodotta dall'intermediario, risulta identificato con il relativo codice a far data dal 27/01/2023. Dai *log* prodotti detto codice risulta sia prima che dopo

l'esecuzione dell'operazione contestata. Quanto alla fase di accesso all'area riservata dell'*home banking* in data 02/10/2024, alle ore 9:35:25, dai citati *log* (e dalle relative legende) si evincono i seguenti fattori autenticazione: fattore di conoscenza (PIN), inserito senza errori, e il secondo fattore (notifica *push* autorizzata con *face id*). Quanto all'esecuzione dell'operazione, dalla documentazione prodotta risulta alle 09:43 l'evidenza del fattore di possesso (OTP inserito con successo, analogo a quello riscontrato in corrispondenza del login). Considerato lo stretto lasso di tempo intercorso tra accesso ed esecuzione dell'operazione, è quindi possibile ritenere che l'operazione sia stata autorizzata con il riutilizzo di uno dei due fattori di autenticazione utilizzati per l'accesso 8 minuti prima e, come detto, il fattore di possesso rappresentato dall'OTP. A questo punto, tuttavia, il bonifico risulta bloccato dai sistemi antifrode dell'intermediario (cfr. nei *log* l'indicazione delle ore 09:44: il bonifico di € 7.499,00 è in stato '*blocked*') e di ciò viene data informativa a parte ricorrente, come risulta da un mail *alert* delle ore 09:43 in atti (sui cui si tornerà dopo). Ma di ciò si ha comunque conferma anche da quanto dichiarato sia in denuncia che nel ricorso da parte ricorrente e, soprattutto, dall'evidenza prodotta e cioè la mail inviata da parte ricorrente alle ore 10:02 del 2/10/2024, con cui è stato specificatamente confermato il bonifico sospeso con invio della foto della stessa parte ricorrente che tiene in mano la propria carta di identità. In atti, vi è, poi, la conferma dello sblocco che si colloca alle ore 14:49:30 del 02/10/2024. Alla luce di quanto precede e dei fatti che hanno caratterizzato la truffa ritiene il Collegio che l'onere della prova fissato dalla normativa rilevante nella specie sia stato adempiuto, sussistendo gli estremi per imputare a parte ricorrente una colpa grave: rilevano in tal senso non solo il fatto che parte ricorrente abbia acconsentito, sia pure nella convinzione di annullare dei bonifici da lei autorizzati (e non oggetto del contendere), che il truffatore accedesse da remoto al suo *device* fornendo il relativo codice - richiesta di accesso che all'evidenza di pone al di fuori della normale operatività del servizio clienti e/o antifrode degli intermediari al pari della richiesta di codici, PIN e *password* alla cui segretezza ogni cliente è tenuto per contratto e per legge -, ma anche e soprattutto la mail di conferma del bonifico che l'intermediario aveva bloccato. In particolare, tale mail vale come autorizzazione del bonifico dopo la ricezione di un messaggio che ben avrebbe dovuto allertare parte ricorrente sull'inverosimiglianza dell'intera vicenda. Risulta, in particolare, agli atti che lo stesso era stato originariamente richiesto come 'istantaneo' e come tale è stato per l'appunto bloccato "*per la [sua] sicurezza*" con *push* a parte ricorrente delle ore 09:40:26 (*push* che conteneva importo e beneficiario) e con mail di pochi secondi dopo in cui si specificava "*KO per motivi di sicurezza*", "*Bonifico a Rischio Antifrode*", "*Bonifico sospetto rilevato*". Ritiene, inoltre, il Collegio di dover evidenziare come il fatto che la chiamata ricevuta risultasse provenire da un numero riconducibile all'intermediario non sia di per sé significativa, perché è ormai noto il meccanismo dello *spoofing* e della facilità con cui si possa oggi far figurare un numero chiamante ovvero un mittente di un SMS o di un messaggio W***P diverso da quello effettivo, anche a prescindere dalla mera somiglianza del logo che appare sullo schermo della chiamata (diverso dalla denominazione che compare negli SMS) e di tutti i fatti che hanno connotato la truffa e che, quanto meno il secondo giorno, avrebbero dovuto ingenerare un qualche sospetto verso l'interlocutore. Inoltre, gli SMS prodotti, pur intestati a '***', contengono errori di punteggiatura, alternano il 'tu' al 'lei' e non sembrano contenere alcun messaggio genuino. A quanto precede va soggiunto che, dopo i bonifici effettuati il 1° ottobre 2024 (che emergono dai citati SMS), l'intermediario ha bloccato, come già detto, il bonifico qui contestato, ma parte ricorrente lo ha confermato autorizzandolo con la mail di cui si è pure riferito. Dunque, nella specie, il sistema di monitoraggio è stato attivato.

Infine, risulta agli atti che l'intermediario ha tentato il recall in data 03/10/2024, giorno in cui parte ricorrente si è avveduta della truffa, ma lo stesso ha dato esito negativo.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE