Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI PALERMO

composto dai signori:

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

Relatore VINCENZO MELI

Seduta del 23/01/2026

FATTO

Con ricorso pervenuto il 15.09.2025 il ricorrente riferisce di essere contitolare, insieme alla moglie, di un conto corrente presso l'intermediario resistente. In data 10.07.2025 riceveva un SMS da parte dell'intermediario, con il quale veniva informato dell'avvenuta modifica del PIN di accesso alla propria area riservata. Non avendo modificato il PIN, seguiva le istruzioni contenute nell'SMS, limitandosi ad accedere alla propria applicazione di *home banking*. Durante tali passaggi non cliccava su nessun link, né comunicava il proprio PIN, in quanto non era stato contattato telefonicamente da nessuno. In data 29.07.2025 e 30.07.2025 venivano ordinati 6 bonifici non autorizzati dal suo conto. Successivamente all'effettuazione dei bonifici, sempre in data 29.07.2025, il ricorrente veniva contattato telefonicamente dai truffatori. Il sedicente operatore antifrode dell'intermediario acquistava la fiducia del ricorrente, motivando la sua chiamata tramite la richiesta di delucidazioni sui tre bonifici sospetti eseguiti. Per aumentare la sua credibilità, il sedicente operatore elencava al ricorrente dettagli precisi ed informazioni presenti esclusivamente sul profilo del ricorrente ed accessibili al personale autorizzato dell'intermediario. Dopo alcune verifiche, egli informava il ricorrente che il suo conto era stato bloccato e che quindi l'accesso all'App sarebbe stato precluso. Durante la telefonata, il ricorrente riceveva degli SMS, apparentemente provenienti dall'intermediario, con i quali gli venivano spiegate la presa in carico delle segnalazioni volte al disconoscimento delle operazioni e, inoltre, la necessità di non accedere all' *home banking,* al fine di permettere al sistema informatico il ripristino dei dati durante il passaggio a nuove coordinate bancarie onde sarebbero stati trasferiti il saldo residuo e l'ammontare dei bonifici non autorizzati. Gli stessi messaggi precisavano di seguire attentamente le direttive dell'apparente consulente. Sempre nel corso della telefonata, il truffatore lo invitava ad accedere alla sua App al fine di verificare l'autenticità delle dichiarazioni e lo informava, altresì, che, dopo la verifica, sarebbe stato

bloccato il conto corrente. Solo successivamente, l'accesso all'*home banking* veniva precluso a seguito della comparsa della maschera "ERRORE IMPREVISTO", circostanza questa che induceva il ricorrente a credere che il conto corrente fosse effettivamente bloccato. Al termine della telefonata, il truffatore lo tranquillizzava e provvedeva a fissare un appuntamento alle ore 14:00 del 30.07.2025. La mattina successiva, in data 30.07.2025, mentre si trovava all'interno di un terminale aeroportuale in attesa del volo per rientrare a casa, nel tentativo di anticipare l'appuntamento, provava a contattare il numero del servizio clienti dell'intermediario. Alle ore 08:14 la chiamata si interrompeva dopi 16 secondi a causa della debolezza del segnale all'interno del terminal. Alle 08:15 la chiamata durava circa un minuto, con risposta automatica che informava della disponibilità operativa a partire dalle ore 09:00. Nella medesima giornata, riceveva una telefona dal truffatore che confermava il corretto andamento delle procedure. Alle ore 14:57 e 16:29, riceveva due telefonate dove veniva rassicurato sulla migrazione al nuovo conto corrente, sul nuovo n. IBAN. Durante tutto questo periodo, il ricorrente non forniva alcun codice OTP, PIN, o alcuna password o username e, inoltre, non veniva mai invitato a cliccare su di un link civetta, né tantomeno lo ha fatto. Digitando il nuovo codice IBAN si accorgeva di un presunto errore e decideva di contattare il servizio clienti dell'intermediario. Durante le conversazioni intercorse con l'operatore, apprendeva che il nominativo dell'altro presunto operatore/truffatore non è presente negli archivi dell'intermediario. Nella stessa sede, l'operatore non svolgeva alcuna verifica, né tantomeno un recupero del conto corrente, limitandosi ad indicare un numero al quale chiamare per il recupero del PIN al fine di accedere all'app di *home banking*. Invano contattava tale utenza indicata dal vero operatore dell'intermediario. Alle 18:15, nell'istante in cui effettuava accesso alla sua applicazione dal proprio smartphone, veniva richiamato dal truffatore con le stesse modalità sopraindicate. Nel corso della telefonata il truffatore dichiarava che se fosse stato realmente un truffatore non avrebbe chiamato a truffa compiuta, precisando al ricorrente di non avere mai richiesto alcun suo dato personale e bancario e di non poter conoscere il codice PIN. In data 31.07.2025, il ricorrente provvedeva a contattare il servizio clienti dell'intermediario e, nel corso delle telefonate, apprendeva di essere di essere incorso in una truffa e che il giorno precedente i truffatori avevano effettuato altre tre operazioni di pagamento, per un totale di euro 34.748,00. L'operatore avviava su richiesta la procedura di disconoscimento delle operazioni non autorizzate ed esortava al blocco delle carte. Verificava che all'app di *home banking* era associato un dispositivo diverso da quello del ricorrente. Verosimilmente, una volta ottenuto l'accesso, i truffatori associavano un ulteriore dispositivo cellulare, utilizzato quale strumento per l'invio e la ricezione delle autorizzazioni necessarie alle operazioni disposte. Tale circostanza parrebbe riconducibile a una grave vulnerabilità dei sistemi di cybersicurezza dell'intermediario. Afferma di non avere mai ricevuto alcun *alert* in merito ai bonifici disconosciuti, mentre riceveva gli *alert* relativi alle disposizioni di pagamento disposte dai truffatori tramite la carta di debito.

In data 05.08.2025, l'ufficio reclami dell'intermediario formulava una proposta transattiva volta al superamento della lite. A questa seguiva l'accredito della somma pari a euro 15.744,00 nel conto corrente del ricorrente. Posto che il superamento della controversia pone uno svantaggio a carico dell'oblato, quale rinuncia dell'intero ammontare, non può applicarsi in radice la disciplina ex art 1333 c.c. e, pertanto, l'importo accreditato sul conto corrente deve eventualmente considerarsi quale acconto del maggior danno subito.

In data 09.08.2025 comunicava tramite pec di non accettare la proposta transattiva.

Chiede, pertanto, il, rimborso dell'intera somma prelevatagli, ammontante ad euro 81.892,00, dai quali detrarre gli euro 15.744,00 già rimborsati dalla banca.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Afferma che il cliente contattava l'intermediario solo il giorno successivo rispetto ai fatti di cui si discute e l'operatore riferiva l'esecuzione

dei sei bonifici oggetto dell'odierno ricorso. Successivamente, il ricorrente inoltrava Modulo di Contestazione, al quale l'intermediario forniva riscontro comunicando che, in via del tutto eccezionale, avrebbe provveduto al rimborso parziale di euro 15.744,00, ma che non vi erano i presupposti per procedere con il rimborso totale di tutte le operazioni contestate. Dette operazioni sono state in vigenza del D. Lgs. 27 gennaio 2010, n. 11 e, in particolare, assume rilievo la disciplina di cui all'art. 10 del citato decreto, che per il caso di disconoscimento di operazioni di pagamento da parte dell'utente pone in capo all'intermediario l'onere, da una parte, di "*provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*" (comma 1); dall'altra, di *"… fornire la prova della frode, del dolo o della colpa grave dell'utente*" (comma 2). Quanto al primo profilo dell'autenticazione forte, la modifica introdotta dalla PSD2 prevede che l'autenticazione delle operazioni di pagamento elettronico debba essere basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza, possesso e inerenza. Quanto al secondo profilo, relativo alla colpa grave dell'utente, la normativa pone in capo all'utente del servizio di pagamento l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e, a tal fine di adottare "*tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate*". La Banca adotta un sistema di autenticazione forte di accesso all'Area Riservata e di autorizzazione delle disposizioni di pagamento nel pieno rispetto delle previsioni normative sopra menzionate. Essa non può essere ritenuta responsabile dell'utilizzo dei Codici da parte di soggetti non legittimati fino al momento in cui il Cliente le comunica il loro smarrimento o furto e chiede il blocco dell'operatività del Servizio, a meno che l'eventuale conseguenza dannosa per il Cliente derivi da un evento direttamente imputabile alla Banca stessa.
Dalla documentazione in atti emerge che si è registrata l'installazione della nuova app su un *device* diverso da quello in uso al Cliente (Samsung SM-A057G). Nello specifico, alle ore 15.37 del 10 luglio 2025 è stata attivata la nuova app dell'intermediario su di uno smartphone "S***G"; è stata consentita l'installazione dell'app su altro *device*, da cui sono state poi impartite le disposizioni oggetto del ricorso o direttamente da parte del Cliente o in ragione di una cooperazione fornita dalla stessa al presunto frodatore; la modifica del dispositivo è avvenuta senza anomalie e nel rispetto della "Strong Customer Authentication"; Non è noto se il dispositivo smartphone S***G sia un ulteriore dispositivo in uso al ricorrente o sia del frodatore, ma dai log allegati emerge che le disposizioni in contestazione sono state effettuate ed autorizzate da quest'ultimo dispositivo, o direttamente dal ricorrente o dal frodatore medesimo in seguito alla inopinabile cooperazione colpevole tra il Cliente e lo stesso, di cui, tuttavia, non viene fatta alcuna menzione dal Cliente né in sede di denuncia, né in sede di presentazione dell'odierno ricorso; il Cliente è reticente nel fornire una ricostruzione dettagliata dei fatti occorsi nell'arco temporale compreso tra il 10 luglio 2025 (data in cui è effettivamente avvenuta l'installazione della nuova app su un altro *device*) ed il 29 luglio 2025 (data in cui sono stati eseguiti i primi 3 bonifici fraudolenti), limitandosi ad informare di essere stato contattato da un finto operatore da un numero riconducibile alla Banca e di aver ricevuto una serie di SMS aventi ad oggetto: disposizioni di bonifico, variazione IBAN e disattivazione app.
E' alquanto palese che il ricorrente abbia consentito l'installazione della nuova APP sul device del presunto frodatore, violando il dovere di tenere un comportamento idoneo a garantire la sicurezza del dispositivo ed il suo utilizzo. Inoltre, risulta che le disposizioni dei bonifici (effettuate in data 29 luglio ed in data 30 luglio 2025) siano state correttamente autorizzate tramite autenticazione forte. La Banca ha, adeguatamente e sufficientemente provato la corretta contabilizzazione, registrazione e autenticazione dei bonifici. Trattandosi di bonifici istantanei, non ha potuto annullarli, proprio in considerazione della lavorazione istantanea di questo genere di operazioni, che vanno immediatamente a buon fine. La

truffa ha potuto giungere a consumazione solo - e proprio - in ragione della cooperazione attiva del Cliente, il quale – come emerge dall'analisi dei LOG – ha autorizzato lui stesso la disposizione di bonifico oggi in contestazione dalla nuova app o ha consentito al/i frodatore/i stesso di installare l'app sul proprio *device* e quindi di autorizzare successivamente l'operazione. Il cliente ha ricevuto la notifica *alert* dell'installazione dell'app (laddove non fosse stata fatta da lui), a seguito della quale avrebbe potuto e dovuto prendere immediati contatti con la propria Banca, impedendo così il procrastinarsi della truffa in proprio danno. Non attribuire il minimo peso a simili *alert* costituisce una condotta gravemente negligente.
In merito alla chiamata da numero apparentemente riconducibile alla banca e alla sua eventuale idoneità a trarre in inganno i clienti, precisa l'intermediario che si tratta oramai dell'esistenza e dell'utilizzo, assolutamente risaputo e pubblicizzato anche dai mass media, di applicazioni, scaricabili da chiunque, che permettono di far visualizzare al ricevente un tag impostato dal chiamante, con la conseguenza che le chiamate in entrata appaiono come genuine.
Con replica e controreplica, le parti hanno sostanzialmente ribadito le proprie ragioni.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte al ricorrente, attraverso una serie di bonifici da lui non autorizzati.
Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare:
- l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).
In particolare, 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 (o dolo) dell'utente.
Parte ricorrente lamenta l'esecuzione fraudolenta di 6 bonifici istantanei, 3 eseguiti in data 29.07.2025 e 3 eseguiti in data 30.07.2025, per un importo totale di € 81.982,00, tutti disposti in favore del medesimo beneficiario.
- 29.07.2025, 16:39, € 3.250,00
- 29.07.2025, 16:42, € 18.985,00
- 29.07.2025, 16:45, € 24.999,00
- 30.07.2025, 16:16, € 3.250,00
- 30.07.2025, 16:20, € 18.499,00
- 30.07.2025, 16:23, € 12.999,00.
Il ricorrente conferma che la banca gli ha rimborsato € 15.744,00, che dichiara di accettare come acconto rispetto al rimborso del totale prelevatogli.
L'intermediario afferma che, preliminarmente alla disposizione delle operazioni contestate, **è** stata registrata in data 10.07.2025 l'installazione dell'app su di un nuovo dispositivo. Rappresenta che, a tal fine, sia necessario accedere all'app dal nuovo dispositivo, inserendo codice cliente, data di nascita e codice PIN segreto. Una volta effettuato questo passaggio, il sistema permette di scegliere lo Smart

Code da utilizzare, scegliendo se utilizzare o meno i dati biometrici. Per completare l'attivazione dell'app sul nuovo dispositivo, è necessaria poi l'autenticazione tramite *Push* OTP inviata al numero di cellulare del cliente e da inserire sul nuovo dispositivo.
Sulla base delle evidenze prodotte e sopra riportate, risulta, in effetti, che in data 10.07.2025 vi è stata l'installazione dell'app dell'intermediario su un nuovo dispositivo. In particolare, tale installazione appare essere avvenuta in conformità al regime di autenticazione a due fattori.
Dalla documentazione sopra riportata risulterebbe infatti che l'accesso in app dal nuovo dispositivo sia avvenuta tramite l'inserimento del codice PIN (elemento di conoscenza) e codice *push* OTP inviato all'utenza ***6939 (elemento di possesso), che corrisponde all'utenza del ricorrente.
Con riferimento alle 3 operazioni di bonifico istantaneo disposte in data 29.07.2025, le stesse sono state autorizzate con le medesime modalità e l'intermediario produce la documentazione tecnica per ognuna di esse. Evidenzia, in linea generale, che il sistema di autenticazione opera attraverso i seguenti passaggi: il ricorrente effettua dapprima l'accesso in app inserendo il codice smartcode selezionato e il codice OTP ricevuto tramite *push* sul *device*. In seguito all'accesso inserisce i dati dell'operazione da disporre dalla schermata bonifici, per poi autenticare l'operazione tramite l'inserimento dello smartcode dal *device* associato.
Nel caso di specie, sulla base delle evidenze prodotte, risulta che l'operazione è avvenuta in seguito all'accesso in App tramite autenticazione a due fattori e, in particolare, l'inserimento dello smartcode (elemento di conoscenza) e l'autorizzazione della push ricevuta sul device associato (elemento di possesso).
Una volta poi inseriti i dati dell'operazione (es. beneficiario, importo), la stessa è stata autorizzata tramite l'inserimento dello smartcode dal *device* associato.
Si ritiene, pertanto, che le disposizioni delle operazioni di bonifico siano avvenute nel rispetto del regime di autenticazione forte a due fattori c.d. SCA. Ciò vale sia per le operazioni disposte il 29.07.2025, sia per quelle disposte il 30.07.2025.
Si può, dunque, procedere a valutare gli eventuali profili di colpa grave nella condotta del ricorrente.
Nella denuncia il ricorrente afferma che:
- l'utenza dal quale proveniva la telefonata sembra apparentemente ricollegabile all'intermediario;
- di avere ricevuto degli SMS apparentemente provenienti dall'intermediario;
- di avere tentato di contattare il servizio clienti, senza però riuscire ad interloquire con nessun operatore stante la circostanza, da lui ammessa, di aver contattato il servizio clienti dopo l'orario di servizio;
- di non avere comunicato dati e credenziali del suo conto a terzi;

Il ricorrente non si esprime sugli eventi del 10.07.2025, precisati invece in ricorso.
E' evidente che si è di fronte ad un caso di *Caller ID spoofing* e *SMS spoofing*. Si deve, dunque valutare il grado di attendibilità delle comunicazioni che il ricorrente ha ricevuto, venendone ingannato, nonché valutare la condotta complessiva del ricorrente.
Secondo l'orientamento dei Collegi, nelle fattispecie di *spoofing* non è, infatti, generalmente ravvisabile la colpa grave del cliente, a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio, come errori grammaticali e/o lessicali, presenza di link non riferibile all'intermediario. Dagli screenshot depositati, emerge che, in effetti, SMS e chiamate provengono da numeri che sembrano riconducibili a quelli dell'intermediario o dalla chat di questo, ma il testo di alcuni SMS riporta, tuttavia, degli errori, come il passaggio dalla seconda alla terza persona singolare, che avrebbero dovuto mettere in guardia il ricorrente. Egli, peraltro, mostra di avere tenuto una condotta incauta, accedendo al proprio *home banking* a seguito di istruzioni impartitegli attraverso dette comunicazioni, con ciò verosimilmente consentendo, sia pure inconsapevolmente, ai truffatori di impadronirsene e di

impadronirsi dei suoi dati personali. Ciò ha consentito loro di accreditare per l'accesso al conto un nuovo *device*, dal quale hanno potuto operare. Egli stesso, infine, ammette di avere contattato il servizio clienti senza la solerzia resa necessaria dalle anomalie che aveva già riscontrato.
Dalla documentazione prodotta dalle parti non risulta, tuttavia, l'attivazione di sistemi di alert.
Orbene, secondo le posizioni dei Collegi, la mancata attivazione del servizio di sms alert (o altro assimilabile, come notifica tramite App dell'intermediario oppure e-mail, con una valutazione di equivalenza da condurre caso per caso) costituisce un profilo di responsabilità dell'intermediario, salvo l'esplicito rifiuto dell'utente ad avvalersene. Poiché l'alert, inviato dopo il compimento di una operazione, ha l'obiettivo di mettere in guardia il titolare dello strumento di pagamento, dandogli modo di impedire ulteriori operazioni, è posizione condivisa dei Collegi che, in caso di mancato invio dell'sms alert, non sussiste responsabilità dell'intermediario qualora le operazioni disconosciute siano avvenute nell'arco temporale di 5 minuti. Al di sotto di tale intervallo, infatti, neppure la presenza dell'alert consentirebbe al titolare dello strumento di pagamento di agire per impedire ulteriori operazioni (si vedano Collegio di Palermo, dec. n. 13261/2020; 1624/2023; 2344/2024).
Nel caso di specie, sono dunque da restituire integralmente tutte le operazioni dalla terza in poi, per un totale di € 59.747,00.
Dalle evidenze prodotte emergono anche indici di frode, in base al punto 2 della lett. a) dell'art. 8 del DM n. 112/2007 e agli orientamenti dei Collegi. Si è di fronte, infatti, ad operazioni di bonifico verso lo stesso IBAN del beneficiario (alcuni di importo rilevante). I Collegi hanno precisato che, sebbene il D.M. faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche *online*) in ragione dell'unicità della *ratio* sottesa a tale a tale normativa. Ciò perché, secondo l'orientamento dei Collegi, i principi del D.M. n. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario. Il Collegio Abf può quindi valorizzare anche indici di frode ulteriori a quelli del D.M. 112/2007 in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.
Per quanto concerne infine la quantificazione del rimborso da riconoscere all'utente, i Collegi hanno convenuto che la valutazione della responsabilità del PSP per l'anomalia delle operazioni debba essere formulata in un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto: la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti. Questo Collegio, in conformità all'orientamento di cui sopra, ha stabilito che vanno rimborsate tutte le operazioni, nella misura del 20%, salvo una diversa distribuzione in concreto del concorso di colpa tra le parti (si vedano dec. n. 4200/2024 e 4148/2024).
Considerato che le operazioni dalla terza in poi devono essere integralmente rimborsate per assenza di un sistema di alert, il calcolo del 20% va effettuato solo sulle prime due operazioni per un totale di euro 4.447,00 (20% di € 22.235,00). Il totale da rimborsare è dunque pari ad € 64.194,00 (4.447,00 + 59.747,00). Considerato, tuttavia, che il ricorrente ha già ottenuto il rimborso di € 15.744,00, che l'intermediario ha imputato alle prime tre operazioni, residua da rimborsare la somma di € 48.450,00.

PER QUESTI MOTIVI

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto al rimborso dell'importo complessivo di € 48.450,00.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE