Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 04/12/2025

FATTO

Il ricorrente in data 10 aprile 2024 riceveva una telefonata sul proprio numero di cellulare da un numero apparentemente proveniente dall'intermediario, con cui veniva reso edotto della necessità di bloccare un pagamento fraudolento.
Cliccava su un link ricevuto tramite SMS e seguiva le indicazioni del sedicente operatore; nel corso della telefonata, venivano eseguiti due bonifici per un importo complessivo di euro 5.530,00 e un pagamento con la carta di debito, pari a euro 2.980,00.
Successivamente, disconosceva tali operazioni e presentava reclamo alla banca, la quale forniva riscontro negativo poiché le operazioni contestate risultavano correttamente eseguite con autenticazione forte a due fattori.
Agisce dinanzi all'Arbitro per ottenere il rimborso della somma complessiva di euro 8.510,00.
L'intermediario respinge la richiesta di rimborso ritenendo infondato il disconoscimento delle operazioni correttamente autorizzate mediante il sistema di autenticazione a due fattori e nel rispetto delle disposizioni relative alla Strong Customer Authentication (SCA).
A tal proposito, la banca sottolinea l'importanza di seguire una serie di passaggi autorizzativi necessari a garantire la sicurezza dell'operazione. In primo luogo, per accedere all'Area Riservata, il cliente deve utilizzare le credenziali statiche, scelte in fase di registrazione. Inoltre, per assicurare l'autenticazione forte, è previsto l'inserimento di un codice OTP, inviato via SMS al numero di telefono registrato dal cliente durante l'apertura del rapporto. Qualora l'autenticazione forte non venga effettuata

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

correttamente, l'accesso alle informazioni sarà limitato al solo saldo del conto e alle operazioni di pagamento effettuate negli ultimi 90 giorni.
La banca evidenzia, inoltre, che relativamente all'operazione di pagamento tramite carta, sono richiesti alcuni dati specifici della stessa, come il PAN, la data di scadenza e il CVV dinamico, il quale viene generato all'occorrenza, solo dopo l'accesso all'Area Riservata e l'inserimento dell'OTP. L'operazione viene infine confermata inserendo una One Time Password, ricevuta anch'essa tramite SMS.
Per quanto attiene ai bonifici, a seguito di un blocco all'area riservata del Cliente, superato da accesso genuino da abituale dispositivo, è stato invece necessario il riconoscimento Biometrico, unitamente all'inserimento di OTP pervenuto sul cellulare del ricorrente.
L'intermediario deduce che non avrebbe mai in alcun modo potuto impedire l'esecuzione delle operazioni poiché, nonostante il blocco dell'area riservata del Ricorrente, tutti gli accessi e le operazioni sono state disposte sempre dall'abituale dispositivo in uso al Cliente, il quale con la sua condotta colposa ha consentito il finalizzarsi della frode.
Per tali ragioni, l'intermediario chiede all'Arbitro di rigettare il ricorso.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 10 aprile 2024. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.
Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.
2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".
3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del

possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".
Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.
L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".
Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).
4.- La parte ricorrente contesta l'esecuzione di due bonifici per un importo complessivo di euro 5.530,00 effettuati verso il medesimo beneficiario e un pagamento on line con la carta di debito, pari a euro 2.980,00, eseguiti il 10 aprile 2024.
4.1.- Tutti gli accessi precedenti e tutte le operazioni disconosciute dal ricorrente (log area riservata righe 56 a 63 – Allegato 3) sono state registrate tramite Riconoscimento Biometrico" [Medio autentificación (colonna G) = 106] mediante l'abituale dispositivo in uso al cliente (colonna J).
Giova richiamare sul punto la Question ID 5516_2020: accesso al conto e riutilizzo di un fattore di autenticazione ai fini della SCA.
Il quesito si interrogava sulla possibilità per l'utilizzatore, una volta avuto accesso al conto di pagamento on line tramite il solo fattore di conoscenza, in conformità alla possibile esenzione dalla SCA, di riutilizzare la suddetta credenziale statica e combinarlo con un secondo elemento di autenticazione per autorizzare un'operazione di pagamento.
Sul punto, l'EBA ha risposto positivamente, affermando che, come già chiarito dalla Question ID 4141_2018 il Regolamento Delegato consente al cliente di riutilizzare uno dei fattori di autenticazione inseriti per l'accesso al conto di pagamento online per disporre un'operazione di pagamento online nell'ambito della medesima sessione, purché l'associazione di entrambi fattori produca il dynamic linking richiesto dall'art. 5 del Regolamento stesso.
Tale principio trova applicazione anche allorquando l'accesso al conto non sia presidiato da SCA, in quanto riconducibile a una delle ipotesi per le quali è prevista l'esenzione ai sensi dell'art. 10 del Regolamento Delegato.
L'ultimo accesso del Cliente con autenticazione forte è stato eseguito il 02/02/2024 con username e password e OTP [Medio autentificación (colonna G) = 121] ricevuto tramite SMS sul numero di cellulare (3408410161) univocamente associato al suo Conto Corrente (Allegato 6a).
Una volta acceduti all'home banking nelle modalità sopra descritte, i truffatori hanno aumentato il plafond della carta tramite l'OTP ulteriormente trasmesso al cellulare del ricorrente.
Non risulta l'enrollment dell'app su altro dispositivo.
4.2.- L'intermediario afferma che per autorizzare operazioni di pagamento tramite carta di debito è necessario l'inserimento delle credenziali statiche (PAN e data di scadenza), il CVV dinamico e l'inserimento di un OTP per confermare l'operazione di pagamento.
L'intermediario precisa, inoltre, che il CVV della carta è generabile esclusivamente nell'area riservata previa autenticazione con username e password e tramite un ulteriore OTP all'uopo dedicato.

Nel caso in esame, alle 18:09:55 (log area riservata riga 60 - Allegato 3), è stata registrata la generazione di un CVV dinamico della Carta di debito mediante autenticazione forte: accesso con Riconoscimento Biometrico [Medio autentificación (colonna G) = 106] e inserimento di OTP [Tipo firma (colonna H) = 05] ricevuta tramite SMS sul numero di cellulare univocamente associato al Conto (Allegato 6b).
Secondo questa ricostruzione, dunque, il CVV non è un codice statico rinvenibile sulla carta, ma è un codice dinamico generato su richiesta del cliente.
Tenuto conto di quanto precede, per disporre l'operazione disconosciuta risulterebbero essere stati richiesti i seguenti fattori di autenticazione costituiti da: a) Username e Password (fattore di conoscenza) per accedere all'area riservata, necessaria per la generazione in App del codice CVV; b) codice OTP dinamico (fattore di possesso), richiesto non solo in occasione della generazione del CVV ma anche per la conferma dell'operazione.
Infine, le operazioni sarebbero state convalidate con un ulteriore codice dinamico, del pari ricevuto via sms, con un messaggio contenente in chiaro i dettagli dell'operazione.
Il sistema adottato dall'intermediario ai fini dell'autenticazione così ricostruito risulta pertanto SCA compliant considerato nella sua globalità (Collegio di Roma, decisione n. 2840 del 22/03/2023), in quanto:
o il CVV dinamico viene generato con inserimento di un OTP sms dall'interno dell'area personale del cliente. Poiché l'accesso all'area personale richiede l'uso di password + PIN della carta + OTP sms (accesso web) o PIN/Touch ID + APP registrata certificata (accesso via APP), la generazione del CVV dinamico prevede in concreto l'uso di almeno due diversi fattori, uno di conoscenza o inerenza e l'altro di possesso
o la procedura di autenticazione delle operazioni, nel prevedere l'utilizzo del CVV dinamico (generato all'interno dell'area riservata, come specificato al punto i), recupera un fattore dal processo di generazione di tale codice (conoscenza o inerenza, a seconda del tipo di accesso) e vi aggiunge l'elemento di possesso rappresentato da un OTP sms inviato al numero certificato del cliente.
4.3.- Alle 18:27:23 e 18:27:28 (log bonifici righe 1 e 2 - Allegato 5), sono stati registrati due tentativi di bonifico da € 4.900,00, che facevano scattare un blocco all'area riservata del Cliente (log area riservata righe 63 e 64 - Allegato 3).
Il blocco è stato superato da accesso genuino da abituale dispositivo (colonna J) alle 18:28:39 (log area riservata riga 65 - Allegato 3) con Riconoscimento Biometrico [Medio autentificación (colonna G) = 106].
Di conseguenza, alle 18:30:43 (log bonifici riga 3 - Allegato 5), veniva eseguito un bonifico di € 4.900,00 con doppio fattore:
i. accesso con Riconoscimento Biometrico [Medio autentificación (colonna G) = 106] (primo fattore - inerenza);
ii. inserimento di OTP [Tipo firma (colonna H) = 05] (secondo fattore - possesso) tramite SMS sul numero di cellulare (3408410161) univocamente associato al Conto Corrente (Allegato 6b).
Successivamente, alle 18:34:20 (log bonifici riga 4 - Allegato 5), veniva eseguito anche il secondo bonifico di € 540,00 con le medesime modalità.
5.- Quanto alle modalità della truffa, il ricorrente in data 10 aprile 2024 riceveva una telefonata sul proprio numero di cellulare da un numero apparentemente proveniente dall'intermediario, con cui veniva reso edotto della necessità di bloccare un pagamento fraudolento.
Cliccava su un link ricevuto tramite SMS e seguiva le indicazioni del sedicente operatore; nel corso della telefonata, venivano eseguiti due bonifici per un importo complessivo di euro 5.530,00 e un pagamento con la carta di debito, pari a euro 2.980,00.
In effetti, il numero riportato in denuncia sembra riferibile al servizio clienti dell'intermediario e la truffa sembra dunque aver preso le mosse da una fattispecie di vishing caller Id spoofing.

Al riguardo, secondo un consolidato orientamento del Collegio, la chiamata proveniente da un numero apparentemente riconducibile all'intermediario (vishing caller ID) è equiparabile all'sms spoofing e ove ne ricorrano i presupposti è possibile ravvisare un concorso di colpa (Collegio di Roma, decisione n. 8749/2024).
In simili ipotesi, l'orientamento prevalente tra i Collegi territoriali dell'ABF ravvisa un concorso colposo delle parti, imputando all'intermediario la colpa di "non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo" (così Collegio di Milano, decisione n. 17467/2021). Si richiede a tal fine solo l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con il numero verde dell'intermediario (così Collegio di Milano, decisione n. 22105/2021).
La frode, così congegnata, non sembra in effetti differire in maniera significativa dalle ipotesi di "spoofing", ossia dalle ipotesi di smishing in cui il messaggio "esca" reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). E, secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, nelle fattispecie di spoofing è al più ravvisabile "un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (in questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022).
Tuttavia, la parte ricorrente non ha prodotto con il ricorso né la lista chiamate né copia del messaggio truffaldino.
6.- Nella riunione del 23 ottobre 2025 il Collegio ha chiesto al ricorrente copia delle schermate relative al registro chiamate del giorno della truffa, nonché copia degli SMS relativi alla truffa
In ottemperanza alla richiesta di integrazione istruttoria, il ricorrente ha prodotto copia della lista chiamate – registrata il giorno della truffa – in cui compare in effetti il contatto telefonico apparentemente proveniente dalla banca.
Nondimeno, si osserva che la parte ricorrente ha oscurato la parte relativa al nome del mittente e che accanto al numero indicato dalla freccia compare un punto esclamativo rosso, probabilmente quale segnalazione di un alert.
Inoltre, anche per quanto attiene alla schermata del messaggio truffaldino contenente soltanto il link sono riscontrabili alcune anomalie, giacché la chat è priva dell'intestazione del mittente e il messaggio non è né seguito, né preceduto da altri messaggi.
Tanto premesso in ordine al caso concreto, si fa presente che in generale il Collegio richiede l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con il numero verde dell'intermediario (così, Collegio di Roma, decisione n. 8749/24; Collegio di Milano, decisione n. 22105/2021).
7.- Occorre poi rilevare che l'intermediario rappresenta che, dopo l'operazione con carta, il sistema ha bloccato i due tentativi di bonifico – indirizzati al medesimo beneficiario e disposti a distanza di alcuni decimi di secondo l'uno dall'altro.
Detto blocco è stato automaticamente superato dall' accesso genuino da abituale dispositivo della parte ricorrente che ne ha consentito l'esecuzione a distanza di circa (soli) quattro minuti, anche se dalle evidenze prodotte dall'intermediario risulta che l'IP associato alle operazioni risulta sempre il medesimo.
Si fa presente che, secondo l'orientamento dei Collegi, i principi del D.M. 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 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

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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.
I Collegi hanno inoltre 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 normativa.
Per quanto concerne infine la quantificazione del rimborso da riconoscere all'utente, i Collegi hanno convenuto che la valutazione della responsabilità del PSP 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 . Infatti, il D.M. non ha un valore precettivo in materia di disconoscimento delle operazioni non autorizzate e non è ravvisabile una diretta correlazione tra l'integrazione dell'indice di frode e il numero di operazioni da rimborsare.
Occorre dunque valutare se nel caso in esame, avendo disposto un blocco temporaneo dell'Area riservata, l'intermediario avrebbe dovuto predisporre ulteriori misure per superarlo.
In un caso simile, riguardante il medesimo intermediario, il Collegio di Torino ha accertato la responsabilità concorrente dell'intermediario per aver dato esecuzione a un ordine di bonifico dopo averne bloccati previamente tre (Collegio di Torino, decisione n. 10061/24).
Ed invero, ad avviso di questo Collegio occorre osservare che il sistema di monitoraggio utilizzato, seppur allertato dalle modalità operative adottate dei truffatori, non è risultato del tutto adatto allo scopo pur a fronte delle anomalie riscontrate.
Invero, il sistema automatico di controllo della banca nella fase iniziale ha operato correttamente (individuando e bloccando almeno alcune delle operazioni sospette), ma la truffa avrebbe potuto essere sventata (almeno in parte) soltanto qualora il sistema fosse stato programmato diversamente per gestire correttamente e diligentemente la fase della verifica successiva al blocco (richiedendo ad esempio una autorizzazione consapevole da parte del cliente). La semplice richiesta di verifica non automatizzata delle operazioni bloccate avrebbe infatti consentito al cliente di avvedersi della truffa.
8.- Alla luce di quanto sopra esposto, il Collegio accoglie parzialmente il ricorso e ritiene che la quota di responsabilità da addebitare all'intermediario in relazione alla fattispecie concreta vada determinata ex art. 1226 c.c. nella misura di euro 2.000,00 che dovrà essere versata alla parte ricorrente.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 2.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA