Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 20/10/2025

FATTO

La ricorrente, titolare di un conto corrente abilitato all'operatività on line intrattenuto presso la banca convenuta, chiede il rimborso della somma sottratta da terzi (€ 9.221,01) all'esito di una truffa a cagione della quale sono stati eseguiti nove bonifici istantanei, tra il 19 e il 21 gennaio 2025, dalla medesima successivamente disconosciuti. In particolare, dal contenuto del ricorso e dalle dichiarazioni rilasciate in sede di denuncia sporta presso le competenti autorità, in data 22/01/2025, si evince che la ricorrente: in data 18/01/2025 ha ricevuto un messaggio su un'APP di messaggistica recante un link che la indirizzava su un'altra piattaforma di social media dove le veniva proposto un semplice lavoro a distanza – consistente nell' "*apporre dei like*" su prodotti o servizi – dietro compenso; ha fornito, su richiesta dell'offerente il proprio codice IBAN; in data 18/01/2025 ha ricevuto tre bonifici a titolo di compenso per l'attività svolta; in data 20/01/2025 si è recata presso la filiale competente per segnalare l'accaduto ricevendo dal titolare rassicurazioni sul piano della sicurezza nell'esecuzione dei bonifici nella misura in cui la procedura prevede "un riscontro sul […] telefono circa l'autenticità del movimento"; in data 21/01/2025 ha eseguito un controllo sull'APP di home banking riscontrando diversi bonifici non autorizzati; in data 21/01/2025 si è recata presso un diverso sportello dell'intermediario asserendo che nell'occasione, su suggerimento degli operatori, sono stati elevati i limiti di importo per i bonifici in uscita; lo stesso giorno ha disposto il "blocco" del conto corrente. Ritenendo di essere rimasta vittima di una frode sofisticata, la ricorrente, ascrivendo all'intermediario la responsabilità dell'evento dannoso per non avere approntato idonei presidi di sicurezza a tutela dei servizi erogati, ha disconosciuto le operazioni di pagamento e chiesto il rimborso all'intermediario ricevendo riscontro negativo. Insoddisfatta dell'esito del reclamo, la ricorrente invoca la tutela dell'Arbitro affinché: condanni

l'intermediario al rimborso del controvalore delle transazioni non autorizzate, dalla medesima complessivamente quantificate in € 9.300,00; disponga la consegna "*della documentazione bancaria richiesta, inclusi i log di accesso, firme, moduli sottoscritti e cronologia operativa*".
Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente rilevando che in esito all'esame dei tracciati informatici estratti dai propri sistemi, le operazioni di pagamento sarebbero risultate correttamente autenticate, registrate e contabilizzate senza evidenze di malfunzionamenti o compromissione dei sistemi utilizzati per la loro esecuzione, previo accesso al *remote banking* mediante inserimento del nome utente, della password e degli ordini di bonifico convalidati a seguito della ricezione delle notifiche in APP (con la descrizione dell'operazione da autorizzare). Deduce dunque la colpa grave della correntista la quale, a differenza di quanto affermato nel ricorso, non si sarebbe recata presso uno sportello del PSP per segnalare una sospetta attività fraudolenta in proprio danno e la compromissione del proprio smartphone, bensì per richiedere l'innalzamento del limite giornaliero dei bonifici, trovandosi verosimilmente impossibilitata ad effettuare le ultime due operazioni di pagamento. La resistente obietta, del resto, che in sede di denuncia e di reclamo la ricorrente non ha fatto alcun riferimento agli asseriti colloqui con il personale preposto o al malfunzionamento del dispositivo e alla sua origine. Osserva che la cliente avrebbe potuto in qualsiasi momento richiedere il blocco del servizio di *remote banking* in filiale o chiamando l'apposito numero verde; anziché disporre l'aumento dei massimali. Ritiene quindi che le operazioni disconosciute siano state eseguite personalmente dall'utente eccependo, di conseguenza, l'inapplicabilità della disciplina di tutela prevista per le operazioni non autorizzate. Conclude chiedendo all'Arbitro la declaratoria di rigetto del ricorso in quanto infondato.
In sede di repliche alle controdeduzioni dell'intermediario, la ricorrente rileva che il documento di sintesi prodotto dall'intermediario, recante i nuovi massimali per i bonifici, reca una sottoscrizione non corrispondente alla propria. Insiste per l'accoglimento del ricorso chiedendo che venga disposta, "*se utile*", l'acquisizione delle registrazioni delle videocamere di sorveglianza nonché la verifica di "*incongruenza della firma apposta sul documento di sintesi rispetto a quelle autentiche*" presenti in altri documenti.
Con memoria di controreplica, l'intermediario eccepisce l'infondatezza della contestazione concernente la sottoscrizione apocrifa del documento di sintesi, poiché non confortata da alcuna perizia calligrafica a sostegno dell'assunto, né la ricorrente ha sporto denuncia per tali fatti. Insiste, dunque, per le conclusioni rassegnate in sede di controdeduzioni.

DIRITTO

La ricorrente, titolare di un conto corrente abilitato all'operatività on line intrattenuto presso la banca convenuta, chiede il rimborso della somma sottratta da terzi (€ 9.221,01) a conclusione di nove bonifici istantanei eseguiti da ignoti tra il 19 e il 21 gennaio 2025, dalla medesima successivamente disconosciuti.
La banca convenuta ha negato il ristoro della somma reclamata ritenendo la cliente gravemente responsabile della frode subita, sul rilievo che le operazioni sarebbero state dalla stessa correttamente autorizzate attraverso un sistema di autenticazione a doppio fattore, sicchè ha escluso che possa riconoscersi la tutela prevista dalla normativa speciale sopra richiamata.
Il rilievo è infondato.
Al riguardo si osserva che, secondo le più recenti posizioni condivise dai Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale sui servizi di pagamento, prescindendo dalla nozione civilistica di "consenso", dispone che la manifestazione di volontà deve essere prestata nella forma convenuta tra il pagatore stesso e il PSP (cfr. ABF Coll. Bari, Dec. n. 11402/2024; Coll. Milano, Dec. n. 12842/2024). Nella vicenda che occupa, in disparte gli eventuali profili di colpa da negligenza in ipotesi

ascrivibili alla correntista, non constano dichiarazioni della ricorrente in ordine all'eventuale esecuzione integrale delle operazioni da parte sua. Vero è che le registrazioni elettroniche prodotte dall'intermediario sembrerebbero indicare che l'inserimento degli ordini di bonifico, come la ricezione delle notifiche push autorizzative siano avvenuti sul device registrato della ricorrente, identificato con DeviceID "***c31a" e User Agent "***N8EG" (la ricorrente non disconosce la paternità del device in questione).
Anche l'esame del foglio "*Log operazioni*" prodotto dall'intermediario, unitamente al file "*Legenda*", evidenzia l'utilizzo del device registrato in fase di inserimento degli ordini di bonifico ("col. Descrizione operazione = App mobile – Bonifico – Apertura maschera") e di autenticazione tramite validazione della OTP, verosimilmente generata dall'invio della notifica push ("col. Descrizione operazione = App verifica OTP sca"), giacché in relazione a tali fasi è indicato il medesimo *user agent* (***N8EG), coincidente con quello indicato in sede di *enrollment* del device registrato della ricorrente. Il foglio "*Richieste SCA*" sembra inoltre confermare l'invio della notifica *push* autorizzativa sul *device* registrato della ricorrente (DeviceID= ***c31a).
Pur tuttavia, il medesimo complesso di evidenze contiene elementi di segno contrario, quali: l'associazione contemporanea di due diversi indirizzi IP in occasione dei *log-in* eseguiti nel contesto dell'operatività fraudolenta; il testo delle notifiche *push* autorizzative dei bonifici, ove si legge "*Autorizzi il Bonifico effettuato dal sito web* […]"; la presenza di notifiche *push* apparentemente volte ad autorizzare accessi via *web*.
L'intermediario non svolge allegazioni specifiche in merito alle rilevate circostanze né fornisce spiegazioni utili a chiarirle. Non vi è dubbio pertanto che il ricorso vada deciso sulla base delle disposizioni del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. n. 218/2017 (che ha attuato la Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno), secondo cui il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricade, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme illecitamente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore (v. combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010; Provvedimento Banca d'Italia 5.7.2011, Sez. IV, § 2). In particolare, a mente dei commi 1 e 2 dell'art. 10 (d.lgs. n. 11/2010, cit.): "Qualora l'utente di servizi di pagamento neghi di aver 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 e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore 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. 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".
Nel caso in esame, dalla documentazione in atti consta l'esecuzione di nove bonifici istantanei, disposti tra il 19 e il 21 gennaio 2025, addebitati sul conto della ricorrente per il complessivo importo di € 9.221,01 (segnatamente: il 19 gennaio € 28,01 - h. 14:52, € 45,00 - h. 17:28, € 12,00 - h. 17:53; il 20 gennaio € 128,00 - h. 10:11, € 328,00 - h. 14:32, € 988,00 - h. 15:20; 21 gennaio € 2.012,00 - h. 9:16; € 2.830,00 - h. 12:23; € 2.850,00 - h. 12:27).
Al riguardo, l'intermediario afferma che le operazioni contestate sono state eseguite previo log-in all'area riservata di remote banking, "tramite username e password", e ricezione delle relative notifiche push in APP con la descrizione dell'operazione da autorizzare. Tuttavia non constano allegazioni in merito agli specifici fattori utilizzati; inoltre. dai tracciati elettronici in atti, seppure vi è traccia della

registrazione delle attività di accesso in APP, nulla si evince in relazione all'attività di log-in da web (ad eccezione del solo invio di notifiche push).
Per vero, a sostegno dell'allegata regolarità del processo autorizzativo, l'intermediario ha prodotto: un file di "Log" in formato foglio di calcolo composto da 10 fogli così denominati "Dati utente", "Disposizione pagamenti", "Rubrica anagrafica", "Sms", "Sms enrollment", "Notifiche push", "Log operazioni", "Log enrollment", "Storico OTP", "Messaggi"; un file in formato foglio di calcolo denominato "Tab legenda LOG"; un file di testo con "Note illustrative lettura file LOG". Orbene, dall'esame congiunto dei citati tracciati appare che tutte le operazioni disconosciute siano state disposte a valle della ricezione di apposite notifiche push parlanti da parte del device registrato della ricorrente, identificato con DeviceID "***c31a" e User Agent "***N8EG" (elemento di possesso). Tuttavia non si riscontrano allegazioni specifiche e/o evidenze in merito all'eventuale secondo fattore utilizzato (di conoscenza o inerenza); né constano dichiarazioni confessorie della ricorrente sul punto (arg. ex art. 2730 cod. civ.).
In proposito giova rammentare che ai sensi dell'art. 10-bis del d.lgs. n. 11/2010: "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi". Inoltre, l'art. 24 del Regolamento Delegato n. 389/2018 dispone che: "I prestatori di servizi di pagamento assicurano che solo l'utente dei servizi di pagamento sia associato, in modo sicuro, alle credenziali di sicurezza personalizzate, ai dispositivi e al software di autenticazione" (comma 1); "l'associazione tramite un canale a distanza dell'identità dell'utente dei servizi di pagamento alle credenziali di sicurezza personalizzate e ai dispositivi o al software di autenticazione è effettuata ricorrendo all'autenticazione forte del cliente" (comma 2, lett. b).
Ebbene, ritiene il Collegio che le evidenze prodotte non costituiscano prova esaustiva e concludente idonea a dimostrare la conformità delle procedure adottate dal PSP alle misure di strong customer authentication imposte dalla normativa di settore, in tutti i passaggi illustrati dalla convenuta. Simili lacune depongono per il non corretto assolvimento dell'onere probatorio gravante sull'intermediario, ai sensi degli artt. 10, 10-bis, d. lgs. n. 11/2010, cit. (cfr. ABF Coll. Bari, Dec. n. 11625/2024), la cui valutazione, in aderenza al dato normativo, costituisce un prius logico-giuridico rispetto all'esame di eventuali profili di colpa ascrivibili alla titolare del conto abilitato all'operatività di remote banking (cfr. ABF Coll. Napoli, Dec. n. 6124/2024). Tanto induce a concludere che le operazioni di pagamento eseguite a mezzo bonifici istantanei oggetto di disconoscimento, siano state perfezionate con modalità non conformi agli standard di sicurezza definiti dalla regolamentazione vigente in materia, come anche declinati dall'EBA negli orientamenti del 21 giugno 2019.
Per le ragioni innanzi esposte, le conseguenze pregiudizievoli delle operazioni di pagamento oggetto di disconoscimento, addebitate sul conto della ricorrente, devono essere interamente accollate all'intermediario resistente per difetto di prova sulla conformità a SCA dell'autenticazione e della relativa esecuzione (cfr. ABF Coll. Bari, Dec. n. 5149/2025). Di conseguenza, assorbita ogni ulteriore domanda, il Collegio dichiara l'intermediario tenuto al rimborso in favore della ricorrente dell'importo complessivo di euro 9.221,00.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 9.221,00.
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.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI