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) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) QUARTA	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FRANCESCO QUARTA

Seduta del 23/03/2026

FATTO

Parte ricorrente, titolare di un conto corrente cointestato intrattenuto presso la convenuta, coadiuvato dalla cointestataria che con nota del 30/10/2025 ha aderito al ricorso, sostiene che in data 21/06/24 sono state eseguite transazioni fraudolente, in prevalenza tramite CBILL, con addebito sul c/c.
Fa presente che la banca in data 28/06/24 accreditava sul c/c le somme relative alle operazioni oggetto di disconoscimento e in data 02/10/24 le riaddebitava, comunicandogli che le proprie infrastrutture tecnologiche non avevano rilevato anomalie o malfunzionamenti e che tali operazioni erano state autorizzate tramite le credenziali associate al codice titolare del servizio a distanza.
Ritiene la banca responsabile per non aver attivato i meccanismi di monitoraggio e blocco previsti dalla PSD2, che avrebbero consentito di rifiutare l'esecuzione di operazioni che apparivano anomale.
Chiede il rimborso delle somme sottratte, pari a € 16.259,07.
L'intermediario afferma che il ricorrente è intestatario di un conto corrente, a cui è collegata una carta di debito.
Precisa che in data 26/06/2024 il ricorrente ha presentato denuncia e ha disconosciuto, previa compilazione dell'apposito modulo, n. 14 operazioni di pagamento tramite bollettini CBILL eseguite il 21/06/2024, dell'importo di € 14.799,72 a favore di vari enti, nonché un'operazione dell'importo di € 1.459,35 effettuata con carta di debito, sempre il 21/06/2024, per un totale di € 16.259,07.
Soggiunge che, ricevuta la notizia della frode, ha tentato il recupero delle somme attivando le relative procedure, tuttavia con esito negativo comunicato in data 02/10/2024.
Osserva che l'importo del *petitum* andrebbe in ogni caso decurtato della somma di € 70,73, rimborsata in data 29/07/2024 dall'ente beneficiario di due pagamenti CBILL contestati.

Soggiunge che l'importo di € 12.186,88, relativo ai cinque pagamenti CBILL a favore di Agenzia delle Entrate, è bloccato presso tale ente e che verrà restituito al ricorrente previa presentazione del provvedimento dell'Autorità giudiziaria che autorizza lo sblocco delle somme.
Circa le modalità di funzionamento del servizio internet banking, afferma che per poter accedere ai servizi online è richiesto l'inserimento simultaneo di password statiche (PIN e codice Titolare) e password dinamica (OTP), nello specifico impiegata per l'autorizzazione di operazioni dispositive, generati via APP o via SMS.
Precisa che, nel caso di generazione via app, è necessaria la selezione della notifica ricevuta sullo smartphone associato e la digitazione del PIN o, se abilitati, l'utilizzo dell'impronta digitale o del riconoscimento facciale.
Circa la corretta autenticazione, ritiene che le operazioni in esame, disconosciute dal cliente, siano state eseguite dopo essere state "autenticate, correttamente registrate e contabilizzate" e non hanno "subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconveniente". A sostengo di tale affermazione, produce l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta dal ricorrente.
Evidenzia che il ricorrente si connette prevalentemente tramite APP dal proprio device identificato con il codice univoco 46***a6, che sarebbe "lo stesso utilizzato per autorizzare l'operatività disconosciuta".
Aggiunge che, in data 21/06/2024 alle ore 12.04, viene eseguito un accesso da WEB browser con inserimento del PIN e dell'OTP, generato attraverso il device con codice univoco 46***a6.
Fa presente che, prima dell'esecuzione dell'operazione, sul device della ricorrente è stata inviata una push del seguente tenore: "Stai autorizzando l'accesso al sito web della banca" e dopo l'inserimento del PIN, un'altra push dal testo: "è stato eseguito il 21/06/2024 alle 12:04 un accesso al sito [dell'intermediario] da un browser non utilizzato ultimamente. Non sei stato tu? Contatta la Filiale Digitale."
Precisa che in data 21/06/2024, alle ore 12:08, è stato disposto da APP un pagamento di € 1.495,35 con carta di debito e la transazione risulta essere stata validata con codice OTP previa digitazione del PIN, così come confermato dalla tracciatura, da cui si evincono le push pervenute sul device del ricorrente prima e dopo l'esecuzione dell'operazione.
Successivamente, sempre in data 21/06/2025, sono stati disposti da WEB browser pagamenti di bollettini CBILL, alle ore 12:13, 12:15, 12:16, 12:18, 12:19, 12:21, 12:23, 12:24, 12:25, 12:35, 12:36, 12.37, 12:38, 12:39 a favore di vari enti e società. Precisa che tutte le transazioni risultano essere validate con codice OTP previa validazione del PIN (Foglio tracciatura, colonna R denominata "MSG INPUT", al cui interno viene riportata la modalità di generazione della credenziale dinamica OTP "authType: PIN"), che "vanno a buon fine" (Foglio tracciatura, colonna R denominata "MSG INPUT", al cui interno viene riportato il dettaglio dell'operazione con il codice, il numero del bollettino e l'importo).
Soggiunge che il cliente ha ricevuto una *push* dal testo "Stai autorizzando il pagamento della bolletta CBILL pe un importo di € […] sul sito" e che gli importi indicati nelle push sono comprensivi della commissione di € 1,30, tranne per il pagamento di € 174,41 comprensivo della commissione di € 1,00.
Sostiene, dunque, che tutte le operazioni sono state autenticate correttamente, senza anomalie, in conformità ai requisiti della SCA.
Sottolinea, una volta di più, di aver inoltrato numerose notifiche push, con descrizione delle singole operazioni, ignorate del ricorrente.
Sostiene, quindi, che deve escludersi ogni responsabilità dell'intermediario, ai sensi degli artt. 7 co. 2 e 12 co. 3 del D. Lgs. n. 11/2010.
Chiede, pertanto, di rigettare il ricorso e, nella denegata ipotesi che il Collegio ritenga di poter ravvisare profili di responsabilità nell'accaduto in capo all'intermediario, di definire la ripartizione fra le parti del danno ai sensi dell'art. 1227, primo e secondo comma c.c. con l'applicazione della franchigia di € 50,00 contemplata dalla normativa in materia di servizi di pagamento.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

DIRITTO

La domanda di parte ricorrente, avente ad oggetto il rimborso delle somme oggetto di disconoscimento (15 pagamenti tramite bollettini CBILL, per un valore complessivo di € 14.799,72, e un pagamento con carta di debito, del valore di € 1.459,35), non può trovare accoglimento.
Le operazioni contestate in addebito si collocano temporalmente 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.
Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *strong customer authentication* - SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente.
In linea con le indicazioni fornite dall'art. 10-*bis*, comma 1, d.lgs. 11/2010, i prestatori di servizi di pagamento sono tenuti a utilizzare l'autenticazione forte *"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"*.

Pertanto, sia la tokenizzazione dello strumento di pagamento sia i successivi pagamenti effettuati non possono essere lasciati privi della procedura di autenticazione forte. Come recentemente affermato dal Collegio di Coordinamento (decisione n. 9559/2024), *"di fronte al disconoscimento delle operazioni di pagamento effettuato dall'utente, si deve innanzitutto verificare che l'intermediario abbia assolto l'onere, posto a suo carico dall'art. 10, d.lgs. 11/2011, di dimostrare che l'operazione di pagamento è stata effettuata mediante uso della SCA in tutte le fasi rilevanti"*.
Il primo accertamento da compiere, in ordine logico, riguarda dunque la prova che lo strumento di pagamento fosse assistito da un sistema di autenticazione forte dell'utilizzatore (a due fattori). Nel caso di specie, l'intermediario ha correttamente comprovato di avere dotato gli strumenti di pagamento di presidi di sicurezza di tipo "forte" (Strong Customer Authentication - SCA). A supporto dell'autenticazione, della registrazione e della contabilizzazione delle operazioni contestate, l'intermediario ha allegato alle controdeduzioni un file di *"tracciature informatiche"* (allegato n. 9), che il Collegio reputa idoneo allo scopo. Infatti, risulta adeguatamente provato che l'esecuzione di tutte le operazioni disconosciute ha rispettato i requisisti della "Conoscenza" (codice OTP dinamico generato, per ogni operazione, a seguito della digitazione del PIN, noto solo al cliente) e del "Possesso" (APP installata sul dispositivo identificato dal codice univoco "46***6a6" su cui sono pervenute le notifiche push autorizzative).
La legenda esplicativa, versata in atti dall'intermediario, aiuta il Collegio a decifrare le complesse tabelle e stringhe di registrazione e contabilizzazione delle operazioni.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Il Collegio di coordinamento, con pronuncia n. 22745/2019, ha chiarito che "*[…] la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l' "autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*".
Sul punto, il Collegio trae elementi di valutazione dalla denuncia presentata dal ricorrente alle FF.OO. il 26/6/2024, da cui si ricava che:

- in data 21/06/2024, alle ore 12:02, riceveva un SMS contenente il codice per attivare "l'app" su un certo smartphone e, successivamente, una telefonata proveniente da un'utenza riconducibile all'intermediario;
- l'interlocutore gli dava notizia di alcune operazioni sospette sul suo conto corrente in favore di enti e società per un importo di € 16.342,16, invitando, dunque, a verificare il conto direttamente da APP;
- verificata l'attendibilità del numero chiamante e la sussistenza dei pagamenti, eseguiva una "procedura operativa" necessaria, secondo l'interlocutore, a effettuare lo storno dei pagamenti e il blocco del conto e delle carte;
- dopo aver completato la procedura, riceveva una notifica in app che dava conferma del blocco;
- il sedicente operatore richiedeva di disinstallare l'APP a causa di un virus presente sul cellulare;
- conclusa l'operazione telefonica, a cui avrebbe dovuto far seguito altra telefonata, mai giunta, si recava presso la filiale dell'intermediario, in cui un operatore gli comunicava che l'ufficio antifrode della banca aveva segnalato dette operazioni come sospette e aveva provveduto a bloccare il conto e le carte.

Tutte le predette informazioni, unitamente alle varie notifiche push inviate dall'intermediario (dal testo "*Stai autorizzando il pagamento della bolletta CBILL pe un importo di € […] sul sito*"), precedute da altre notifiche del tenore "*Stai autorizzando l'accesso al sito web della banca"* e "*è stato eseguito il 21/06/2024 alle 12:04 un accesso al sito [dell'intermediario] da un browser non utilizzato ultimamente. Non sei stato tu? Contatta la Filiale Digitale"*, denotano una condotta gravemente colposa da parte dell'utente, il quale avrebbe potuto tempestivamente impedire il susseguirsi di eventi lesivi e non lo ha fatto, sia pure sotto l'effetto dei denunciati raggiri ad opera di terzi malintenzionati.
Decisivo è un ulteriore dato, messo in rilievo dall'intermediario: la denunciata variazione del *device* associato al conto risulta riscontrabile solo dalle ore 12.54 del 21/06/2024, dunque successivamente all'operatività contestata. Il che induce a ritenere che tutte le operazioni disconosciute siano state eseguite dal device normalmente in uso da parte del ricorrente, senza che questi ne abbia mai lamentato la perdita o la sottrazione.
Sulla base del consolidato orientamento dei Collegi ABF, preso atto delle minime allegazioni da parte del ricorrente nella sua denuncia sulle circostanze di fatto della frode, unitamente alla mancata segnalazione di perdita o sottrazione fraudolenta del *device* o dei codici di sicurezza, rilevato che tutte le notifiche push (sufficientemente eloquenti dello stato di avanzamento delle singole fasi dell'operatività disconosciuta) sono state pacificamente inviate sul dispositivo del ricorrente e da lui stesso vidimate tramite l'app, il Collegio considera gravemente colpevole la condotta del ricorrente e pertanto inadempiuti gli obblighi di conservazione posti dalla legge in capo dell'utilizzatore.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE