COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 19/05/2025

FATTO

La società ricorrente fa presente di essere titolare di un conto di pagamento presso l'intermediario resistente che alla data del 13 ottobre 2024 recava un saldo attivo di € 177.673,49.
Riporta, inoltre, che il 14 ottobre 2024 il proprio legale rappresentante, accedendo al *remote banking*, ha notato con propria sorpresa che il saldo era stato pressoché azzerato tramite l'esecuzione non autorizzata di 5 bonifici di € 29.900,00 ciascuno e un bonifico di € 28.130,00 in favore di una propria carta prepagata dotata di IBAN emessa da un terzo intermediario, per un totale di € 177.630,00.
Soggiunge che, contestualmente, sono stati eseguiti n. 6 bonifici non autorizzati da tale carta prepagata in favore di soggetti sconosciuti.
Tanto premesso, ritiene che l'intermediario resistente abbia negligentemente omesso di bloccare le operazioni, da ritenersi sospette, e di inviare opportuni *alert*, in violazione degli obblighi contrattuali e legislativamente previsti.
Costituitosi, l'intermediario premette che il rappresentante legale della società ricorrente era l'unico soggetto autorizzato a operare sul conto e che il dispositivo mobile registrato ai fini SCA era di quest'ultimo, come evincibile dalla conversazione intercorsa il 5 ottobre 2024 con il proprio Servizio Clienti. In particolare, precisa che in tale occasione lo stesso ha riferito di avere "rotto il telefono" e di averne "comprato uno nuovo" richiedendo, quindi, di sostituire il dispositivo associato in precedenza con uno nuovo, associato con successo il successivo 8 ottobre 2024.

Osserva, inoltre, che dai *log* informatici risulta che nel periodo 1° ottobre - 31 ottobre 2024 non sono stati eseguiti accessi con dispositivi diversi da quello del rappresentante legale della società ricorrente e che quest'ultimo ha ricevuto, aperto e letto le e-mail di conferma dei bonifici contestati.
Precisa che tutti i bonifici contestati sono stati autorizzati con SCA, tramite validazione di apposita notifica *push* dal dispositivo associato al conto.
Riferisce che, per associare un dispositivo mobile e conseguentemente attivare il sistema autorizzativo SCA *compliant*, occorre:
- scaricare l'APP di *homebanking* sullo smartphone;
- attivare sul dispositivo l'autenticazione a due fattori, che consiste specificamente nel riconoscimento tramite elementi biometrici a scelta del cliente e sulla base dei requisiti tecnici del proprio dispositivo;
- inserire il codice di conferma ricevuto via SMS;
- attivare le notifiche.

Precisa che il profilo può essere collegato a un solo dispositivo.
Riporta, inoltre, che, per autorizzare le singole operazioni, è previsto l'invio di una notifica *push* sul dispositivo associato, configurante un fattore di possesso, e l'accesso sul dispositivo e la conferma dell'operazione utilizzando il sistema di riconoscimento attivo sullo smartphone, configurante un fattore di inerenza.
Tanto premesso, osserva, da un lato, che gli importi relativi ai bonifici non sono usciti dalla disponibilità del legale rappresentante della società dal momento che sono stati accreditati su un conto intestato allo stesso; e, dall'altro lato, che non può essere chiamato a rispondere per le ulteriori operazioni eseguite a valere su tale conto.
Quanto alle contestazioni in ordine al mancato blocco delle operazioni, fa presente che, nel caso di specie, non sussistevano i presupposti per procedervi. Precisa che i propri meccanismi di monitoraggio consistono in:
- un modello di *scam cashout*, che interviene in caso di superamento della soglia di € 500,00 per transazioni nelle quali il beneficiario sia nuovo e con un *Bank Identifier Code* sospetto;
- un modello di allerta avente lo scopo di rilevare attività di *phishing* nelle transazioni mediante bonifico avviate da un cliente contattato telefonicamente;
- n. 37 modelli di allerta automatica volti alla rilevazione di *Account Take Over* (c.d. "ATO", ossia attinenti all'accesso al conto di un cliente da parte di un frodatore) a fronte di *trigger event* quali l'associazione di un nuovo dispositivo, il collegamento di un nuovo IP, l'aggiunta di un beneficiario, se avvenuti da meno di 24 ore;
- un sistema di attribuzione di un punteggio agli accessi (c.d. *login score*), che indica se una connessione è sospetta, in base a diversi *input*, quali ad esempio l'indirizzo IP, il Paese e la Regione di connessione, il *browser*.

Soggiunge che anche il beneficiario risultava già noto poiché era già stato eseguito un bonifico a suo favore il 26 ottobre 2023 e che, comunque, non può ritenersi integrato un c.d. rischio di frode di cui all'art. 8 del D.M. 112/2007.
In sede di repliche, la società ricorrente eccepisce la mancata prova da parte dell'intermediario resistente che "*l'operazione del relativo inserimento, al fine di confermare l'operazione di bonifico, sia avvenuta inequivocabilmente per volontà e impegno manuale del cliente*". Ritiene, inoltre, che la documentazione prodotta dall'intermediario sia contraddittoria, insufficiente e inattendibile; in particolare che non sia stata in particolare provato l'invio di opportuni alert via SMS.
Osserva che il danno subito è dovuto ad "*ignote ingerenze sul telefonino cellulare del legale rappresentante*" e che l'involontarietà dei bonifici è attestata dalla circostanza che per tutta la giornata del 14 ottobre 2024 l'APP di *homebanking* risultava "*in manutenzione*".

Insiste, quindi, per l'accoglimento del ricorso.
In sede di controrepliche, l'intermediario eccepisce l'inapplicabilità della disciplina di cui agli artt. 10 ss. del d.lgs. n. 11/2010 e dell'onere di fornire la prova che i bonifici contestati siano stati autorizzati tramite SCA poiché gli stessi risultano eseguiti in favore di un rapporto di titolarità del legale rappresentante della società ricorrente intrattenuto presso un altro intermediario e, quindi, i relativi importi non sono usciti dalla "*sfera di dominio*" di quest'ultimo.
Ribadisce che, come evincibile dai log allegati, non è stato registrato alcun accesso non autorizzato al conto da parte di dispositivi diversi da quelli riconducibili al legale rappresentante della società cliente.
Precisa, inoltre, di avere allegato alle controdeduzioni:
- la visura camerale della società ricorrente acquisita in sede di *onboarding* il 19 aprile 2024 con lo scopo di evidenziare l'identità del rappresentante legale che, a tale data e all'epoca dei fatti, era l'unico soggetto autorizzato ad operare sul conto;
- la conversazione intrattenuta tra il 7 e l'8 ottobre 2024 dal rappresentante legale della ricorrente con il servizio clienti per chiedere il cambio del *device* associato per spiegare perché nelle schermate dei logs di accesso al sistema nel periodo intercorrente tra il 1° e il 31 ottobre 2024 si osservino due dispositivi differenti associati al conto;
- i log dei bonifici eseguiti il 14 ottobre 2024 per dimostrare la disposizione tramite il dispositivo associato e l'autorizzazione mediante SCA;
- i log degli accessi al *remote banking* nel periodo intercorrente tra il 1° e il 31 ottobre 2024 per dare atto del cambiamento del *device* utilizzato, peraltro sempre geolocalizzato in Italia, con indicazione di latitudine e longitudine esatte della posizione, e per dimostrare che non risultano accessi da dispositivi terzi;
- evidenze delle conferme di invio delle e-mail di conferma dell'autorizzazione dei bonifici recanti il testo dei messaggi, l'orario di invio, coincidente con quello di esecuzione, e le conferme di ricezione e apertura;
- la contabile di un precedente bonifico eseguito in favore del medesimo IBAN per dimostrare che il beneficiario era già noto;
- un *report* redatto da una società di consulenza nell'ambito dell'*audit* svolto annualmente al fine di confermare la piena conformità alla PSD2.

Chiarisce, quindi, nel dettaglio le risultanze dei *log* relativi all'autorizzazione dei bonifici e il significato dei valori presenti.
In ultimo, osserva che l'immagine prodotta dalla società ricorrente con l'intenzione di attestare un preteso malfunzionamento dell'APP di *home banking* nella giornata in questione non riporta né data né orario, alcun elemento che la renda riferibile alla propria APP e appare anche manomessa "*come è possibile desumere dal triangolo sproporzionato e appiattito al centro della stessa*".
Insiste, quindi, per le conclusioni rassegnate in sede di controdeduzioni.

DIRITTO

La domanda proposta dalla società ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di n. 6 bonifici istantanei non autorizzati – eseguiti il 14 ottobre 2024 tra le 15:28 e le 16:12 in favore di un conto di pagamento di titolarità del proprio legale rappresentante, acceso presso un altro intermediario – per un totale di € 177.630,00.
Risulta pacifico che gli importi delle operazioni contestate sono stati accreditati su un rapporto intrattenuto dal rappresentante legale della società ricorrente presso un diverso

intermediario, a valere del quale sono stati eseguiti successivamente ulteriori bonifici, poi disconosciuti, in favore di terzi soggetti.

In via preliminare, il Collegio ritiene infondata la tesi sostenuta dall'intermediario di non avere l'obbligo di dimostrare l'avvenuta autorizzazione delle operazioni oggetto di ricorso tramite SCA, poiché gli importi non sarebbero usciti dalla "*sfera di dominio*" del legale rappresentante della società cliente, unico soggetto abilitato ad operare sul conto. Al riguardo si osserva che, di recente, il Collegio di Coordinamento, con la decisione n. 8671/2024, ha ritenuto sottratti all'obbligo della SCA solamente "*i pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario*", anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente. Questo Collegio ha applicato i medesimi principi anche quando le operazioni di costituzione della provvista sono avvenute tra rapporti dello stesso titolare intrattenuti presso due diversi intermediari in caso di cointeressenza tra gli stessi (v. Collegio di Bari decisione n. 4082/2025). Tale orientamento, tuttavia, non può trovare applicazione al caso di specie in cui i conti sono di titolarità di due diversi soggetti – il primo della società e il secondo del rappresentante legale – e sono, altresì, radicati presso due PSP diversi non legati da cointeressenze, in quanto appartenenti a gruppi diversi e non collocano l'uno i prodotti dell'altro.

Nel merito, il Collegio rileva che le operazioni contestate dal ricorrente 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 gennaio 2018. Inoltre, le operazioni contestate dal ricorrente sono state eseguite successivamente all'entrata in vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, 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 (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 2011.

In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore 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". Il comma 2 del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere 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" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è, altresì, precisato che "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".

Ai sensi del successivo art. 12, comma 2 bis, "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". Per "autenticazione forte" si intende "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" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "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".

Al riguardo, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia). La *ratio* di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coordinamento, decisioni n. 3947/2014 e, da ultimo, n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, comma 2, d.lgs. n. 11/2010).

Tratteggiato il quadro normativo di riferimento, occorre premettere che, nel caso di specie, l'intermediario afferma che le operazioni contestate sono state eseguite mediante l'invio di una notifica *push* sul dispositivo associato (fattore di possesso) e l'accesso sul dispositivo con conseguente conferma dell'operazione utilizzando il sistema di riconoscimento attivo sullo *smartphone* (fattore di inerenza). L'intermediario precisa che il 5 ottobre 2024, prima dell'operatività contestata, il rappresentante legale della società ricorrente, unico soggetto abilitato a operare sul conto, ha richiesto al Servizio Clienti la modifica del *device*

associato e che il nuovo abbinamento si è perfezionato il successivo 8 ottobre 2024. Allega evidenze comprovanti la conversazione con il Servizio Clienti, non contestata dalla ricorrente, mentre non risultano in atti evidenze relative al processo di *enrollment* del nuovo dispositivo.

Il Collegio rileva che dalla documentazione in atti, segnatamente dagli estratti dei log riferibili alle operazioni contestate e dalle relative spiegazioni tecniche allegate, si evince l'utilizzo del *device* associato e non contestato dalla ricorrente (fattore di possesso), ma non l'utilizzo del secondo fattore allegato (sistema di sblocco previsto dallo *smartphone* per la validazione della notifica *push* pervenuta sul *device*). Al contempo, non constano in atti dichiarazioni confessorie quanto all'eventuale validazione della *push* con il sistema di sblocco dello *smartphone.*

Inoltre, secondo l'orientamento consolidato dell'Arbitro, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

Ne consegue, pertanto, l'accoglimento dell'istanza di rimborso dell'importo relativo alle 6 operazioni di bonifico contestate, per il mancato superamento dell'onere della prova sull'adozione della SCA da parte dell'intermediario resistente (cfr. Collegio di Bari, decisione n. 4082/2025).

Non può trovare accoglimento la domanda di rimborso delle spese legali, in quanto non supportata da evidenze documentali.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 177.630,00.

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

Firmato digitalmente da
ANDREA TUCCI