

## COLLEGIO DI NAPOLI

composto dai signori:

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| (NA) CARRIERO   | Presidente                                                |
| (NA) GIGLIOTTI  | Membro designato dalla Banca d'Italia                     |
| (NA) COCCIOLI   | Membro designato dalla Banca d'Italia                     |
| (NA) MIOLA      | Membro di designazione rappresentativa degli intermediari |
| (NA) VERDICCHIO | Membro di designazione rappresentativa dei clienti        |

Relatore MASSIMO MIOLA

Seduta del 10/02/2026

## FATTO

La ricorrente, titolare di una carta prepagata rilasciata dall'intermediario A e di un conto corrente presso l'intermediario B, riferisce di aver ricevuto un messaggio apparentemente proveniente da quest'ultimo, con il quale veniva invitata a cliccare su un link che la reindirizzava all'APP collegata alla propria carta e al conto corrente. Precisa che l'interlocutore era in possesso di suoi dati sensibili, inclusi il numero di conto corrente e quello della carta prepagata. Riferisce, inoltre, che il truffatore, inducendola a credere che fosse necessario verificare il corretto funzionamento del servizio, disponeva un accredito sul conto corrente dell'importo di € 490,00 e le richiedeva contestualmente la restituzione della somma mediante bonifico in favore di un conto corrente, il cui IBAN veniva comunicato nel corso della conversazione telefonica.

La ricorrente espone che, una volta eseguita la prima operazione, il sedicente operatore procedeva ad un ulteriore accredito del medesimo importo sulla carta prepagata emessa dall'intermediario A e la ricorrente effettuava un secondo bonifico istantaneo pari a € 490,00, in favore del medesimo beneficiario del primo. La ricorrente riferisce di essersi successivamente recata presso la filiale degli intermediari, ove un operatore le illustrava le modalità del raggio subito. In tale occasione apprendeva che i due accrediti, ciascuno di € 490,00, erano stati prelevati dal libretto di risparmio a lei intestato e acceso presso l'intermediario B.

Insoddisfatta dell'interlocuzione prodromica al ricorso e ravvisando molteplici profili di colpa in capo agli intermediari, la ricorrente si rivolge all'Arbitro, chiedendo il rimborso integrale delle somme illecitamente sottratte, pari ad euro 980,00 e lamentando la carenza, in capo agli intermediari, di adeguati sistemi di

protezione informatica.

L'intermediario B, costituitosi, rileva preliminarmente che il ricorso risulta formalmente proposto anche nei confronti dell'intermediario A, e che si costituisce nel presente procedimento in qualità di effettivo titolare dei rapporti giuridici oggetto della controversia. Precisa, infatti, che la ricorrente è intestataria presso di sé di una carta prepagata, del conto corrente, nonché di un libretto di risparmio.

Rappresenta che, in data 12.05.2025, la ricorrente riceveva un SMS contenente un link, sul quale cliccava inserendo le informazioni richieste. Successivamente veniva contattata da un'utenza telefonica privata e, nel corso della conversazione con l'interlocutore, disponeva una prima operazione di bonifico istantaneo in favore di un conto corrente intestato a soggetto sconosciuto. In un secondo momento, sempre su indicazione del medesimo interlocutore, eseguiva una ulteriore operazione di bonifico istantaneo. Una volta resasi conto di essere rimasta vittima di una truffa, la ricorrente presentava in data 14.05.2025 apposito modulo di disconoscimento, senza tuttavia allegare documentazione probatoria idonea a ricostruire la dinamica della frode. L'intermediario evidenzia che, come ammesso dalla stessa ricorrente, le operazioni in contestazione risultano essere state interamente da lei eseguite e che, pertanto, i relativi addebiti sono esclusivamente ascrivibili alla sua condotta.

L'intermediario ritiene, quindi, evidente che la ricorrente sia stata vittima di uno schema di frode riconducibile alla c.d. "manipolazione", in cui il soggetto raggirato dispone volontariamente operazioni di pagamento nell'illusione di proteggere i propri risparmi.

Sottolinea che le operazioni contestate sono state eseguite nel pieno rispetto dell'art. 10-*bis* del D. Lgs. n. 11/2010, essendo state autorizzate solo a seguito di una corretta e regolare autenticazione forte del cliente (Strong Customer Authentication – SCA), mediante l'utilizzo di due fattori appartenenti alle categorie della conoscenza (ossia qualcosa che solo l'utente conosce, nel caso di specie il codice \*\*\*ID) e del possesso (qualcosa che solo l'utente possiede, ossia il dispositivo sul quale viene ricevuta la notifica push in App).

Con riferimento alla creazione della provvista, l'intermediario precisa che la stessa è avvenuta mediante riscatto di titoli detenuti dalla ricorrente, operazione effettuata tramite canali online. Ritiene pertanto che il frodatore, entrato nella disponibilità del conto grazie alle credenziali e ai codici OTP comunicatigli dalla cliente, abbia autorizzato entrambe le operazioni. Evidenzia, inoltre, che gli SMS ricevuti dalla ricorrente indicavano chiaramente il tipo di operazione in corso, rendendo evidente che il codice OTP sia stato consapevolmente fornito al truffatore.

L'intermediario evidenzia che successivamente alla creazione della provvista, la ricorrente abbia dato puntuale seguito alle istruzioni impartite dal frodatore, disponendo personalmente i bonifici oggetto di disconoscimento. L'intermediario fornisce, inoltre, evidenza informatica della regolarità sia della fase di creazione della provvista dal libretto di risparmio al conto corrente e alla carta prepagata; dell'enrollment della carta prepagata e della carta di debito ai sistemi di autorizzazione dinamica; sia della fase di login, avvenuta mediante inserimento delle credenziali e dei codici OTP o del codice \*\*\*\*\*ID;– della fase dispositiva delle operazioni, autorizzate secondo procedura SCA, con utilizzo del codice \*\*\*\*\*ID. Precisa che tutti i codici OTP risultano inviati al numero telefonico certificato della cliente.

Quanto ai sistemi di autenticazione adottati, l'intermediario evidenzia di aver implementato una procedura primaria, basata su push notification in App e codice \*ID, e una procedura secondaria, fondata su OTP via SMS e password. Nel caso di specie, le operazioni dispositive sono state autorizzate mediante la procedura primaria, pienamente conforme alla normativa vigente. Ritiene, pertanto, inconfutabile che sia stata adottata una SCA idonea a garantire la sicurezza dei servizi offerti, senza che siano emerse anomalie o malfunzionamenti.

L'intermediario ricorda, infine, che l'informativa sulle operazioni in entrata e in uscita viene trasmessa mediante push notification in App e tramite servizio di SMS alert. Atteso che le operazioni contestate sono state autorizzate a seguito dell'associazione della carta su un nuovo dispositivo, resa possibile

dall'inserimento dei codici OTP inviati con specifica indicazione dell'operazione da autorizzare, risulta evidente la violazione, da parte della cliente, dell'obbligo contrattuale di non condividere credenziali e codici personali.

L'intermediario conclude, pertanto, che le operazioni contestate sono state volontariamente eseguite dalla ricorrente nell'ambito di una frode posta in essere da terzi, alla quale l'intermediario è rimasto del tutto estraneo. Evidenzia, altresì, come dalla ricostruzione dei fatti emerga non solo l'assenza di responsabilità dell'intermediario, ma anche una condotta caratterizzata da colpevole credulità da parte della ricorrente, che ha eseguito fino all'ultimo le istruzioni impartite da uno sconosciuto interlocutore. Alla luce di quanto esposto, richiamate anche le campagne informative sulla sicurezza delle operazioni di pagamento svolte mediante plurimi canali, l'intermediario chiede il rigetto nel merito del ricorso. Tanto premesso, si rileva quanto segue in

## DIRITTO

La controversia attiene alla richiesta di rimborso di somme indebitamente sottratte a seguito di operazioni fraudolente compiute *on line*.

Il ricorso non merita di essere accolto.

Preliminarmente, giova rilevare che le operazioni contestate risultano essere state il 12/05/2026. Pertanto, esse rientrano nell'ambito di applicazione del d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal D.Lgs. 218/2017, di recepimento della direttiva 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-bis del d. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, il parere dell'EBA del 21 giugno 2019).

Come costantemente rilevato da questo Arbitro, la novellata normativa ha rafforzato il regime di speciale protezione e di altrettanto speciale *favor probatorio* a beneficio degli utenti, introdotto dal d. lgs. n. 11/2010 ante modifica e ripetutamente evidenziato da numerose decisioni dell'ABF, anche del Collegio di Coordinamento (cfr. decisioni n. 991/2014; n. 5304/2014; n. 3498/2012; n. 21285/2021).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario. In particolare, ai sensi dell'art. 10, comma primo, d. lgs. 11/2010, si stabilisce che, in caso di disconoscimento di un'operazione di pagamento da parte dell'utente, è onere del prestatore di servizi di pagamento provare che la stessa operazione è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; in difetto della prova della corretta autenticazione, viene meno, per il prestatore dei servizi, la possibilità stessa di riferire le operazioni contestate al cliente. L'art. 12, comma 2-bis stabilisce, inoltre, che «*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*»,

Con specifico riferimento al requisito di autenticazione forte (SCA), L'art. 10-bis, comma 1, del d.lgs. n.11/2010 dispone che, in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, «*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*». L'art. 1, lett. q), del d.lgs. n.11/2010 ("Definizioni") definisce per «*autenticazione: la procedura che consente al prestatore di*

*servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore".* La definizione di autenticazione forte (SCA) è fornita dalla successiva lettera *q-bis*), che riprende l'art. 4 del Regolamento 2018/389, specificando che per autenticazione forte del cliente 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"*.

Ai sensi dell'art. 38 del Regolamento Delegato (UE) 2018/389 della Commissione Europea, tale requisito si applica a tutte le transazioni successive al 14/09/2019. Inoltre, nella *Opinion* del 21 giugno 2019 (EBA-Op-2019-06) l'EBA ha fornito chiarezza sugli elementi utili alla SCA, con un ulteriore livello di dettaglio, attraverso specifici esempi di soluzioni tecniche, per ciascuna categoria di elementi, *compliant* o meno con le disposizioni regolamentari.

Venendo al caso di specie, la ricorrente disconosce un primo bonifico istantaneo di € 490,00 disposto in data 12.05.2025 dalla carta prepagata emessa dall'intermediario A; e un secondo bonifico istantaneo di € 490,00 disposto in data 12.05.2025 dal conto corrente intrattenuto presso l'intermediario B. E' agli atti evidenza del blocco della carta prepagata (ore 17.44) e del conto corrente, (ore 17.45): disposto dalla ricorrente in data 12.05.2025, quindi successivamente alle operazioni disconosciute

Come emerge anche dalla denuncia all'Autorità di P.S., la ricorrente, titolare di una carta prepagata rilasciata dall'intermediario A e di un conto corrente presso l'intermediario B, riferisce di aver ricevuto un messaggio apparentemente proveniente da quest'ultimo, con il quale veniva invitata a cliccare su un link che la reindirizzava all'APP collegata alla propria carta e al conto corrente. Precisa che l'interlocutore era in possesso di suoi dati sensibili, inclusi il numero di conto corrente e quello della carta prepagata. La ricorrente riferisce, inoltre, che il truffatore, inducendola a credere che fosse necessario verificare il corretto funzionamento del servizio, per due volte di seguito disponeva un accredito sul conto corrente dell'importo di € 490,00 e le richiedeva contestualmente la restituzione della somma mediante bonifico in favore di un conto corrente, il cui IBAN veniva comunicato nel corso della conversazione telefonica. La ricorrente dichiara di avere eseguito personalmente i bonifici oggetto di contestazione, sia pure per effetto di un raggiro perpetrato da terzi.

Il Collegio rileva pertanto che la vicenda si caratterizza nei termini di una frode di tipo manipolativo, nella quale la ricorrente, dopo aver interagito via SMS e per via telefonica con sedicenti operatori degli intermediari e aver fornito credenziali che hanno consentito la previa creazione della provvista mediante trasferimenti interni dal proprio libretto al conto e alla carta, ha disposto personalmente, su induzione dei truffatori, due bonifici istantanei di € 490,00, ciascuno in favore di un terzo sconosciuto. Al riguardo, il Collegio evidenzia che secondo gli orientamenti condivisi dai Collegi, quando eseguita per intero dal pagatore, l'operazione deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura").

Il Collegio evidenzia che, in ogni caso, l'intermediario ha fornito evidenza del processo di autenticazione adottato per le singole operazioni, da cui si ricava l'impiego di un codice di sicurezza "\*ID" su notifica in app della cliente.

Con riferimento alla fase di creazione della provvista, l'intermediario riferisce che i frodatori, dopo essere entrati nell'home banking personale della cliente, mediante l'utilizzo delle credenziali di accesso e dei codici OTP da lei stessa comunicati, in quanto ricevuti sul proprio numero telefonico securizzato, hanno disposto due operazioni di girofondi finalizzate alla costituzione della provvista, entrambe regolarmente autorizzate tramite l'inserimento di ulteriori codici OTP inviati alla cliente, come risulta dalle evidenze informatiche prodotte. A tale riguardo, il Collegio si richiama all'orientamento espresso

dal Collegio di Coordinamento, da ultimo ribadito nella decisione n. 8671/2024, secondo cui le operazioni di girofondi effettuate tra rapporti intestati al medesimo cliente e accesi presso il medesimo intermediario possono essere sottratte all'obbligo di applicazione della SCA, in quanto operazioni meramente interne e, di per sé, non immediatamente idonee a determinare una perdita patrimoniale. Quanto alle operazioni dispositive, secondo le opinioni condivise dei Collegi sarà comunque possibile rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode.

Tuttavia, il Collegio rileva che nel caso di specie non ricorrono tali condizioni. E' evidente, infatti, la condotta tenuta dalla ricorrente, la quale ha incautamente disposto le operazioni di bonifico verso un soggetto terzo sconosciuto, e non è direttamente collegabile alle circostanze riportate all'attenzione dei preposti organi giudiziari. Si aggiunga che è la ricorrente stessa a dichiarare di essere stata contattata da un terzo soggetto sconosciuto al quale si è affidata, senza tuttavia allegare documentazione che dimostri l'avvenuto contatto fraudolento.

Sempre la ricorrente ha eseguito pedissequamente le azioni richieste del frodatore, fidandosi di quest'ultimo, eseguendo di propria volontà le operazioni in questione, partecipando così, seppure inconsapevolmente, alla truffa in suo stesso danno.

A tale riguardo l'intermediario ha eccepito che il ricorrente non ha fornito informazioni utili alla ricostruzione dell'accaduto, né ha prodotto evidenze documentali relative alla truffa. Nel caso di specie, il ricorrente si è limitato, infatti, a dichiarare genericamente, e senza allegazione documentale, di aver ricevuto un SMS che lo invitava a cliccare su un link, nonché di avere avuto un'interlocuzione telefonica con un sedicente operatore dell'intermediario, senza fornire la schermata dell'SMS nonché evidenza del numero telefonico con cui è intervenuta l'interlocuzione. Pertanto il Collegio non può accertare se il ricorrente sia incorso in un caso di legittimo affidamento circa la genuinità dell'interlocuzione con l'intermediario, ovvero abbia fatto dichiarazioni volutamente generiche destinate a limitare la propria responsabilità.

**P.Q.M.**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE