

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) RUGGIERO	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARIANELLO

Seduta del 27/01/2026

FATTO

La ricorrente riferisce di avere subito lo spostamento fraudolento di € 5.000,00, che deteneva sotto forma di buoni postali, dal conto corrente alla carta di credito alla medesima intestata. Tale somma le è stata successivamente sottratta mediante due operazioni di bonifico. Nella denuncia specifica di avere ricevuto, in data 04/06/2025, una telefonata da un numero sconosciuto ed un operatore, parlandole in russo (lingua madre della ricorrente), le comunicava che aveva guadagnato € 24.000,00 tramite degli investimenti effettuati in precedenza. Il medesimo operatore la convinceva a continuare la conversazione in videochiamata ed accedere alla propria *app*. In tal modo l'istante verificava di avere ricevuto due bonifici dell'importo totale di € 5.000,00.

A questo punto l'interlocutore affermava che per ricevere il resto dell'importo guadagnato era necessario effettuare un bonifico su un conto estero. La ricorrente, una volta terminata la conversazione, si avvedeva che i soldi accreditati erano in realtà relativi alla liquidazione di titoli dalla stessa detenuti e che erano stati effettuati due bonifici da lei mai autorizzati, per un importo totale di € 4.980,00. Insoddisfatta della prodromica interlocuzione avuta con l'intermediario nella fase precedente al ricorso, l'istante si è rivolta all'Arbitro, chiedendo la restituzione dell'importo sottratto.

L'intermediario, regolarmente costituito nel presente procedimento, riferisce preliminarmente di depositare le controdeduzioni per conto della società titolare effettiva del rapporto giuridico, dallo stesso detenuta.

Il convenuto rappresenta che in data 04/06/2025 la cliente, intestataria di un libretto di risparmio e di una carta di credito, riceveva una telefonata da una numerazione sconosciuta, con la quale un

interlocutore le spiegava la necessità di eseguire delle operazioni per ricevere degli emolumenti relativi ad investimenti non meglio specificati. Parte ricorrente dichiara di avere seguito le indicazioni e di avere effettuato i pagamenti richiesti. Dalle allegazioni informatiche depositate in atti si evince che la cliente riceveva il 04/06/2025 due ricariche sulla carta di propria titolarità ed il giorno successivo prelevava l'intero importo dallo strumento di pagamento. In data 05/06/2025 risultavano versati ulteriori importi sulla carta, che venivano utilizzati per eseguire le operazioni successivamente contestate. Le predette operazioni sono state autorizzate tramite *sms* contenenti una *otp*, inviati sull'utenza telefonica della ricorrente. Le *otp* risultano spedite sia per le operazioni necessarie alla creazione della provvista che per quelle che hanno generato un'effettiva perdita patrimoniale.

Il resistente chiede preliminarmente che l'importo delle due operazioni disconosciute venga rideterminato nella somma di € 4.980,00, invece di € 5.000,00 come indicato dalla ricorrente.

Quest'ultima, come risulta dalle evidenze in atti, è stata oggetto di una frode riconducibile allo schema del "*phishing*" classico, nel quale la malcapitata, comunicati i propri codici, consente al frodatore di predisporre operazioni dispositive, partecipando in tal modo, seppur inconsapevolmente, alla truffa in suo stesso danno. Appare verosimile, infatti, che la cliente abbia comunicato al malfattore le *otp* ricevute, consentendo l'esecuzione delle operazioni contestate.

In merito alla creazione della provvista, si rinvia a quanto stabilito dal Collegio di Coordinamento nella decisione n. 8671/2024 secondo cui: *"I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente"*.

Le operazioni disconosciute sono state eseguite inoltre in conformità dell'art. 10-bis del D.lgs. n. 11/2010, ovvero in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti, rispettivamente, alle categorie della conoscenza (qualcosa che solo l'utente conosce, ossia la *password* personale) e del possesso (qualcosa che solo l'utente possiede, ovvero la digitazione dei diversi codici *otp* ricevuti sul telefono securizzato in precedenza).

Ne deriva che per l'accesso all'*internet banking* è necessario l'inserimento di *password* statiche e dinamiche e che, una volta collegati al servizio, per le operazioni dispositive è altresì necessario il codice *otp*, inviato via *sms*.

Nel caso in esame sono state regolarmente effettuate le seguenti operazioni:

- a) l'*enrollment* della carta al sistema autorizzativo di tipo dinamico, funzionante mediante l'invio di *otp* al numero di cellulare dell'istante;
- b) la fase di *log-in*, in cui la ricorrente si è autenticata tramite la digitazione delle proprie credenziali (*user-id* e *password*), nonché il successivo inserimento del codice *otp*;
- c) anche la fase dispositiva delle operazioni oggetto di ricorso è sempre avvenuta tramite SCA, con inserimento della *password* e del codice *otp* ricevuto.

L'intermediario rileva che i propri sistemi di autenticazione prevedono una procedura primaria tramite *push notification in app* e codice ID, nonché una secondaria mediante l'inserimento dell'*otp* inviata a mezzo *sms*, utilizzata nel caso in esame. Poiché non si è verificato alcun cambiamento dell'utenza telefonica, ne consegue che le operazioni contestate potevano essere effettuate soltanto dalla titolare dello strumento di pagamento, che era in possesso del *device* su cui è stato inviato il messaggio *sms* con il codice autorizzativo. Il blocco delle carte è avvenuto soltanto dopo l'esecuzione delle operazioni contestate e, in ogni caso, l'intermediario mette a disposizione dei propri clienti un servizio di *push notification in app* e un servizio di *sms alert*.

Nelle conclusioni il resistente chiede all'Arbitro il rigetto del ricorso.

In sede di repliche la ricorrente contesta la ricostruzione di controparte, sostenendo di essere stata vittima di una truffa telefonica particolarmente sofisticata, avvenuta la sera del 04/06/2025. Il giorno seguente si è subito recata nella filiale vicino casa, dove veniva rassicurata poiché dai sistemi non risultava alcuna anomalia ed i suoi investimenti apparivano intatti. Le veniva comunque suggerito di

sporgere denuncia. Durante la giornata lavorativa non aveva modo di controllare il conto e soltanto alle ore 18:30, accedendo alla sua *app*, scopriva che dal conto corrente le erano stati sottratti € 5.000,00 e che una somma ulteriore, trasferita senza alcuna autorizzazione, era apparsa sul conto. L'istante, impaurita da possibili ed ulteriori movimenti fraudolenti, decideva di prelevare i contanti rimasti per metterli al sicuro, visto che la filiale era ormai chiusa. La mattina successiva bloccava il conto e sporgeva regolare denuncia.

La ricorrente ribadisce di non avere mai comunicato codici, *otp* o altre credenziali sensibili a terzi. La truffa è stata perpetrata con tecniche di *vishing*, che consentono ai truffatori di accedere ai dati del dispositivo tramite sofisticati strumenti informatici. La cliente ha fornito solo informazioni personali di base, non idonee a consentire operazioni bancarie. Appare verosimile ritenere che l'intermediario non abbia attivato le necessarie misure di sicurezza, dal momento che non le è pervenuto alcun avviso per i trasferimenti anomali e le movimentazioni sul conto.

L'istante reitera la richiesta di rimborso di € 5.000,00; in via subordinata, qualora venisse riconosciuto un minimo concorso della cliente, chiede il rimborso di almeno il 70 per cento dell'importo, ai sensi dell'art. 1227, co.1, del Codice Civile.

L'intermediario, nelle controrepliche, si riporta integralmente a quanto già sostenuto in sede di controdeduzioni.

DIRITTO

La presente controversia attiene alla richiesta di parte ricorrente relativa al disconoscimento di due operazioni di bonifico per complessivi € 4.980,00, effettuati a beneficio di due diversi soggetti in data 05/06/2025 a distanza di circa quattro minuti l'una dall'altra (ore 10:10:05 e ore 10:14:26).

La ricorrente indica erroneamente l'importo totale di € 5.000,00, forse ricomprendendovi anche le spese di procedura.

Occorre rilevare che le operazioni contestate risultano essere state eseguite il 05/06/2025 e, pertanto, ricadono nell'ambito di applicazione del D.lgs. 27/01/2010, 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. 15/12/2017, 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 13/01/2018.

In particolare, le fonti normative che regolano la *strong customer authentication* (c.d. SCA) sono rinvenibili negli artt. 97 e 98 della PSD 2, nell'articolo 10-*bis* del D.lgs. n. 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 14/09/2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, il parere dell'EBA del 21/06/2019).

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

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 o della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, D. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia del 05/07/2011.

Il ricorso è fondato e merita parziale accoglimento per le considerazioni che seguono.

La ricorrente in sede di denuncia dichiara di avere ricevuto, in data 04/06/2025, una telefonata da un numero sconosciuto ed un operatore le comunicava che aveva guadagnato € 24.000,00 tramite degli investimenti effettuati in precedenza. Il medesimo operatore la convinceva a continuare la

conversazione in videochiamata nonché ad accedere alla propria *app*. In tal modo l'istante verificava di avere ricevuto due bonifici dell'importo totale di € 5.000,00. A questo punto l'interlocutore affermava che per ricevere il resto dell'importo guadagnato era necessario effettuare un bonifico su un conto estero. La ricorrente, una volta terminata la conversazione, si avvedeva che i soldi accreditati erano in realtà relativi alla liquidazione di titoli dalla stessa detenuti e che erano stati effettuati due bonifici da lei mai autorizzati, per un importo totale di € 4.980,00. L'istante dichiara di non avere comunicato a terzi credenziali o altri dati sensibili, disconoscendo le operazioni effettuate.

Premesso quanto sopra, a fronte del disconoscimento di operazioni fraudolente da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi degli artt. 10, c. 1 e 2 e 10-*bis* del d.lgs. n. 11/2010. In mancanza di tale dimostrazione, l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute. Nel caso di specie, l'intermediario ricostruisce i singoli passaggi esecutivi, fornendo le relative evidenze informatiche.

Al riguardo, anche con riferimento alle contestazioni della ricorrente, circa l'efficacia probatoria della documentazione tecnica prodotta, si rammenta che, secondo gli orientamenti condivisi dei Collegi, tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico *standard* per l'inserimento e la tracciatura dei fattori di autenticazione forte, per valutare l'assolvimento dell'onere della prova della SCA possono essere valutati (oltre ai *log*) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. Eventuali dichiarazioni confessorie della cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

La provvista per l'effettuazione delle citate operazioni è stata costituita mediante due operazioni di rimborso di buoni dematerializzati sul libretto di deposito intestato alla ricorrente, una delle quali è stata effettuata il giorno prima delle operazioni disconosciute (ovvero il 04/06/2025), mentre la seconda risulta compiuta il giorno seguente. Il controvalore delle operazioni di rimborso dei buoni è stato successivamente trasferito sulla carta prepagata tramite quattro operazioni di ricarica, di cui due effettuate il 04/06/2025 e le altre due il 05/06/2025.

L'intermediario, pur richiamando il principio di diritto affermato dal Collegio di Coordinamento nella decisione n. 8671/2024 secondo cui *"I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente"*, allega evidenze che confermano l'avvenuta autenticazione mediante un duplice fattore di sicurezza sia nella fase del *log-in* (*password* e *otp*) che in quella autorizzativa. In quest'ultima fase, tuttavia, sussiste l'anomalia che l'*otp* necessaria per la liquidazione del buono risulta richiesta da un *computer* situato all'estero ed è stata inviata all'utenza telefonica della cliente.

Le due operazioni di bonifico disconosciute sono state predisposte sul sito *web* dell'intermediario ed autorizzate tramite inserimento delle *otp* inviate.

L'intermediario allega evidenza della fase di *log-in* al sito *web*, avvenuta mediante *password* (elemento di conoscenza) e *otp* (elemento di possesso), nonché della fase autorizzativa avvenuta tramite inserimento delle *otp* ricevute (elemento di possesso).

Anche in questo caso l'anomalia consiste nel fatto che la richiesta autorizzativa, effettuata tramite inserimento dell'*otp* ricevuto, proviene da un dispositivo situato all'estero.

Ne consegue che le due operazioni contestate risultano eseguite in conformità dell'art. 10-*bis* del D. lgs. n. 11/2010, in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti rispettivamente alle categorie della conoscenza (qualcosa che solo l'utente conosce) e del possesso (qualcosa che solo l'utente possiede) e, pertanto, risultano *compliant* alla SCA.

Per quanto attiene al comportamento della ricorrente, nel caso di specie la stessa è incorsa in una

fattispecie di colpa grave.

Alla luce delle dichiarazioni di natura confessoria rese in sede di denuncia, infatti, l'istante ammette di avere ricevuto una chiamata da un numero non riconducibile all'intermediario ed anche le interlocuzioni effettuate con il sedicente operatore risultano poste in essere con modalità comunicative non utilizzate dalla banca per i contatti con la clientela.

Gli elementi sopra indicati consentono, quindi, di ricondurre la presente fattispecie alla truffa effettuata tramite il c.d. *smishing/vishing*, per la quale i Collegi sono soliti ritenere che *"il cliente è vittima di una colpevole credulità"* (in senso conforme, Collegio di Coordinamento ABF, n. 3498/2012).

In tale ipotesi l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente si realizzano con metodi ormai piuttosto noti (*e-mail*, *sms* e telefonate civetta, false comunicazioni di scadenza, invito all'aggiornamento di *database*) che il cliente, dispiegando un minimo di diligenza, sarebbe oggettivamente in grado di schivare, anche per le accresciute campagne di informazione e di sensibilizzazione che i *media* e gli stessi intermediari hanno da tempo attuato.

La non riferibilità della fattispecie in esame al novero delle "operazioni non autorizzate" non comporta, peraltro, che il convenuto sia da ritenere senz'altro esente - in modo automatico ed in misura compiuta - da ogni responsabilità. Occorre, infatti, valutare il comportamento che l'intermediario ha tenuto nel caso concreto e verificare se tale contegno abbia apportato un contributo causale - valutato alla luce del rapporto contrattuale intercorrente con la cliente ai sensi dell'art. 1227 c.c. - alla verificazione dell'evento (Collegio ABF Napoli, n. 6488/2023).

Pertanto, alla luce della documentazione prodotta in atti, occorre verificare se sussistano gli indici di frode identificati dall'art. 8 del D.M. n. 112/2007 che, tuttavia, non hanno un valore precettivo diretto ma rappresentano degli utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario).

Nel caso di specie la lista dei movimenti prodotta dall'istante, riferita alle operazioni effettuate negli otto mesi anteriori ai bonifici disconosciuti, dimostrano come questi ultimi non fossero assolutamente in linea con l'operatività abituale sia per l'ammontare che per la tempistica dell'operazione. Il movimento di maggiore importo rinvenibile, infatti, ammonta ad € 180,00, mentre nel caso in esame, sono state effettuate nell'arco di due giorni operazioni di ammontare oscillante tra i duemila e tremila euro, nonché due bonifici di pari importo (in senso conforme, Collegio ABF Milano, n. 8435/2023).

Dalla documentazione prodotta dall'intermediario, inoltre, si evidenzia la circostanza che le richieste autorizzative provenivano da *device* localizzati geograficamente in località ben distanti dal luogo di domicilio della ricorrente (una da un altro continente e l'altra dall'Europa).

Per quanto concerne l'attivazione di sistemi di *alert*, si evidenzia che: *"Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto"* (Collegio di Coordinamento ABF, n. 24366/2019).

A tale riguardo il convenuto ha prodotto evidenza dell'invio di *sms alert* per ciascuna delle operazioni contestate, che risultano consegnati al numero di telefono indicato dalla ricorrente. Quest'ultima ha provveduto al blocco della carta alle ore 08:48 del 06/06/2025, ovvero dopo due giorni dall'effettuazione della prima operazione non autorizzata.

Tenuto conto di tutte le predette circostanze, della condotta tenuta dall'intermediario e di tutti gli altri elementi desumibili dal caso concreto, il Collegio ritiene equo imputare a parte ricorrente il concorso di colpa nella causazione dell'evento dannoso in una misura pari al 50 per cento, con conseguente responsabilità dell'intermediario per la parte residua a titolo risarcitorio.

Ne consegue, pertanto, che all'istante deve essere riconosciuto il diritto alla restituzione dell'importo di

€ 2.490,00, oltre agli interessi legali dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto della ricorrente al risarcimento del danno per l'importo di € 2.490,00 oltre interessi legali dalla data del reclamo nei sensi di cui in motivazione.

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