

## COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) PALMIERI	Membro di designazione rappresentativa dei clienti

Relatore GIANFRANCO COCCIOLI

Seduta del 12/11/2024

### FATTO

Infruttuoso il prodromico reclamo, il ricorrente, intestatario di un conto corrente presso l'istituto bancario resistente, deduce che in data 30 ottobre 2023, contattato telefonicamente da un numero corrispondente a quello della linea telefonica del servizio clienti della resistente, parlava con un soggetto che, presentatosi come operatore della sua banca, gli comunicava che erano stati rilevati un accesso sul suo conto da remoto mediante uno smartphone localizzato in Tenerife e, inoltre, altro accesso al portale personale della banca tramite l'account, da cui era scaturita la compromissione delle credenziali.

L'interlocutore soggiungeva che, ai fini di provocare la disconnessione del dispositivo smartphone non riconosciuto, era necessario avviare una procedura di sicurezza che consisteva nell'invio di codici OTP sul cellulare dell'istante, operazione che il ricorrente poneva in essere dopo aver verificato sul sito internet che il numero telefonico fosse un numero ufficiale della banca.

Evidenziata l'esistenza di sms confermativi dell'avvio della procedura, anch'essi provenienti dal mittente delle precedenti comunicazioni relative al conto corrente, l'interlocutore riferiva che chi ne era stato autore era riuscito ad entrare online sul conto corrente e a disporre un bonifico di € 9.100,00, cosicché aveva bisogno dell' OTP ricevuto sul cellulare.

Il ricorrente, alle 14.40 del 30 ottobre 2023, provvedeva a comunicare all'interlocutore

telefonicamente il codice OTP ricevuto ed a tentare l'accesso sul suo conto corrente tramite l'applicazione telefonica della banca. Eseguito il login, accertava movimentazioni di denaro a lui non riconducibili, quali smobilizzo di conti di deposito e bonifico in uscita, oltre che di una notifica pendente di autorizzazione di pagamento con carta che prontamente rifiutava.

A quel punto, terminava la telefonata e immediatamente si recava a sporgere denuncia.

Alle ore 15.03 dello stesso giorno (30/10/2023), si metteva in contatto con il servizio clienti della banca, onde segnalare gli accessi abusivi al suo conto e le abusive disposizioni, conseguenze della condotta truffaldina subita. Nel corso della telefonata comunicava di trovarsi nella caserma dei carabinieri per la presentazione della denuncia e riceveva i dettagli delle operazioni registrate dalla banca in data 30/10/2023 (smobilizzo di tre 'conto deposito', disposizione bonifico in uscita verso destinatario ignoto).

Il ricorrente chiedeva pertanto esplicitamente il blocco totale del conto e della relativa carta, disconoscendo tutte le operazioni in uscita compiute il 30/10/2023, con particolare riguardo alla disposizione di bonifico in uscita di € 9.100,00, della quale chiedeva l'annullamento e la revoca.

L'operatore riferiva che per eseguire tale richiesta era necessario inviare via mail al servizio clienti la denuncia.

Alle ore 16:13 del 30 ottobre 2023 l'istante tramite mail inviava la denuncia con esplicita richiesta di annullamento di tutte le operazioni del predetto giorno, inoltrandola alle ore 16:59 del 30 ottobre 2023 anche tramite pec.

Il giorno seguente ribadiva quanto richiesto telefonicamente.

Solo in data 7/11/2023 un operatore riferiva che era necessario riformulare le richieste ed inviare nuova ed ulteriore mail al servizio clienti. Alfine il ricorrente riceveva la copia della ricevuta del bonifico fraudolento il 14.11.2023.

Inoltrato il 30 novembre 2023 un invito a stipulare una convenzione di negoziazione assistita ai sensi della L. n. 162/2014, onde ottenere lo storno dell'importo del bonifico di € 9.100,00, riceveva il 22 dicembre 2023 la risposta negativa della Banca circa il suo rifiuto a procedere alla convenzione di negoziazione assistita.

Tanto premesso, nel richiamare la normativa applicabile, contesta la condotta della banca, sostenendo che la stessa non abbia provveduto ad eseguire il recall del bonifico, nonostante la tempestiva richiesta del cliente.

L'intermediario, costituitosi, eccepisce preliminarmente la mancanza del preventivo reclamo, sostenendo che non possa essere considerato tale l'invito alla stipula di convenzione di negoziazione assistita.

Nel merito rileva che tutte le operazioni sono state correttamente autorizzate, mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del ricorrente con autenticazione forte a due fattori (*strong customer authentication*), registrate e contabilizzate senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Riferisce che l'esecuzione di un bonifico richiede l'inserimento dell'ordine di bonifico all'interno dell'area riservata accessibile utilizzando le credenziali statiche (*username* e *password*) scelte dal cliente, con conseguente richiesta di autenticazione forte mediante OTP trasmesso via SMS la prima volta che il cliente accede e successivamente qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto mediante autenticazione forte.

In caso di accesso senza autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: - saldo del conto; - operazioni di pagamento eseguite negli ultimi 90 giorni.

La conferma dell'ordine di bonifico avviene mediante inserimento di *one time password* (OTP) inviata al numero di cellulare indicato dal cliente in sede di apertura del rapporto,



validato dalla Banca e associato univocamente al conto corrente.

Soggiunge che tutti i passaggi di cui sopra risultano essere stati correttamente realizzati per l'operazione oggetto di contestazione, come si evince dalla stessa denuncia nonché dai log informatici (allegati) dai quali emerge che i terzi avevano conseguito l'accesso all'area riservata del cliente attraverso l'inserimento di username e password. Sebbene taciuto dal Ricorrente, l'accesso era stato reso possibile ai terzi grazie alla condivisione delle credenziali di accesso da parte del cliente. A seguito dell'accesso all'area riservata i terzi svincolavano due conti deposito di € 4.010,63 ed € 4.010,14. L'autorizzazione delle cancellazioni dei depositi avveniva tramite inserimento di appositi OTP. In particolare, la Banca inviava due codici OTP al numero di cellulare comunicato dal cliente in sede di registrazione, che il medesimo, come riconosciuto sia in denuncia sia in sede di Ricorso, provvedeva a riferire ai terzi. Una volta svincolati i soldi, i terzi predisponavano un bonifico di € 9.100,00, autorizzato mediante inserimento di apposito codice OTP inviato al numero di cellulare comunicato dal cliente in sede di registrazione e condiviso con i terzi. Costoro svincolavano un terzo conto deposito dell'importo di € 3.005,90. Anche tale operazione veniva eseguita grazie alla collaborazione del cliente che condivideva con i terzi apposito codice OTP inviato al suo numero di cellulare. Successivamente, verificavano i dati della carta per cercare di eseguire delle operazioni di pagamento anche con quest'ultima. Anche in questo caso, i terzi potevano accedere ai dati della carta solo grazie alla condivisione del codice OTP da parte del Ricorrente. I terzi quindi provavano ad eseguire diverse operazioni di pagamento, come riferito ed allegato dal ricorrente, senza riuscirvi in quanto egli, leggendo attentamente il contenuto dei messaggi SMS contenenti i codici autorizzativi, si asteneva dal condividere tali codici. I codici OTP allegati alle presenti controdeduzioni presentano un orario distinto rispetto a quello indicato nei file riportanti i log comprovanti le operazioni, in quanto la registrazione dell'invio dei codici viene eseguita utilizzando quale fuso orario di riferimento il fuso GMT. Alla luce di quanto dedotto, parte resistente rileva che l'operazione è stata eseguita solo grazie alla collaborazione del ricorrente il quale in modo gravemente colposo ha violato l'art. 7 del D.Lgs. 11/2010. In merito alla revoca dei bonifici, precisa che l'art. 10 del D. Lgs. 27 gennaio 2010, n. 11 prevede espressamente che una volta ricevuto dal prestatore di servizi di pagamento del pagatore, l'ordine di pagamento non può essere revocato dall'utente. Si precisa che l'ordine di pagamento al momento della richiesta di storno da parte del Ricorrente era già stato eseguito in quanto il conto corrente beneficiario era un conto corrente sempre aperto presso la convenuta banca.

L'istante si oppone all'eccezione di inammissibilità, rilevando che l'invito alla negoziazione è da intendersi quale atto equipollente al reclamo.

Nel merito si riporta al ricorso, dichiarando di non aver ancora ricevuto il rimborso.

L'intermediario ribadisce quanto già enunciato nelle difese contenute nelle controdeduzioni.

## DIRITTO

Va rigettata l'eccezione preliminare sollevata dall'intermediario, secondo cui non sarebbe equipollente al reclamo l'invito alla stipula di una convenzione di negoziazione assistita di cui alla Legge n. 162/2014, notificata in data 30/11/2023 e riscontrata, negativamente, il 22/12/2023.

In forza delle disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari, emanate dalla Banca d'Italia, "Il ricorso all'ABF è preceduto da un reclamo preventivo all'intermediario" (Sez. VI, § 1). "Il ricorso



*all'ABF è tuttavia possibile in caso di fallimento di una procedura conciliativa già intrapresa; in questo caso – fermo restando quanto previsto dall'art. 5, comma 1-bis, del decreto legislativo 4 marzo 2010, n. 28 – il ricorso può essere proposto entro il termine di 12 mesi dal fallimento della procedura conciliativa, indipendentemente dalla data di presentazione del reclamo” (Sez. I, § 4).*

Nel caso di specie, l'istanza di invito alla stipulazione di una convenzione di negoziazione assistita contiene la contestazione oggetto del ricorso ed è stata presa in considerazione dall'intermediario che l'ha respinta, dando conseguentemente una risposta negativa alla possibilità di accedere ad una soluzione concordata della controversia (in tal senso anche la decisione n.2256/2020 del collegio di Palermo).

Ciò assodato in via preliminare, il ricorso nel merito merita parziale accoglimento.

Come si desume dal precedente svolgimento del processo, il ricorso ha ad oggetto la contestazione di un bonifico, frutto dell'attività fraudolenta di terzi, e la richiesta di rimborso della relativa somma, tenuto anche conto che al fine di eseguirlo è stata utilizzata la somma complessiva di tre conti deposito, previo loro smobilizzo.

A fronte del disconoscimento di operazione disconosciuta, incombe sul prestatore di servizi di pagamento l'onere di provare che essa sia stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, del d.lgs. 11/2010, secondo cui: *“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”.*

Ai sensi del secondo comma della richiamata disposizione, la dimostrazione dell'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non lo esonera dalla responsabilità, se non dopo aver provato che l'utente ha agito con frode, dolo o colpa grave.

Va al riguardo tenuta presente la disciplina 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) in vigore dal 13.01.2018.

In particolare, la c.d. strong customer authentication (cd. SCA) è disciplinata dagli artt. 97 e 98 della PSD2, dall'articolo 10 bis del D. Lgs. n. 10/2011, dalle 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 dai criteri interpretativi forniti dall'EBA e, in particolare, dal parere dell'EBA del 21 giugno 2019.

Come statuito dal Collegio di Coordinamento (decisione n. 22745 del 10 ottobre 2019), l'onere probatorio previsto nei commi 1 e 2 dell'art. 10 del decreto richiamato deve necessariamente essere assolto dal PSP con riguardo ad ambedue i profili (autenticazione ed esecuzioni delle operazioni di pagamento, nonché colpa grave dell'utilizzatore), da considerarsi necessari e complementari. Alla stregua di ciò, come chiarisce ulteriormente il Collegio di Coordinamento nella predetta decisione, 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 interpretata nel senso che la produzione documentale diretta a fornire la dimostrazione dell'"autenticazione" e della formale regolarità dell'operazione contestata non esaurisce, di per sé, l'onere probatorio, in quanto è indispensabile che l'intermediario provveda specificatamente a indicare una serie di



elementi di fatto caratterizzanti le modalità esecutive dell'operazione, sulla cui base possa trarsi la prova della colpa grave dell'utente.

Se ne arguisce che, nel caso in cui l'intermediario costituito abbia fornito prova dell'autenticazione e della regolarità formale dell'operazione, il collegio possa affermare la sussistenza della colpa grave sulla base di prove dirette oppure di elementi presuntivi, in grado di determinare inferenze logiche, tanto più incisive se sostenute dall'*id quod plerumque accidit*.

Nel caso di specie, l'accesso all'area riservata avviene mediante inserimento delle credenziali statiche, costituite da username e password, nonché dell'OTP che l'utente riceve a mezzo Sms, nei casi di primo accesso e qualora siano trascorsi più di 180 giorni dall'ultimo accesso del cliente al conto corrente con autenticazione forte .

In mancanza di autenticazione forte, l'accesso del cliente è limitato all'acquisizione di informazioni relative al saldo del conto ed alle operazioni di pagamento eseguite negli ultimi 90 giorni. Una volta effettuato l'accesso (anche senza SCA), per le eventuali e conseguenti operazioni dispositive l'utente deve inserire l'OTP che gli viene inviato con sms sul cellulare preventivamente associato al rapporto.

L'autenticazione mediante OTP inserito in app è, secondo l'interpretazione adottata già da alcune decisioni ABF, comunque conforme alle prescrizioni della normativa in materia, anche alla luce delle specificazioni dell'EBA (Collegio di Roma, dec. n. 11778/21) .

Nell'ambito di una unica sessione operativa, la duplicità e l'autonomia dei fattori è assicurata dall'elemento di conoscenza già inserito al momento dell'accesso, e dall'OTP (elemento di possesso) successivamente inserito per eseguire l'operazione di pagamento. Per completezza si evidenzia che, in alcune pronunce, i Collegi hanno affermato che sia onere dell'intermediario fornire la prova della sussistenza dei presupposti (accesso successivo al primo e non oltre 180 giorni dall'ultimo accesso mediante SCA) per effettuare l'accesso meramente informativo.

Tanto premesso, va sottolineato che l'accesso al conto di pagamento online è avvenuto mediante inserimento delle credenziali statiche , come si desume dalle schermate prodotte (cfr., "*Autenticación con usuario y password personales*" in corrispondenza della voce "*Medio de autenticación*" v. colonna O del file).

Oltre alla protezione data dalle credenziali statiche, l'intermediario ha prodotto documentazione dalla quale si ricava l'invio del codice OTP con SMS sul cellulare del ricorrente collegato al conto. Nelle relative schermate sono indicati anche i codici utilizzati nell'operazione. L'invio degli sms è confermato anche dagli screenshot prodotti dal ricorrente.

Quanto all'esecuzione del bonifico, parte resistente produce documentazione dalla quale si desume che essa ha avuto luogo con l'inserimento dell'Otp. Anche per quanto riguarda tale profilo la ricezione dell'SMS è provata dallo screenshot in cui è indicata la stessa password temporanea.

In ordine alle operazioni di svincolo, l'intermediario ha prodotto evidenze che attestano l'invio del codice OTP, a mezzo SMS, sul cellulare del ricorrente. L'invio degli SMS appare confermato dagli screenshot prodotti dall'istante, contenenti i medesimi codici riportati nelle schermate documentate.

I due SMS non contengono indicazioni di sorta relativamente alle operazioni autorizzate, anche se era onere del ricorrente provare la loro riferibilità ad altre attività.

In proposito, comunque, rileva quanto precisato dal Collegio di Coordinamento nella recente decisione n. 8671 del 23 luglio 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*".



Vero che il Collegio ha precisato che occorre pur sempre predisporre meccanismi di monitoraggio che, sulla base anche dell'analisi della tipicità operativa dell'utente, consentano di individuare operazioni di pagamento, non autorizzate o fraudolentemente poste in essere .

E' anche incontrovertibile, però, che dalle risultanze processuali non emerge alcunché in ordine all'inerzia dell'Intermediario, né parte ricorrente ha anche solo allegato elementi dai quali poterla desumere.

Quanto all'eventuale sussistenza di un contegno del ricorrente tale da consentire la configurabilità di una sua colpa grave , la cui ricorrenza esclude la responsabilità dell'intermediario , ai sensi dell'art. 7 del d lgs n.11.2010 , va rilevato che già dalla descrizione della vicenda truffaldina , effettuata in maniera circostanziata dal ricorrente nel suo atto introduttivo di questo procedimento e nella denuncia da lui presentata e qui prodotta , risulta evidente che le operazioni sono state compiute a causa di una sua condotta gravemente e significativamente superficiale.

Occorre anzitutto rilevare che l'illecito è stato consumato con una pluralità di richieste del terzo.

Ognuna di esse ha dato il suo contributo causale al conseguimento dello scopo truffaldino. E tuttavia proprio la constatazione che l'azione criminosa non si è esaurita col compimento di un solo atto evidenzia che parte ricorrente, non appena ricevuta la prima telefonata da parte del soggetto sconosciuto, ha avuto la possibilità di prendere contatto con la sua banca e di acquisire informazioni esaurienti in ordine alla provenienza della chiamata telefonica e, soprattutto, alla sussistenza effettiva degli accessi, dal truffatore prospettati per ottenere la consegna delle credenziali del conto.

Una cautela , questa, che è ragionevole supporre sarebbe stata praticata da chiunque si fosse trovato in una situazione simile, tenuto anche conto che almeno da due lustri è stata intensificata la campagna di informazione con cui gli istituti bancari cercano di provocare nel cliente una maggiore consapevolezza circa i rischi che si corrono quando qualcuno chiede le credenziali, solitamente spacciandosi per un dipendente e prospettando anomalie dannose tali da spingere il cliente ad assecondare le richieste di accesso.

E' dunque evidentemente configurabile una condotta gravemente colposa che, comportando l'esclusione della responsabilità del prestatore di servizi finanziari, ai sensi dell'art. 7 citato, rende infondata la pretesa di attribuire a parte resistente la responsabilità dell'operazione e di ottenere, oltre al rimborso, anche il risarcimento dei danni.

D'altra parte, il contratto che disciplina il servizio, versato in atti dallo stesso intermediario, prevede un massimale per ciascuna operazione di bonifico Sepa ordinario di € 6.000,00, regola che, nel contesto specifico, assurge a misura di cautela a presidio della sicurezza del pagamento. Nel caso di specie, i truffatori, dopo avere svincolato i fondi occorrenti, hanno eseguito in unica soluzione un bonifico di oltre € 9.000; sul punto, l'intermediario non fornisce alcun chiarimento né elemento idoneo a giustificare la deroga al limite contrattuale. Quindi, anche a fronte della condotta non esente da colpa del cliente, questi ha diritto ad ottenere l'immediata restituzione dell'importo sottratto per la parte eccedente gli € 6.000.

Occorre sottolineare peraltro che l'intermediario ha dedotto che l'intera somma, bloccate prima che fossero messe a disposizione del beneficiario, non sono state restituite al ricorrente, dal momento che l'autorità giudiziaria, che ne aveva richiesto il blocco, non ne aveva ancora autorizzato il trasferimento.

Ha soggiunto di averla sollecitata senza esito, dichiarando che avrebbe messo le somme a disposizione del ricorrente, *"nel più breve tempo possibile"*, dopo il loro sblocco da parte dell'Autorità procedente .

Da queste dichiarazioni si ricava l'ammissione, da parte dell'intermediario, di essere



Arbitro Bancario Finanziario  
Risoluzione Stragiudiziale Controversie

Decisione N. 27 del 02 gennaio 2025

tenuto a restituire al ricorrente le somme in questione . Ne è conferma, peraltro , la sua richiesta di declaratoria di cessazione della materia del contendere , dal momento che essa presuppone logicamente l'implicito riconoscimento che il cliente ha diritto di ricevere le somme , una volta sbloccate.

### **P.Q.M.**

**In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo di € 3.000,00 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

Firmato digitalmente da  
GIUSEPPE LEONARDO CARRIERO