

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) PERLINGIERI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNI PERLINGIERI

Seduta del 31/03/2026

FATTO

Con il ricorso del 18 ottobre 2025, si riferisce che

- il 20 giugno 2025, la società ricorrente, titolare di un conto corrente con funzioni di *internet banking*, riceveva tre sms provenienti dalla banca, con i quali gli veniva comunicato l'inserimento di bonifici da € 8.100,00, € 1.900,00 e € 2.700,00, mai disposti dal cliente;
- nelle ore successive, tali comunicazioni risultavano non più visualizzabili, essendo probabilmente rimosse dai malfattori;
- subito dopo i primi messaggi la ricorrente era raggiunta da diverse telefonate provenienti da un sedicente operatore della resistente; in particolare, era intrattenuto in una conversazione telefonica per oltre un'ora e 34 minuti avente a oggetto eventuali accessi da parte di terzi e presunte procedure di annullamento dei bonifici, con frequenti attese giustificate come 'tempi tecnici';
- durante la telefonata l'interlocutore forniva al ricorrente dati riservati del conto, inclusi numero della carta d'identità, recapito telefonico e parole segrete, convincendolo della genuinità della chiamata; lo avvisava anche della necessità di aggiornare l'app, tentativo che il ricorrente provava a fare senza riuscirci; il cliente non eseguiva alcuna procedura di autenticazione: non chiamava il numero verde e non riceveva messaggi OTP, quindi non autorizzava alcun bonifico;
- terminata la chiamata, il ricorrente contattava il reale Servizio Antifrode, riferendo l'accaduto e chiedendo il blocco dei bonifici;
- in tale sede, gli veniva comunicato che i conti destinatari erano intestati a soggetti sconosciuti e veniva rassicurato sull'immediato intervento;

- a seguire, dall'estratto conto risultava che il bonifico di € 1.900,00 era stato recuperato perché si trattava di un giroconto verso altro suo conto; quello di € 2.700,00 era stato stornato per mancanza di provvista; mentre quello da € 8.100,00 era stato eseguito e rimaneva sottratto;
 - durante l'esecuzione dei bonifici, il ricorrente non poteva controllare le notifiche, contattare la filiale o accedere all'app, poiché la sua linea era occupata. L'Ufficio Reclami afferma che i bonifici sarebbero stati autorizzati alle 13:01:03, alle 15:05:05 e alle 15:15:48, ma non spiega come il cliente, impegnato in telefonata dalle 11.54 alle 13.28, possa aver inserito OTP e chiamato tre volte il numero verde dell'intermediario;
 - il ricorrente non ha mai cliccato alcun *link*, né autorizzato alcuna operazione: nel momento in cui riceveva gli *alert*, i truffatori erano già entrati nel suo *internet banking* e stavano effettuando trasferimenti non autorizzati, impedendogli di intervenire;
 - la vicenda è riconducibile al fenomeno del *phishing*, con acquisizione fraudolenta di credenziali e utilizzo illegittimo dei sistemi bancari, mentre la prevenzione – basata su riconoscimenti digitali e autenticazioni forti – non è stata garantita dal sistema della banca.
- L'istante si rivolge al Collegio per ottenere il rimborso dell'importo fraudolentemente sottratto, pari € 8.100,00, trattandosi di operazione posta in essere da terzi a seguito della compromissione dei sistemi di sicurezza dell'intermediario, senza alcun concorso del correntista.
- Con controdeduzioni dell'1 dicembre 2025, si costituisce la banca convenuta, per precisare che
- il ricorrente, titolare e legale rappresentante della società intestataria di due conti sui quali risultano attivi i servizi di *internet banking* con *secure call*, effettuava le operazioni contestate attraverso il sistema di Strong Customer Authentication previsto contrattualmente, che richiede, ai fini dell'accesso, l'inserimento di User ID e *password* e la chiamata dal numero certificato al Numero Verde, e, per le operazioni dispositive, un ulteriore OTP generato tramite *secure call*;
 - dai *log* estratti dai sistemi informatici risulta che il 20 giugno 2025, alle ore 12:44, veniva effettuata una *secure call* e che l'ID Utente corrispondente a quello del ricorrente veniva correttamente inserito;
 - successivamente, alle 12:59 era inserito il bonifico di € 8.100,00, anch'esso registrato correttamente; al riguardo, la banca evidenzia che la *secure call* delle 13:01 conferma la validazione dell'operazione tramite il numero certificato del ricorrente;
 - dalla medesima analisi dei *log* risulta inoltre che alle ore 13:03 era disposto un secondo bonifico di € 1.900,00 con causale '*giroconto*', verso un conto intestato allo stesso Cliente; tale operazione attivava il meccanismo delle domande di sicurezza, ulteriore presidio antifrode di iniziativa della banca, che prevede la somministrazione casuale di due domande scelte tra sei definibili in fase di *enrollment*; anche in questo caso il Cliente forniva al primo tentativo risposte corrette;
 - alle ore 13:05 era poi fornita la relativa autorizzazione tramite *secure call*;
 - infine, alle ore 13:14, il ricorrente disponeva un terzo bonifico istantaneo di € 2.900,00 verso un conto cointestato con la moglie: anche qui risultano effettuate una *secure call* e due domande di sicurezza, entrambe correttamente risolte, e l'operazione viene autorizzata alle 13:15;
 - due dei tre bonifici contestati erano eseguiti a favore dello stesso ricorrente o del suo nucleo familiare, circostanza indicativa dell'assenza di una truffa sofisticata;
 - per tutte le operazioni, venivano inviati sms *alert* al numero certificato del Cliente, e la banca adotta un'articolata politica informativa antifrode con avvisi *online* e comunicazioni, che il sistema impone al Cliente di visionare tramite flag;
 - la denuncia non chiarisce come si sarebbe verificato l'evento fraudolento;
 - il Cliente non produce i presunti messaggi civetta, sostenendo addirittura che sarebbero stati rimossi dai malfattori, mentre – contraddittoriamente – risultano ancora memorizzati i successivi messaggi contenenti gli OTP delle 12:55, 13:01 e 13:05;
 - i numeri telefonici da cui il Cliente afferma di aver ricevuto le chiamate non sono collegabili all'Istituto e manca ogni evidenza di urgenza o sofisticazione dell'asserita frode, rilevando come il Cliente abbia comunque dato seguito a comunicazioni anomale nonostante due dei tre bonifici avessero come

beneficiario lui stesso;

- tutte le operazioni erano regolarmente autorizzate mediante SCA, i sistemi non subivano alcuna compromissione e l'evento è imputabile esclusivamente alla colpa grave del ricorrente per aver seguito le indicazioni di sedicenti operatori.

In conclusione, la banca chiede che il ricorso sia rigettato. In via subordinata, per il caso in cui si dovesse ravvisare una responsabilità della banca, chiede di tener conto del comportamento colpevole e imprudente del ricorrente, rilevante ai fini di un concorso di colpa ex art. 1227 c.c.

Con memorie di replica dell'8 gennaio 2026, il ricorrente contesta le avverse deduzioni, in quanto incongruenti rispetto ai dati oggettivi. In particolare, dalla lista delle *secure call* emergerebbero anomalie temporali tali da rendere illogica la pretesa autorizzazione consapevole dei bonifici, poiché tra le operazioni indicate intercorrono intervalli tali da comportare la naturale scadenza della sessione di *internet banking*, che avrebbe imposto un nuovo accesso con credenziali e OTP mai effettuati dal cliente. Inoltre, dalle chiamate in uscita del ricorrente non risulta alcuna telefonata verso il numero verde negli orari indicati dalla Banca, mentre risultano solo due brevi chiamate intorno alle 11:51-11:52, non riconducibili a procedure dispositive; al contrario, la cronologia delle chiamate in entrata mostra che alle 11:54 il ricorrente riceveva una telefonata dal numero truffaldino, durata un'ora e trentaquattro minuti, circostanza che rende impossibile che egli potesse, nello stesso arco temporale, chiamare il numero verde, ottenere codici OTP e autorizzare operazioni. Tale circostanza è confermata anche dalla dichiarazione della coniuge, che ha assistito agli eventi e riferito che il cliente, pochi minuti prima delle 12:00, era impegnato in una lunga telefonata con un sedicente operatore antifrode che affermava di bloccare operazioni sospette già disconosciute. Il ricorrente ipotizza che i malfattori, introdottisi nel sistema della banca, abbiano disposto illecitamente i pagamenti senza necessità di carpire credenziali o inviare *link* fraudolenti, essendo già in possesso di tutti i dati del rapporto, comprese parole segrete che avrebbero dovuto essere note solo al titolare. Ribadisce di non aver mai autorizzato né disposto alcuna operazione e osserva che, se avesse intenzionalmente eseguito i bonifici contestati, non avrebbe avuto motivo di denunciarne immediatamente l'illiceità. Alla luce di ciò, l'istante egli insiste nella richiesta di restituzione delle somme sottratte, richiamandosi integralmente alle conclusioni del ricorso.

La banca deposita controrepliche del 29 gennaio 2026, per ribadire che il bonifico istantaneo di € 8.100,00 del 20 giugno 2025 alle ore 12:59 era correttamente eseguito e autorizzato dall'utente. Ricostruiti il sistema di sicurezza e i fattori di autenticazione richiesti, afferma quindi di aver dimostrato l'autenticazione a doppio fattore. Contesta inoltre che la ricostruzione temporale dei fatti offerta dal ricorrente sia incompatibile con i log. Sulle telefonate, la banca evidenzia che quelle ricevute dalla cliente provengono da numerazioni non riconducibili all'Istituto. La cronologia mostra due *secure call* in uscita alle 11:51:08 e alle 11:52:11 e, in parallelo, telefonate da numeri sospetti, con una di durata significativa (oltre 1 ora e 30 minuti), elemento che può integrare un comportamento gravemente colposo del Cliente. La banca eccepisce l'inammissibilità della dichiarazione della coniuge, trattandosi di prova testimoniale non ammessa nel presente procedimento. Infine, richiama quanto già dedotto circa la mancata produzione del messaggio civetta e, più in generale, della scarsa contestualizzazione dei fatti, elemento da cui si può inferire una condotta gravemente colposa del cliente.

DIRITTO

La controversia ha a oggetto la richiesta di accertamento della illegittimità della condotta della banca in relazione ad alcune operazioni contestate. È questione, in particolare, di un bonifico istantaneo di importo pari ad € 8.100,00, eseguito il 20 giugno 2025 e autorizzato tramite c.d. *secure call* proveniente dal numero certificato dal cliente.

Secondo la ricostruzione dei fatti operata dal ricorrente, anche in sede di denuncia/querela, il 20 giugno

2025 riceveva tre sms provenienti dalla banca, con i quali gli veniva comunicato l'inserimento di tre bonifici, rispettivamente da € 8.100,00, € 1.900,00 e € 2.700,00, in vero mai disposti. Nelle ore successive, tali comunicazioni risultavano non più visualizzabili. Subito dopo i primi messaggi, il ricorrente era raggiunto da diverse telefonate provenienti da un sedicente operatore della resistente, una delle quali della durata di oltre un'ora e trentaquattro minuti avente a oggetto eventuali accessi da parte di terzi e presunte procedure di annullamento dei bonifici. Il ricorrente non eseguiva alcuna procedura di autenticazione: non chiamava il numero verde e non riceveva messaggi OTP, quindi non autorizzava alcun bonifico. A ogni modo, terminata la chiamata, il cliente contattava il reale Servizio Antifrode, riferendo l'accaduto e chiedendo il blocco dei bonifici; in tale sede, gli veniva comunicato che i conti destinatari erano intestati a soggetti sconosciuti e veniva assicurato sull'immediato intervento.

A seguire, dall'estratto conto risultava che il bonifico di € 1.900,00 era stato recuperato perché si trattava di un giroconto verso altro conto dell'istante; quello di € 2.700,00 era stato stornato per mancanza di provvista; mentre quello da € 8.100,00 era stato eseguito e rimaneva sottratto.

L'intermediario deduce che l'operatività contestata era eseguita tramite il servizio di *internet banking* dotato di un sistema di autenticazione forte, che prevede che l'accesso avvenga a mezzo di inserimento di *UserId*, *password* e chiamata dal numero di telefono certificato del Cliente al Numero Verde dell'intermediario (c.d. *secure call*); e che, per effettuare un'operazione dispositiva, è necessario l'inserimento di un ulteriore codice OTP generato a seguito della chiamata dal telefono certificato del Cliente al predetto Numero Verde. Il Cliente deve, quindi, chiamare il numero verde e digitare il codice OTP; il sistema *secure call* verifica il numero di cellulare che ha chiamato (in questo caso il numero certificato del ricorrente) e il processo di validazione dell'operazione va a buon fine se viene accertata dal sistema la corrispondenza tra numero cellulare abilitato, contratto e codice OTP digitato.

L'intermediario produce i *log* relativi alla fase di accesso, dai quali emerge una chiamata *secure call* delle 12:44:28, e, a seguire, un accesso all'area riservata di *internet banking* alla data e all'ora di disposizione del bonifico disconosciuto di € 8.100,00 (ore 12:59 del 20 giugno 2025). Produce anche documentazione relativa all'operazione di bonifico, ed evidenza della *secure call* effettuata dal numero certificato del Cliente in corrispondenza del medesimo orario del bonifico (13:01), al fine della validazione della relativa operazione dispositiva.

Sono assolti i fattori della conoscenza e del possesso richiesti dalla normativa europea (regolamento 389/2018/UE).

Per altro verso, la parte ricorrente eccepisce di non aver effettuato la chiamata al numero verde per la *secure call*, atteso che alle ore 13:01, ovvero durante l'esecuzione del bonifico, era impegnato in una telefonata con i malfattori durata un'ora e trentaquattro minuti. A supporto, allega i tabulati telefonici ricevuti dal proprio gestore telefonico, dai quali effettivamente emergono chiamate verso il numero verde della resistente solo alle 11:51 e 11:52, dunque ben prima dell'esecuzione del bonifico, avvenuta alle ore 13:01. Allega anche evidenza della telefonata ricevuta alle ore 11:54 e durata appunto oltre un'ora e mezzo, da cui si evince che al momento dell'esecuzione del bonifico l'utenza certificata del ricorrente era impegnata in un'altra conversazione.

Se è possibile per un truffatore poter eseguire un *spoofing* verso l'intermediario – facendo cioè comparire, nel processo di autorizzazione di *secure call*, come numero chiamante quello del cliente –, viene meno il fattore di autenticazione di possesso legato al numero di cellulare dell'utente, secondo un meccanismo del tutto assimilabile a quello della 'sim swap fraud', nel quale il fattore di possesso (il numero di cellulare del cliente) viene compromesso tramite l'appropriazione, da parte del malfattore, del numero di cellulare certificato mediante la richiesta di emissione di una nuova sim da parte dell'operatore telefonico (Collegio di Torino, decisione n. 4920 del 2024).

Nel caso di specie, il presidio posto dal fattore di possesso viene aggirato tramite il meccanismo dello *spoofing* verso il numero di Secure Call.

È pacifico l'orientamento dell'Arbitro secondo cui la 'sim swap fraud' opera non sul versante della colpa

grave del cliente, ma su quello dell'autenticazione, rendendo in tal modo insufficiente la prova della SCA offerta da parte dell'intermediario. In considerazione, da un lato, del rischio di impresa connesso all'affidamento parziale a terzi soggetti – l'operatore telefonico – della procedura di autenticazione delle operazioni di pagamento (attraverso l'invio dell'OTP con sms su cellulare) e, dall'altro, dell'eventuale emersione anche di fenomeni di *phishing*, il ricorso va accolto integralmente: in tale fattispecie la sostituzione della sim card deve essere infatti equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10, d.lg. n. 11 del 2010.

A eguale soluzione deve giungersi nel caso sottoposto all'attenzione di questo Collegio, tal ch  va accertato il diritto del ricorrente al rimborso delle somme oggetto dell'operazione contestata.

P.Q.M.

In accoglimento del ricorso, il Collegio accerta il diritto della societ  ricorrente alla restituzione dell'importo di € 8.100,00.

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