Repubblica Italiana

# Tribunale di Bologna

**In Nome del Popolo Italiano**

ha pronunciato la seguente

## SENTENZA

resa ai sensi dell'art. 281 sexies ultimo comma cpc

nella causa n. [redacted] tra le parti:

PARTE ATTRICE

- Difesa: Avv.to CONTESSA MARIO PIO;
- Domicilio: VIA CESARE BATTISTI 2 40124 BOLOGNA presso lo studio dell'Avv.to Mario Pio Contessa

PARTE CONVENUTA

in persona della o del legale rappresentante pro-tempore

-
-

Decisa a Bologna il 20/03/2026 sulle seguenti conclusioni:

Parte Attrice:

*"accertare e dichiarare l'inadempimento contrattuale e/o di qualsivoglia altro titolo di [redacted] nei confronti degli attori succitati, nonché la responsabilità unica ed esclusiva di quest'ultima, (Banca presso la quale gli attori hanno acceso il rapporto di conto corrente n. [redacted]) in quanto il citato istituto di credito ha omesso di porre in essere tutte le misure necessarie alla prevenzione delle frodi informatiche - bancarie , disposte dalla legislazione comunitaria - nazionale vigente (in particolare la Strong authentication) e, per l'effetto, Voglia condannare [redacted] S.p.a. al pagamento in favore dei [redacted] dell'importo di € 17.000,00, pari alla somma loro sottratta in data 29/02/2024, oltre interessi non maturati sulle siffatte somme dalla messa in mora fino al saldo; oltre alla rifusione di tutti i danni patiti e*

*patiendi dagli attori che saranno accertati e quantificati dall'Ill.mo Giudice adito in corso di causa e, in ogni caso, alla definizione del presente giudizio"*

Parte Convenuta:

"*IN VIA PRINCIPALE*

*"per tutte le ragioni esposte, respingere le domande tutte ex adverso formulate perché infondate, sia in fatto che in diritto; - per tutte le ragioni esposte, accertare e dichiarare la colpa grave del sig. [illegible] e l'assenza di qualsivoglia responsabilità in capo alla Banca; - per tutte le ragioni esposte in narrativa, accertare e dichiarare la correttezza e la diligenza di operato della Banca, la quale ha sempre operato nel pieno rispetto della PSD2 e del D.lgs. n. 11/2010; - per tutte le ragioni esposte in narrativa, respingere integralmente le domande avversarie volte ad ottenere il "risarcimento del danno" per l'asserita quanto indimostrata responsabilità contrattuale e/o extracontrattuale attribuita alla Banca; IN VIA SUBORDINATA - nella denegata quanto non creduta ipotesi di accoglimento della domanda di [illegible] determinare l'importo dovuto dalla Banca tenendo in debita considerazione il comportamento colpevole ed imprudente tenuto dal sig. [illegible] in data 29 febbraio 2024 rilevante ai fini del concorso di colpa ai sensi dell'art. 1227 c.c., per le ragioni esposte in narrativa"*

## Ragioni di fatto e di diritto della decisione

1. [illegible]

1. di essere cointestatari del conto corrente n. [illegible] acceso presso [illegible] collegato tramite la APP della Banca sul proprio dispositivo *smartphone;*
2. in data 29 febbraio 2024 [illegible] riceveva sul proprio *smartphone* una chiamata dal [illegible] con cui un operatore qualificatosi come dipendente dell'istituto gli chiedeva di confermare se la disposizione operata dal suo conto corrente verso un conto estero (bonifico bancario) fosse stata o meno dallo stesso autorizzata;
3. smentita la provenienza della disposizione, l'operatore confermava l'avvenuto blocco del bonifico e allo stesso tempo l'invito a "*contattare prontamente l'Ufficio Anti - Frode della Banca al numero 02440707805*";
4. contattato l'Ufficio *Anti - Frode*, una voce elettronica richiedeva le credenziali di accesso al conto corrente; nel prosieguo della telefonata la voce elettronica veniva sostituita da quella di un operatore fisico che gli proponeva di implementare immediatamente alcune operazioni dissimulatorie sul conto finalizzate a bloccare il tentativo di frode in atto;
5. in particolare, l'operatore lo invitava prima a impostare una apposita deviazione di chiamata a beneficio del numero [illegible], provare ad effettuare dalla propria applicazione un bonifico verso una banca estera e verificare subito dopo dall'applicazione come in realtà alcuna operazione di bonifico verso l'estero risultasse addebitata sul proprio conto;
6. [illegible] tuttavia in quel frangente non riteneva di impostare la deviazione di chiamata e di procedere al bonifico verso un conto estero;

7. alle 18:33 del medesimo giorno, ricontattato dallo stesso operatore fisico e comparso sul display del suo cellulare il numero di telefono su nuovo invito acconsentiva questa volta di autorizzare la deviazione delle chiamate relative al proprio account associato all'applicazione verso il numero
8. autorizzata la deviazione delle chiamate, da quel momento l'attrice e l'attore non hanno avuto più possibilità di accedere al conto corrente tramite l'applicazione della Banca;
9. a seguito di una segnalazione ricevuta dalla Banca l'1° marzo 2024 gli istanti appuravano che dal loro conto risultavano eseguiti due bonifici verso un conto straniero, rispettivamente di € 14.000,00 e di € 3.000,00.

Secondo la prospettazione di parte attrice, in capo alla Banca convenuta è configurabile una responsabilità fondata sulla carenza dei sistemi di sicurezza utilizzati dovuta all'omessa adozione secondo la vigente normativa di ogni rimedio necessario ad evitare la commissione di truffe informatiche in danno dei clienti.

Le carenze contestate sono riferibili essenzialmente al fatto che l'operazione di modifica del numero di cellulare del ull'account personale, è stata comunicata con una semplice notifica sull'applicazione avente ad oggetto la "*modifica contatti alert*", messaggio che è del tutto incomprensibile a chiunque non sia esperto di ambienti informatici. Il messaggio non contiene chiari dettagli sull'operazione effettuata in quel momento dall'utente. Inoltre, non risulta previsto un sistema di autenticazione differenziato con utilizzo di password distinte rispettivamente per l'accesso via app o home banking. Ancora, la dipendenza esclusiva dall'OTP tramite SMS non consente di fatto di poter verificare la legittimità di un nuovo dispositivo sostituito attraverso una operazione di sostituzione del numero di riferimento effettuabile tramite il portale web.

Pertanto, parte attrice chiede la condanna di pa al risarcimento del danno quantificato in euro 17.000,00 oltre interessi dalla messa in mora al saldo.

si difende eccependo:

1. i bonifici di euro 3.000,00 ed euro 14.000,00 effettuati in data 29 febbraio 2024 risultano autorizzati da parte d dal proprio dispositivo *smartphone,* previo l'utilizzo delle credenziali personalizzate del correntista e con l'inserimento del PIN personale all'interno della "*APP*" della Banca installata e associata all'utenza del Cliente;
2. entrambe le disposizioni bancarie sono state precedute dalla modifica del contatto certificato associato all'utenza internet banking de ossia dal numero del suo cellulare operazione questa avvenuta mediante un processo multifattoriale con SCA;
3. i File di *Log* versati in atti dalla Banca provano che le operazioni di modifica del contatto certificato del o, di attivazione di una nuova APP su un nuovo dispositivo e le disposizioni di bonifico oggetto di contestazione sono state tutte correttamente autenticate, registrate e contabilizzate mediante corretto utilizzo del doppio fattore di autenticazione;
4. i File di *Log* dimostrano che la Banca ha sempre e tempestivamente inviato sui contatti certificati del le comunicazioni/*alert* informative riferite a

ciascuna delle operazioni tempo per tempo richieste/eseguite tramite internet banking.

Secondo la prospettazione di parte convenuta la responsabilità della frode subita dalle parti istanti è da ascrivere esclusivamente al comportamento gravemente negligente di [redacted] il quale, fornendo le proprie credenziali personalizzate abbinate alla propria utenza, di fatto ha collaborato attivamente con il terzo frodatore consentendo a terzi ignoti di poter effettuare dal proprio conto corrente le operazioni di bonifico contestate.

Pertanto, [redacted] chiede il rigetto della domanda.

2.

La domanda è fondata.

Il giudizio verte sull'accertamento della responsabilità e degli obblighi restitutori o risarcitori dell'intermediario finanziario e del destinatario del pagamento in caso di frode, ad opera di terzi ignoti, in relazione a disposizioni avvenute tramite strumenti elettronici, quali l'home banking, non volute dal titolare del conto.

Il D.lgs. 27/01/2010 n. 11 modificato dal D. Lgs. 15 dicembre 2017 n. 218 attribuisce ai prestatori di servizi di pagamento i rischi derivanti dalle condotte fraudolente dei terzi che simulano un consenso del pagatore, dando quindi avvio ad una operazione non voluta dal titolare delle somme: la maggiore capacità dei prestatori di servizi di pagamento di elaborare meccanismi sicuri di gestione e trasmissione del consenso, nonché di tempestiva ed esatta esecuzione degli ordini di pagamento come ricevuti, comporta una responsabilità aggravata degli stessi ove abbiano dato seguito ad un'operazione non autorizzata e i relativi rischi di impresa comportano l'obbligo in capo agli stessi, di assicurare che le credenziali di autenticazione attribuite ai propri clienti "non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento" e di prevenire i "rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate" (artt. 8 e 11 D.lgs. n. 11 del 2010).

Per altro verso, le utenti e gli utenti del servizio devono:

1) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati;
2) comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza, in particolare, tale ultima disposizione consente al prestatore di servizi di pagamento di comprendere, per tempo, la discrasia tra consenso e manifestazione procedimentalizzata dello stesso;
3) adottare "*tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate*" (art. 7 n. 2, D.lgs. n. 11 del 2010).

Con riferimento alla prova di autenticazione ed esecuzione delle operazioni di pagamento, nel caso di operazioni di pagamento eseguite senza il consenso dell'utente ma effettuate dal prestatore di servizi a seguito della corretta ricezione di un ordine, l'art. 10 D.lgs. n.

11/2010 pone sulla banca l'onere di 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; nel caso di mancato assolvimento dell'onere probatorio, l'intermediario è tenuto a riaccreditare immediatamente e, in ogni caso, al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito, l'importo sottratto sul conto corrente del cliente, secondo quanto previsto dall'art. 11 del D. Lgs. 11/2010.

Sul punto, secondo la giurisprudenza di legittimità, *"la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente" (cfr. Cass. Sez. III sent.3780/2024 e nello stesso senso sent. 18045/2019 e ordin. n.26916/2020).*

In un caso analogo a quello per cui si controverte, nella già menzionata sentenza n. 3780/2024, si legge che "la diligenza della banca va a coprire operazioni che devono essere ricondotte nella sua sfera di controllo tecnico, sulla base anche di una valutazione di prevedibilità ed evitabilità tale che la condotta, per esonerare il debitore, la cui responsabilità contrattuale è presunta, deve porsi al di là delle possibilità esigibili della sua sfera di controllo". Nella vicenda in esame, la Cassazione ha ritenuto idoneo a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento l'invio al titolare della carta di appositi sms alert di conferma di ogni singola operazione.

Nel caso di specie, non è in contestazione l'invio di due specifici alert riferiti all'attivazione della deviazione di chiamata a beneficio del numero necessaria per impartire le disposizioni di bonifico su un altro dispositivo:

a) Messaggio SMS del 29.02.2024 alle ore 18: 44:31 al – "Gentile Cliente, abbiamo ricevuto la richiesta di inserire il nuovo numero non l'hai richiesto tu, contatta il Servizio Clienti";
b) Messaggio MAIL del 29.02.2024 alle ore 18: 44:31 alla casella - OGGETTO Modifica recapito telefonico da profilo personale "ti confermiamo che il numero di cellulare stato inserito in data 29/02/24 alle ore 18.44. Se non hai richiesto tu l'inserimento di questo numero, contatta con urgenza il Servizio Clienti. Ti ricordiamo che nessun operatore della Banca ti chiamerà mai per chiederti un'OTP o un codice ricevuto via SMS. Se ricevi una notifica che ti avvisa di una modifica al tuo profilo che non hai effettuato tu, ti invitiamo a bloccare la Strong Authentication per impedire accessi non autorizzati alla tua posizione".

Entrambi i messaggi risultano inviati dalla Banca alla stessa ora del medesimo giorno (ore 18: 44:31 del 29.02.2024), ma il loro contenuto informativo è, con tutta evidenza, diverso.

Più in particolare, il secondo messaggio (b) è perfettamente efficace nel disvelare il tipo di meccanismo decettivo attivato nel caso di specie ("Se non hai richiesto tu l'inserimento di questo numero, contatta con urgenza il Servizio Clienti. Ti ricordiamo che nessun operatore della Banca ti chiamerà mai per chiederti un'OTP o un codice ricevuto via SMS. Se ricevi una notifica che ti avvisa di una modifica al tuo profilo che non hai effettuato tu, ti invitiamo a bloccare la Strong Authentication per impedire accessi non autorizzati alla tua posizione").

Sennonchè, questo messaggio è stato inviato sulla mail, che non è detto sia il canale di ricevimento delle comunicazioni più immediatamente accessibile, sia perché non è scontato che vi sia la notifica sullo smartphone, sia perché se vi è una contestuale comunicazione su sms è lecito supporre che la comunicazione sulla mail sia dello stesso tenore (cosa che, tuttavia, non era), ciò che potrebbe suggerire di non aprire la notifica eventualmente ricevuta, sia perché non è detto che i server di posta elettronica siano sempre funzionanti.

Il tenore del messaggio via SMS è più generico e, in relazione alla tipologia di meccanismo decettivo avvenuta nel caso di specie (indirettamente confermata anche dalla narrativa di parte convenuta, che dà atto in particolare del cambio di contatto telefonico), resta del tutto compatibile con la rappresentazione della realtà alterata dal raggiro ("Gentile Cliente, abbiamo ricevuto la richiesta di inserire il nuovo numer l'hai richiesto tu, contatta il Servizio Clienti").

Esistendo dunque una via "migliore" per ingenerare nel cliente un forte sospetto in merito alla genuinità del contatto e quindi spingerlo ad adottare "..tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate" (art. 7 commi 1 e 2 D.lgs. n. 11 del 2010), cioè, in base a quanto sopra detto, mandare su sms (posto che era indubitabile che il cliente stesse, manovrato da altri, agendo con il telefono in mano) lo stesso messaggio mandato invece sulla mail, non può ritenersi assolto l'onere probatorio gravante sul prestatore di servizi di dimostrare di aver avvisato il cliente in modo adeguato a consentirgli di intraprendere le opportune contromisure per attuare il blocco degli accessi non autorizzati alla sua posizione.

La responsabilità aggravata per i prestatori di servizi di pagamento ex D.lgs. 27/01/2010 n. 11 modificato dal D. Lgs. 15 dicembre 2017 n. 218 implica l'allocazione nella sfera giuridico-patrimoniale dei medesimi dei rischi derivanti dalle condotte fraudolente dei terzi che simulano un consenso del pagatore, quindi l'equivalente economico della provvista sottratta (qui non in contestazione nel *quantum*).

La particolare insidiosità di questo meccanismo di truffa esclude il concorso del danneggiato nella causazione del fatto lesivo.



3.

Le spese di lite seguono la soccombenza e sono liquidate, come da dispositivo, secondo i parametri di cui al DM n. 147 /2022, fase istruttoria e decisionale nei minimi.

**P.Q.M.**

Il Tribunale di Bologna definitivamente pronunciando, così provvede:

1) condanna pagare a parte attrice euro 17.000,00, oltre rivalutazione e interessi dal 29 febbraio 2024 a titolo di risarcimento del danno patrimoniale;
2) condanna rifondere in favore di parte attrice le spese di lite, liquidate in euro 3.650,00 (di cui 264,00 per esborsi e il resto per compensi) oltre spese generali, imposta e contributi.

Bologna, 20/03/2026

Il giudice

Paolo Siracusano