REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

Il Tribunale di Monza, Prima Sezione Civile, nella persona del Giudice monocratico, dott. Carlo Albanese, ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. R.G. 321/2025 promossa

DA

Parte_1 C.F. *C.F._1* , residente in Paderno Dugnano, via Sciesa n. 3, elettivamente domiciliato presso l'indirizzo pec: *Email_1* intestato all'Avv. Francesco Panunzi che lo rappresenta e difende, anche disgiuntamente con l'Avv. Enrico Francolini, come da procura posta in calce al ricorso introduttivo;

RICORRENTE

NEI CONFRONTI DI

Controparte_1 C.F. *P.IVA_1* e P.I. *P.IVA_2* , con sede in *CP_1* , via Rovagnati n. 1, in persona del procuratore speciale Avv. *Controparte_2* elettivamente domiciliata in Milano, via Francesco Sforza n. 15 presso lo studio dell'Avv. Fabio Civale che lo rappresenta e difende come da procura posta in calce alla comparsa di costituzione e risposta;

RESISTENTE

Oggetto: Condanna al risarcimento del danno subito per inadempimento contrattuale.

CONCLUSIONI DELLE PARTI

Per l'udienza del l5.1.2026, nel richiamare quelle rassegnate nei rispettivi atti costitutivi, le parti hanno precisato le seguenti conclusioni:

PER *Parte_1*

"*Voglia l'Ill.mo Tribunale adito, contrariis reiectis:*

1) per le ragioni di fatto e di diritto di cui al ricorso che precede, condannare il *Controparte_1* *[...]* *in persona del legale rapp.te pro tempore, alla restituzione in favore del Sig.* *Parte_1* *dell'importo di € 40.000,00 addebitatogli con l'operazione non autorizzata oggetto del presente ricorso, mediante riaccredito con data valuta al 16 novembre 2022 ex art. 11, primo comma,*

D. Lgs. 11/2010, ovvero, in subordine, della minor somma che sarà ritenuta di giustizia, in ogni caso oltre:

- interessi legali sulla sorte, ex art. 1284, primo comma, c.c., dal reclamo del 22 novembre 2022 al deposito del ricorso (€ 3.100,00);

- interessi legali sulla sorte, ex art. 1284, quarto comma, c.c., dal deposito del ricorso al saldo.

2) con vittoria delle spese e dei compensi del presente giudizio e del procedimento ad esso prodromico tenutosi dinanzi all'Arbitro Bancario Finanziario, oltre forfait spese generali al 15%, iva e cpa come per legge, da distrarsi in favore dei sottoscritti difensori che se ne dichiarano antistatari".

PER IL *Controparte_1*

"*Voglia l'Ill.mo Tribunale adito, contrariis rejectis, previa ogni più ampia ed opportuna declaratoria, così giudicare:*

IN VIA PRELIMINARE

- accertare e dichiarare l'inammissibilità, improponibilità, improcedibilità del ricorso ex art. 281-undecies c.p.c. per i motivi illustrati in narrativa ovvero accertare e dichiarare che le difese svolte dalle parti richiedono un'istruzione piena per i motivi illustrati in narrativa e, ai sensi dell'art. 281-duodecies c.p.c., disporre con ordinanza non impugnabile la prosecuzione del processo nelle forme del rito ordinario (stante la complessità della causa) fissando l'udienza di cui all'art. 183 c.p.c., rispetto alla quale decorrono i termini previsti dall'art. 171-ter c.p.c.;

NEL MERITO

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. *Pt_1* *e l'assenza di qualsivoglia responsabilità in capo a* *CP_1* *;*

- per tutte le ragioni esposte in narrativa, accertare e dichiarare la correttezza e la diligenza di operato di *CP_1* *;*

IN VIA SUBORDINATA

- nella denegata quanto non creduta ipotesi di accoglimento della domanda attorea, determinare l'importo dovuto da *CP_1* *tenendo in debita considerazione il comportamento colpevole ed imprudente tenuto dal sig.* *Pt_1* *rilevante ai fini del concorso di colpa ai sensi dell'art. 1227 c.c..*

IN VIA ISTRUTTORIA

Con ogni riserva di merito e istruttoria.

Con vittoria di spese, competenze e relativi compensi unici, oltre oneri accessori come per legge.

Il tutto liquidato ai sensi e per gli effetti D.M. 55/2014, con maggiorazione ex art. 4, comma 1-bis D.M. 55/2014".

IN FATTO

Parte_1 ha convenuto in giudizio, con le forme del rito semplificato di cognizione, il proprio istituto di credito chiedendone la condanna alla restituzione della somma di € 40.000,00 indebitamente sottrattagli con un bonifico bancario indebitamente effettuato da terzi previa utilizzazione, senza alcuna preventiva autorizzazione, delle credenziali del proprio conto corrente bancario.

Al fine di censurare l'operato del *Controparte_1* ha richiamato i seguenti eventi verificatisi in data 16.11.2022 e nelle giornate immediatamente successive deducendo, in particolar modo:

- che il 16.11.2022 aveva ricevuto sulla propria utenza telefonica mobile un s.m.s. proveniente dalla società NEXI, emittente la carta di credito in uso e collegata al proprio conto corrente bancario intrattenuto presso il *Controparte_1*
- che tale messaggio era collocato all'interno della pregressa cronologia di s.m.s. inviategli dal medesimo intermediario NEXI e riportava il seguente contenuto: "*NEXI informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web*" nonché un *link* che rinviava ad una pagina *web* identica a quella dell'intermediario, così come evincibile dal documento n. 3 prodotto unitamente al ricorso;
- che egli, titolare di una carta di credito emessa da NEXI, nutrendo il fondato timore di non poter più operare attraverso tale strumento di pagamento, quotidianamente utilizzato, aveva acceduto al sito internet riportato all'interno del messaggio utilizzando il *link* ivi indicato;
- che, tuttavia, dopo pochissimi istanti aveva ricevuto un secondo messaggio con cui era stato informato che di lì a breve sarebbe stato contattato da un operatore al fine di poter ripristinare la normale funzionalità del proprio strumento di pagamento e, difatti, così era stato, essendo stato chiamato sulla propria utenza telefonica mobile da un asserito operatore di NEXI, il quale gli aveva riferito la necessità di disinstallare dal proprio telefono l'applicazione del *Controparte_1* *[...]* in quanto causa del blocco della carta di credito: il tutto era avvenuto senza alcuna necessità di fornirgli un **c**odice dispositivo o un OTP autorizzativo trattandosi della mera disinstallazione di un'applicazione dal proprio *smartphone*;
- che, nel corso della telefonata, era pervenuto sul proprio cellulare un s.m.s. di conferma, anch'esso ricevuto a valle della genuina corrispondenza con NEXI, con cui si invitava il cliente ad attendere 1/3 giorni lavorativi prima di reinstallare nuovamente l'applicazione della banca: ad esso aveva, poi, fatto seguito un ulteriore s.m.s. di avviso di un appuntamento telefonico per il giorno 17.11.2022, alle ore

13:00, nel corso del quale era stato informato della prossima risoluzione dei problemi tecnici con fissazione di un nuovo appuntamento per la giornata successiva;

- che il 18.11.2022, nuovamente contattato da un sedicente operatore NEXI, gli era stato riferito essere ancora in corso le verifiche tecniche e della necessità di attendere ancora un paio di giorni prima di procedere con l'installazione dell'applicazione al fine di accedere al proprio conto corrente *on-line*;

- che solo in tale occasione, insospettito dalle insolite lungaggini negli accertamenti tecnici effettuati, non aveva dato seguito alle istruzioni ricevute, autonomamente reinstallando l'applicazione del *[...] CP_1* ed apprendendo solo allora, senza avere ricevuto alcuna notifica da parte della banca, dell'esecuzione di un bonifico di € 40.000,00, mai autorizzato, in favore di tale "*Persona_1*" sull'IBAN IT18U0760103200001061464473 di *CP_3* avente la seguente causale: "*acquisto trilocale*";

- che nella medesima occasione aveva scoperto dell'avvenuta modifica, effettuata da terzi, dell'indirizzo di posta elettronica ove avrebbe dovuto essergli comunicata l'avvenuta esecuzione delle operazioni e la deviazione delle chiamate in entrata su un altro numero di telefono cellulare, il tutto con lo scopo di agevolare, senza che il titolare del conto potesse avvedersene, l'intento criminoso di eseguire operazioni fraudolente prive del consenso di quest'ultimo;

- che, proposte sia una denuncia-querela contro ignoti che un reclamo avverso il comportamento, gravemente inadempiente, posto in essere *CP_1* e NEXI, con decisione emessa in data 25 maggio 2023, l'ABF aveva disposto che l'intermediario corrispondesse in proprio favore la somma di € 40.000,00, oltre interessi maturati sino al saldo effettivo, decisione rimasta inattuata stante la mancata spontanea esecuzione del *CP_1* e la necessità di instaurazione del presente giudizio.

Sulla scorta di tali allegazioni ha imputato all'istituto di credito di non avere adottato, nell'ambito della propria responsabilità di tipo contrattuale così come delineata dalla normativa vigente, tutte le misure idonee a garantire un adeguato livello di sicurezza ai fini dell'accesso al proprio *home banking* e per l'esecuzione di pagamenti.

Nel costituirsi in giudizio il *CP_1* ha contestato l'avversa pretesa risarcitoria, sostenendo di avere adottato, nel pieno rispetto della normativa approntata dal legislatore comunitario e nazionale, un sistema di autenticazione c.d. "forte" per la procedura di login all'*home banking* del proprio cliente e per l'autorizzazione delle disposizioni di pagamento, eccependo ulteriormente la sussistenza di una colpa grave imputabile a quest'ultimo.

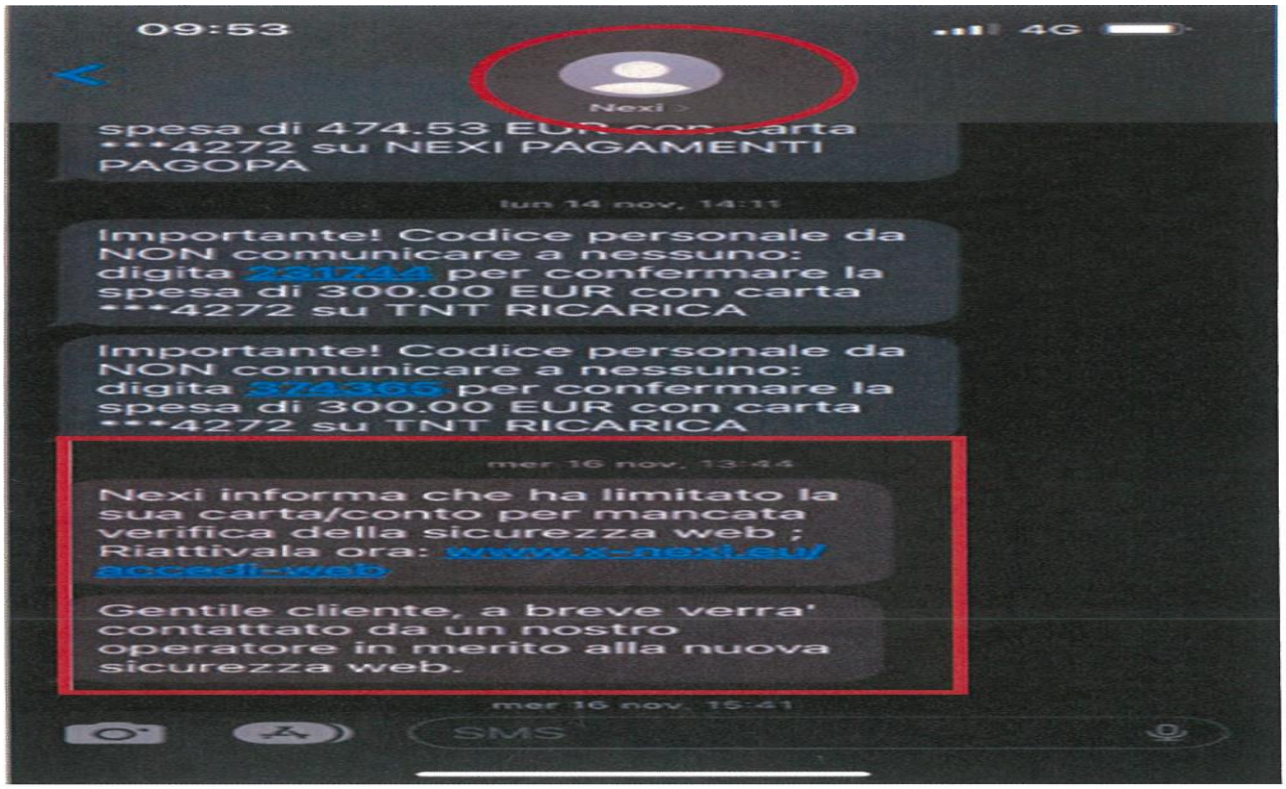
Senza svolgimento di alcuna attività istruttoria, neppure essendo stata richiesta la concessione dei termini di cui all'art. 281 *duodecies*, comma 4, c.p.c., riassegnato il fascicolo al presente magistrato, all'udienza del 15.1.2026, previa discussione orale ai sensi dell'art. 281 *sexies* c.p.c., la causa è stata

trattenuta in decisione con riserva di deposito della sentenza integrale nel termine previsto dal terzo comma.

IN DIRITTO

Alla luce della documentazione prodotta ritiene il Tribunale che la domanda proposta dal ricorrente, volta ad ottenere il rimborso, da parte dell'intermediario resistente, della somma di € 40.000,00 indebitamente sottrattagli dal conto corrente a sé intestato con un bonifico bancario effettuato da terzi rimasti non identificati con la tecnica dello "spoofing", sia fondata e per le ragioni di seguito esposte debba essere accolta.

Prima di dare conto delle ragioni della fondatezza della pretesa risarcitoria avanzata dal correntista è, tuttavia, opportuno rilevare non essere contestato in giudizio che ai danni di *Parte_1* si sia concretizzata un reato di truffa, seppur ne siano stati rimasti sconosciuti gli autori, e che altrettanto pacifiche sono le seguenti modalità di esecuzione dell'evento criminoso, così come già sommariamente delineate nella superiore premessa, anch'esse non specificamente contestate dalla società resistente e che è opportuno ritracciare: in data 16 novembre 2022 il cliente ha, infatti, ricevuto il seguente s.m.s. (apparentemente) proveniente dall'intermediario NEXI, emittente della propria carta di credito, con cui gli sono state rappresentate delle limitazioni sullo strumento di pagamento utilizzato e sul conto corrente d'appoggio con invito a cliccare su un link al fine di risolvere il problema[1].

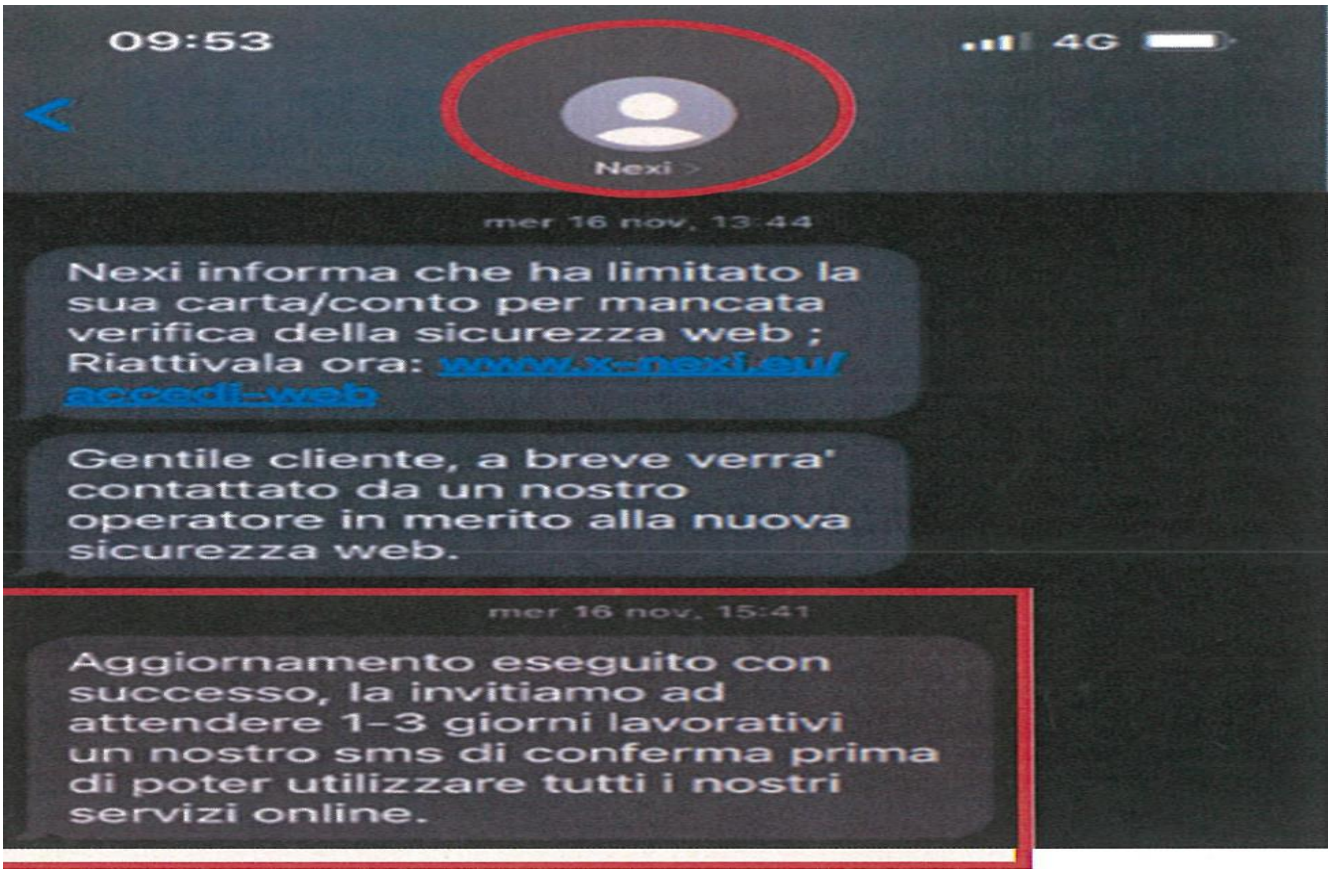


[1] Tal è il tenore letterale del messaggio ricevuto: il seguente contenuto: "*NEXI informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web*".

Come si vede, dalla superiore schermata e in conformità a quanto dedotto da parte attrice, il messaggio era effettivamente inserito all'interno della cronologia dei messaggi precedenti che non è contestato in giudizio gli fossero stati recapitati dal medesimo intermediario NEXI con conseguente ragionevole affidamento del cliente in ordine alla veridicità di quanto comunicatogli.

Eseguito l'accesso, è stato re-indirizzato ad ana pagina web anch'essa (apparentemente) identica a quella dell'intermediario NEXI e, ricevuta una telefonata proveniente da un sedicente operatore asseritamente riconducibile al medesimo intermediario del quale aveva seguito tutte le indicazioni, ha disinstallato l'App del *Controparte_1* *Parte_2* smartphone, la quale è stata individuata quale causa del blocco della carta.

Ha ricevuto, quindi, un s.m.s. di conferma, per effetto del quale era stato invitato ad attendere 1-3 giorni prima di utilizzare nuovamente i servizi on-line, il tutto come si evince dalla seguente schermata:



A tale messaggio sono seguiti ulteriori s.m.s. di fissazione di ulteriori appuntamenti telefonici con l'operatore, in data 18.11.2022 è stato nuovamente contattato e da quest'ultimo informato che sarebbe stato necessario attendere ancora un paio di giorni prima di poter re-installare l'applicazione.

Solo a questo punto, insospettito per un tale insolito ritardo, ha provveduto a reinstallarla scoprendo, una volta avuto accesso al proprio conto *on-line*, l'avvenuta esecuzione di un bonifico di € 40.000,00 -

da sé mai autorizzato – effettuato in favore di terzi soggetti a sé non riconducibili. Il tutto, altrettanto pacificamente, è intervenuto previa modifica dell'indirizzo e-mail cui sono state indirizzate le comunicazioni dell'intermediario ed alterazione della funzionalità telefonica, essendo stata disposta una deviazione delle chiamate in entrata presso un diverso dispositivo.

Non essendo stata la superiore dinamica specificamente contestata dalla resistente, ciò che è necessario ponderare in questa sede ai fini dell'accertamento della responsabilità contrattuale imputata al *CP_1 [...]* è se siano state da quest'ultimo approntate a tutela del proprio cliente tutte le misure idonee a garantirgli la sicurezza dell'accesso ai propri sistemi informatici e se, di contro, lo stesso comportamento tenuto da *Parte_1* sia stato connotato o meno da colpa grave, tendo ben conto che la disciplina normativa in tema di gestione dei servizi bancari di pagamento è contenuta nel d. lgs. n. 11/2010, emanato in recepimento della direttiva europea 2007/64/CE, c.d. PSD -Payment *CP_4* Directive, successivamente modificato dal d. lgs. n. 218/2017, entrato in vigore il 13 gennaio 2018, in attuazione della c.d. direttiva PSD2.

Orbene, se l'art. 7 della normativa richiamata delinea quali sono gli obblighi posti a carico dell'utente, ovverosia l'utilizzo degli strumenti di pagamento in conformità al contratto, la tempestiva comunicazione alla banca in caso di smarrimento, furto, appropriazione indebita o uso non autorizzato del proprio strumento di pagamento, l'adozione di misure idonee a garantire la sicurezza e l'adeguata custodia dei dispositivi in dotazione, l'art. 8 individua quelli posti a carico del prestatore del servizio, tra i quali, in particolar modo trattandosi di un soggetto professionale al contrario dell'utente-consumatore, la necessità di assicurare che i dispositivi "*non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento*".

La normativa impone alla banca di adottare le misure più idonee, alla luce ed in linea con lo sviluppo tecnologico, volte ad impedire l'utilizzo abusivo dello strumento di pagamento.

Ed è proprio al fine di innalzare i livelli di sicurezza e chiarire gli obblighi minimi posti a carico dei prestatori dei servizi che la direttiva PSD2, n. 2015/2366/UE, recepita dall'Italia con d. lgs. n. 218/2017, ha introdotto la c.d. autenticazione forte del cliente (Strong Customer Authentication - SCA), asseritamente rispettata dal *CP_1*, ovverosia una procedura volta alla convalida dell'identificazione di un utente che si fonda sull'uso di due o più elementi di autenticazione (c.d. "autenticazione a due fattori"), appartenenti ad almeno due tra le seguenti categorie:

- conoscenza (qualcosa che solo l'utente conosce, come una password o un PIN);
- possesso (qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone);
- inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale).

Si tratta di elementi che debbono essere tenuti indipendenti tra loro sì che un'eventuale violazione di uno di essi non comprometta necessariamente l'affidabilità degli altri.

Si aggiunga che il d.lgs. n. 11/2010, agli artt. 10 e 12, pone a carico dell'intermediario l'onere di dimostrare che le operazioni disconosciute dal cliente e inerenti al conto corrente siano state autenticate, registrate e contabilizzate correttamente, che le stesse non abbiano subito gli effetti pregiudizievoli di un malfunzionamento delle procedure necessarie per la loro esecuzione e, infine, che l'utente non abbia impedito la verificazione della transazione illecita in violazione dei doveri comportamentali previsti a proprio carico, operando con dolo o colpa grave.

Grava, quindi, al correntista unicamente l'onere di dimostrare la fonte del proprio diritto e l'allegazione dell'abusiva utilizzazione dello strumento di pagamento in proprio danno operando in questa materia, anche in virtù del principio del rischio di impresa e della vicinanza della prova, la regola generale di ripartizione dell'onere della prova previsto in materia di responsabilità contrattuale agli artt. 1218 c.c. e 2697 c.c..

Il creditore che agisce per l'adempimento, la risoluzione e/o, come nella specie, per il risarcimento del danno deve, pertanto, esclusivamente provare la fonte del proprio diritto e allegare l'inadempimento di controparte, spettando al debitore la prova dell'esatto adempimento ovvero di fatti impeditivi, modificativi o estintivi del diritto altrui.

Numerose sono le sentenze emesse in materia dalla Suprema Corte volte a circoscrivere la diligenza dell'intermediario a cui il presente organo giudicante non può non uniformarsi.

Si consideri, ad esempio, la sentenza n. 2950/2017, secondo cui "*(...) anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (ciò che rappresenta interesse degli stessi operatori), appare del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore di servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici da parte di terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo*".

Sullo specifico tema delle truffe realizzate tramite la tecnica del c.d. "spoofing" una recente sentenza della Suprema Corte di Cassazione ha, poi, ulteriormente chiarito che: "*La giurisprudenza di questa Corte è [...] consolidata nel senso di ritenere che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, va esclusa se ricorre una situazione di colpa grave dell'utente configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento ma il riparto*

degli oneri probatori posto a carico delle parti segue il regime della responsabilità contrattuale. Mentre, pertanto, il cliente è tenuto soltanto a provare la fonte del proprio diritto ed il termine di scadenza, il debitore, cioè la banca, deve provare il fatto estintivo dell'altrui pretesa, sicché non può omettere la verifica dell'adozione delle misure atte a garantire la sicurezza del servizio. Ne consegue che, essendo la possibilità della sottrazione dei codici al correntista attraverso tecniche fraudolente una eventualità rientrante nel rischio d'impresa, la banca, per liberarsi dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore" (Cass. civ. n. 3738 del 12/02/2024, conf. a Cass. civ. sez. 1, n. 2950 del 3/2/2017; Cass. civ., sez. 3, n. 18045 del 5/7/2019; Cass. civ., sez. 6-3, n. 26916 del 26/11/2020).

Sulla scorta di tali principi, la responsabilità dell'istituto di credito può, quindi, escludersi o attenuarsi solo qualora nel comportamento del cliente sia ravvisabile un profilo di colpa grave il quale, con tutta evidenza, va rigorosamente provato dall'intermediario, chiamato in tal caso a fornire - come detto ed in ottemperanza ai principi dell'onere della prova in materia contrattuale - anche la dimostrazione di aver adottato ogni misura idonea a garantire la sicurezza del servizio offerto.

E, a ben vedere, è proprio una tale prova a non essere stata adeguatamente offerta dalla resistente come si evince, d'altro canto, già solo da quanto acclarato nella decisione assunta sul medesimo caso quivi in esame dall'ABF di Milano nella seduta del 25.5.2023, prodotta dal ricorrente al documento n. 4, utilizzabile e valutabile ai fini del decidere unitamente a tutti gli ulteriori elementi documentali rispettivamente allegati, e, in particolar modo, dalle seguenti locuzioni riportate alle pagine 4 e 5:

"*Il Collegio, venendo allo specifico caso oggetto di decisione, rileva che l'intermediario afferma che l'operazione disconosciuta sia stata preceduta dall'accesso al conto e dalla registrazione di un nuovo dispositivo sull'app, con attivazione del servizio "smart OTP"; dall'accesso all'app dal nuovo dispositivo e dalla modifica dell'indirizzo e-mail associato all'utenza; dall'ulteriore accesso all'app dal nuovo dispositivo per l'esecuzione del bonifico disconosciuto.*

Quanto al login e alla registrazione di un nuovo dispositivo, con attivazione del servizi o "smart OTP", l'intermediario sostiene che il processo di enrollment prevede sempre l'inserimento di Utenza + Password + otp ricevuto via SMS, tuttavia non produce alcuna evidenza dell'inserimento di questa sequenza (Utenza + Password + PIN) né vi è evidenza dell'inserimento dell'OTP, o dell'invio dello stesso sul cellulare del cliente; inoltre, in relazione all'attivazione della licenza sul nuovo dispositivo i log riportano la dicitura ESITO = OK, che parrebbe indicare il buon fine dell'operazione, ma non è prodotta alcuna legenda al riguardo.

Quanto all'accesso, la legenda specifica che, ai fini del login, l'applicazione richiede l'inserimento di Utenza + Password + PIN e che la dicitura ESITO = 000 conferma l'inserimento di tutti i parametri di

sicurezza previsti, tuttavia, dall'esame dei log è emerso che non vi è evidenza dell'inserimento di Utenza + Password + PIN e che l'esito dell'evento è uguale a 0, quindi un risultato che non evidenzia l'inserimento corretto di tutti i parametri di sicurezza.

Quanto all'accesso all'app e alla modifica dell'indirizzo e-mail, dall'esame dei log si rileva che non vi è evidenza dell'inserimento di Utenza + Password + PIN ai fini dell'accesso, né dell'inserimento del PIN ai fini della variazione dei dati personali e che l'esito dell'evento è uguale a 0, quindi un risultato che non evidenzia l'inserimento corretto di tutti i parametri di sicurezza.

Infine, in relazione all'esecuzione del bonifico disconosciuto, avvenuto alle ore 15.53, subito dopo il login, nella legenda l'intermediario rappresenta che detta transazione è avvenuta con inserimento del PIN dispositivo per autorizzare l'operazione che viene riepilogata mediante notifica in APP, ma dall'esame dei log si rileva che non vi è evidenza dell'inserimento del PIN ai fini dell'autorizzazione del bonifico e che l'esito dell'evento è uguale a 0, quindi un risultato che non evidenzia l'inserimento corretto di tutti i parametri di sicurezza.

Il Collegio, per tutto questo, esclude che si possa considerare raggiunta la prova della corretta autenticazione richiesta all'intermediario, rendendo, allora, irrilevante qualunque valutazione in merito alla condotta tenuta dalla ricorrente. L'intermediario, pertanto, deve sopportare tutta l'operatività disconosciuta, incrementata, come richiesto, degli interessi dal reclamo al saldo".

In particolare, alla luce di quanto riportato agli ultimi tre capoversi si evince come l'esito dell'accesso all'App e dell'esecuzione del bonifico non evidenzi l'inserimento corretto di tutti i parametri di sicurezza e, a ben vedere, ciò non è neppure smentito dalla relazione di parte prodotta dalla resistente al documento di cui alla lettera A), a maggior ragione se si considera che, scorrendo la documentazione prodotta dall'istituto di credito su cui la medesima perizia è fondata, si evince come la stessa coincida quasi integralmente con quella già prodotta dal *CP_1* nel procedimento conclusosi innanzi all'ABF e, in particolare:

- il documento n. 1, "*contratto conto corrente sig.* *Pt_1* , era già stato prodotto come documento n. 1 (cfr. il documento n. 5 del ricorrente, pagine 17 e seg.);
- il documento n. 2, "*accordo quadro servizi di banca telematica DesioLine*", era già stato prodotto come documento n. 2 (documento n. 5, pagine 40 e seg.);
- il documento n. 3, "all*egato tecnico File Log* *CP_1* *, non citato nella Consulenza Tecnica di cui al doc. a*", era già stato prodotto come documento n. 3 (documento. 5, pagine 47 e seg.);
- il documento n. 3a, "*evidenza bonifico contestato*", era già stato prodotto come doc. 3a (cfr. documento n. 5, pagina 50);

- il documento n. 3b, "di*chiarazione conformità Allegato tecnico File Log CP_1 di cui al doc. 3*", è una mera dichiarazione di conformità del documento n. 3a;
- il documento n. 4, "*denuncia del Cliente*", era già stato prodotto come documento n. 4 (cfr. il documento n. 5, pagina 51);
- il documento n. 5a, "*modulo ricorso ABF sig. Pt_1* , era già stato prodotto come documento n. 5a (cfr. documento n. 5, pagine 56 e seg.);
- il documento n. 5b, "*ricorso ABF sig. Pt_1* , era già stato prodotto come documento n. 5b (cfr. documento n. 5, pagine 65 e seg.);
- il documento n. 6, "*comunicazione Banca – Cliente relativa a cambio indirizzo email*", era già stato prodotto come documento n. 6 (cfr. documento n. 5, pagina 74);
- il documento n. 7, "*comunicazione Banca – Cliente relativa a cambio indirizzo email*", era già stato prodotto come documento n. 7 (cfr. documento n. 5, pagina 75);
- il documento n. 8, "*reclamo Cliente*", era già stato prodotto come documento n. 8 (cfr. documento n. 5, pagina 76 s.);
- il documento n. 9, "*comunicazione presa in carico del reclamo da parte della Banca*", era già stato prodotto come documento n. 9 (cfr. documento n. 5, pagina 78);
- il documento n. 10, "*riscontro al reclamo CP_1* ", era già stato prodotto come documento n. 10 (cfr. documento n. 5, pagine 79 e seg.);
- il documento n. 11, "*evidenza rubrica Banca – no coincidenza n. 025465744 con numeri della Banca*", era già stato prodotto come documento n. 11 (cfr. documento n. 5, pagina 82);
- i documenti n. 11a, "*evidenza da internet di no coincidenza n. 025465744 con numeri della Banca*", e 11b, "*evidenza da internet di no coincidenza n. 3512368729 con numeri della Banca*", non erano stati prodotti ma consistono in una mera "*schermata google*" che non pare assumere alcuna rilevanza ai fini del decidere;
- il documento n. 12, "*evidenza rubrica Banca – no coincidenza n. 3512368729 con numeri della Banca*", era già stato prodotto come documento n. 12 (cfr. documento n. 5, pagina 83);
- il documento n. 13, "*comunicazione «La tua sicurezza è la nostra priorità»*", era già stato prodotto come documento n. 13 (cfr. documento n. 5, pagina 84);
- il documento n. 14 "*evidenza presa visione della comunicazione di cui al doc. 13 da parte del Cliente*", era già stato prodotto come documento n. 14 (cfr. documento n. 5, pagina 86);
- il documento n. 15, "Pop *Up «Attenzione alle Truffe»*", era già stato prodotto come documento n. 15 (cfr. documento n. 5, pagina 87);

- il documento n. 16, "*evidenza lettura Pop Up di cui al doc. 15 da parte del Cliente*", era già stato prodotto come documento n. 16 (cfr. documento n. doc. 5, pagina 88);
- il documento n. 17, "*evidenza sistema SMS Alert*", era già stato prodotto come documento n. 17 (cfr. documento n. 5, pagina 89);
- il documento n. 18, "*evidenza recall Banca*", era già stato prodotto come documento n. 18 (cfr. documento n. 5, pagina 90);
- il documento n. 19, "*esito negativo recall Banca*", era già stato prodotto come documento n. 19 (cfr. documento n. 5, pagina 91).
- i documenti n. 20, "*controdeduzioni ABF Banca*", e 21, "*controrepliche ABF Banca + allegati*", erano già stati prodotti ed esaminati dall'ABF, come si evince dalla medesima decisione depositata in questa sede.

Sulla scorta della pronuncia emessa dall'ABF di Milano il documento cui essa fa principalmente riferimento è quello n. 3 ri-depositato in questa sede, (il quale alla legenda di cui alla terza pagina testualmente recita: "*ESITO = 000 --> l'evento è confermato correttamente con inserimento di tutti i parametri di sicurezza previsti dal Servizio richiamato dall'applicazione*") e, unitamente ad esso, a riprova della correttezza delle informazioni ivi riportate, in questa sede il *CP_1* *CP_5* ha prodotto, quale allegato 3b, la seguente dichiarazione di conformità a firma *Testimone_1*, dell'ufficio Sicurezza *Controparte_1*: "*Con la presente si dichiara che i log relativi al contenzioso in oggetto (doc. n. 3), estratti dai sistemi di registrazione log dell'applicativo di home bamking (ovvero i sistemi coinvolti nella disposizione di un pagamento da Internet Banking), sono stati convertiti in formato PDF mantenendo inalterato il loro contenuto e sono pertanto da ritenersi una copia conforme all'originale*".

Ne consegue la correttezza di quanto affermato dall'ABF nella superiore decisione, il cui esito può essere posto a fondamento del decidere, emergendo dall'esame dei log e dal seguente estratto del documento n. 3 (di cui sono state omesse le ultime due colonne in quanto non rilevanti), non esservi evidenza dell'inserimento del PIN ai fini dell'autorizzazione del bonifico in quanto l'esito dell'evento è uguale a 0, cioé un risultato che non evidenzia l'inserimento corretto di tutti i parametri di sicurezza:

Canale	Codice ABI	Utente	Codice Servizio	TimestAmp Chiamata	Divisa	Esito	Evento	Importo
mobile	3440	03440 I6250	BONIFICO SEPA	16-NOV-22 03.53.10.331000 000 PM	EUR	0	AUTORIZZA	40000

L'intermediario non ha, quindi, assolto gli oneri probatori previsti per l'esclusione della prpopria responsabilità contrattuale da inadempimento.

Volendo in ogni caso esaminare il comportamento dell'utente al fine di appurarne un'aventuale corresponsabilità, peraltro integrabile solo da colpa grave, è opportuno evidenziare che costante giurisprudenza arbitrale (cfr. in tal sensi il Collegio di Milano, decisione n. 5716/2023; Collegio di Torino, decisioni n. 3653/2023 e n. 16048/2022) ritiene che l'eventuale negligenza del cliente possa venire in rilievo solo qualora l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert.

Sebbe questione sarebbe in astratto irrilevante, essendosi escluso che l'intermediario abbia adottato le adeguate misure di sicurezza volte a scongiurare quanto di fatto verificatosi, ritiene il Tribunale che il *CP_1* non abbia fornito la prova di una specifica condotta colposa posta in essere dalla cliente.

La fattispecie in esame è, infatti, qualificabile quale truffa realizzata tramite sms *spoofing*, misto a ID *caller spoofing*. Tale modalità di azione è considerata potenzialmente più decettiva ed insidiosa rispetto al comune phishing, che si ritiene possa essere, invece, contrastato con l'uso di una diligenza minima, in considerazione della sua diffusione e della generalmente scarsa idoneità a trarre in inganno i clienti.

Tale inquadramento fattuale rileva proprio ai fini della valutazione giuridica del comportamento posto in essere dal ricorrente notoriamente affermandosi che, allorquando il truffatore abbia adottato un sistema tecnicamente sofisticato, operi una presunzione di assenza della colpa in capo al soggetto truffato, "a *meno che non si rinvengano […] indici di inattendibilità o anomalia del messaggio; in tale caso potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'atro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario*" (cfr. in tal senso ABF Roma 1° settembre 2022 n. 12005).

Ancora, nel fenomeno del c.d. spoofing il cliente "fisiologicamente" comunica a terzi truffatori le credenziali di accesso al proprio conto online; è, infatti, la modalità standard tramite la quale vengono compiute tali truffe (non per altro la truffa è definita come reato a cooperazione con la vittima) sicché la comunicazione a terzi delle credenziali di accesso al proprio conto può essere indice di colpa grave del ricorrente solo ove le modalità ed il contesto nel quale la comunicazione venga compiuta rendano la stessa espressiva di manifesta negligenza inescusabile (cfr. sul punto Tribunale di Milano, sez. VI, n. 322 del 18/01/2023).

Ebbene, ritiene il Tribunale che il ricorrente abbia tenuto comportamenti diligenti e idonei a evitare azioni truffaldine a proprio danno o, quantomeno, che non siano ravvisabili nel comportamento tenuto profili di colpa grave.

Come, infatti, si evince dagli *screen-shot* sopra riportati ha verificato che il messaggio ricevuto provenisse dal consueto contatto dal quale aveva già ricevuto comunicazioni relative al rapporto in essere con NEXI e l'utente che l'ha contattato si è identificato come operatore bancario sicché non v'era alcuna ragione per ritenere sospette le superiori circostanze.

Nonostante il diligente comportamento del cliente, ripetutamente contattato alla medesima utenza, la truffa ha avuto esito positivo proprio in quanto finemente architettata e particolarmente insidiosa e ciò esclude che si tratti di una semplice truffa a cui la ricorrente avrebbe potuto sottrarsi con l'uso della ordinaria diligenza.

Accertato, pertanto, che la resistente non abbia fornito prova evidente e apprezzabile della corretta autenticazione e del corretto funzionamento del sistema forte (come richiesto ai sensi del d.lgs. 11/2010) e, nemmeno, la responsabilità per colpa grave del ricorrente, la domanda risarcitoria volta al ristoro del pregiudizio subito per effetto dell'indebita effettuazione del bonifico datato 17.11.2022 va accolta, con conseguente condanna del *Controparte_1* a restituirgli la somma pari ad € 40.000,00 oltre interessi nella misura prevista dall'art. 1284, comma 1, c.c. maturati a decorrere dalla data di proposizione del ricorso innanzi all'ABF di Milano e nella maggior misura prevista dall'art. 1284, comma 4, c.c. maturati a decorrere dalla data di deposito del ricorso introduttivo del presente giudizio sino a quella del saldo effettivo.

Le spese del giudizio, da distrarsi in favore del procuratore antistatario, seguono la soccombenza e vengono liquidate come da dispositivo sulla scorta dei compensi medi previsti dal D.M. n. 55/2014, come integrato dal D.M. n. 147/2022, per le sole fasi concretamente espletate di esame e studio, introduttiva e decisoria.

Non sussistono, di contro, i presupposti per la rifusione delle spese stragiudiziali sostenute nell'ambito del procedimento arbitrale stante la non indispensabilità di farsi assistere da un difensore.

P.Q.M.

Il Tribunale di Monza, Prima Sezione Civile, definitivamente pronunciando, ogni diversa istanza ed eccezione disattesa o assorbita, così dispone:

1. in accoglimento della domanda proposta, condanna il *Controparte_1* in persona del lgale rapp.te *p.t.*, a corrispondere in favore di *Parte_1* la complessiva somma di € 40.000,00, oltre interessi nella misura prevista dall'art. 1284, comma 1, c.c. maturati a decorrere dalla data del 20.2.2023 e, nella maggior misura prevista dall'art. 1284,

comma 4, c.c., a decorrere dalla data del 20.1.2025 sino a quella del saldo effettivo;

2. condanna il *Controparte_1* in persona del lgale rapp.te *p.t.*, a rifondere in favore di *Parte_1* le spese di lite sostenute nell'ambito del presente giudizio che, liquidate in complessivi € 6.345,00, di cui 545,00 per spese esenti e 5.800,00 per compensi, oltre 15% per rimborso forfettario C.P.A. ed I.V.A., come per legge, vanno distratte in favore dell'Avv. Francesco Panunzi, dichiaratosi antistatario;
3. rigetta ogni ulteriore domanda.

Così deciso in Monza in data 19 gennaio 2026

Il Giudice

dott. Carlo Albanese