N. 5956/2022 R.G.

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

TRIBUNALE ORDINARIO DI PERUGIA

Il Tribunale di Perugia - sezione II civile -, in composizione monocratica, in persona del Giudice Dott. Federico Fiore ha pronunciato la seguente

SENTENZA

nella causa iscritta al n. 5956 R.G. dell'anno 2022

tra

rappresentati e difesi per delega allegata all'atto di citazione dall'Avv. Maria Laura Ficola presso il cui studio in Foligno, Via Rutili 12, sono elettivamente domiciliati

- attori -

contro

per sona del direttore co rappresentata e difesa per delega allegata alla comparsa di costituzione e risposta dall'A presso il cui studio in Roma, Via Barbieri 6 e elettivamente domiciliata .

- convenuta

avente ad oggetto: Bancari (deposito bancario, cassetta di sicurezza, apertura di credito bancario, anticipazione bancaria, conto corrente bancario, sconto bancario).

CONCLUSIONI DELLE PARTI

All'udienza del 3.2.2026:

per l'avv. Maria Laura Ficola sostituita

dall'Avv. " *in via preliminare chiede la rimessione in istruttoria e l'accoglimento delle istanze istruttorie nella ipotesi in cui i fatti di ausa non venissero ritenuti incontestati o documentalmente dimostrati, in ogni caso insiste per l'accoglimento delle conclusioni come precisate precisata nella memoria ex art 183, 6° comma n. 1 c.p.c.." ;*

per l S ostituito dall'A mini il quale " *precisa le conclusioni riportandosi a quelle rassegnate nella co parsa di costituzione e risposta ed in via istruttoria per il rigetto delle richieste avverse già rigettate, per le ragioni di cui alla terza memoria istruttoria."*

RAGIONI IN FATTO E IN DIRITTO DELLA DECISIONE

1.1 Con atto di citazione notificato il 23.12.2022 l M hanno convenuto in giudizio innanzi al Tribunale di Perugia la a. per ottenere il rimborso delle somme illegittimamente prelevate dal proprio conto corrente per un importo di euro 49.232,21 oltre rivalutazione monetaria ed interessi di mora.

Gli attori hanno allegato di essere cointestatari del conto corrente n. 5102002697 presso la Banca convenuta cui accedevano da remoto tramite applicazione sui loro telefoni cellulari i cui numeri erano conosciuti dalla Filiale della Banca presso la quale era stato aperto il conto. In data 1 aprile 2022, alle ore 16:19:54, all'utenza telefonica del iungeva un messaggio SMS dal numero di , dal quale provenivano abitualmente le comunicazioni della Banca convenuta dal seguente tenore: " *informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web. Riattiva ora http://aderisci.live/*". Successivamente il 7 aprile 2022 alle ore 16:38:45 perveniva altro messaggio SMS sempre dal numero di con il quale " *Informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web. Riattiva qui http://clicca-ora.live/*" . Allarmato dall'imminente blocco del servizio il apriva il link presente sul messaggio SMS della delle ore 16:38:45, ed era così indirizzato alla pagina web dove veniva visualizzato un pannello di accesso alla Banca I on la richiesta delle proprie credenziali. Seguendo le

indicazioni fornitegli dalla procedura guidata della pagina WEB della Banca E , la pagina restituiva un errore di accesso mostrando un'ulteriore maschera con la possibilità di compilare una richiesta di supporto inserendo il proprio recapito telefonico per ricevere assistenza dalla Banca. Conclusa la procedura di richiesta di supporto tecnico, il l ceveva alle ore 16:56:37 una chiamata dal numero + 39 060060, numero di Assistenza Clienti , cui il si rivolgeva usualmente per informazioni di varia natura. L'operatore, qualificatosi come addetto servizio clienti L, rappresentava al di aver riscontrato delle anomalie sul conto corrente, invitandolo, a cancellare l'applicazione installata sul cellulare per reinstallarla subito dopo, nonché ad eseguire le istruzioni che gli sarebbero state successivamente inviate dalla l tramite messaggi SMS. Seguiva quindi l'invio di una serie di SMS a logo sempre l , contenenti i passaggi da eseguire (indirizzo link; codici numerici da inserire) che l'attore effettuava seguendo le indicazioni dell'operatore che restava al telefono. Al termine delle operazioni l'operatore chiedeva al i di aspettare per circa 24 ore per l'invio da parte del servizio assistenza della Banca E dell'ultimo codice necessario a riavviare in sicurezza l'applicazione, previo contatto della Banca. Il giorno seguente il non essendo stato contattato per l'orario stabilito dall' addetto della Banca chiamava la Banca convenuta al numero di Assistenza Clienti +39 06 0060 il quale lo informava che era stata perpetrata ai suoi danni una frode informatica, con prelievo dal conto corrente della pressoché integrale somma ivi giacente pari ad Euro 49.232,21, attraverso un'unica disposizione di pagamento a mezzo bonifico bancario a favore dell'iban IT 19E0760103400001059936417 intestato a tale K e con la causale "*acconto acquisto casa*" . L'attore chiedeva, pertanto, il blocco immediato di qualsiasi disposizione di pagamento dal proprio conto non autorizzata né da lui né dalla , ricevendo, tuttavia, risposta da parte dell'operatore che non era possibile bloccare l'operazione. Veniva quindi bloccata qualsiasi credenziale del conto e carte ad esso connesse, risultando nei giorni successivi impossibile per i clienti accedervi . In data 8 aprile 2022 il l sporgeva una prima denuncia innanzi alla Questura di Perugia per il tramite del padre,

, essendo sia lui sia la moglie positivi al Covid-19 .In data 9 aprile 2022 gli attori inviavano formale comunicazione alla Banca per il tramite del proprio legale richiedendo, a titolo risarcitorio, l'integrale restituzione dell'importo sottratto ai sensi e per gli effetti di cui al D.Lgs n. 11/2010, come modificato dal D.Lgs 15 dicembre 2017, n. 218 e della normativa unionale di riferimento. In data 13 aprile 2022, risultando ancora bloccato l'accesso al conto, il Sig. L , non appena uscito dalla quarantena da Covid-19, si recava alla propria Filiale per avere copia cartacea degli estratti del conto e della lista movimenti e con successiva missiva del 14 aprile 2022 disconosceva formalmente le annotazioni riportate negli estratti conto e nella lista movimenti consegnatigli dalla Banca, segnatamente in merito all'operazione di bonifico del 7.04.2022 di Euro 49.232,21 Nella medesima giornata, inoltre, il presentava in proprio una seconda denuncia-querela presso la Questura di Perugia

La Ba sl procedeva a riscontrare la prima missiva di richiesta di risarcimento danni del 9 aprile 2022 nella data del 27 aprile 2022 negando ogni sua responsabilità verso i clienti invocando la esimente di cui all'art. 7, comma 4 D.lgs 11/2010.

Nel maggio del 2022, il Sig. i ha incaricato una società specializzata di eseguire copia forense del dispositivo cellulare su cui si era consumata la frode, nonché dei vari messaggi SMS e telefonate ricevuti. Nella relazione peritale che ne seguiva l'episodio occorso all'attore veniva inquadrato dal perito quale ipotesi di "*spoofing*", concretizzantesi quando un malintenzionato invia deliberatamente informazioni false per presentarsi con l'ID di altro utente.

Dall'analisi tecnica emergeva che si trattava di applicazione malevola tipo *Trojan* atta a sviare gli SMS e la messaggistica relativa ai permessi con mittente . Ed in tal modo era consentito l'accesso al codice cliente e al pin per disporre e completare il bonifico. In data 17 novembre 2022 gli attori attivavano il procedimento di mediazione ex D.lgs 28/2010 al quale la Banca convenuta comunicava di non voler aderire.

Per tali motivi gli attori chiedevano l'accoglimento delle seguenti conclusioni "…. - - *ACCERTARE E DICHIARARE la responsabilità della E ro*

S.p.a. per i fatti di cui è causa e per le ragioni espresse, alla luce delle norme che vengono in rilievo sotto concorrenti profili per come evidenziati in atto, accertando e dichiarando che la disposizione di pagamento realizzatasi sul conto corrente n. 5102 002697 degli attori in data 7.04.2022 di Euro 49.232,21 a favore di iban IT 19E0760103400001059936417 con nominativo .

e causale "acconto acquisto casa" non è stata autorizzata dagli attori né è a loro riferibile; per l'effetto

- CONDANNARE B s.r.l., in persona del legale rappresentante pro tempore, alla corresponsione a favore degli attori, anche a titolo risarcitorio, della somma di Euro 49.232,21 ovvero alla diversa somma che verrà ritenuta, oltre interessi legali di mora dalla data della diffida (9.04.2022), e comunque, ai sensi dell'art. 1284 c.c., dalla data della domanda sino ad effettivo soddisfo, nonché rivalutazione monetaria dal dovuto sino a soddisfo, anche a titolo di maggior danno ex art. 1224, comma secondo c.c. per i fatti e motivi espressi.

Riservata a separato giudizio la richiesta dei maggiori danni subiti e subendi dagli attori.

In ogni caso: con vittoria di spese e compensi, oltre spese generali, cpa e iva come per legge.".

1.2 La B [illegible] S.p.a. si costituiva in giudizio in data 10.7.2023 contestando la sussistenza della invocata responsabilità nella vicenda occorsa agli attori ed allegando che l'accesso al proprio servizio di *home banking* era possibile tramite apposita *app* B[illegible] o tramite il sito *web* B[illegible].it e prevedeva l'utilizzo di una combinazione di fattori statici, quali il PIN, noto solo al cliente, e dinamici codice *OTP* generato dal *mobile token*. Secondo la convenuta, quindi i propri sistemi erano assolutamente sicuri ed inviolabili da parte di soggetti estranei al cliente titolare del rapporto bancario salvo che il cliente stesso non fornisca spontaneamente a terzi le proprie credenziali riservate ovvero altri mezzi per accedere al proprio conto corrente, come avvenuto da parte del [illegible]i, consentendo loro di operarvi liberamente. La Banca riteneva l'assenza di una propria condotta colposa stante l'adeguatezza dei sistemi di sicurezza informatica utilizzati quali il sistema di sicurezza forte, conforme

alla normativa europea PSD II, attuata dal d.lgs. 27/2010 e che gli attori fossero stati vittima di una frode informatica di tipo phishing evoluto, realizzata mediante una combinazione di messaggi SMS fraudolenti apparentemente provenienti dalla banca (smishing), contatti telefonici con sedicenti operatori bancari (vishing) e con la manipolazione del mittente e dei contatti (spoofing). Il tuttavia aveva cliccato su un link malevolo ricevuto via SMS, inserito le proprie credenziali bancarie su un sito clonato della Banca, disinstallato volontariamente l'app ufficiale B ed istallato un'applicazione fraudolenta, "*BancaSicura*" che aveva consentito a terzi di intercettare SMS e codici OTP inviati dalla Banca. .Tali condotte, emergenti anche dalla consulenza tecnica di parte attrice, costituivano, pertanto, una evidente violazione degli obblighi di diligenza e custodia delle credenziali personali previsti dal contratto e dalla normativa di settore (artt 7- 10- 10-bis e art. 12, comma 4 del D.Lgs 11/2010) e le predette operazioni non erano riconducibili a malfunzionamenti imputabili alla banca i cui sistemi informatici non erano stati compromessi. La Banca evidenziava, inoltre, che tali modalità di frodi erano state oggetto di campagne di informazione con le quali si invitavano i clienti a non fornire a nessuno i codici segreti e personali necessari per l'accesso ai servizi di home banking, né tantomeno scaricare applicazioni diverse dalla quella ufficiale .

Sosteneva, infine, di avere esperito le attività di recupero presso la banca destinataria del bonifico, una volta allertata dell'avvenuta frode, senza tuttavia riuscire nell'intento

Per questi motivi il convenuto p.a.chiedeva l'accoglimento delle seguenti conclusioni "…. - *in via principale, respingere, perché infondate in fatto e in diritto, tutte le domande formulate dai Sigg.ri*

i per le ragioni dedotte in narrativa;

- *in ogni caso, con vittoria di spese e competenze di causa"*

1.3 All'esito della prima udienza di comparizione e trattazione del 11.7.2023 venivano assegnati alle parti i termini perentori previsti dall'art. 183, 6°comma c.p.c.. La causa era, quindi, istruita documentalmente rigettandosi all'udienza del 11.7.2024, le istanze istruttorie formulate dagli attori venendo fissata l'udienza per la

precisazione delle conclusioni. A seguito del mutamento del Giudice assegnatario del fascicolo la causa perveniva all'udienza del 3.2.2026 nella quale i procuratori delle parti precisavano le rispettive conclusioni, come in epigrafe indicate, ed il Giudice tratteneva la causa in decisione, assegnando i termini di legge per il deposito delle comparse conclusionali.

****

In via preliminare si osserva che per consolidata giurisprudenza della Suprema Corte, il Giudice, nel motivare concisamente la sentenza secondo i dettami di cui all'art. 118 disp. Att., non è affatto tenuto ad esaminare specificamente ed analiticamente tutte le questioni sollevate dalle parti, ben potendosi egli limitare alla sola trattazione delle questioni - di fatto e di diritto - *"rilevanti ai fini della decisione"* concretamente adottata, di modo che le restanti questioni non trattate non andranno necessariamente ritenute come "omesse" ben potendo esse risultare semplicemente assorbite (ovvero superate) per incompatibilità logico giuridica con quanto concretamente ritenuto provato dal giudicante. Difatti, si richiama sul punto il principio e enunciato dalla giurisprudenza di legittimità, in base a cui "*la conformità della sentenza al modello di cui all'art. 132 n. 4 c.p.c., e l'osservanza degli art.115 e 116, c.p.c., non richiedono che il giudice di merito dia conto dell'esame di tutte le prove prodotte o comunque acquisite e di tutte le tesi prospettate dalle parti, essendo necessario e sufficiente che egli esponga, in maniera concisa, gli elementi in fatto ed in diritto posti a fondamento della sua decisione, offrendo una motivazione logica ed adeguata, evidenziando le prove ritenute idonee a confortarla, dovendo reputarsi per implicito disattesi tutti gli argomenti, le tesi e i rilievi che, seppure non espressamente esaminati, siano incompatibili con la soluzione adottata e con l'iter argomentativo seguito*" (Cassazione civile , sez. III, 27 luglio 2006, n. 17145).). Inoltre, sempre in via preliminare, vengono in questa sede integralmente richiamate le ordinanze istruttorie rese in corso di causa e quindi vengono rigettate tutte le istanze istruttorie riproposte dalle parti in sede di precisazione delle conclusioni.

Tanto premesso la domanda proposta in giudizio da parte degli attori concerne il risarcimento del danno patrimoniale a titolo di responsabilità contrattuale imputabile

alla Banca convenuta in ordine alla articolata frode informatica compiuta ai danni degli attori il cui conto corrente è stato sostanzialmente svuotato con un unico bonifico bancario disposto in data 7.4.2022 ad opera di terzi e formalmente disconosciuto da parte degli attori. Gli attori hanno, infatti, richiesto in via principale l'accertamento della responsabilità della Banca convenuta allegando che la disposizione di pagamento effettuata sul proprio conto corrente n. 5102002697 del 7.4.2022 per euro 49.232,21 non era stata da loro autorizzata né tantomeno ad essi riferibile.

Le modalità attraverso cui la truffa informatica si è svolta non sono controverse ragion per cui la causa è stata ritenuta documentalmente istruita senza necessità di ricorrere ad ulteriori approfondimenti istruttori richiesti dagli attori nella propria seconda memoria istruttoria. In particolare la consulenza informatica prodotta dagli attori e non oggetto di contestazione da parte della convenuta ha accertato che (doc. 6 fascicolo degli attori) :" *Dai fatti riferiti e dall'analisi del contenuto del dispositivo risulta che il committente utilizzava attraverso lo SmartPhone la regolare applicazione di Banca* *e riceveva le notifiche relative alle operazioni bancarie in una specifica conversazione SMS, con intestatario denominato appunto "I* *". Infatti in tale conversazione SMS è possibile visionare alcuni dei messaggi di notifica inviati dalla banca nel periodo recente – il primo risale al 10/01/2022 - a fronte della normale e regolare operatività. Tale canale di comunicazione con la banca ed il relativo contenuto veniva perciò ritenuto "sicuro" dal committente poiché abitualmente utilizzato dall'istituto per trasmettere al proprio cliente le sopra citate notifiche. un primo SMS fraudolento che contiene un avviso di limitazione della carta/conto per la mancanza di una verifica di sicurezza ed un link per la riattivazione del servizio:"* *informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web. Riattiva ora http://aderisci.live/".*

Il cliente dava credito a questo messaggio, in quanto pervenuto, come affermato in precedenza, attraverso un canale di comunicazione ritenuto sicuro, cioè mediante un SMS nella conversazione usuale di Banca *, ma non eseguiva alcun attività per la mancata esigenza, nell'immediato, di utilizzare il proprio conto.*

Con le stesse modalità in data 07/04/2022 alle ore 16:38:45(UTC+2) è presente un ulteriore SMS fraudolento ricevuto, che contiene il medesimo avviso di limitazione della carta/conto anche se con un link diverso dal precedente: ". Informa che ha limitato la sua carta/conto per mancata verifica dellasicurezza web. Riattiva qui http://clicca-ora.live/".

Tali SMS rappresentano a tutti gli effetti l'origine della frode: non sono stati inviati da Banca ı ma dai truffatori, utilizzando tecniche definite di "spoofing" per manipolare il mittente del messaggio in modo da impersonare l'istituto ed ottenere la completa fiducia del cliente.

Nello specifico gli SMS ricevuti hanno tratto in inganno la vittima poiché veicolati con lo stesso mittente e nella stessa conversazione dove abitualmente il committente riceve le notifiche lecite ed originali inviate da Banca Ł ,[1].

Per tali motivi, ritenendo perciò il mittente attendibile, il committente ha davvero temuto un blocco del servizio e subito dopo la ricezione del secondo messaggio fraudolento del 07/04/2022 alle ore 16:38:45 ha aperto il link attraverso il browser del dispositivo.

I link inviati nei messaggi, nel caso specifico il link "http://app.clicca-ora.live/" inoltrato attraverso il secondo messaggio e aperto dal committente, alla data della frode rimandava ad una pagina web dove veniva visualizzato un pannello di accesso a Banca -- con la richiesta delle proprie credenziali

Si trattava di una pagina verosimile ma fasulla, implementata proprio per permettere ai criminali di impossessarsi con l'inganno dei codici di accesso dell'utente.

In genere i link che accompagnano questo tipo di attacchi informatici possono avere

---

[1] "*Lo spoofing si verifica infatti quando un malintenzionato invia deliberatamente informazioni false per presentarsi con l'ID (in questo caso il mittente degli SMS o il numero di telefono del mittente di una chiamata telefonica) di un altro utente. La maggior parte dello spoofing si effettua utilizzando servizi VoIP (Voice over Internet Protocol) o telefoni IP con VoIP normalmente impiegati per trasmettere comunicazioni attraverso la rete Internet e non attraverso l'infrastruttura classica di telefonia mobile*". (doc. 4 fascicolo degli attori).

una durata limitata nel tempo, poiché per ospitare le pagine web e le applicazioni malevole vengono spesso utilizzati server web anche essi compromessi.

Al momento della nostra verifica, avvenuta successivamente l'acquisizione del 22/04/2022 e cioè diversi giorni dopo la truffa, il link veniva segnalato come malevolo dal servizio "Google Safe Browsing" ma non risultava ancora segnalato dai maggiori antivirus o sandbox online.

Segno evidente di una campagna di attacco nuova, mutevole ed in corso d'opera.

Nelle azioni eseguite dal committente, cioè aprendo il link e inserendo le credenziali, la pagina restituiva un errore di accesso e mostrava una ulteriore maschera con la possibilità di compilare una richiesta di supporto con fornendo il proprio recapito telefonico per ricevere assistenza dalla banca. In tale fase, ovvero attraverso la falsa pagina di accesso, i truffatori ottenevano dalla vittima le proprie credenziali.

Successivamente il committente, continuando a seguire le indicazioni fornite dai malviventi e conclusa la procedura di richiesta di supporto, riceveva una chiamata dal numero +39 060060, cioè da un numero attestato a Banca , come riscontrato in diverse fonti, come ad esempio da una banale ricerca in Google o meglio ancora nel sito ufficiale della banca l come da immagini a seguire Anche tale chiamata veniva quindi effettuata con tecniche di "spoofing" del numero telefonico e nel corso della stessa telefonata il "falso" operatore telefonico rassicurava il committente sulle operazioni da compiere e lo induceva a scaricare ed installare nel proprio dispositivo, da un link inviato a mezzo SMS con le modalità descritte in precedenza, un'applicazione denominata " anca Sicura".

Attraverso un'attività di reverse engineering condotta a partire dal file "BancaSicura.apk" e descritta successivamente in questo documento, è stato possibile riscontrare che la stessa sia un'applicazione malevola di tipo "Trojan.android.spybank" che all'atto dell'installazione richiede i permessi per accedere alle funzioni di gestione della messaggistica per la lettura e per la ricezione di SMS oltre che ad altri permessi critici.

Tale applicazione, cosi come avviene in generale per altri Trojan, consente all'attaccante di "filtrare" gli SMS inviati da Banca in modo da disporre dei

codici OTP necessari per completare le operazioni di bonifico.

A termine dell'installazione dell'applicazione "BancaSicura.apk" e a conclusione della falsa chiamata telefonica il committente riceveva un SMS di avvenuta presa in carico della pratica con relativo codice identificativo, sempre su attestazione Banca . . Con tale messaggio in pratica i truffatori tranquillizzavano la vittima e rimandavano ulteriori operazioni al giorno successivo. In modo da avere i tempi idonei per il consolidamento del bonifico bancario utilizzato per la sottrazione illecita di denaro.

Per tali motivi il caso si configura a tutti gli effetti come un caso di "phishing" ovvero un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale e nel caso specifico fingendosi Banca l attraverso tecniche di "spoofing" sulle utenze telefoniche".

In punto di diritto si deve osservare come la giurisprudenza di legittimità abbia in un primo momento inquadrato la responsabilità dell'istituto di credito, nel caso in cui vengano compiute disposizioni non autorizzate dal cliente su conto corrente mediante accesso abusivo a sistema di *home banking*, nell'ambito della responsabilità per trattamento dei dati personali (cfr. Cassazione, sez. I, 23 maggio 2016 n. 10638).

Pertanto, la giurisprudenza di legittimità ha ripartito l'onere della prova nelle controversie fondate su tale titolo di responsabilità secondo i criteri prescritti dall'art. 15 del d.lgs. 196/2003, il quale dispone che *"chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile"*, con la possibilità per l'istituto di credito di offrire prova liberatoria dalla propria responsabilità dimostrando di aver adottato tutte le misure idonee ad evitare il danno secondo le conoscenze acquisite in base al progresso tecnico, alla natura dei dati, alle caratteristiche specifiche del trattamento, mediante adozione di misure idonee e preventive per impedire l'accesso o il trattamento non autorizzato ai sensi dell'art. 31 e 36 del d.lgs. 196/2003. Secondo la Cassazione, infatti, "*in base al rinvio all'art. 2050 c.c., operato dall'art. 15 del codice della*

privacy, l'istituto che svolga un'attività di tipo finanziario o in generale creditizio (...) risponde, quale titolare del trattamento di dati personali, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la captazione dei suoi codici di accesso e le conseguenti illegittime disposizioni di bonifico, se non prova che l'evento dannoso non gli è imputabile perché discendente da trascuratezza, errore (o frode) dell'interessato o da forza maggiore".

La Cassazione ha, quindi, rilevato che ad analoga conclusione si perviene applicando le disposizioni del d.lgs. D.Lgs. 27 gennaio 2010, n. 11 di attuazione della direttiva 2007/64/CE successivamente modificato dal d.lgs. n. 218/2017, di attuazione della direttiva 2015/2366/EU.[2].

---

[2] Anche prima del recepimento da parte del legislatore italiano della direttiva comunitaria, la disciplina in materia di servizi di pagamento ruotava intorno al consenso del soggetto pagatore al quale va ricondotta l'operazione svolta, e tanto sulla scorta dei principi generali in materia di obbligazioni e contratti (cfr. Cass. sent. 13777/2007: "*non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire le sicurezza del servizio...; infatti, la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento e assumendo quindi come parametro la figura dell'accorto banchiere*"). In tal senso si sono pronunciate Cass. civ., Sez. VI - 1, Ordinanza, 12/04/2018, n. 9158, Cass. civ., Sez. I, 03/02/2017, n. 2950 e Cass. civ., Sez. I, Sentenza, 23/05/2016, n. 10638, *"In tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei 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 di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare od a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. Ne consegue che, anche prima dell'entrata in vigore del D.Lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente*".

In particolare, l'art. 8, comma 1, dispone che "*Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: (a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7 [che sono: utilizzare lo strumento di pagamento in conformità con i termini che ne regolano l'emissione e l'uso e comunicare senza indugio al prestatore di servizi di pagamento, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza*].

L'art. 10 prevede, inoltre, che, "*qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già 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*"; il comma 2 aggiunge che "*quando l'utente di servizi di pagamento neghi di aver autorizzato un''operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente*".

La normativa in esame, quindi, prevede come regola generale una responsabilità dell'istituto di credito in caso di operazione non autorizzata dal cliente, a meno che questa non derivi dal dolo o dalla colpa grave del medesimo, con la precisazione che grava sull'operatore bancario l'onere di provare che l'illecita operatività ad opera di terzi, con riferimento alle disposizioni contestate, sia stata resa possibile dal dolo o dalla colpa grave del cliente.

Ancora più di recente, la Suprema Corte è tornata sul tema ribadendo *"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., Sez. III, 12/02/2024, n. 3780).

La Corte ha, quindi, innanzitutto ribadito la propria posizione sul riparto degli oneri di prova in materia affermando che "*La giurisprudenza di questa Corte, qualificata in termini contrattuali la responsabilità della banca, ha affermato che la diligenza posta a carico del professionista, per quanto concerne i servizi posti in essere in favore del cliente, ha natura tecnica e deve valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento assumendo come parametro quello dell'accorto banchiere (Cass. n. 806 del 2016); dunque 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*".

Applicando i suddetti principi consegue che, mentre il cliente è tenuto soltanto a provare la fonte del proprio diritto, cioè il contratto di conto corrente, ed il termine di scadenza 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*" (nel caso di specie, secondo la Corte la banca avrebbe dovuto opportunamente provare "*di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, quali ad esempio l'invito al titolare della carta di appositi sms allert di conferma di ogni singola operazione, sulla base di un principio di buona fede nell'esecuzione del contratto*") con la conseguenza che, in assenza di tale prova è imputabile alla banca il rischio che terzi accedano ai profili dei clienti con condotte fraudolente.

Con la stessa richiamata sentenza, la Corte si è poi pronunciata anche sulla rilevanza della condotta del cliente evidenziando che la responsabilità della banca è esclusa quando ricorre una situazione di colpa grave dell'utente.

Tutto ciò premesso, deve innanzitutto precisarsi che la frode informatica perpetrata ai danni degli attori si è concretizzata con modalità particolarmente insidiose all'epoca dei fatti in quanto il cd. "phishing" è stato preceduto da un attacco di "spoofing"[3].

Alla luce dei sopra richiamati principi era onere della Banca convenuta dimostrare di

---

[3] *Per spoofing, nel linguaggio informatico, s'intende la manipolazione dei dati trasmessi in una rete telematica, consistente nella falsificazione del proprio indirizzo IP, oppure nell'utilizzo abusivo di user name e password di altri utenti. In particolare, lo spoofing dell'ID chiamante è la pratica per cui la rete telefonica indica al destinatario di una chiamata che l'originatore della chiamata è una stazione diversa dalla vera stazione di origine.*

In estrema sintesi, la differenza tra phishing e spoofing sta nel fatto che lo spoofing nasconde l'origine di una comunicazione in modo da far sembrare che è stata inviata da qualcun altro, mentre il phishing adotta tattiche di social engineering per indurre le persone ad aprire messaggi o fare clic su collegamenti e, quindi, divulgare dati sensibili.

Nella più recente casistica, lo spoofing e il phishing sono spesso correlati perché gli aggressori tendono a utilizzare metodi di spoofing per rendere più credibili i loro attacchi di phishing." (Trib. Lamezia Terme n. 117 del 5.2.2026).

aver adottato dei sistemi specificamente volti a prevenire lo spoofing dei propri numeri telefonici e l'inserimento di SMS fraudolenti nei thread di comunicazioni legittime con i propri clienti ovvero dimostrare l'impossibilità tecnica di scongiurare tale tipo di aggressione, per essere la stessa al di fuori della sua sfera di controllo.

In un caso sovrapponibile a quelle per cui è causa che ha visto convenuta la medesima banca per una frode informatica ai danni di un proprio cliente avvenuta il 7.3.2022, a meno di un mese prima dell'evento di che trattasi, il Tribunale di Milano nella sentenza n. 1514 del 21.2.2025 ha osservato che " *Non si ritiene, pertanto, che la convenuta abbia fornito la prova dell'adozione da parte dell'attore di un contegno di straordinaria e inescusabile leggerezza che imponga di escludere che abbia rispettato quella minima prudenza esigibile ed osservabile da tutti. La predisposizione da parte della convenuta di un sistema di autenticazione forte per l'operatività del servizio di home banking di per sé non rappresenta il massimo delle cautele tecnologicamente possibili per contrastare – tra gli altri – i fenomeni di phishing, bensì il minimo della cautela pretesa dal legislatore per evitare che il prestatore di servizi di pagamento risponda in ogni caso (quindi anche nell'ipotesi di colpa grave del pagatore) di qualsiasi operazione non autorizzata, salva la frode ai sensi dell'art. 12.2-bis del d.lgs. 11/2010 ..... A ciò si aggiunga la considerazione per cui la convenuta non ha provato di aver approntato tale sistema di autenticazione forte, essendosi limitata a produrre la schermata del sito di Banca di Italia, contenente le specifiche della Strong Customer Authentication (all. 7 comparsa di costituzione e risposta), documento del tutto inidoneo a provare che la stessa ne sia dotata, in linea con la normativa vigente.*

Lo stesso consulente di parte, del resto, ha rilevato un vulnus nel sistema di sicurezza della banca, avendo ravvisato "nella possibilità di interazione tra l'applicazione dell'istituto e terze applicazioni" che "la strong customer authentication operabile (...) [fosse] soggetta a possibile vulnerabilità di interazione e simulazione da parte di altra applicazione, perdendo dunque la caratteristica di robustezza alla base dell'applicazione stessa".

Per quanto riguarda l'attività di informazione alla clientela sui rischi delle frodi

informatiche allegata dalla Banca convenuta nella suindicata sentenza è stato osservato che " *La convenuta ha, inoltre, documentato di aver realizzato, sul proprio sito campagne di informazione sul fenomeno del phishing (all. 5 comparsa). Tali comportamenti, benché indispensabili per la creazione di una cultura del risparmio che, con il tempo, renda i consumatori più avveduti rispetto ai pericoli connessi con l'operatività bancaria ed in particolare con l'operatività on line, sono di per sé è inidonei ad evitare la perpetrazione di questo tipo di frodi, tanto più tenuto conto di come l'informativa sul sito internet del fornitore del servizio di pagamento delle modalità di esecuzione delle frodi on line non dà alcuna garanzia di lettura e comprensione effettiva da parte del cliente né dà garanzia del riconoscimento effettivo dei tentativi di truffa.*

Deve rilevarsi, inoltre, che le modalità con le quali è stato truffato l'attore non sono state descritte in nessuna delle comunicazioni anti-phising prodotte dalla convenuta (all. 5 comparsa), la quale non ha provato, quindi, nello specifico, di aver adottato alcuna cautela né di aver fornito al suo cliente alcuna informazione che gli avrebbe consentito di riconoscere la truffa della quale è stato vittima. Infatti, come sopra evidenziato le telefonate provenivano tutte dal numero "+39060060" che compariva sulla schermata del telefono dell'attore (vedi documento n. 1 bis allegato all'atto di citazione), numero effettivamente riconducibile a ".

Nel caso di specie il primo documento informativo prodotto dalla banca non consente di verificare la data di pubblicazione sul sito internet della convenuta mentre un secondo documento risalente al 4.8.2020, anche a voler ammettere che sia stato inviato agli attori, non era sufficientemente specifico per poter utilmente prevenire la frode informatica compiuta ai danni degli attori (doc.1 e 5 fascicolo della convenuta)

Come risulta dalla perizia allegata in giudizio dagli attori " *Al momento della nostra verifica, avvenuta successivamente l'acquisizione del 22/04/2022 e cioè diversi giorni dopo la truffa, il link veniva segnalato come malevolo dal servizio "Google Safe Browsing" ma non risultava ancora segnalato dai maggiori antivirus o sandbox online. Segno evidente di una campagna di attacco nuova mutevole ed in corso d'opera* ..... concludendo che "*.....caso trattato è a tutti gli effetti un caso di*

"phishing" eseguito da criminali che attraverso una campagna massiva hanno evidentemente attaccato i correntisti di Banca , tra cui il Sig.

I malintenzionati hanno ingannato la vittima convincendola a fornire i propri codici di accesso e ad installare l'applicazione malevola, fingendosi Banca attraverso tecniche di "spoofing" sulle utenze telefoniche.

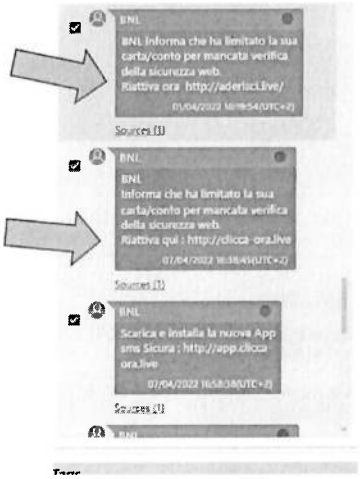
Gli SMS e la telefonata, inoltrati con tali metodiche, hanno avuto successo poiché veicolati attraverso le utenze ritenute sicure dal committente, in quanto perfettamente coincidenti con le classiche impiegate dall'istituto bancario".

Da ciò consegue come la convenuta non abbia assolto all'onere probatorio posto a suo carico in ordine all'adozione di misure atte a prevenire frodi informatiche e all'adeguatezza dei sistemi informatici utilizzati all'epoca delle operazioni disconosciute, non risultando, dalle modalità concrete attraverso la quale si è sviluppata la frode informatica a danno degli attori né un comportamento dell'utilizzatore qualificabile quale doloso o gravemente colposo.

In particolare, devono essere valorizzate le seguenti circostanze fattuali :

- l'invio dei due SMS illeciti è avvenuto all'interno del canale comunicativo ufficialmente utilizzato dalla Banca convenuta e, pertanto, come riferito nella perizia informatica allegata in atti " *Tale canale di comunicazione con la banca ed il relativo contenuto veniva perciò ritenuto "sicuro" dal committente poiché abitualmente utilizzato dall'istituto per trasmettere al proprio cliente le sopra citate notifiche.*; *Nello specifico gli SMS ricevuti hanno tratto in inganno la vittima poiché veicolati con lo stesso mittente e nella stessa conversazione dove abitualmente il committente riceve le notifiche lecite ed originali inviate da Banca . Per tali motivi, ritenendo perciò il mittente attendibile, il committente ha davvero temuto un blocco del servizi e subito dopo la ricezione del secondo messaggio fraudolento del 07/04/2022 alle ore 16:38:45 ha aperto il link attraverso il browser del dispositivo.*

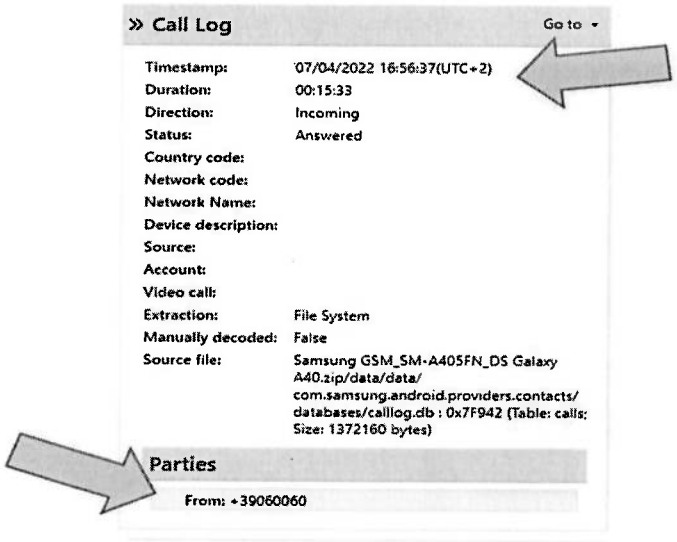
A seguire il dettaglio dei due messaggi fraudolenti nella conversazione SMS con intestazione "BNL" presente nel dispositivo:



b) il fatto che – contrariamente a quanto accaduto in altre fattispecie esaminate dalla giurisprudenza di merito – il messaggio non contenesse alcun errore grammaticale;

c) la circostanza che il link "http://app.clicca-ora.live/" inoltrato attraverso il secondo sms e aperto dal L i conducesse ad una pagina web dove veniva visualizzato un pannello di accesso a Banca con la richiesta delle proprie credenziali

d) la circostanza che la chiamata ricevuta dall'apparente operatore provenisse da un numero fisso 39 060060 riferibile alla Banca convenuta.



Come condivisibilmente ritenuto dalla Corte di Appello di Venezia nella sentenza n. 498 del 7.3.2026 " .. *Ora, l'essere stata contattata proprio dal numero del Servizio Clienti della banca della quale era cliente-correntista, e che oltretutto abitualmente utilizzava, tanto da averlo memorizzato nella rubrica del proprio telefono cellulare, ha costituito un indubbio elemento decettivo per l'attrice, Invero, anche ammesso che la stessa abbia involontariamente "assecondato" il truffatore inserendo nel sistema il token che nella prospettiva della banca avrebbe integrato l'autorizzazione al trasferimento dei fondi, appare del tutto evidente come ciò costituisca l'effetto tipico della condotta ingannatoria, che laddove efficacemente posta in essere (come evidentemente è stato nella fattispecie) induce il correntista a comportarsi in maniera "collaborativa" con l'ignoro autore della frode nella "ignara" convinzione che le disposizioni così adempiute provengano effettivamente dalla stessa banca.*

Diversamente opinando – e quindi ritenendo che il correntista versi sempre in stato di colpa grave (come tale ostativo alla restituzione della somma distratta) per il solo fatto di essersi comportato in maniera tale da agevolare il frodatore ponendo in essere atti che, ex post, si sono rivelati di agevolazione (sia pure "inconsapevole") della altrui condotta illecita – dovrebbe inevitabilmente ritenersi che l'utente versi sostanzialmente sempre in colpa grave e che, per contro, il prestatore dei servizi di

pagamento vada corrispondentemente sempre esente da responsabilità, così sovvertendosi il sopra richiamato impianto normativo (artt. 5, co. 1; 7, co. 2; 10, co. 1 e 2) volto a porre il rischio dell'utilizzo indebito dello strumento di pagamento a carico del PSP e non già dell'utente, a meno che questi non sia stato colluso con il frodatore e comunque non ne abbia agevolato l'operatività con grave colpa".

L'insieme di tutti i suindicati elementi, complessivamente considerati, induce a ritenere che non possa essere addebitato agli attori di aver tenuto una condotta gravemente colpevole rilevante ai sensi del comma 2 dell'art. 10 d.lgs. 11/2010, tenuto anche conto che le specifiche modalità fraudolente utilizzate nel caso di specie erano particolarmente insidiose e più difficoltose da riconoscersi con la normale diligenza.

La domanda formulata dagli attori deve, pertanto, trovare accoglimento e la banca convenuta deve essere condannata al risarcimento dei danni nella misura di euro 49.332,21 oltre rivalutazione monetaria ed interessi legali dalla costituzione in mora avvenuta in data 9.4.2022 (doc. 10 fascicolo degli attori) al saldo.

Le spese processuali seguono la soccombenza della convenuta e sono liquidate come in dispositivo ai sensi del D.M. 147/22, applicando i parametri medi considerata la ridotta attività istruttoria tenuto conto del valore della causa determinato ai sensi dell'art. 5 del predetto decreto, delle questioni trattate e dell'attività effettivamente svolta.

P.Q.M.

il Tribunale di Perugia, seconda sezione civile, in composizione monocratica, definitivamente pronunciando sulla domanda come in epigrafe proposta, ogni contraria istanza, eccezione e deduzione disattesa, così provvede:

- **accoglie** le domande proposte da I nei confronti della I che viene condannata al pagamento in favore degli attori dell'importo di euro 49.332,21 oltre rivalutazione monetaria ed interessi legali dalla costituzione in mora avvenuta in data 9.4.2022 al saldo;
- **condanna** .a. alla refusione delle spese di lite in favore degli attori che si liquidano, in assenza di notula, in euro 595,80 per spese

documentate ed in euro 7.000,00 per onorari oltre spese generali, cpa ed iva di legge.

Perugia, 5 maggio 2026

Il Giudice

Federico Fiore