

Sentenza n. 1656/2025 pubbl. il 01/02/2025

RG n. [REDACTED]

Sentenza n. cronol. 635/2025 del 01/02/2025

N.R.G. [REDACTED]



Repubblica Italiana
In nome del popolo italiano
Tribunale Ordinario di Roma
Sezione XVI civile
Sezione specializzata in materia di imprese

Il Tribunale di Roma, in persona del giudice unico, dott. Stefano Iannaccone, ha pronunciato la seguente

sentenza

nella causa civile di I grado iscritta al n. [REDACTED] del ruolo generale per gli affari contenziosi dell'anno 2023, trattenuta in decisione all'udienza del 26/11/2024 e vertente

tra

[REDACTED], elettivamente domiciliata in Roma, Viale Liegi, n. 58, presso lo studio degli avv. Vincenzo Cancrini, Beatrice Cancrini e Paolo Cariani, che la rappresentano e difendono congiuntamente e disgiuntamente giusta procura alle liti allegata all'atto di citazione

- **Attrice**

e

[REDACTED], in persona del l.r.p.t., elettivamente domiciliata in Roma, [REDACTED] presso lo studio dell'avv. [REDACTED] che la rappresenta e difende giusta procura alle liti allegata alla comparsa di costituzione e risposta;

- **Convenuta**

Conclusioni delle parti:

Per l'attrice: *"Voglia l'On.le Tribunale adito, contrariis reiectis,*

- Accertare e dichiarare che sulla base dei fatti meglio indicati in atti, nelle giornate del 19-20-21 ottobre 2022 la sig.ra [REDACTED] subiva la sottrazione dal proprio conto corrente ad opera di ignoti ed in favore dei Sigg. [REDACTED] sconosciuti all'Esponente, della somma di complessivi € 115.793,00 (euro centoquindicimilasettecentonovantatre/00), mediante n.3 bonifici meglio indicati in atti, resi possibili dal mancato e/o insufficiente funzionamento dei sistemi di sicurezza dei servizi di pagamento elettronico e/o di home banking



e/o app mobile collegati al conto corrente della stessa sig.ra [REDACTED]
[REDACTED] predisposti dalla medesima convenuta [REDACTED], più in generale, resi possibili per fatto e/o colpa grave della convenuta per le ragioni tutte meglio indicate in atti;
- Accertare e dichiarare altresì la grave violazione del Regolamento UE/2016/679 e del D.lgs. 196/2003, nonché il grave inadempimento del contratto di conto corrente e dei contratti ad esso collegati (bancomat, servizi di pagamento, carta di credito, carta di debito, home banking, mobile APP o similare), imputabile alla convenuta [REDACTED], ai sensi degli artt. 1453, 1455, 1176, 2° co., 1375, e 1856 c.c. e/o, comunque, la responsabilità della stessa [REDACTED] ex D. Lgs. n. 11/2010 ed ex art. 2050 c.c. per le ragioni tutte meglio indicate in atti e, per l'effetto,
- condannare la convenuta [REDACTED] in persona del legale rappresentante pro-tempore, a risarcire in favore dell'attrice, Sig.ra [REDACTED] i danni tutti da quest'ultima patiti e patiendi, pari al ristoro per intero delle somme alla stessa sottratte mediante phishing (o smishing), come meglio indicato in atti, dal Suo conto corrente [REDACTED] [REDACTED] pari ad Euro 115.793,00 (euro centoquindicimilasettecentonovantatre/00) o alla maggiore o minore somma che verrà accertata in istruttoria e/o ritenuta dovuta, nonché al danno morale e/o non patrimoniale, forfettariamente quantificato in euro 30.000,00 (trentamila/00) o nella maggiore o minore somma che risulterà provata in istruttoria o, in difetto, equitativamente determinata, essendosi trovata la stessa Sig.ra [REDACTED] il proprio conto corrente improvvisamente svuotato a causa dell'illecito subito, anche di rilevanza penale quale frode informatica ai sensi dell'art. 640-ter c.p. o altra fattispecie criminosa. Il tutto, oltre interessi e rivalutazione monetaria dalla domanda fino al soddisfo, come per legge.
Con vittoria di spese e compensi professionali, compreso rimborso spese generali ed accessori, come per legge".

Per la convenuta: "Voglia il Tribunale adito, disattesa ogni istanza contraria o diversa, così giudicare:

- nel merito, respingere, perché infondate in fatto e in diritto, tutte le domande formulate dalla Sig.ra [REDACTED] nei confronti della Banca convenuta per le ragioni dedotte in narrativa;
- in ogni caso, con vittoria di spese e competenze di causa".

Svolgimento del processo e motivi della decisione

[REDACTED] correntista di [REDACTED] dal 2001, citava in giudizio [REDACTED] deducendo:

- che in data 19/10/2022, alle ore 14:38, avrebbe ricevuto sul proprio telefono cellulare,



un SMS contrassegnato dall'identificativo [REDACTED] e contenente il seguente testo: [REDACTED]
Informa che ha limitato la sua carta/conto per mancato aggiornamento della sicurezza web Riattivala [https://s.id/Modulo\[REDACTED\]](https://s.id/Modulo[REDACTED])

- che, ritenendo attendibile il messaggio, in quanto proveniente da un'utenza apparentemente intestata all'istituto di credito, avrebbe cliccato sul *link* contenuto nell'SMS;
- che, una volta aperto il c.d. *link* civetta, le credenziali di accesso al *Mobile Token* (ID e *password*) sarebbero state carpite mediante inserimento automatico con impronta digitale, senza il previo inserimento manuale di codici da parte della correntista;
- che alle ore 14:42 avrebbe ricevuto una telefonata da un'utenza apparentemente intestata a [REDACTED], nel corso della quale un falso operatore della banca l'avrebbe indotta a disinstallare l'*app* di *home banking* di [REDACTED] e a reinstallarla tramite un *link* appositamente recapitato via SMS durante la telefonata;
- che l'installazione del *software* malevolo sarebbe valsa a dirottare l'inoltro degli SMS alert provenienti dalla banca, nonché a disattivare il sistema di notifiche *push* dell'*app* di *home banking* di [REDACTED];
- che durante la stessa telefonata sarebbe stato effettuato un bonifico tramite *Mobile Token* di importo pari ad Euro 48.951,00 in favore di tale [REDACTED] soggetto ignoto alla titolare del conto;
- che il giorno successivo essa attrice avrebbe ricevuto una nuova telefonata dalla stessa utenza, durante la quale l'operazione fraudolenta si sarebbe ripetuta con le stesse modalità: la [REDACTED] intimata dall'interlocutore di non rivelare le credenziali di accesso, sarebbe stata indotta a disinstallare e reinstallare il *software* malevolo, con conseguente nuovo dirottamento degli SMS *alert* e disattivazione del sistema di notifiche *push*.
- che a tale telefonata sarebbe seguita, dopo due tentativi di accesso falliti e il reset del *mobile Token* [REDACTED] da parte del truffatore, l'effettuazione di un bonifico di importo pari al precedente in favore dello stesso soggetto
- che in data 21/10/2022, per la terza volta, la frode si sarebbe ripetuta con le medesime modalità, determinando l'effettuazione, all'insaputa dell'attrice, di un terzo bonifico, di importo pari ad € 17.891,00 in favore di [REDACTED] individuo anch'esso ignoto all'attrice;
- che in data 25/10/2022 l'attrice si sarebbe recata in filiale ed avrebbe preso contezza dell'accaduto e, di conseguenza, avrebbe sporto denuncia contro ignoti presso la



stazione dei Carabinieri di Fiumicino (doc. 10 fascicolo di parte attrice).

Tanto premesso in fatto, l'attrice deduceva in diritto:

- che la banca non avrebbe garantito un'adeguata sicurezza dei dati relativi alle informazioni personali dei correntisti, quali l'identità, l'utenza telefonica, le notizie bancarie e finanziarie relative ai prodotti e ai servizi in possesso della Banca (*data breach*);
- che la negligenza della banca configurerebbe una ipotesi di responsabilità *ex art. 2050 c.c.*, dal momento che le misure adottate da quest'ultima sarebbero state inidonee ad evitare il danno;
- che, in particolare, l'informazione preventiva offerta dalla banca in materia di rischi connessi al servizio di *home banking* sarebbe stata ambigua e che i sistemi di protezione rafforzati impiegati da [REDACTED] non sarebbero stati comunque sufficienti ad escluderne la responsabilità;
- che la condotta della banca rileverebbe anche dal punto di vista della responsabilità contrattuale, perché contraria ai canoni di diligenza professionale rivenienti dagli artt. 1176, c.2 e 1856 c.c.;
- che, in particolare, [REDACTED] avrebbe omissso di verificare la concreta riferibilità soggettiva delle operazioni compiute da terzi sul conto dell'attrice, nonostante l'anomalia dei movimenti registrati sullo stesso;
- che la diligenza dell'accorto banchiere avrebbe imposto alla banca di prendere contatto telefonico diretto con l'attrice e/o di sospendere le operazioni in attesa di un riscontro esatto della provenienza degli atti dispositivi dall'effettiva titolare del conto corrente;
- che tale obbligazione si sarebbe resa necessaria alla luce dell'improvviso mutamento delle credenziali e delle modalità di accesso al mobile token, dell'inserimento reiterato di credenziali errate e soprattutto in ragione degli importi esorbitanti dei bonifici rispetto alla pregressa operatività del conto.

Si costituiva in giudizio la [REDACTED] con comparsa di risposta depositata in data 17/07/2023, eccependo:

- che, in forza dell'art. 8 del contratto di conto corrente concluso dall'attrice con la banca, [REDACTED] non sarebbe tenuta ad alcun generale dovere di rimborso in ordine alle disposizioni di pagamento disconosciute ma poste in essere utilizzando le credenziali e gli strumenti di sicurezza in possesso del correntista;
- che la stessa [REDACTED] si sarebbe prontamente attivata per la revoca dei bonifici e la



restituzione delle somme oggetto di frode informatica, seppure con esito negativo, in ragione del diniego delle banche destinatarie della richiesta, motivato dall'insufficienza dei fondi presenti nei c/c beneficiari delle operazioni per cui è causa;

- che la frode si sarebbe consumata grazie alla condotta gravemente colposa di [REDACTED] la quale avrebbe consegnato le credenziali di accesso agli *hacker* cliccando sul link ricevuto il 19/10/2022, in spregio agli obblighi di segretezza e custodia cui era contrattualmente e per legge tenuta e alle ripetute raccomandazioni che la Banca avrebbe fornito sui diversi canali utilizzati dalla propria clientela;
- che l'assenza di cautela di controparte non sarebbe scusabile, in quanto le modalità con cui è stata perpetrata la frode rientrerebbero tra quelle più diffuse, che qualunque cliente dotato di normale avvedutezza e prudenza dovrebbe essere in grado di individuare;
- che non vi sarebbe stata alcuna intrusione e/o violazione del sistema informatico di [REDACTED];
- che la Banca avrebbe messo a disposizione dei clienti tutti gli strumenti utili a prevenire il verificarsi di eventi fraudolenti, implementando un sistema di autenticazione forte (autenticazione a due fattori) conforme a quanto richiesto dalla normativa nazionale ed europea vigente in materia;
- che nessuna anomalia sarebbe stata registrata sui sistemi di sicurezza della Banca in relazione alle operazioni *de quibus*;
- che nessun obbligo ulteriore graverebbe sulla banca in relazione alle operazioni di pagamento effettuate dai clienti avvalendosi del meccanismo di autenticazione forte e in assenza di anomalie e/o malfunzionamenti riscontrati nei propri sistemi di sicurezza;
- che la domanda di risarcimento del danno non patrimoniale formulata da controparte, oltretché infondata, sarebbe in ogni caso sprovvista di supporto probatorio.

Dato atto che in data 03/04/2023 [REDACTED] esperivano il tentativo obbligatorio di conciliazione con esito negativo, la causa veniva istruita sulla base della documentazione versata in atti dalle parti. All'udienza del 26/11/2024 queste precisavano le rispettive conclusioni come da relativo verbale e la causa veniva trattenuta in decisione.

La domanda risarcitoria proposta da [REDACTED] deve essere accolta per le ragioni che seguono.

Ai sensi degli artt. 5, lett. f); 24; 32 del Regolamento UE n. 679 del 2016 (c.d. GDPR) il titolare



del trattamento dei dati personali è tenuto a *“garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali”*, nonché ad *“essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento”*.

I fatti oggetto di causa tradiscono l'avvenuta captazione da parte di terzi malintenzionati di dati inerenti al rapporto contrattuale in essere tra le parti. In particolare, l'attrice indica quelli relativi all'identità, all'utenza telefonica e alle informazioni bancarie e finanziarie, inferendo che le lesioni subite non si sarebbero realizzate se non vi fosse stato un *data breach*, cioè una violazione dei sistemi informatici di [REDACTED]

Tuttavia, è errato ritenere che il numero di telefono, gli estremi del conto corrente e l'identità dei correntisti possano essere carpiri solo mediante una violazione dei sistemi della banca. Tali informazioni ben potrebbero essere state acquisite *aliunde* dagli *hacker*, indipendentemente dalla condotta colposa del titolare del trattamento. Né le notizie di stampa prodotte dall'attrice (doc. 4) potrebbero fondare alcuna presunzione circa il presunto *data breach*, per difetto dei requisiti di gravità, precisione e concordanza.

D'altro canto, l'adozione di sistemi di autenticazione forte mediante verifica a due fattori – statico, ID e password, e dinamico, codici OTP – è da ritenersi in astratto una misura tecnica adeguata a garantire la sicurezza dei dati dei correntisti. Tale è la prassi di sicurezza adottata da [REDACTED]

Sotto questo profilo, dunque, si esclude la fondatezza di ogni addebito di responsabilità a carico della parte convenuta *ex art. 82 GDPR*.

Quanto agli addebiti sollevati avverso [REDACTED] *ex art. 2050 c.c.*, essi sono assorbiti dalla disciplina contrattuale di cui agli artt. 1176, c. 2; 1218ss.; 1856 c.c. e artt. 7; 8; 10; 10-bis; 12 d.lgs. 27 gennaio 2010 n. 11, trattandosi di una ipotesi di c.d. concorso oggettivo alternativo di responsabilità.

La fattispecie in esame, infatti, contempla la pretesa lesione di un diritto unitario (credito nascente dal contratto di conto corrente) e deve essere sussunta sotto la disciplina dell'illecito contrattuale.

L'art. 7 d.lgs. cit. definisce gli *“obblighi dell'utente di servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate”*, stabilendo, per quel che qui interessa, che:

“1. L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di:



- a) 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;
- b) 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";

"2. non appena riceve uno strumento di pagamento, adotta[re] tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate".

Il successivo art. 8 determina gli obblighi del prestatore del servizio, stabilendo, per quel che qui rileva, che questi sia tenuto a:

- *"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";*
- *"c) assicurare che siano sempre disponibili strumenti adeguati affinché l'utente dei servizi di pagamento possa eseguire la comunicazione di cui all'articolo 7, comma 1, lettera b) [...]".*

A mente dell'art. 12, poi:

"[...]

- *2. Salvo il caso in cui abbia agito in modo fraudolento, l'utente non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera c). [...]*
- *2-ter. Il pagatore non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento, o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali del prestatore di servizi di pagamento o dell'ente cui sono state esternalizzate le attività.*
- *3. Negli altri casi, salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita.*
- *4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi*



di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3".

L'art. 10 regola la distribuzione dell'onere della prova, stabilendo che il prestatore del servizio debba dimostrare sia che l'operazione di pagamento controversa *"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"*, sia che questa sia stata *"autorizzata dall'utente medesimo"*, *"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"*.

Ai sensi degli artt. 1176, 1856 e 1710 c.c., infine, la Banca è tenuta all'osservanza del canone della *diligenza professionale*, il quale, nella speciale materia in questione, si risolve nella *diligenza dell'accorto banchiere*. Tale parametro fa sì che *"la diligenza della banca va[da] 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"* (Cass. Civ., Sez. I, 4 settembre 2024, n. 23683).

Sulla scorta del quadro normativo di cui s'è dato conto, è stato condivisibilmente affermato in giurisprudenza che *"nell'ambito di questo sistema di responsabilità e, più in generale, del fenomeno del phishing, il fatto che il pagatore comunichi a terzi truffatori le credenziali di accesso al proprio conto on line è un evento fisiologico, essendo la modalità standard tramite la quale vengono compiute tali truffe e quindi quella in ragione della quale è predisposta, a livello internazionale e nazionale, tutta la normativa anti-phishing. La comunicazione a terzi delle credenziali di accesso al proprio conto e per l'operatività sul proprio conto può essere espressiva di una colpa grave del pagatore solo quando, per le modalità ed il contesto nel quale viene compiuta, sia espressiva di straordinaria e inescusabile leggerezza che consenta di escludere il rispetto di quella minima prudenza esigibile ed osservabile da tutti"* (Trib. Milano sez. VI, 01/12/2022, n. 9475).

Nel caso di specie, la lesione patrimoniale subita dall'attrice è stata resa possibile dall'inserimento automatico delle credenziali di accesso al mobile token mediante impronta digitale a seguito dell'apertura del c.d. link civetta (v. doc. 19, p. 7 fascicolo di parte attrice, nonché memoria 1, p. 9, punto 2).

A tal proposito, giova sottolineare la non decisività, di per sé, della circostanza che la trasmissione dei dati di accesso statici al mobile token sia avvenuta mediante impronta



digitale, cioè senza l'inserimento manuale di ID e password. Come si evince dalla stessa consulenza tecnica di parte prodotta da [REDACTED] alle 14.40 del 19/10/2022, le credenziali in questione venivano inserite nel link [https://s.id/Modulo\[REDACTED\]](https://s.id/Modulo[REDACTED]) e non risulta dirimente la circostanza che ciò sia avvenuto mediante compilazione automatica ovvero tramite inserimento del dato biometrico.

Tramite la suddetta operazione, veniva carpito da terzi l'elemento statico della catena di sicurezza dei dati della correntista. Il successivo download di app contraffatte valeva a consegnare agli *hacker* il fattore dinamico (codici OTP) e ad impedire alla correntista di ricevere gli SMS Alert relativi alle operazioni ordinate da costoro.

La reale provenienza dei contatti presi con l'attrice a partire dal 19/10/2022 è stata fraudolentemente occultata attraverso la tecnica del c.d. *spoofing*, tale da ingenerare un affidamento della cliente sulla riferibilità alla [REDACTED] delle istruzioni telefonicamente ricevute dal falso operatore.

La convenuta ha eccepito che tali modalità decettive avrebbero dovuto essere tempestivamente rilevate all'attrice, la quale sarebbe stata raggiunta da campagne di informazione prodotte come all. 1 e 4.

Tuttavia, la circostanza – puntualmente contestata dall'attrice con la prima memoria istruttoria – non può dirsi dimostrata.

A fronte della contestazione della [REDACTED] era onere della convenuta dare prova dell'invio delle stesse o, comunque, della messa a disposizione delle stesse a beneficio dell'attrice.

Tale circostanza non può essere desunta dall'esame dei suddetti documenti, consistendo questi ultimi in un memorandum unilateralmente predisposto dalla convenuta, privo di data, apparentemente estratto dal sito web della stessa banca (all. 1) e in una comunicazione via mail della quale è sconosciuta la casella di posta elettronica di recapito (all. 4). Peraltro, quest'ultima comunicazione si limitava ad avvisare il destinatario del rischio di comunicare al telefono i propri codici di sicurezza (cosa non avvenuta nel caso di specie) ma non allertava in alcun modo la clientela in merito ai rischi connessi al download di app.

Peraltro, a prescindere dalle considerazioni che precedono, va osservato che nel caso di specie l'operazione di *phishing* è stata caratterizzata da particolari modalità, tali da escludere la colpa grave della correntista.

Infatti, non soltanto nel primo SMS ricevuto il 19 ottobre 2022 non è presente alcun indice di manifesta falsità, ma i successivi contatti telefonici, anch'essi eseguiti mediante *spoofing*, sono stati connotati da particolare verosimiglianza.



È pacifico, infatti, che il falso operatore, oltre ad aver adoperato una numerazione riconducibile al gruppo [REDACTED], abbia riferito un numero di matricola fittizio ed abbia più volte richiesto alla correntista di non rivelare le proprie credenziali di accesso al servizio di home banking. Posto che l'utente di tali servizi è tenuto, secondo la regola generale di cui agli artt. 1176, c.2 e 1227, c.2, ad osservare l'ordinaria diligenza, si ritiene che le concrete modalità attuative del raggio abbiano reso inesigibile una condotta alternativa della correntista (cfr. Trib. Milano, sent. 13 aprile 2022, n. 3295). Per tali ragioni si esclude che la colpa grave di Miriam Tibaldi abbia costituito una concausa dell'evento lesivo da lei subito.

A ciò si aggiunga che la CTP di parte attrice, corroborata in parte qua dalla documentazione ad essa allegata, ha consentito di appurare che la truffa in danno dell'attrice è stata resa possibile mediante l'installazione sul telefono della [REDACTED] di un *malware*, utilizzando il quale terzi sarebbero stati in grado di schermare la ricezione degli alert, delle notifiche push e delle OTP. E' dunque provato che la conoscenza di dette informazioni da parte di terzi non fosse dipesa dalla comunicazione, gravemente colposa, delle stesse da parte della correntista, quanto piuttosto dall'esecuzione di un articolato ed insidioso raggio, posto in essere in danno della [REDACTED] oggettivamente insuscettibile di essere tempestivamente rilevato con l'uso di quella diligenza minima richiesta ai fini dell'esclusione dell'elemento soggettivo della colpa grave.

Quanto infine alla pretesa risarcitoria relativa al danno non patrimoniale, essa è priva di fondamento.

Difetta, infatti, l'individuazione di un diritto costituzionalmente garantito oggetto di lesione, nonché la prova di un danno conseguenza concretamente prodottosi nella sfera esistenziale dell'attrice quale conseguenza dell'illecito subito sul piano patrimoniale.

P.Q.M.

Il Tribunale di Roma, in persona del dott. Stefano Iannaccone, così provvede:

- I. condanna [REDACTED] al pagamento in favore dell'attrice della somma di € 115.793,00, oltre interessi legale dalla domanda al soddisfo;
- II. rigetta le ulteriori domande di parte attrice;
- III. condanna la parte convenuta alla rifusione in favore dell'attrice delle spese di lite, che liquida in € [REDACTED] oltre spese generali, IVA e CPA come per legge.

Roma, 01/02/2025

il Giudice

dott. Stefano Iannaccone

