REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

IL TRIBUNALE DI ROMA

Sezione XVI civile

Il Tribunale, in persona del Giudice Unico, dott. Giuseppe Di Salvo, ha emesso la seguente

SENTENZA

nella causa civile di I grado iscritta al n. 72141 del ruolo generale per gli affari contenziosi dell'anno 2019, trattenuta in decisione all'udienza del 14-03-2023 e vertente

TRA

[redacted],

C.F. [redacted], elettivamente domiciliata in Roma, via [redacted] presso lo studio dell'avv. [redacted] che la rappresenta e difende, giusta delega depositata in via telematica unitamente alla comparsa di costituzione di nuovo difensore

ATTRICE

E

I[redacted] S.P.A.,

C.[redacted] con sede legale in [redacted], in persona del legale rappresentante pro-tempore, elettivamente domiciliata in Roma, V[redacted] presso lo studio degli avv.ti V[redacted] che la rappresentano e difendono, giusta procura depositata in via telematica unitamente alla comparsa di costituzione e risposta

CONVENUTA

NONCHE' NEI CONFRONTI DI

V[redacted] S.P.A.,

C.F. [redacted] con sede legale in [redacted] in persona del legale rappresentante pro-tempore, elettivamente domiciliata in Roma, via [redacted] presso lo studio dell'avv. [redacted] che la rappresenta e difende, giusta procura depositata in via telematica unitamente alla comparsa di costituzione e risposta

CHIAMATA IN CAUSA

CONCLUSIONI

All'udienza di precisazione delle conclusioni del 14-03-2023, le parti concludevano come da verbale in atti e la causa veniva trattenuta in decisione, con assegnazione dei termini ex art. 190 c.p.c.

SVOLGIMENTO DEL PROCESSO:

Con atto di citazione ritualmente notificato, S[redacted] conveniva in giudizio I[redacted]., chiedendo l'accoglimento delle seguenti conclusioni:

"Voglia l'On.le Tribunale adito, rigettata ogni contraria istanza, eccezione e deduzione:

(i) accertare e dichiarare la responsabilità della I[redacted] in persona del legale rappresentante pro tempore, per la sottrazione dell'importo di € 181.119,20 dal conto corrente intestato alla Sig.ra [redacted], mediante le operazioni di pagamento non autorizzate e disconosciute dalla correntista, per tutte le ragioni indicate in narrativa;

(ii) per l'effetto, condannare I[redacted] S.p.A., in persona del legale rappresentante pro tempore, a rimborsare alla Sig.ra A[redacted] l'importo illegittimamente sottratto dal conto corrente alla medesima intestato, pari a € 181.119,20, detratta la franchigia di € 150,00 prevista dall'art. 5 (a) del Contratto Servizi Via Internet, Cellulare e Telefono, per un

totale di € 180.969,20, ovvero la diversa somma, maggiore o minore, che risulterà in corso di causa, oltre interessi ex art. 1284 cod. civ. e rivalutazione monetaria dalla domanda giudiziale al soddisfo;

(iii) in caso di accoglimento della domanda formulata da I volta ad accertare la responsabilità solidale di V. nella vicenda per cui è causa, condannare la predetta terza chiamata V in persona del legale rappresentante pro tempore, al pagamento, in favore della sig.ra , delle somme che saranno accertate e liquidate in favore della predetta attrice, oltre interessi ex art. 1284 cod. civ. e rivalutazione monetaria dalla domanda giudiziale al soddisfo;

(iv) con vittoria di spese e onorari, oltre rimborso forfetario, i.v.a. e c.p.a. come per legge."

A sostegno delle proprie ragioni l'attrice esponeva di essere titolare del conto corrente n. 06812028579750142 aperto presso Banca e di aver sottoscritto, in data 8-10-2014, il contratto "Servizi Via Internet, Cellulare e Telefono" n. , che disciplinava l'utilizzo tramite strumenti a distanza dei servizi offerti dall'istituto di credito, tra cui l'accesso al conto corrente mediante l'*home banking*.

L'attrice riferiva che, in data 1-03-2019, aveva riscontrato l'impossibilità di usare il proprio cellulare per effettuare chiamate in entrata e in uscita, per cui il 2-03-2019, recatasi presso il centro D sito in Roma, via Fucini n. 2, aveva ottenuto la sostituzione della vecchia SIM lasciando inalterata la vecchia utenza telefonica.

L'attrice esponeva poi che, in data 5-03-2019, aveva effettuato l'accesso al conto corrente mediante *home banking* e si era accorta dell'avvenuta sottrazione di € 178.100,00 tramite la disposizione di 12 bonifici non autorizzati, eseguiti tra il 28-02-2019 e il 2-03-2019 a favore della società C con

sede in Estonia, a lei sconosciuta; nonché, della sottrazione di ulteriori € 3.000,00 tramite due prelievi *cardless* eseguiti in data 2-03-2019 presso l'ATM n[redacted] gestito dalla Banca (ABI [redacted]), da lei non effettuati. Pertanto, considerati altresì gli addebiti commissionali per € 19,20 legati alle suddette operazioni, l'attrice affermava di aver subito una perdita complessiva di € 181.119,20.

La S[redacted], da un lato, evidenziava che le operazioni in contestazione erano state ordinate da terzi nonostante non avesse mai smarrito, lasciato incustodite o comunicato ad alcuno le proprie credenziali di accesso ai servizi di *home banking*, dall'altro, riferiva di non aver ricevuto dall'istituto di credito alcuna comunicazione a fronte delle operazioni di pagamento non autorizzate, nonostante avesse attivato sulla propria utenza telefonica il servizio di ricezione di un codice di sicurezza via SMS in caso di operazioni sensibili, sospette o in caso di pagamenti veloci effettuati senza il dispositivo O-Key.

L'attrice, quindi, esponeva di aver contattato, in data 5-03-2019, il numero verde di Banca [redacted]o per comunicare l'avvenuta frode e conoscere i dettagli delle operazioni illegittimamente disposte sul c/c; di aver sporto, poi, in data 6-03-2019, formale denuncia contro ignoti presso il Dipartimento di Polizia Postale e delle Comunicazioni sito in Roma, [redacted] in base alle informazioni ricevute dall'istituto di credito.

Inoltre, l'attrice riferiva che, in data 11-03-2019, aveva formalmente disconosciuto le suddette operazioni presso la filiale di [redacted] sita in via [redacted]; che, in data 2-08-2019, aveva trasmesso alla banca formale diffida, al fine di ottenere il rimborso delle somme illegittimamente sottratte dal c/c; che, non avendo ottenuto alcun riscontro, in data 6-11-2019, aveva avviato il procedimento di mediazione presso l'A[redacted]ma, il quale si era concluso con esito negativo.

La [redacted] specificava che la truffa era stata eseguita mediante l'introduzione illecita di terzi nel sistema telematico

della banca per la captazione dei propri codici d'accesso, oltre che per mezzo della clonazione della SIM card associata alla propria utenza telefonica. Per cui, ribadendo che non era configurabile a suo carico alcuna condotta negligente, l'attrice imputava alla banca la responsabilità dell'illegittima sottrazione di denaro dal c/c, contestandole l'omessa custodia dei propri dati personali e delle credenziali, l'omessa predisposizione di adeguati sistemi di sicurezza, nonché, una condotta gravemente colposa consistente nel mancato intervento dinanzi ad operazioni di pagamento obiettivamente anomale, al fine di predisporne il blocco, almeno temporaneo.

Per le suddette ragioni, l'attrice riteneva che I[redacted] avesse violato gli oneri posti a suo carico dal Regolamento UE n. 2016/679 (GDPR) in materia di protezione dei dati personali, dal D.lgs. 27 gennaio 2010 n. 11, attuativo della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno, nonché dall'art. 5 del contratto "Servizi via Internet, Cellulare e Telefono"; che, pertanto, la banca fosse obbligata a risarcirle la somma illegittimamente addebitata sul conto, detratta la franchigia di € 150,00 prevista dall'art. 5 del contratto, per una somma pari a € 180.969,20.

Da ultimo, l'attrice contestava alla banca di aver consentito operazioni di pagamento tramite bonifico eccedenti i limiti contrattualmente previsti (giornaliero di € 25.000,00 e mensile di € 50.000,00), chiedendo, in relazione a tale specifico inadempimento, di essere risarcita almeno della somma di € 166.600,00.

Si costituiva in giudizio I[redacted] S.p.A., in persona del legale rappresentante *pro tempore*, contestando quanto *ex adverso* dedotto poiché infondato in fatto ed in diritto e chiedendo l'accoglimento delle seguenti conclusioni:

"*Piaccia al Tribunale Ill.mo, respinta ogni contraria domanda, istanza, deduzione ed eccezione:*

1) respingere ogni avversa domanda in quanto inammissibile o comunque infondata per tutti i motivi ed eccezioni indicate in

atti, anche in ragione della esclusiva responsabilità di V[redacted] S.p.A., che si chiede di accertare;

2) in via subordinata, in caso di accoglimento (totale o parziale) della domanda avversaria, accertare la responsabilità solidale di V[redacted] S.p.A. e, in quest'ultimo caso, determinare la sua quota di responsabilità in misura non inferiore all'80% o nella diversa misura che sarà ritenuta di giustizia, con conseguente condannare di quest'ultima a corrispondere a I[redacted] un importo pari alla percentuale della condanna;

3) condannare l'attrice e la terza chiamata a corrispondere alla banca le spese, ai diritti ed agli onorari di causa".

A sostegno delle proprie ragioni, la convenuta esponeva di aver stipulato con S[redacted] in data 8-10-2014, il contratto "Servizi Via Internet, Cellulare e Telefono" che consentiva alla cliente di accedere al proprio conto corrente e di operare sullo stesso tramite *home banking;* nonché, di aver aggiornato il suddetto contratto, in data 04-05-2017, attraverso la stipula del contratto "M[redacted], per adeguare il servizio all'evoluzione tecnologica e alle nuove regole previste dalla normativa di settore interna e comunitaria. In particolare, il contratto "[redacted] sottoscritto dall'attrice prevedeva l'autenticazione a distanza della cliente tramite il sistema di autenticazione forte "a due fattori", basato cioè su elementi interdipendenti, ovvero sull'inserimento di credenziali statiche (UserId e Pin) consegnate alla cliente al momento dell'apertura del rapporto e di credenziali dinamiche aventi efficacia temporanea (codice OTP o OTS) generate dal sistema a completamento di ciascuna operazione da remoto ed inviate alla correntista tramite SMS sul cellulare certificato, nonché tramite notifica push sull'APP di I[redacted] precedentemente scaricata.

La convenuta specificava che il sistema di sicurezza adottato per il servizio di *home banking* era conforme allo stato dell'arte, tanto da essere certificato ISO/IEC 27001, cioè era tale da soddisfare lo *standard* internazionale per la sicurezza delle informazioni. Ciò, nel pieno rispetto delle indicazioni introdotte

[redacted]

dalla c.d. PSD 2 (Dir. UE 2015/2366 del Parlamento Europeo e del Consiglio del 25-11-2015), nonché dell'art. 10 bis d.lgs. n. 11/2010 attuativo delle norme comunitarie (nonostante all'epoca dei fatti lo stesso non fosse ancora entrato in vigore).

I[redacted]o, dunque, sosteneva che la conclusione delle operazioni fraudolente non era imputabile a difetti strutturali o al malfunzionamento contingente del sistema di *internet banking* utilizzato (come dimostrava il fatto che le operazioni contestate erano state tutte regolarmente autenticate tramite l'inserimento delle credenziali statiche e dinamiche, nonché correttamente registrate e contabilizzate), ma alla negligenza e mancanza di cautela dell'attrice, che non aveva conservato adeguatamente le credenziali statiche per accedere al servizio (Userid e PIN), consentendo a terzi di venirne a conoscenza e che non aveva adottato tempestive iniziative per bloccare l'operatività fraudolenta; nonché, all'illegittima duplicazione della scheda SIM della S[redacted], di cui era responsabile V[redacted], che aveva permesso agli autori della truffa di ottenere le credenziali dinamiche (OTP e OTS), indispensabili per completare l'esecuzione dei pagamenti a distanza.

Pertanto, la convenuta da un lato riteneva che la condotta gravemente colposa della [redacted], violativa degli obblighi di custodia e di comunicazione sulla stessa gravanti in base all'art. 7 D.Lgs. 11/2010 e alle norme contrattuali, integrasse un inadempimento tale da comportare l'addebitabilità alla cliente della perdita subita ex art. 12 c. 4 D.lgs. n. 11/2010, o almeno, il riconoscimento del concorso dell'attrice alla causazione dell'evento lesivo *ex* art. 1227 c.c. Dall'altro, procedeva alla chiamata in causa, a norma dell'art. 106 c.p.c., di V[redacted].p.A., per formulare nei confronti della stessa domanda di manleva, contestando al gestore telefonico una responsabilità esclusiva o almeno solidale (da inadempimento contrattuale o, comunque, ex artt. 1228 e 2049 c.c. per fatto illecito dei propri dipendenti) per l'esecuzione delle operazioni truffaldine ad opera di terzi, giacché V[redacted] aveva illegittimamente rilasciato un

duplicato della carta SIM dell'attrice senza eseguire le necessarie verifiche sull'identità del richiedente.

In seguito alla chiamata in causa ricevuta, si costituiva tempestivamente in giudizio V[redacted]., in persona del legale rappresentante pro-tempore, chiedendo l'accoglimento delle seguenti conclusioni:

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

In via preliminare:

Accertare e dichiarare l'inammissibilità dell'azione di inadempimento contrattuale così come esercitata da I[redacted] nei confronti di [redacted]a.

In via principale:

Rigettare tutte le domande proposte nei confronti di [redacted] perché infondate in fatto ed in diritto ed in ogni caso non provate.

In via subordinata:

per i motivi esposti in narrativa, nella denegata e non creduta ipotesi in cui dovesse essere ritenuta una qualche responsabilità da parte di V[redacted] in relazione agli asseriti danni lamentati da parte attrice:

a) accertare e dichiarare ai sensi dell'art. 1227 c.c. la partecipazione colposa totale, ovvero parziale, di Banca [redacted] e dell'attrice Sig.ra S[redacted] nella causazione dei pretesi danni dalla stessa asseritamente patiti, e/o evitabili usando l'orinaria diligenza, e, per l'effetto, anche per quanto detto in narrativa, rigettare le domande di parte attrice;

b) nella non creduta ipotesi in cui [redacted] fosse, eventualmente, chiamata a corrispondere all'attrice e/o ad altra parte processuale, qualsivoglia somma a titolo di indennizzo e/o risarcimento danni ovvero nella denegata ipotesi di accoglimento totale e/o parziale delle domande attoree e/o altra parte processuale, accertare e dichiarare l'esclusiva responsabilità di Banca [redacted] in persona del legale rappresentante pro tempore, in ordine ai fatti per cui è causa, tenendo

[redacted]

assolta/indenne [redacted] *da qualsivoglia pronuncia pregiudizievole ovvero, a titolo di garanzia e/o manleva, tenuta Banca* [redacted] *in persona del legale rappresentante pro tempore, a pagare e/o restituire a V*[redacted] *quanto eventualmente quest'ultima fosse condannata a corrispondere all'attrice e/o ad altra parte processuale ovvero, a titolo di ripetizione e/o rivalsa e/o regresso, tenuta Banca* [redacted] *in persona del legale rappresentante pro tempore, a pagare e/o restituire a V*[redacted] *quanto eventualmente quest'ultima fosse condannata a corrispondere all'attrice e/o ad altra parte processuale, il tutto oltre interessi.*

Il tutto con vittoria di spese e competenze di lite da attribuirsi all'Avv. [redacted] *per fattane anticipazione."*

V[redacted] [redacted] [redacted] eccepiva, innanzitutto, l'inammissibilità dell'azione per inadempimento contrattuale promossa da I[redacted] nei propri confronti, rilevando la carenza di legittimazione attiva della banca a fronte dell'insussistenza di obblighi contrattuali verso la stessa.

L'operatore telefonico, nel contestare ogni responsabilità in merito all'accaduto, riferiva poi di essersi limitato a sostituire la scheda SIM dietro richiesta di chi appariva il legittimo titolare dell'utenza telefonica e, pertanto, specificava di avere adempiuto ai propri oneri, non avendo il potere/dovere di accertare l'autenticità dei documenti mostrati al momento della richiesta sostitutiva.

[redacted], inoltre, specificava che il furto dell'identità digitale della S[redacted] era stato precedente al furto dell'identità telefonica della stessa mediante la sostituzione della SIM, costituendone l'antecedente logico. L'autore della truffa al momento della sostituzione della SIM era necessariamente già in possesso delle credenziali statiche (Userid e Codice PIN) indispensabili per accedere al servizio di *home banking*. Solo inserendo le suddette credenziali statiche, infatti, il truffatore aveva potuto ricevere tramite SMS o sull'APP scaricata sul

dispositivo mobile in uso (in cui aveva inserito la nuova SIM), i codici dinamici "OTP" e "OTS" generati dal sistema di *home banking*, necessari al completamento delle operazioni contestate.

Dunque, V[redacted] riteneva che la frode fosse fondata principalmente sull'utilizzo improprio dei dati personali dell'attrice (Userid e Codice PIN), di cui solo la correntista e la banca potevano essere a conoscenza.

Pertanto, l'operatore telefonico contestava all'istituto di credito di non aver tutelato adeguatamente i dati personali della S[redacted], adottando le contromisure tecnologiche necessarie a prevenire e/o bloccare tempestivamente attacchi e/o incidenti informatici; nonché, sotto altro aspetto, riteneva la banca responsabile di non aver segnalato alla correntista le operazioni sospette e/o di non averle tempestivamente bloccate, nonostante le disposizioni di pagamento fossero palesemente anomale.

In conseguenza, la società chiedeva che la condotta negligente di I[redacted] fosse valutata ex art. 1227 c.c.

D'altra parte, V[redacted] riteneva che l'illecito accesso al conto *online* dell'attrice fosse avvenuto anche tramite la collaborazione della stessa che, non adottando la dovuta diligenza nella custodia delle proprie credenziali bancarie, aveva agevolato il compimento delle operazioni fraudolente.

La società contestava altresì alla S[redacted] di non aver informato la banca del malfunzionamento del telefono cellulare al fine di bloccare tempestivamente il proprio conto *online*, posto che le operazioni bancarie in contestazione erano collegate anche all'utilizzo della SIM; nonché, di aver atteso due giorni dalla perdita della possibilità di effettuare chiamate prima di recarsi presso lo *store* V[redacted] per ricevere chiarimenti, e, quattro giorni prima di controllare il saldo del conto corrente e avere contezza delle operazioni illecite.

Pertanto, V[redacted] riteneva che anche la condotta di [redacted], gravemente colposa, dovesse essere valutata ex art. 1227 c.c.

All'udienza del 15-9-2020 parte attrice chiedeva di estendere la domanda nei confronti della chiamata in causa V[redacted] S.p.A. e, su istanza delle parti, il Giudice concedeva i termini ex art. 183 c. 6 c.p.c.

La causa veniva istruita sulla base della documentazione versata in atti dalle parti e tramite l'espletamento di CTU; all'udienza del 14-03-2023 queste precisavano le conclusioni come da relativo verbale e la causa veniva trattenuta in decisione con i termini per il deposito delle conclusionali e delle repliche.

MOTIVI DELLA DECISIONE

La domanda formulata da Sa[redacted] è solo in parte fondata, pertanto deve essere accolta, ma nei limiti di cui *infra*.

Giova evidenziare, ai fini della delimitazione del *thema decidendum*, che l'attrice nel presente giudizio ha chiesto accertarsi la responsabilità di Banca I[redacted] e di V[redacted] per l'effettuazione, ad opera di soggetti ignoti, di n. 12 bonifici per la somma complessiva di € 178.100,00, emessi, tra il 28-02-2019 e il 2-03-2019, dal c.c. n. 06812028579750142 alla medesima intestato; nonché, per l'illegittima sottrazione di ulteriori € 3.000,00 dallo stesso conto corrente, tramite due prelievi *cardless* eseguiti in data 2-03-2019 presso l[redacted]. In conseguenza, l'attrice ha domandato alle parti convenute il rimborso (anche in solido tra loro) della somma corrispondente alla perdita complessivamente subita (detratta la franchigia di € 150,00, come da contratto), nonché il versamento degli interessi legali e della rivalutazione monetaria, dichiarando il proprio incolpevole coinvolgimento nella frode bancaria informatica denominata "*Sim Swap Fraud*", consistente nella sottrazione di denaro da un c/c ad opera di terzi tramite l'ottenimento fraudolento del duplicato della SIM del correntista, che consente, previo accesso all'*home banking* (utilizzando nome utente e password del cliente, precedentemente al medesimo

carpiti), di ottenere i codici dinamici temporanei indispensabili al perfezionamento delle operazioni di gestione del conto e di pagamento a distanza.

Per parte propria, I[redacted]. ha contestato le domande attoree ed ha domandato il loro integrale rigetto, sostenendo il concorso colposo di S[redacted] nella causazione dell'evento lesivo; in via subordinata, ovvero in caso di accoglimento delle avverse domande, la banca ha chiesto accertarsi la responsabilità esclusiva o solidale di V[redacted], con conseguente condanna della stessa a rifonderle quanto, eventualmente, da corrispondere agli attori.

Di contro, V[redacted] ha domandato la reiezione delle domande *contra se* proposte contestando il concorso colposo della banca e della S[redacted] nella verificazione delle operazioni fraudolente, nonché, in via gradata, l'accertamento dell'esclusiva responsabilità di I[redacted] S.p.A. per le perdite subite dall'attrice e, conseguentemente, ha chiesto la condanna del solo istituto di credito a soddisfare la richiesta restitutoria della stessa.

Orbene, l'analisi della fattispecie concreta, effettuata considerando le peculiari dinamiche della *Sim Swap Fraud* alla luce delle difese proposte dalle parti, del quadro istruttorio di cui si dispone e della normativa applicabile, ha rilevato profili di responsabilità a carico sia dell'attrice che di [redacted] S.p.A., come di seguito illustrato.

Innanzitutto, deve darsi atto che in data 8-10-2014, S[redacted] ha stipulato con I[redacted]. il contratto "Servizi Via Internet, Cellulare e Telefono" [redacted] (cfr. doc. 1 allegato all'atto di citazione) per accedere al proprio conto corrente (c/c n. 06812028579750142) ed operare sullo stesso tramite *home banking*; che, in data 04-05-2017, il suddetto contratto è stato aggiornato tramite la stipula del contratto "[redacted] n. 04350290 (cfr. doc. 1 allegato alla comparsa di costituzione e risposta di I[redacted]). In base alla suddetta normativa contrattuale, le parti hanno pattuito che l'esercizio

dei servizi bancari a distanza sarebbe avvenuto tramite il sistema di autenticazione forte della cliente denominato "a due fattori", che prevede l'utilizzo congiunto di credenziali statiche (delle quali fa parte, per espressa previsione dell'art. 1 del contratto [redacted] anche il cellulare certificato - nel caso di specie abbinato al numero [redacted]) e di credenziali dinamiche inviate tramite SMS o notifica push nell'App scaricata sul cellulare certificato, consistenti in codici temporanei, generati sia per completare l'accesso al servizio che per autorizzare le disposizioni di pagamento. Ciò, conformemente all'art. 10 bis del d.lgs. n. 11/2010, introdotto con il d.lgs. n. 218/2017, nonostante all'epoca dei fatti di causa la norma non fosse ancora in vigore.

Il d.lgs. n. 11/2010, attuativo della direttiva 2007/64/CE (c.d. PSD1), da ultimo novellato con il d.lgs. n. 218/2017, emanato per recepire la nuova direttiva relativa ai servizi di pagamento 2015/2366/UE in vigore dal 13 gennaio 2018 (c.d. PSD2), individua in relazione all'utilizzo degli strumenti di pagamento elettronici e/o tramite canali a distanza che possano comportare un rischio di frode o di altri abusi, gli obblighi posti a carico del prestatore dei servizi e quelli gravanti sull'utente.

Quest'ultimo, ai sensi dell'art. 7, è tenuto: ad utilizzare gli strumenti di pagamento secondo i termini d'uso pattuiti con il prestatore dei servizi ed esplicitati nel contratto quadro; a comunicare allo stesso, non appena ne venga a conoscenza, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento di pagamento, al fine di consentirne il blocco; ad adottare tutte le misure idonee a proteggere dall'altrui ingerenza i dispositivi di accesso personalizzati, tra cui le credenziali di sicurezza personalizzate.

In base al successivo art. 12 c. 3, qualora l'utente dei servizi di pagamento violi uno dei suddetti obblighi con dolo o colpa grave o agisca in modo fraudolento, assume la responsabilità delle perdite relative all'utilizzo abusivo dello strumento di pagamento, per intero; diversamente, ha diritto di ottenere dal

prestatore dei servizi il rimborso della somma illecitamente sottrattagli, al netto di una franchigia di 50 euro, da applicarsi in caso "di operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita".

Quindi, come espressamente previsto dall'art 10 c. 2 d.lgs. 11/2010, il prestatore di servizi di pagamento può escludere la propria responsabilità per l'utilizzo non autorizzato dello strumento di pagamento ad opera di terzi, provando la frode dell'utilizzatore o il suo inadempimento per dolo o colpa grave, che costituiscono fatti impeditivi del risarcimento del danno ex art. 2697 c. 2 c.c.

Del resto, anche la giurisprudenza di legittimità ha affermato che "*la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa se ricorre una situazione di colpa grave dell'utente*" (cfr. Cass. 05/07/2019, n. 18045).

Specularmente, il d.lgs. n. 11/2010 pone anche a carico del gestore dei servizi di pagamento il rispetto di obblighi determinati, tra i quali rientrano: l'obbligo di assicurare, tramite l'adozione delle misure più idonee alla luce dello sviluppo tecnologico, che i dispositivi personalizzati per l'utilizzo dello strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato (art. 8 c. 1 lett. a); l'obbligo di assicurare che siano sempre disponibili gratuitamente strumenti adeguati affinché l'utilizzatore possa effettuare la comunicazione di cui all'art. 7 c. 1 lett. b (art. 8 c. 1 lett. c); l'obbligo di impedire l'utilizzo dello strumento di pagamento in seguito al blocco (art. 8 c. 1 lett. d); l'obbligo di attuare l'autenticazione forte del cliente, quando l'utente accede al suo conto di pagamento *online*, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione tramite un

canale di pagamento a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi (art. 10 bis c. 1).

Di talché, per far sì che l'utilizzatore sopporti le perdite derivate da un uso illegittimo dello strumento di pagamento ad opera di terzi, non è sufficiente che il prestatore del servizio dia prova di una condotta fraudolenta o dell'inadempimento degli obblighi ex art 7 d.lgs 11/2010 sorretto da dolo o colpa grave del cliente, dovendo altresì dimostrare, preventivamente, di aver adempiuto i doveri di tutela del consumatore prescritti a suo carico dal decreto (cfr. Cass. 26/11/2020, n. 26916).

L'art. 10 c. 1 d.lgs. 11/2010 afferma infatti che, qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione 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 altri inconvenienti".

In conclusione, è possibile affermare che l'imputazione di responsabilità all'utilizzatore dello strumento di pagamento, ex art. 12 c. 3 d.lgs 11/2010, presuppone che l'istituto di credito raggiunga una duplice prova, ossia: quella di aver usato un elevato grado di diligenza nell'adempimento dei propri oneri e quella che dimostri, con sufficiente grado di attendibilità giuridica, l'inadempimento degli obblighi del cliente dovuto a frode, dolo o colpa grave.

Nel caso di specie, I[redacted], a riprova della condotta negligente contestata alla S[redacted], nonché, a sostegno della regolarità formale delle operazioni fraudolente, ritenute correttamente autenticate, registrate e contabilizzate, oltreché eseguite secondo un sistema di autenticazione a due fattori supportato dalla certificazione UNI CEI ISO IEC 27001:2017 (cfr. docc. 5 e 6 all. a comparsa di costituzione e risposta della banca) da cui si evince l'elevato livello di sicurezza dello strumento di pagamento, confermato anche dalla CTU disposta nel corso dell'istruttoria (cfr. CTU pag. 14), ha prodotto in atti i

file log contenenti la tracciatura delle operazioni bancarie eseguite sul portale *home banking* dell'istituto di credito, nonché i *file log* da cui evincere specificamente gli accessi, gli SMS, le notifiche push, le caratteristiche degli IP unici relativi agli accessi, concernenti le operazioni in oggetto (cfr. docc. da 15 a 18 all. alla memoria 183 c. 6 n. 2 di I[redacted]).

Esaminata, anche tramite il supporto tecnico-scientifico del CTU, le cui conclusioni essendo immuni da vizi tecnico-argomentativi devono essere nella loro complessità condivise, la documentazione informatica, da ritenersi valida ed efficace nonostante le contestazioni delle parti avversarie, del tutto generiche e non esplicative dei motivi della pretesa inattendibilità della stessa, è stato possibile individuare la sequenza temporale delle operazioni effettuate sull'utenza V[redacted] intestata alla S[redacted]

Pertanto, è stato accertato che, in data 25-2-2019, S[redacted] ha correttamente effettuato l'*enrollment* dell'App di [redacted] sull'utenza [redacted] in uso su dispositivo iPhone XR, attivando il sistema O-Key Smart necessario per la generazione/ricezione di codici OTP e, dunque, per operare sull'*online banking* associato alla sua utenza telefonica, tramite il corretto inserimento delle credenziali statiche e di quelle dinamiche inviate dal sistema. Ciò, del resto, risulta comprovato anche dalla ricezione, alle h 20:34, della seguente notifica push: "*Attenzione. Stai attivando l'app I[redacted] sul dispositivo iPhone XR. Non hai richiesto tu l'attivazione? Contatta la Filiale online al numero 8[redacted]. Sei all'estero? Chiama il +39 8[redacted]*; nonché dalla ricezione, alle 20:37, dell'SMS: "*ATTENZIONE O-Key Smart è attiva su iPhone XR. Opera da questo dispositivo!*".

È stato altresì accertato che il 26-02-2019 alle h 16:32:24, dall'indirizzo IP:5.90.235.81. localizzato in zona Torre del Greco, ovvero da un indirizzo IP diverso da quello normalmente riconducibile alla S[redacted], è stata correttamente eseguita un'operazione di *login* sul conto *online* dell'attrice e, quindi, è

stata avviata un'operazione di *enrollment* dell'App della banca analoga a quella eseguita il giorno precedente, ma su un diverso dispositivo mobile (iPhone 6). Risulta poi dai *file log* che, alle h 16:32:27, sull'utenza telefonica [redacted] è stato ricevuto l'SMS: "*Usa il codice 237412 per attivare O-key Smart. ATTENZIONE NON FORNIRE A NESSUNO QUESTO CODICE! Usalo solo all'interno dell'APP Mobile sul tuo telefono*"; che, il suddetto codice OTP è stato correttamente inserito alle 16:32:55; che, alle 16:33 sull'utenza telefonica 3333390957 è stato inviato un SMS con l'indicazione di attivazione del sistema O-Key Smart su iPhone 6, del tutto simile a quello inviato il giorno precedente.

Confermando l'allegazione di V[redacted], la CTU espletata nel corso dell'istruttoria ha poi verificato che, nel pomeriggio del 28-2-2019, presso il punto vendita [redacted] cod. [redacted] point [redacted] sito nel comune di Napoli, la SIM n. [redacted] relativa all'utenza [redacted] di cui era titolare la S[redacted] è stata disattivata e sostituita dalla SIM n. [redacted] (sulla quale è rimasto operativo il numero telefonico [redacted]) con causale "furto/smarrimento" secondo le dichiarazioni del richiedente la sostituzione.

L'espletata CTU ha poi accertato che alle h 19:03 e 19:06 del 28-2-2019 sono stati inviati sull'utenza [redacted] e ricevuti sul telefono iPhone 6 localizzato in zona Torre del Greco, dotato della SIM duplicata, i codici di sicurezza necessari per completare 2 bonifici europei di tipo istantaneo a favore della società CB [redacted]; che, alle 19:09, è stato inviato e ricevuto il codice di sicurezza necessario per completare l'operazione di aumento dei limiti operativi, che ha consentito di innalzare il limite dispositivo giornaliero da € 15.000,00 ad € 30.000,00 ed il limite mensile da € 60.000,00 ad € 120.000,00; che successivamente, alle h 19:10 e 19:13 sono stati inviati e ricevuti i codici di sicurezza necessari per completare altri 2 bonifici europei istantanei in favore della predetta società. Allo stesso modo, il 1-3-2019 dalle h 00:04 alle 00:16 ed il 2-3-2019 dalle h 00:15 alle 00:35, sono stati inviati sull'utenza

3333390957 e ricevuti sul telefono iPhone 6 localizzato in zona Torre del Greco, dotato della SIM duplicata, i codici di sicurezza necessari per completare ulteriori 8 bonifici europei di tipo istantaneo in favore del medesimo destinatario; mentre, alle h 00:59 e 1:03 del 2-3-2019, l'utenza [redacted] ha ricevuto i codici di sicurezza necessari per completare 2 operazioni *cardless* presso la cassa automatica della filiale del Gruppo [redacted] di Napoli, [redacted] anch'esse andate a buon fine.

Orbene, alla luce delle superiori risultanze istruttorie, ritenendo le argomentazioni logico-inferenziali di I[redacted] attendibili ed adeguatamente circostanziate, si deve ragionevolmente presumere che S[redacted], in data 26-02-2019, contattata dall'autore della truffa, abbia incautamente comunicato i dati indispensabili per accedere all'*home banking* e rendere operativa l'APP di I[redacted] sull'iPhone 6, da cui sono stati disposti gli ordini di bonifico.

Tale deduzione discende dalle seguenti circostanze di fatto comprovate in corso di causa: la sostituzione della SIM n. [redacted] in possesso dell'attrice con la SIM n. [redacted]tilizzata dal truffatore, è avvenuta il 28-02-2019, per cui il 26-02-2019 è stata la S[redacted] a ricevere sull'utenza [redacted] l'SMS contenente il codice di attivazione della nuova APP (OTP 237412), che, 28 secondi dopo la ricezione dell'SMS sul cellulare della S[redacted] è stato correttamente utilizzato da un soggetto operante da un indirizzo IP localizzato in zona Torre del Greco, per completare il *download* del servizio *O-key Smart* sull'iPhone 6 da cui sono stati disposti i bonifici fraudolenti.

Pertanto, avuto riguardo alla dinamica e alle tempistiche dell'operazione di *enrollment* eseguita il 26-2-2019, appare del tutto logico desumere che sia stata l'attrice a comunicare in tempo reale al *phisher* il codice OTP 237412, nonché le credenziali statiche (Userid e Pin), inserite correttamente dal truffatore al primo tentativo pochi secondi prima dell'inserimento del codice

dinamico 237412, in quanto anch'esse necessarie per scaricare l'APP di [redacted] sullo *smartphone* iPhone 6.

Ciò, considerando altresì che la suddetta ricostruzione dei fatti non risulta contraddetta da evidenze istruttorie di segno opposto, in quanto l'attrice, che ha attribuito la conoscenza dei codici da parte del frodatore ad un possibile *malware* sui propri dispositivi, non ha depositato in atti lo *smartphone* iPhone XR né il PC di sua proprietà, perché fosse esaminato l'*hard disk* interno degli stessi a dimostrazione dell'erroneità del ragionamento presuntivo dell'istituto di credito. Né le deduzioni di [redacted] possono essere contraddette dall'affermazione del CTU secondo cui il messaggio "Recupero delle transazioni in attesa di validazione OTP" (che appare nel *file log* "tracciatura" 21 volte tra le 16:37:22 e le 17:37:06 del giorno 26-2-2019) sia univocamente indice della indisponibilità del codice OTP necessario ad operare da parte del truffatore. Tale affermazione, infatti, non può riguardare l'operazione di *enrollment* dell'APP sull'iPhone 6, che si è correttamente conclusa alle 16:33, dopo l'inserimento al primo tentativo dei codici statici (Userid e Pin) e del codice dinamico 237412, come risulta dai *file log* e come è stato altresì riscontrato dallo stesso CTU.

Sulla base delle risultanze istruttorie, dunque, deve concludersi che l'indisponibilità da parte del *phisher* dei codici OTP necessari ad operare risultante dalla dicitura "Recupero delle transazioni in attesa di validazione OTP" si riferisca a dei tentativi di movimentazione del conto corrente successivi all'*enrollment* dell'APP sul cellulare del truffatore, avvenuta con il corretto e tempestivo inserimento (al primo tentativo) sia delle credenziali statiche che dell'OTP 237412, i quali evidentemente sono stati forniti dalla S[redacted] in tempo reale.

Il che spiegherebbe anche la necessità del *phisher* di procedere, in data 28-2-2019, alla sostituzione della SIM per ricevere le ulteriori credenziali dinamiche indispensabili all'esecuzione dei bonifici, una volta scaricata l'applicazione ed accertata l'impossibilità di disporre operazioni di pagamento con

le sole credenziali statiche: passaggio del tutto superfluo qualora il frodatore avesse potuto captare i codici OTP senza la collaborazione della correntista, quindi tramite un *malware*, come parte attrice asserisce sia successo nel caso dell'*enrollment* dell'APP.

Del resto, la condotta gravemente colposa della S[redacted] non consiste solo nell'aver incautamente fornito le proprie credenziali di accesso all'*home banking* al *phisher*, nonostante la massiccia campagna antifrode realizzata da [redacted] a tutela dei propri clienti (cfr. docc. da 9 a 13 all. a comparsa di costituzione e risposta e doc. n. 20 all. alla memoria n. 2 della banca), risultando altresì dal fatto che la stessa ha imprudentemente ignorato: l'avvertimento della banca contenuto nell'SMS ricevuto alle h 16:32:27 del 26-2-2019, di non fornire a terzi il codice dinamico 237412 e di usarlo solo all'interno dell'App Mobile installata sul proprio cellulare; la comunicazione ricevuta con l'SMS delle 16:33 circa l'avvenuta installazione dell'APP C[redacted] su un *i-phone* diverso da quello da lei in uso, posto che l'attrice, ricevuto il suddetto avviso, avrebbe dovuto immediatamente rendere nota alla banca l'anomalia, consentendo all'istituto di credito di intervenire tempestivamente e di sventare il perfezionamento della frode con l'adozione delle opportune misure di sicurezza a tutela del conto corrente (tra cui il blocco cautelativo dello stesso) prima della sostituzione della SIM, avvenuta il 28-2-2019, ossia ben due giorni dopo l'*enrollment* dell'APP sullo smartphone del truffatore.

Per le ragioni di cui sopra, deve ritenersi che I[redacted] abbia dato prova, ex art. 2727 c.c., dell'inadempimento sorretto da colpa grave, da parte della S[redacted], dell'onere di custodia delle credenziali di sicurezza personalizzate, nonché dell'obbligo di comunicazione alla banca dell'uso non autorizzato dello strumento di pagamento, posti a carico della stessa dall'art. 7 del d.lgs. 11/2010. Deve inoltre ritenersi che la banca abbia provato, altresì, di aver predisposto le misure più idonee a garantire la tutela della cliente e ad evitare l'utilizzo

abusivo dello strumento di pagamento da parte di terzi non autorizzati, dapprima tramite una rilevante campagna informativa antifrode; poi, tramite l'adozione di un sistema di autenticazione a due fattori delle operazioni del tutto adeguato allo stato dell'arte (come attestato dalla certificazione UNI CEI ISO IEC 27001:2017 e confermato dalla CTU disposta nel corso dell'istruttoria), il cui regolare funzionamento è stato di fatto vanificato dalla condotta negligente della S[redacted] e dall'illegittima sostituzione della SIM da parte di V[redacted]; da ultimo, tramite l'utilizzo di un sistema informativo idoneo a comunicare in tempo reale alla cliente le operazioni gestorie e le movimentazioni del conto corrente, i cui *allert* del 26-2-2019, tuttavia, sono stati colpevolmente ignorati dall'attrice.

Per i motivi sopra esposti, la responsabilità di I[redacted] S.p.A. per la perdita derivata dalle disposizioni di pagamento in contestazione deve essere esclusa, giacché dal quadro probatorio risulta, con ragionevole certezza, che l'utilizzo abusivo dello strumento di pagamento da parte di terzi sia riconducibile alla condotta gravemente colposa della correntista S[redacted]

Oltre ciò, considerate le caratteristiche strutturali della *Sim Swap Fraud* e la specifica circostanza per cui la truffa non avrebbe potuto comunque perfezionarsi se il frodatore non fosse riuscito ad intervenire sull'utenza telefonica certificata, rendendola inattiva e dirottando a proprio favore l'invio delle credenziali dinamiche OTP e OTS tramite la sostituzione della SIM, deve essere altresì rilevata la responsabilità, concorrente con quella dell'attrice, di V[redacted], la cui condotta negligente, estrinsecatasi nell'omessa verifica dell'identità del richiedente la sostituzione, è causalmente connessa con l'esecuzione delle operazioni disconosciute.

A tal proposito, deve rilevarsi che l'operatore telefonico non ha allegato né dimostrato in alcun modo di aver posto in essere i dovuti accertamenti documentali e di riconoscimento dell'identità del richiedente prima della duplicazione della SIM, incentrando la

propria difesa sull'assunto per cui l'obbligo di identificare il cliente sussiste solo al momento della prima attivazione della SIM e non anche in occasione del rilascio del duplicato della stessa.

Sul punto occorre rilevare che l'art. 55 c. 7 del d.lgs. n. 259 del 2003 ha previsto in capo agli operatori di telefonia mobile un obbligo di identificazione degli abbonati e degli acquirenti prima dell'attivazione del servizio, stabilendo che ogni impresa è tenuta a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'Interno gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, i quali devono essere identificati prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (SIM). A tal fine, le suddette imprese di telefonia sono tenute ad adottare tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici riportati sul documento di identità esibito dal cliente e dei dati relativi al tipo e al numero del documento, nonché tutte le misure atte a garantire la corretta acquisizione della riproduzione del documento presentato dall'acquirente e ad assicurare il corretto trattamento dei dati ottenuti.

Ciò detto, la sussistenza nell'ordinamento di un obbligo di identificazione dei clienti anche per la mera sostituzione della SIM, del tutto similare a quello previsto in caso di attivazione della SIM, si evince senza ombra di dubbio dalla disposizione di cui all'art. 1 c. 46 della l. n. 124 del 2017, che prevede: "Al fine di semplificare le procedure di migrazione tra operatori di telefonia mobile e le procedure per l'integrazione di SIM card aggiuntive o per la sostituzione di SIM card richieste da utenti già clienti di un operatore, con decreto del Ministero dell'Interno, di concerto con il Ministero dello sviluppo economico, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, sono previste misure per l'identificazione in via indiretta del cliente, anche utilizzando il sistema pubblico dell'identità digitale previsto dall'art. 64

del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, in modo da consentire che la richiesta di migrazione e di integrazione di SIM card e di tutte le operazioni ad essa connesse possano essere svolte per via telematica", giacché la *ratio* di tale intervento normativo, ossia semplificare le modalità di identificazione del cliente nelle operazioni di migrazione, integrazione o sostituzione della SIM, trova un antecedente logico necessario nell'esistenza di un dovere in capo agli operatori telefonici di provvedere all'identificazione del cliente in occasione delle operazioni menzionate (cfr. *ex multis* Trib. Milano sent. 8562/2022, Trib. Ivrea sent. 543/2018, Trib. Savona sent. 428/2022).

Ad abundantiam, deve essere evidenziato che proprio la rilevanza del suddetto dovere ha determinato l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) all'emanazione della Delibera n. 86/21/CR dell'8-7-2021, citata dalle parti, ma non applicabile al caso di specie poiché successiva al verificarsi dei fatti di causa, che ha ulteriormente rafforzato l'obbligo di identificazione del richiedente la duplicazione della SIM da parte dei gestori dei servizi di telefonia, con l'espressa intenzione di garantire maggiore protezione ai dati personali dei clienti e di prevenire attività dolose attuabili tramite la sostituzione della SIM dell'utente da parte di soggetti terzi non autorizzati (tra cui, è specificamente citato il furto per via telematica presso gli istituti bancari).

Per i suddetti motivi, deve ritenersi che V[redacted] venendo meno al dovere di diligenza qualificata che si richiede ad un operatore professionale che gestisce dati personali altrui, non ha adempiuto all'obbligo di opportuna identificazione del soggetto che in data 28-2-2019 ha chiesto ed ottenuto la sostituzione della SIM di cui era titolare S[redacted], contribuendo con la sua condotta gravemente colposa, al pari dell'attrice, a rendere possibile la truffa.

[redacted]

V[redacted]A. deve, pertanto, essere condannata a rifondere a S[redacted] la somma di € 90.5596, corrispondente al 50% della perdita subita dall'attrice a seguito delle operazioni fraudolente.

Si deve ritenere, invece, che la correntista non abbia diritto alla restituzione dell'ulteriore 50% della perdita subita, posto che, come già specificato, la condotta gravemente colposa della stessa è stata definitivamente configurata in corso di giudizio quale concausa del perfezionamento dei pagamenti illeciti posti in essere dal frodatore.

In conseguenza, risultano assorbite la domanda di manleva formulata da I[redacted] nei confronti di V[redacted].p.A., nonché l'eccezione di carenza di legittimazione attiva di I[redacted] nei confronti di Vo[redacted] S.p.A. da quest'ultima formulata. Mentre, devono essere respinte la domanda di manleva, la domanda di graduazione della responsabilità ex art. 1227 c.c. e ogni altra domanda formulata da V[redacted] S.p.A. nei confronti di I[redacted] S.p.A.

Alla soccombenza, per ciò che riguarda le domande formulate nei confronti di Banca [redacted] consegue la condanna di S[redacted] e di V[redacted] S.p.A., in solido tra loro, alla rifusione, in favore dell'istituto di credito, delle spese di lite dallo stesso sostenute, nella misura liquidata in dispositivo.

Diversamente, tenuto conto della natura del presente giudizio ed essendo stati accertati profili di responsabilità a carico sia di S[redacted] che di V[redacted] le spese di lite tra dette parti devono essere interamente compensate.

Da ultimo, anche le spese per la espletata CTU seguono la soccombenza, tenuto conto delle domande come innanzi valutate, per il che sono poste definitivamente a carico di S[redacted] e di V[redacted] S.p.A., in solido tra loro, ed in pari misura.

P.Q.M

Il Giudice Unico del Tribunale di Roma, definitivamente pronunciando, ogni contraria istanza, eccezione e deduzione disattesa, nel contraddittorio tra le parti, così provvede:

rigetta la domanda formulata da Sa[redacted] nei confronti di I[redacted] S.p.A. per le ragioni di cui in motivazione;

accoglie parzialmente la domanda formulata da S[redacted] nei confronti di V[redacted] per le ragioni di cui in motivazione e, pertanto, condanna V[redacted]. al pagamento in favore di S[redacted], della somma di € 90.5596, pari al 50% dell'importo corrispondente alla perdita subita dalla correntista a causa delle operazioni illecitamente eseguite sul c/c n. [redacted] alla medesima intestato, oltre interessi legali a decorrere dall'11-11-2019;

dichiara assorbita la domanda di manleva formulata da I[redacted] nei confronti di V[redacted]

dichiara assorbita l'eccezione di carenza di legittimazione attiva di I[redacted] nei confronti di V[redacted] S.p.A., da quest'ultima formulata;

respinge la domanda di manleva, la domanda di graduazione della responsabilità ex art. 1227 c.c. e ogni altra domanda formulata da V[redacted] nei confronti di I[redacted];

condanna S[redacted] e V[redacted], in solido tra loro, al pagamento in favore di Banca [redacted] S.p.A. delle spese di lite dalla stessa sostenute, che liquida in complessivi € 7.600,00 per compensi professionali, oltre spese generali come da tariffa forense, IVA e CPA come per legge;

compensa interamente tra S[redacted] e V[redacted] S.p.A. le spese di lite;

pone definitivamente a carico di S[redacted] e V[redacted]., in solido tra loro ed in pari misura, le spese della espletata CTU.

Così deciso in Roma, in data 5 settembre 2023.

[redacted]

il Giudice Unico

dott. Giuseppe Di Salvo