REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
IL TRIBUNALE DI MILANO
SEZIONE VI CIVILE

Il Tribunale di Milano, VI sezione civile, in composizione monocratica, in persona della dott.ssa Anna Giorgia Carbone, ha emesso la seguente

SENTENZA

nella causa civile iscritta al N. **9645/2022** R.G. promossa da:

CWR S.r.l. (c.f. 06749970155), in persona del legale rappresentante pro tempore, con sede legale sita in Pero (MI) via Figino 66, e **T&T S.r.l** (c.f. 03119930698), in persona del legale rappresentante pro tempore, con sede legale in Pero (MI) via Figino 66/A entrambe elettivamente domiciliate in Milano, Corso Venezia n. 18, presso gli Avv.ti Andrea Monti del Foro di Pescara e Lorenzo Vigasio del Foro di Milano, che le rappresentano e difendono giusta procura in atti

ATTRICI

CONTRO

BPER BANCA S.p.A. (C.F. 01153230360 – P.IVA 03830780361), in persona del procuratore speciale pro tempore, con sede legale sita in Modena, Via San Carlo, 8/20, elettivamente domiciliata in Roma via conca d'Oro n. 285, presso l'Avv. David Giuseppe Apolloni, che la rappresenta e difende giusta procura in atti

CONVENUTA

NONCHE' CONTRO

TELECOM ITALIA S.p.a., oggi anche TIM S.p.a. (P.IVA 00488410010), in persona del legale rappresentante pro tempore, con sede legale sita in Milano, p.za Affari, n. 2 elettivamente domiciliata in Roma, via Oslavia n. 12, presso l'Avv. Fabrizio Badò del foro di Roma, che la rappresenta e difende giusta procura in atti

CONVENUTA

OGGETTO: accesso abusivo home banking

CONCLUSIONI :

Per parte attrice

"*Voglia l'adito Tribunale di Milano, ritenuta la propria competenza per materia, valore e territorio, contrariis rejectis:*

1–NEL MERITO, IN VIA PRINCIPALE

A–accertare e dichiarare la responsabilità delle convenute nella causazione dei danni subiti dalle attrici per effetto delle condotte di cui in narrativa e per l'effetto

B- condannare le convenute a pagare solidalmente tra loro in favore di Cwr S.r.l. la somma € 94.516,26 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria;

C– condannare le convenute a pagare solidalmente tra loro in favore di T & T S.r.l. la somma € 67.991,94 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria;

2–NEL MERITO, IN SUBORDINE

A–accertare e dichiarare, la misura della responsabilità di ciascuna convenuta nella causazione dei danni sopra descritti nella misura indicativa del 50% ciascuna salvo diverso riparto percentuale all'esito dell'espletanda istruttoria e per l'effetto,

B- condannare ciascuna di esse, per quanto di ragione, al pagamento in favore della Cwr S.r.l. della somma € 94.516,26 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria secondo la rispettiva quota di responsabilità;

C–condannare ciascuna di esse, per quanto di ragione, al pagamento in favore della T&T S.r.l. della somma € 67.991,94 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria secondo la rispettiva quota di responsabilità;

3–NEL MERITO, SULLE SPESE

Con vittoria di spese ed onorari di lite e sentenza esecutiva come per legge";

Per parte convenuta Bper Banca S.p.A.

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

IN VIA PRELIMINARE

autorizzare la chiamata in causa del terzo TIM S.p.A. in persona del legale rappresentante pro tempore, Codice Fiscale/Partita IVA e Iscrizione al Registro delle Imprese di Milano: 00488410010, con sede in Via Gaetano Negri, 1 - 20123 Milano, e, per l'effetto, pronunciare decreto di spostamento della prima udienza di comparizione ai sensi e per gli effetti degli artt. 106, 167 e 269 c.p.c. al fine di consentire la chiamata in giudizio nel rispetto dei termini di cui all'art. 163 bis c.p.c.;

NEL MERITO

In via principale:

Rigettare in toto la domanda di parte attrice in quanto infondata in fatto e in diritto per tutte le ragioni esposte in narrativa, con vittoria di spese legali oltre IVA e CAP come per legge.

In via subordinata:

nella denegata e non creduta ipotesi di accoglimento anche solo parziale delle domande promosse da CWR s.r.l. e da T&T s.r.l., riconoscere la esclusiva responsabilità di TIM S.p.A. in persona del legale rappresentante pro tempore nella causazione dei danni lamentati dalle società attrici e, per l'effetto, condannarla a tenere indenne Bper Banca S.p.a. da qualsiasi pregiudizio economico in merito ai fatti di causa, sostituendo, quindi l'istituto di credito nel pagamento di qualsivoglia somma riconosciuta al ricorrente a qualsivoglia titolo.

In via di ulteriore subordine:

nella denegata e non creduta ipotesi di accoglimento anche solo parziale delle domande promosse da CWR s.r.l e T&T s.r.l., accertare e dichiarare il concorso di colpa delle società attrici e di TIM S.p.A. nella misura che sarà ritenuta di giustizia, nella causazione dell'evento."

Per la convenuta Telecom Italia S.p.A.

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

- in via principale, respingere ogni avversa domanda, in quanto destituita di fondamento in fatto ed in diritto;

- sempre, in via principale ed in subordine, nella denegata e non creduta eventualità di accoglimento, anche parziale, delle domande formulate da CWR S.r.l. e T&T S.r.l. nel presente giudizio, accertare e dichiarare l'esclusiva responsabilità, per i fatti per cui è causa, dell'altra convenuta BPER – Banca Popolare per l'Emilia Romagna S.p.a. - C.F./P.IVA: 01153230360 – PEC: bper@pec.gruppobper.it, in persona del legale rappresentate pro tempore, con sede legale in Modena, Via San Carlo, n. 8/2 (41121), e, all'effetto;

- condannare, la stessa BPER – Banca Popolare per l'Emilia Romagna S.p.a. - C.F./P.IVA: 01153230360 – PEC: bper@pec.gruppobper.it, in persona del legale rappresentate pro tempore, con

sede legale in Modena, Via San Carlo, n. 8/2 (41121), al risarcimento d'ogni somma riconosciuta in favore delle attrici CWR S.r.l. e T&T S.r.l. e/o, comunque, a manlevare e tenere indenne, la TIM S.p.a., da ogni conseguenza pregiudizievole derivante dalla pretesa avanzata dalle attrici CWR S.r.l. e T&T S.r.l. con il presente giudizio, condannando la stessa BPER – Banca Popolare per l'Emilia Romagna S.p.a. - C.F./P.IVA: 01153230360 – PEC: bper@pec.gruppobper.it, in persona del legale rappresentate pro tempore, con sede legale in Modena, Via San Carlo, n. 8/2 (41121), a rimborsare a TIM S.p.a. quanto, eventualmente, riconosciuto in favore delle attrici CWR S.r.l. e T&T S.r.l., ovvero a pagare, direttamente, alle predette attrici CWR S.r.l. e T&T S.r.l., ogni somma a questo riconosciuta, oltre le spese legali;

- con vittoria di spese, anche generali, ed onorari".

ESPOSIZIONE DELLE RAGIONI DI FATTO E DI DIRITTO DELLA DECISIONE

1. Premessa – Svolgimento del giudizio

Con atto di citazione in giudizio ritualmente notificato le società CWR s.r.l. e T. & T. s.r.l., in persona del legale rappresentante pro tempore, convenivano in giudizio Bper Banca S.p.A. (quale cessionaria di Banca Intesa Sanpaolo S.p.A.) e Telecom Italia S.p.A. per ivi accertare e dichiarare la responsabilità delle convenute nella causazione dei danni subiti dalle attrici per effetto di abusivi accessi nel sistema di home banking e conseguentemente condannarle al pagamento in solido tra loro in favore di Cwr S.r.l. della somma € 94.516,26 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria, nonché in favore di T & T S.r.l. la somma € 67.991,94 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria. In subordine chiedevano, previo accertamento e declaratoria della responsabilità di ciascuna convenuta nella causazione dei danni sopra descritti nella misura indicativa del 50% ciascuna salvo diverso riparto percentuale all'esito dell'espletanda istruttoria, la condanna delle convenute al pagamento in favore della Cwr S.r.l. della somma € 94.516,26 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria secondo la rispettiva quota di responsabilità, nonché al pagamento in favore della T&T S.r.l. della somma € 67.991,94 o quella maggiore o minore ritenuta di giustizia a seguito dell'istruttoria secondo la rispettiva quota di responsabilità, con vittoria delle spese di lite.

A fondamento della propria pretesa le attrici deducevano che:

- nel dicembre 2020 le attrici intrattenevano rapporti di conto corrente bancario con la Banca Intesa San Paolo S.p.a. presso l'agenzia di Pero (MI), quest'ultima ceduta in data 21 giugno 2021 insieme a tutti i rapporti presso di essa esistenti alla BPER S.p.a.;
- le società odierne attrici erano titolari di due distinti rapporti di conto corrente presso Banca Intesa San Paolo S.p.a, entrambe accesi fin dal 2012 presso la filiale di Pero (Mi), quanto alla CWR S.r.l. con il seguente codice iban IT95L0306933560000003232106, quanto alla T & T S.r.l con il seguente codice iban IT57T0306933560000004444120;
- ai suddetti conti correnti era annesso il servizio di internet banking dedicato alle imprese e denominato INBIZ, il cui funzionamento era incentrato su un c.d. sistema di sicurezza, che prevedeva l'autenticazione dell'utente mediante username e password, cui seguiva una notifica da autenticare. Al servizio di internet banking si accedeva tramite la piattaforma www.intesasanpaoloinbiz.com;
- il numero 3460647695 su cui venivano inviati dal sistema le notifiche con la richiesta di reinserire il PIN era associato ad una sim Tim S.p.a di cui è titolare sin dal 2011 la CWR SRL e nella disponibilità della Sig.ra Michela Brambilla, della CWR S.r.l. e che operava su entrambi i conti;

- il giorno 29 dicembre 2020 la Dott.ssa Michela Brambilla si recava in ufficio per alcuni adempimenti di fine anno sebbene l'azienda fosse chiusa per ferie dal 24 dicembre al 7 gennaio; alle ore 11,45 dopo aver precedentemente, alle 11,00 circa, utilizzato la piattaforma www.intesasanpaoloinbiz.com per effettuare alcune disposizioni di pagamento, la Dott.ssa Brambilla tentava di accedere nuovamente al servizio di internet banking per effettuare ulteriori disposizioni, che tuttavia non riusciva a portare a termine poiché le notifiche contenenti le richieste di reinserimento PIN non arrivavano sul numero dedicato il 3460647695;
- di fronte al perdurare dell'anomalia la Dott.ssa Brambilla contattava alle ore 14,11 il servizio assistenza INBIZ Banca Intesa al numero verde 800312316 per segnalare l'anomalia
- nel corso della telefonata durata circa venti minuti, veniva consigliato dall'operatore di disinstallare e reinstallare nuovamente l'applicazione INBIZ, cosa che la Dott.ssa Brambilla faceva nel corso della stessa chiamata supportata dall'operatore, riconfigurando l'applicazione;
- a seguito di tale operazione la Dott.ssa Brambilla constatava che le notifiche di autenticazione per continuare l'installazione non arrivavano;
- di fronte al perdurare dell'anomalia l'operatore faceva presente alla Dr.ssa Brambilla che il problema non era ascrivibile al sistema operativo della Banca, ma, verosimilmente, all'operatore telefonico, suggerendole di segnalare il problema all'assistenza Tim;
- immediatamente, la Dott.ssa Brambilla si attivava per segnalare l'anomalia ai numeri dedicati all'assistenza Tim, effettuando tra le ore 14,34 e le 15,15, nove chiamate ai numeri di assistenza Tim 119, 187 e 191 in seguito alle quali appurava che la numerazione, il 3460647695, era attiva, e quanto al perdurante mancato ricevimento dei messaggi di autenticazione lo stesso operatore Tim si limitava ad ipotizzare una correlazione tra il disservizio lamentato e le precipitazioni nevose verificatesi in quei giorni ed ai conseguenti problemi di connessione determinate dall'evento atmosferico;
- la Dott.ssa Brambilla, permanendo l'impossibilità di accesso alla piattaforma dell'internet banking, prima di lasciare gli uffici della CWR intorno alle ore 16,30 inviava una mail alla collega Sig.ra Nadia Missaglia, che era in ferie, facendo presente di avere problemi con il telefono utilizzato per accedere ai conti e chiedendole di stampare e inviare i movimenti dei giorni successivi e di mandarglieli il giorno seguente;
- come richiesto dalla Sig.ra Brambilla la Sig.ra Nadia Missaglia provvedeva all'accesso tramite il numero 3381107595 e a stampare ed inoltrare a mezzo email in data 30 dicembre 2020 i movimenti sul conto corrente della CWR;
- la Sig.ra Brambilla solo dopo aver preso visione della mail inviatale dalla collega constatava che in data 29 dicembre dai conti delle società attrici erano stati disposti N. 4 bonifici non autorizzati, di rilevanti importi e precisamente:

  a) in data 29 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Grassi Anna IT50U3608105138273966457398O BB di € 14.950,09 (causale acconto TFR);

b) in data 29 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Troise Giuseppina IT75F3608105138227809827998 BB di € 14.980,45 (causale saldo fattura 583/11/2020 del 30/11/2020);

c) in data 29 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Tullio Salvatore IT75F3681051382278098279 98 BB di € 14.960,36 (causale saldo vostre fatture numero 29/30/31/32 del 04/08/2020);

d) in data 29 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Luna Raffaele IT53J0200830520000105975376 BB di € 49.670,36 (causale pagamento vendita volkswagen amarok v6 tdi);

- constatava, inoltre, che alla data del 30 dicembre risultavano in lavorazione altri 2 bonifici i quali venivano successivamente bloccati:

  e) in data 30 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Antonio Nogarotto IT66H360810513822704876 BB di € 9.800,00 (Bloccato);

  f) in data 30 dicembre 2020 dal c\c avente iban IT95L0306933560000003232106 in favore di Grassi Anna IT50U3608105138273965473980 BB di € 14.500,00 (andato in addebito al 31/12/2020 ma stornato e riaccreditato in data 05/01/2021);

- analogamente dal conto della T&T S.r.l. si constatava che alla data del 29 Dicembre erano stati eseguiti n.4 bonifici non autorizzati:

  a) in data 29 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di Cirillo Luigi IT76N3608105138267826782916784 2 BB di € 14.760,30 (causale Polizze scadenze 31.12-2020);

  b) in data 29 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di Gelsomina Lofredo IT10A3608105138292817692823 BB di € 14.860,39 (Causale TF 12 2020);

  c) in data 29 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di De Felice Luigi IT91M3608105138268473668480 BB di € 14.970,30 (Causale Saldo Fattura 45236 12 2020);

  d) in data 29 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di Karlis Kaucis DE34100110012626159069 3 di BB € 23.400,95 (Causale Fatt 11 2020 scad);

- con valuta 31 Dicembre 2020 risultavano in lavorazione 2 bonifici per i quali successivamente si aveva lo storno e il riaccredito:

  e) in data 31 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di Cirillo Luigi IT76N3608105138267826782916784 2 BB di € 14.550,00 (andato in addebito al 31/12/2020 ma stornato e riaccreditato in data 05/01/2021);

  f) in data 31 dicembre 2020 dal c\c avente iban IT57T0306933560000004444120 di T & T S.r.l. BB in favore di Di Tullio Salvatore IT75F3608105138277856277862 di € 14.700,00 (andato in addebito al 31/12/2020 ma stornato e riaccreditato in data 05/01/2021);

- la Sig.ra Brambilla alle ore 17,00 del 30 dicembre 2020, non appena constatato che dai conti della CWR S.r.l. e della T&T S.r.l. erano stati disposti dei bonifici non autorizzati, cercava di contattare il referente Intesa Sig.ra Guaglianone e chiedeva, inoltre, alla collega Sig.ra Missaglia di avvisare telefonicamente l'assistenza INBIZ per segnalare i fatti e chiedere l'immediato blocco di tutte le operazioni non autorizzate;

- l'operatore Intesa nel corso della telefonata assicurava di aver bloccato tutte le operazioni ancora pendenti ovvero quelle disposte in data 30 dicembre 2020, mentre per quelle del 29 dicembre sarebbe stato necessario recarsi in filiale;
- subito dopo, alle ore 17,00 la Sig.ra Brambilla provava a chiamare telefonicamente il proprio gestore — Guaglianone—ma senza esito essendo il cellulare della signora Guaglianone spento; pertanto inviava alla stessa alle h. 17,53 un'email recante in oggetto la dicitura URGENTE = ADDEBITO ERRATO al funzionario Cristina Guaglianone segnalando che dal conto risultano essere stati disposti bonifici non autorizzati;
- i bonifici non autorizzati sui conti delle due società in data 29 dicembre 2020 risultavano essere stati disposti nella fascia oraria 12,38- 13,29 dello stesso giorno;
- alle 20,53 del 30/12/2020 la Sig.ra Brambilla veniva richiamata dalla Sig.ra Guaglianone sul cellulare, la quale dopo avere appreso dell'accaduto invitava la Sig.ra Brambilla a recarsi in filiale il giorno successivo insieme al Sig. Corbani (legale rappresentante delle società);
- il 31/12 la Sig.ra Brambilla e il Sig. Corbani prima si recavano nella filiale e successivamente andavano a sporgere denuncia-querela a carico di ignoti presso gli Uffici del Compartimento di Polizia Poste e delle Comunicazioni per la Lombardia;
- nell'occasione, il Sig. Corbani apprendeva dagli operanti della Polizia che raccoglievano la denuncia che il tipo di frode perpetrata in danno delle due società si realizzava attraverso il furto delle credenziali di accesso alla piattaforma di internet banking grazie alla tecnica nota come "sim swap". Questa tecnica consisteva nell'ottenere da parte dall'operatore telefonico un duplicato della sim impersonando un referente aziendale, in modo da ricevere su un altro telefono (nelle mani dei malintenzionati) le notifiche di autenticazione con il messaggio di autenticazione necessario per poter accedere al servizio di internet banking.
- lo stesso Sig. Corbani quindi alle ore 19,03 circa del 31 dicembre 2020 allarmato da quanto ascoltato dalla Polizia Postale riguardo questo tipo di truffe, si rivolgeva al servizio clienti TIM S.p.A. per chiedere se avessero ricevuto delle richieste di cambio SIM sul numero aziendale usato per le transazioni bancarie nei giorni precedenti;
- l'operatrice CU221 di nome Erika confermava che il 29 Dicembre 2020 alle ore 10,46 era stato eseguito un cambio SIM su tale numero e che avrebbe provveduto alla segnalazione dell'accaduto all'Ufficio Frodi di Tim S.p.A.;
- il 4 gennaio 2021 alle ore 17,40 circa una nuova chiamata dell'assistenza Tim preannunciava l'avvio di una pratica di rimborso di € 325,00 per ristorare l'utente per "la mancanza dell'operatore". Questa proposta veniva considerata irrisoria e immediatamente rigettata dal Sig. Corbani;
- in data 14 gennaio 2021 il Sig. Corbani in qualità di legale rappresentate p.t. delle società attrici presentava all'istituto di credito ai sensi dell'art. 10 del D.Lgs.n.11/2020 modulo di disconoscimento con contestuale richiesta di rimborso delle somme relative alle operazioni non autorizzate, indicando nello stesso tutte le operazioni disposte sui conti delle società attrici in data 29 dicembre 2020

- in data 13/01/2021 per Euro 79.611,17 ed in data 04/02/2021 per Euro 14.950,09 la Banca provvedeva temporaneamente, e con riserva di ripetizione allo storno delle operazioni disconosciute, al riaccredito sul conto della CWR S.r.l. della complessiva somma di € 94.516,26, ed in data 13/01/2022 sul conto della T&T S.r.l. riaccreditava la complessiva somma di € 67.991,94.
- in data 23 febbraio 2021 la Banca con due PEC comunicava alle società il riscontro negativo delle pratiche di disconoscimento "in quanto è stato accertato che i sistemi di sicurezza della banca non sono stati violati", comunicando altresì di aver provveduto al riaddebito in conto delle somme precedentemente anticipate "SBF";
- in data 1° marzo 2021 a mezzo raccomandata A.R. entrambe le società diffidavano Banca Intesa Sanpaolo S.p.a contestando alla Banca di essere restata inerte nonostante le criticità segnalate, chiedendo il riaccredito di tutte le somme relative alle operazioni non autorizzate e disconosciute;
- alla richiesta di riaccredito con note del 15 aprile 2021 Banca Intesa San Paolo S.p.a. ribadiva alle società attrici di non avere responsabilità per la truffa informatica di cui erano state vittime evidenziando al contempo che come "segnale di attenzione" nei confronti dei clienti si era resa disponibile a riaccreditare somme "pari al 50% degli importi disconosciuti". Nelle stesse note la Banca registrava il diniego alla proposta transattiva precedente ed in altra sede espresso dalle società attrici.

In diritto le attrici contestavano in capo alla Banca la violazione del dovere di diligenza e buona fede ai sensi dell'art.10 D.lgs. 11/2010 in rapporto alla delibera AGCOM334/20/CIR del 19 novembre 2020, invocando una responsabilità di natura contrattuale; anche le ulteriori doglianze relative all'inadeguatezza dei sistemi di sicurezza predisposti da Bper Banca Spa e alla negligente condotta della stessa a seguito delle segnalazioni operate dalla dipendente delle attrici si inseriscono nell'alveo delle responsabilità contrattuali.
Nei confronti di Tim Spa, invece, veniva contestata la violazione dell'art. 6 d.lgd. 259/03, con conseguente richiesta risarcitoria ai sensi dell'art. 2043 c.c., salvo poi rilevare profili di negligenza nella condotta della convenuta e chiedere il risarcimento dei danni anche ex art. 1218 c.c..
A contestazione delle Si costituiva Bper Banca Spa che in via preliminare chiedeva la chiamata in causa di Tim Spa, quale esclusiva responsabile del danno lamentato dalle attrici; in via principale e nel merito chiedeva di rigettare le domande dell'attore, in quanto infondate, in fatto e diritto; in subordine, nella denegata e non creduta ipotesi di accoglimento anche solo parziale delle domande
promosse da CWR s.r.l. e da T&T s.r.l., chiedeva di accertare e riconoscere la esclusiva responsabilità di TIM S.p.A. nella causazione dei danni lamentati dalle società attrici e, per l'effetto, condannarla a tenere indenne Bper Banca S.p.a. da qualsiasi pregiudizio economico in merito ai fatti di causa, sostituendo, quindi l'istituto di credito nel pagamento di qualsivoglia somma riconosciuta al ricorrente a qualsivoglia titolo. In via di ulteriore subordine la convenuta domandava di accertare e dichiarare il concorso di colpa delle società attrici e di TIM S.p.A. nella causazione dell'evento.
La convenuta a sostegno delle proprie domande deduceva che:

- in via preliminare Bper Banca SpA illustrava le modalità di esecuzione di un bonifico on line, composta da tre step:

a) il soggetto titolare del conto doveva inserire le proprie password all'interno dell'ambiente home banking, conosciute solo dallo stesso;
b) il cliente riceveva sul numero di cellulare comunicato la OTP (c.d. One Time Password);
c) il cliente doveva inserire la One Time Password, all'interno della schermata della piattaforma;

- precisava poi che le parti attrici erano due società a responsabilità limitata, con uno specifico ufficio addetto alla contabilità, e che annoverano tra le proprie risorse anche una dipendente laureata che era responsabile amministrativa e contabile, la dott.ssa Michela Brambilla che effettuava quotidianamente bonifici;
- la convenuta rilevava altresì che più persone avevano accesso e codici per operare sui conti

  oggetto di causa, ciò configurando una palese negligenza da parte delle attrici nella tutela dei codici di accesso e addebitando alle stesse la responsabilità per il fatto accaduto;
- contestava inoltre la ricostruzione dei fatti avversaria, ritenendola contraddittoria e in ogni caso non provata: in particolare l'attrice asseriva di aver operato con bonifici durante la mattina del 29 dicembre 2021, salvo poi accorgersi alle ore 11.45 del 29 dicembre 2020 di non ricevere sul numero di cellulare collegato gli sms contenenti l'OTP per l'accesso alla piattaforma ed il perfezionamento di bonifici on line;
- la dottoressa Brambilla avrebbe quindi contattato la Banca solo due ore e mezza più tardi, alle 14,11 e successivamente avrebbe chiamato l'assistenza TIM solo alle 14,34, quasi tre ore dopo;
- i bonifici disconosciuti venivano eseguiti in una fascia temporale compresa tra le 12.38 e le 13.29, precedente al momento in cui la dottoressa avrebbe effettuato la segnalazione alla banca;
- contestava poi la Banca che la dottoressa avesse parlato con l'operatore di Intesa all'orario indicato, anche perché non essendo la titolare del conto corrente interessato non poteva fare alcuna telefonata, in quanto non legittimata a ricevere alcuna informazione al riguardo,
- ad ogni modo l'operatore forniva alla dottoressa tutte le indicazioni corrette, poichè stando alla tesi delle attrici, l'operatore aveva riferito che non vi era alcun problema sui sistemi informatici della banca, invitandola a controllare la sua linea telefonica;
- la dottoressa Brambilla, inoltre, aveva effettuato regolarmente operazioni la mattina del 29 dicembre 2020, sicché l'assistenza non avrebbe potuto accorgersi di eventuali anomalie né essere fondatamente allertata di truffe in corso;
- la convenuta precisava altresì che il telefono in uso alla Brambilla, dal momento in cui la SIM richiesta illegittimamente veniva attivata, aveva smesso di funzionare, sicché la stessa avrebbe dovuto accorgersi che la linea era del tutto inattiva e completamente inutilizzabile;
- la dottoressa avrebbe quindi erroneamente chiamato la banca, anziché verificare lo stato della linea telefonica, stante la circostanza che la scelta del gestore telefonico era rimessa esclusivamente al cliente;

- la richiesta inviata dalla Brambilla alla collega Missaglia sarebbe poi la dimostrazione che le attrici già in data 29.12.2020 potevano controllare i bonifici mediante accesso con altro numero, sicchè la dottoressa aveva già sospetti in merito a quanto stava succedendo e se si fosse attivata più tempestivamente avrebbe visualizzato i bonifici e potuto/dovuto porre in essere tutte le attività necessarie e dirette a scongiurare il perfezionamento delle operazioni non autorizzate;
- la responsabile della contabilità, inoltre, decideva di non recarsi immediatamente nella filiale della banca, ove avrebbe potuto con i funzionari verificare il conto e bloccare le operazioni;
- in definitiva la Dott.ssa Brambilla non si attivava efficacemente per controllare il conto, limitandosi a chiedere alla collega di inviarle l'indomani i movimenti del conto corrente intestato a CWR S.R.L;
- la negligenza delle società sarebbe provata anche dal fatto che già il 29 dicembre 2020 i responsabili della contabilità ed il legale rappresentante sarebbero stati a conoscenza dei problemi di accesso al conto; eppure, per loro stessa ammissione, nonostante la possibilità di accedere al conto tramite un altro telefono cellulare, aspettavano le 17e52 del giorno successivo per attivarsi nella visione dei movimenti e mandando a quell'ora una mail alla responsabile di Banca Intesa;
- per contro a prova dell'efficienza della banca, questa rammentava la telefonata del 30 dicembre 2022 alle 20,53 con cui l'operatore Intesa invitava la signora Brambilla a recarsi in filiale l'indomani mattina.
- A ciò aggiungeva che tali modalità di frodi erano conosciute dalle clienti perché allertate, oltre che dai mezzi di informazione, anche dalla stessa banca.

Nel merito la convenuta affermava che la responsabilità per i fatti occorsi in data 29.12.2020 fosse imputabile unicamente alle attrici per non aver osservato le cautele necessarie nella custodia dei codici di accesso al proprio conto corrente online; in ogni caso era censurabile il comportamento tenuto dalle stesse nelle giornate successive al fatto, stante la tardiva segnalazione al funzionario di Banca Intesa (ora Bper Banca) contattato solo nella serata del 30.12.2020 la consulente dell'istituto di credito, anziché presentarsi immediatamente allo sportello in filiale per bloccare le operazioni. Deduceva altresì la bontà del proprio operato ribadendo che il sistema di sicurezza adottato dalla Banca era più che idoneo a tutelare la clientela da siffatti eventi e che non risultavano esserci stati accessi abusivi al sistema.
In relazione alla chiamata in causa di Tim SpA affermava che quest'ultima avesse omesso ogni controllo e cautela necessari nelle fasi di identificazione dei soggetti richiedenti il cambio di SIM, circostanza questa causalmente influente sulla dinamica degli eventi per cui è causa, sicché ne chiedeva la condanna a manlevarla in caso di accoglimento delle domande attoree nei propri confronti.
Si costituiva altresì Telecom Italia S.p.A. (divenuta TIM S.p.A.) la quale preliminarmente chiedeva di poter chiamare in causa a propria manleva Bper Banca S.p.A. ritenendola a sua volta unica responsabile cui addebitare il danno lamentato dalle attrici.
Nel merito domandava il rigetto di tutte le pretese attoree in quanto infondate in fatto ed in diritto ed in subordine nella denegata e non creduta eventualità di accoglimento, anche parziale, delle domande formulate da CWR S.r.l. e T&T S.r.l. nel presente giudizio, l'accertamento dell'esclusiva responsabilità dell'altra convenuta BPER – Banca Popolare per

l'Emilia Romagna S.p.a. - condannandola al risarcimento d'ogni somma riconosciuta in favore delle attrici CWR S.r.l. e T&T S.r.l. e/o, comunque, a manlevare e tenere indenne, la TIM S.p.a., da ogni conseguenza pregiudizievole derivante dalla pretesa avanzata dalle attrici CWR S.r.l. e T&T S.r.l. condannando la stessa Bper a rimborsare a TIM S.p.a. quanto, eventualmente, riconosciuto in favore delle attrici CWR S.r.l. e T&T S.r.l., ovvero a pagare, direttamente, alle predette attrici CWR S.r.l. e T&T S.r.l., ogni somma a questo riconosciuta, oltre le spese legali.

Sosteneva la convenuta che:

- Telecom non aveva contribuito, con modalità causalmente efficiente, nella generazione della frode per cui è causa, con particolare riferimento alla contestata – da parte delle attrici - attivazione di nuova SIM card dell'utente intestatario CWR S.r.l., in relazione al n. 3460647695;
- le attrici, peraltro, non offrivano, nemmeno alcun documento idoneo a dimostrare il collegamento tra il numero di telefono n. 3460647695 ed i c/c per l'operatività di banca on line;
- dagli accertamenti eseguiti da TIM risultava, effettivamente, che l'utenza telefonica cellulare n. 3460647695 è stata attivata in data 21.5.2013, quale linea Business, intestata alla CWR: detta linea telefonica risultava, allo stato, attiva;
- l'attivazione dei servizi internet avveniva mediante l'utilizzo di codici statici [cioè userid e password, noti solo al correntista] ed utilizzando l'inserimento di un ulteriore codice numerico OTP (one time password) generato, direttamente, dai sistemi operativi della banca e che perveniva al correntista, via sms e che veniva, quindi, recapitato sul proprio cellulare (durata di efficacia del codice di 16 secondi circa, dopo il quale lo stesso risulta inattivo, per ragioni di sicurezza);
- il correntista accedeva ai servizi di banca on line digitando i codici statici, solo a sua conoscenza: userid e password; quindi al momento di impartizione dell'ordine dispositivo, ad es. di pagamento mediante bonifico, doveva inserire il codice OTP, pervenuto, via sms e proveniente dalla banca;
- a decorrere dal 14.9.2019, per espressa disposizione normativa, le operazioni dispositive non potevano più essere autorizzate mediante utilizzo dei codici statici ed OTP generato da token (one time password, da generatore numerico nella disponibilità e fisica custodia del correntista), ma, appunto, attraverso una nuova modalità (richiesta in adeguamento di normativa europea - Dir UE 2015/2366 rec. D.L. 15/12/2017 cd. Dir PSD2, la seconda Direttiva sui servizi di pagamento);
- al tempo dei fatti Banca Intesa e, quindi, oggi, anche, la BPER, avevano anticipato tale termine, modificando il proprio sistema operativo di accesso bancario on line, per mezzo, esclusivamente, di invio sul cellulare dell'utente/correntista di un messaggio, via sms e, quindi, abolendo l'accesso a mezzo di codice generato con dispositivo fisico (token).

Nel merito la difesa di Tim SpA si associava a quanto dedotto da Bper Banca SpA in relazione alla responsabilità esclusiva o quantomeno concorrente delle attrice per omessa custodia dei codici di accesso, salvo poi riconoscere una responsabilità anche in capo alla banca stessa per

omessa vigilanza sul proprio sistema informatico e di sicurezza, chiedendo di essere da questa manlevata in caso di condanna a favore delle parti attrici.
Verificata la regolare costituzione delle parti e concessi i termini istruttori, Il Giudice ammetteva prova per testi; esaurito l'incombente istruttorio, ritenuta la causa matura per la decisione, concedeva termini per gli atti conclusivi e tratteneva la causa in decisione.

2. Sussistenza di profili di responsabilità in capo a Bper Banca SpA e Tim SpA

La causa attiene alla tematica dell'esecuzione di operazioni di pagamento, nello specifico bonifici a distanza tramite servizio di Home Banking. In particolare, si tratta di operazioni eseguite tramite gli strumenti di pagamento, cioè i dispositivi personalizzati, sulla base di un insieme di procedure concordate tra l'utente di servizi di pagamento ed il prestatore di servizi di pagamento utilizzate per disporre un ordine di pagamento mediante una procedura di autenticazione che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, compreso l'uso delle credenziali di sicurezza personalizzate dell'utente.
Ciò posto, nel merito la domanda è fondata e deve essere accolta nei limiti di seguito esposti.
In primo luogo, occorre premettere che le operazioni contestate sono state effettuate in data 29.12.2020, sicché trovano applicazione, in relazione alla fattispecie in esame, le disposizioni di cui al d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. n. 218/2017, di attuazione della direttiva 2015/2366/EU, come correttamente richiamato dalle parti attrici.
In materia la giurisprudenza di legittimità ha provveduto ad inquadrare 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 internet 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. 11/2010, applicabile anche nel presente giudizio. La normativa richiamata sancisce l'obbligo del prestatore del servizio di pagamento di assicurare che i dispositivi personalizzati forniti dai gestori non siano accessibili a soggetti diversi dal legittimo titolare e detta alcune disposizioni specificamente indirizzate a ripartire le responsabilità derivanti dall'utilizzazione del servizio stesso.
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 discenda 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.
La Corte di Cassazione ha altresì precisato che "*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 o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo*" (Cass. n. 2950/2017; v. anche Cass. n. 10638/2016; Cass. n. 9158/2018 Cass. n. 26916/2020 e, da ultimo, Cass. n. 16417/2022).
A tale stregua, spetta, dunque, al prestatore del servizio offrire la prova di avere adottato tutti i migliori accorgimenti della tecnica volti a scongiurare il rischio di impiego fraudolento degli strumenti di pagamento e del comportamento fraudolento o gravemente colposo dell'utilizzatore, tale da escludere la sua responsabilità.
Nel caso di specie, sotto il primo profilo (di cui all'art. 10, comma 1 e all'art. 10 bis, d.lgs. 27 gennaio 2010, n. 11), dalla stessa descrizione della truffa perpetrata si desume che l'istituto di credito fosse dotato di un'autenticazione c.d. "forte", come richiesto dalla normativa vigente. Sul punto mette conto osservare che la predisposizione da parte della convenuta di un sistema di autenticazione forte per l'operatività su conto on line di per sé non rappresenta, come dedotto dalla difesa di parte convenuta, il massimo delle cautele tecnologicamente possibili per contrastare fenomeni fraudolenti simili a quello in specie occorso, 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. Peraltro, nemmeno può rivestire pregio al riguardo l'invocata attività della convenuta, consistita in una campagna informativa di sicurezza mirante a fornire indicazioni

ai clienti in presenza di sospetti casi fraudolenti. Invero, 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 inidonei ad evitare la perpetrazione di questo tipo di frodi, tanto più tenuto conto di come la mail o 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.
Peraltro, la Suprema Corte ha statuito che "*nonostante la banca non abbia alcun dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente, nondimeno, in presenza di circostanze anomale idonee a ledere l'interesse del correntista, la banca, in applicazione dei doveri di esecuzione del mandato secondo buona fede, deve rifiutarne l'esecuzione o almeno informarne il cliente*" (cfr. tra molte Cassazione Civile, 31 marzo 2010, n.7956, sez. I): nel caso di specie la banca era stata avvertita della sussistenza di anomalie sia il giorno stesso del fatto, sia il giorno immediatamente successivo, con molteplici telefonate al numero dedicato e alla consulente di fiducia della società. Tale comportamento è, quindi, di per sé sufficiente a destituire di ogni fondamento le difese della convenuta Bper SpA.
Quanto al secondo profilo, fatta eccezione per l'ipotesi dell'elemento soggettivo del dolo, invero mai prospettato dalle parti, deve ritenersi che l'istituto di credito non abbia adeguatamente provato l'allegata colpa grave del cliente, rinvenibile, in tesi, nell'avere omesso le necessarie cautele per la conservazione delle credenziali personali. La banca e la società di telefonia convenute deducono nei propri scritti difensivi che le attrici oltre alle credenziali avrebbe riferito al truffatore anche il codice OTP, ma tale tesi non ha trovato riscontro probatorio nemmeno nelle deposizioni testimoniali rese da Brambilla e Missaglia (verbale udienza del 15.09.2023) della cui attendibilità non si ha motivo di dubitare atteso che da un lato vertono su circostanze non contestate dalle convenute e dall'altro collimano con le risultanze documentali versate in atti.
Alla luce di tali argomentazioni deve senz'altro affermarsi la responsabilità della banca convenuta in ordine al danno lamentato dalla società attrice, conformemente al prevalente orientamento giurisprudenziale secondo il quale, in caso di operazioni bancarie effettuate a mezzo di strumenti elettronici, la non corretta operatività del servizio bancario mediante collegamento telematico, ivi compresa la possibilità di una abusiva utilizzazione delle credenziali di accesso da parte di terzi, rientra nel rischio d'impresa della banca intermediaria, sulla quale grava pertanto una responsabilità di tipo oggettivo, dalla quale la banca va esente solo provando che le operazioni contestate dal cliente sono attribuibili a dolo o colpa grave di quest'ultimo.
Si è infatti affermato che "i*n 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 o 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" (Cass. 03/02/2017 n. 2950; Cass. 12/04/2018 n. 9158; Cass. 20/05/2022 n. 16417); in precedenza si era affermato che "*in tema di ripartizione dell'onere della prova, al correntista abilitato a svolgere operazioni "on line" che, alla stregua degli artt. 15 del d.lgs. n. 196 del 2003 e 2050 c.c., agisca per l'abusiva utilizzazione (nella specie, mediante illegittime disposizioni di bonifico) delle sue credenziali informatiche, spetta soltanto la prova del danno siccome riferibile al trattamento del suo dato personale, mentre l'istituto creditizio risponde, quale titolare del trattamento di dato, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei codici d'accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile perché discendente da trascuratezza, errore o frode del correntista o da forza maggiore*" (Cass. 23/05/2016 n. 10638).

E ancora riguardo al profilo della prova del dolo o della colpa grave del cliente, la medesima giurisprudenza ha inoltre chiarito che la stessa debba essere fornita positivamente dal prestatore di servizi, non potendo presumersi in ragione dell'idoneità delle protezioni adottate dalla banca, al fine di evitare l'esecuzione di operazioni fraudolente. In questo senso si è pronunciata la Cassazione civile sez. VI, 26/11/2020, n. 26916: "*La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente*".

Nel caso in esame la banca non ha fornito la prova di alcuna specifica condotta dolosa o colposa del cliente alla quale possano ricondursi le operazioni disconosciute dal medesimo, né può affermarsi che le misure tecnologiche di sicurezza adottate dalla convenuta siano tali da escludere la possibilità di abusiva utilizzazione delle credenziali di accesso da parte di terzi, essendo comunque possibile che le operazioni in questione siano riconducibili ad azioni fraudolente di terzi (poste in essere, ad esempio, mediante attacchi di phishing e/o spoofing e/o man in the middle e/o trojan) che hanno interessato i dispositivi e i link di accesso bancari delle risorse aziendali dell'attrice nella giornata e negli attimi antecedenti alle disposizioni digitali oggetto di contestazione.

Al contrario è pacifico perché non contestato che le attrici siano state vittime della truffa denominata "*sim swap*" nell'ambito della quale i criminali dapprima agiscono sottraendo alla vittima le credenziali (statiche) di accesso ai sistemi di home banking attraverso attività di phishing o di altra equivalente; successivamente, si fanno rilasciare in modo fraudolento dalla compagnia telefonica una duplicato della *sim card* intestata a chi deve essere raggirato ed ottengono l'annullamento di quella in uso al titolare, che, mantenendo lo stesso numero, tende a non avvedersi della truffa in corso; così ottenuto il duplicato della *sim*, i criminali informatici sono in grado di ricevere gli sms con i codici OTP e/o OTS (credenziali dinamiche) inviati dalla banca al numero di cellulare ormai in pieno possesso dei truffatori.

Deve pertanto ritenersi che l'attrice sia rimasta vittima di una truffa informatica, essendo i truffatori riusciti — attraverso l'articolata sequela di atti fraudolenti sopra (sinteticamente) descritti — a carpire le credenziali statiche e dinamiche di accesso ai conti online di CWR srl e T&T srl e a compiere con esse bonifici evidentemente non avallati dalle titolari dei conti correnti.

Ebbene, in relazione a tale truffa non può ritenersi sussistente la colpa grave della vittima che, in questo tipo di frodi, a seguito della disattivazione della *sim* ad opera dei truffatori, non riceve alcuna comunicazione dalla banca circa le operazioni in corso di esecuzione e neppure i messaggi contenenti i codici OTP e/o OTS e dunque non è posta in condizione di avvedersi

della truffa in suo danno. Quanto poi all'acquisizione delle credenziali di accesso statiche, non vi è prova che le stesse siano state colposamente fornite dalle attrici ai truffatori nell'ambito di campagna di phishing da questi posta in essere (in questo senso Tribunale di Palermo, 3787/2023).
Né, ai fini dell'art 1227 c.c., la Banca ha provato il concorso di colpa del danneggiato. Infatti, anche a volere ritenere, come prospettano la banca e la compagnia telefonica, che le attrici abbiano incautamente conservato i codici statici, le modalità della truffa sono state talmente capziose e subdole che non può ravvisarsi alcun concorso di colpa nel danneggiato.
Proseguendo con l'analisi dei fatti, è pacifico e non contestato che Tim SpA rilasciava un duplicato della *sim* legata all'utenza 3460647695 a seguito di una richiesta presentata da un soggetto asseritamente titolato all'operazione.
Sul punto Tim SpA non solo non solleva contestazioni circa la sussistenza del fatto, ma nemmeno svolge una difesa circa la legittimità del proprio operato in merito ai necessari controlli relativi all'identificazione del richiedente, come invece previsto dalla legge.
Ciò posto, si osserva che il D.lgs n. 196/2003 come novellato dal D.lgs 101/2018 in attuazione del Reg. EU 2016/679, ha introdotto molteplici disposizioni in tema di diritto della protezione dei dati personali, imponendo al titolare del trattamento di dover provare, in caso di evento dannoso, di aver adottato le migliori soluzioni disponibili a tutela dei dati da lui gestiti.
Infatti è evidente che la gestione si rivela tanto più delicata allorquando la diffusione dei dati personali possa ingenerare problematiche come quella qui in esame.
Ora, valutando la condotta della compagnia telefonica, emerge che la stessa abbia colposamente contribuito alla realizzazione della truffa di cui le attrici sono state vittime, non avendo assicurato alla cliente un'idonea protezione dei suoi dati.
Deve essere infatti stigmatizzato come la Compagnia telefonica abbia provveduto alla sostituzione della *sim* senza operare un preliminare controllo sul regolare funzionamento di quella già consegnata all'utente e senza approfondire i motivi della richiesta dell'istante.
Altresì è incontestato che l'operatore consegnava il duplicato senza richiedere la restituzione della precedente *sim* laddove non funzionante, ovvero la consegna di una denuncia-querela, nel caso di preteso furto o smarrimento.
Anche l'identificazione dell'istante è risultata fallace, ben potendo l'operatore effettuare un confronto delle firme del sottoscrittore del contratto con quella apposta dal terzo nel modulo di richiesta di duplicato.
Tali accorgimenti, per i quali sarebbero nemmeno necessarie particolari dotazioni tecniche ma solo un'adeguata, possibile ed auspicabile formazione del personale, risultano il minimo atto di diligenza che qualsiasi imprenditore di elevate dimensioni e di imponente organizzazione, come una compagnia telefonica, avrebbe dovuto/potuto adottare per scongiurare fatti come quello qui in esame (in tal senso si veda Tribunale di Monza n. 1518/2022).
Pertanto, risulta evidente il nesso causale tra la condotta omissiva dell'operatore rispetto alla truffa informatica ai danni delle attrici, dal momento che, se la nuova *sim* non fosse stata duplicata e consegnata ad un soggetto non autorizzato, l'evento dannoso non si sarebbe verificato.
In conclusione, va riconosciuta a CWR srl a titolo di risarcimento dei danni subiti la complessiva somma di € 94.516,26 e a T&T srl la somma complessiva di € 67.991,94, entrambe in moneta attuale, oltre interessi legali dalla data odierna e sino al soddisfo da porre a carico delle convenute in solido avendo entrambe concorso a cagionare il danno subito dalle attrici.

Sulle somme riconosciute in favore degli attori sono inoltre dovuti gli interessi compensativi per la ritardata corresponsione dell'equivalente pecuniario del danno, posto che, nelle obbligazioni di valore, il debitore è in mora dal momento della produzione dell'evento di danno; peraltro, avuto riguardo ai principi enunciati dalla sentenza n. 1712/1995 delle SS.UU. della Corte di Cassazione, al fine di evitare un lucro ingiustificato per il creditore, e per meglio rispettare la funzione compensativa dell'interesse legale riconosciuto sulla somma rivalutata, gli interessi devono essere calcolati non sulla somma rivalutata (o espressa in moneta attuale) al momento della liquidazione, nè sulla somma originaria, ma debbono essere computati sulla somma originaria che via via si incrementa, a partire dal livello iniziale fino a quello finale, nei singoli periodi trascorsi.

Pertanto, recependo i principi di cui alla sentenza n. 1712 del 17 febbraio 1995 delle Sezioni Unite della Corte di Cassazione la somma corrispondente al capitale rivalutato alla data odierna (euro 110.867,57 ed € 79.754,55) deve essere devalutata alla data del fatto (29.12.2020) e poi progressivamente rivalutata, di anno in anno, secondo gli indici I.S.T.A.T. dal 29 dicembre 2020 fino alla data della presente pronuncia; sull'importo come determinato all'attualità, sono poi dovuti gli ulteriori interessi legali, ex art. 1282 c.c., dalla presente pronuncia fino al saldo effettivo.

Le spese processuali seguono la soccombenza delle convenute e sono liquidate come in dispositivo ai sensi del D.M. 55/2014 come modificato dal D.M. 147/22, 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, ogni contraria istanza ed eccezione disattesa, definitivamente pronunciando sulle domande proposte da C.W.R. S.R.L. e T. & T. S.R.L. contro BPER BANCA S.P.A E TELECOM ITALIA S.P.A (ora TIM S.P.A.) così provvede:

a. accertata la responsabilità Bper Banca S.p.A. e Telecom Italia S.p.A. (ora Tim S.p.A.) condanna le stesse in solido tra loro al pagamento a favore di C.W.R. S.R.L. della somma di € 110.867,57, oltre accessori come specificati in motivazione;

b. accertata la responsabilità Bper Banca S.p.A. e Telecom Italia S.p.A. (ora Tim S.p.A.) condanna le stesse in solido tra loro al pagamento a favore di T. & T. S.R.L. della somma di € 79.754,55, oltre accessori come specificati in motivazione;

c. condanna Bper Banca S.p.A. e Telecom Italia S.p.A. (ora Tim S.p.A.) in solido tra loro a corrispondere a C.W.R. S.R.L. e T. & T. S.R.L. a titolo di spese processuali l'importo di € 14.100,00 liquidato a titolo di compenso di avvocato, oltre rimborso forfetario per spese generali, nella misura del 15% del compenso, oltre ad IVA e CPA come per legge.

Milano, 9 agosto 2024

Il Giudice
Anna Giorgia Carbone