N. [redacted] R.G.

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

TRIBUNALE ORDINARIO di MONZA

SEZIONE I CIVILE

Il Tribunale di Monza, Sezione I Civile, nella persona del Giudice monocratico dott.ssa Chiara Binetti, ha pronunciato la seguente

SENTENZA

nella causa civile di primo grado iscritta al n. [redacted] r.g. promossa da:

Parte_1 (C.F./P.I. *C.F._1*, rappresentato e difeso dall'avv. [redacted], elettivamente domiciliato come in atti

PARTE ricorrente

contro

Controparte_1 (C.F./P.I. *P.IVA_1*), rappresentato e difeso dall'avv. [redacted], elettivamente domiciliato come in atti

PARTE resistente

OGGETTO: Bancari (deposito bancario, cassetta di sicurezza, apertura di credito bancario)

CONCLUSIONI

Le parti hanno precisato le conclusioni come segue:

Per *Parte_1* LIVA
NEL MERITO IN VIA PRINCIPALE
Accertare e dichiarare che il sistema di autenticazione predisposto da *CP_1* non rispetta i requisiti di cui al D.lgs 11/2010
Accertare e dichiarare che, in ogni caso, il sistema di autenticazione e sicurezza predisposto dal *[...]* *CP_1* non ha funzionato correttamente ed è stato violato dai frodatori
Accertare e dichiarare la responsabilità contrattuale del *CP_1* non avendo operato secondo la richiesta diligenza e prudenza ex art. 1176 c.c.
Accertare e dichiarare che la signora *Pt_1* non ha avuto alcun intento fraudolento e non sia incorsa in dolo o colpa grave

Accertare e dichiarare il diritto della signora *Pt_1* ad ottenere il rimborso delle perdite subite e ammontati ad Euro 18.063,00
E per l'effetto, condannare il *Controparte_1* a versare in favore della ricorrente Euro 18.063,00, o la maggiore o minore somma ritenuta di giustizia
NEL MERITO IN VIA SUBORDINATA
Nella denegata ipotesi in cui l' *CP_2* Giudice adito dovesse ravvisare un concorso di colpa della ricorrente, fermo restando l'accertamento della violazione del D.lgs 11/2010 relativamente ai sistemi di autenticazione di *CP_1*
Accertare e dichiarare in ogni caso la prevalente responsabilità della resistente in merito agli eventi occorsi
Accertare e dichiarare che la signora *Pt_1* ha diritto al rimborso almeno del 80% delle somme illegittimamente sottratte dal proprio conto corrente
E, per l'effetto, condannare *Controparte_1* a versare in favore della signora *Pt_1* la somma di Euro 14.811,66 o la maggiore o minore somma ritenuta di giustizia
IN VIA ISTRUTTORIA
Si chiede di sottoporre a interpello formale la resistente e a interrogatorio libero la ricorrente sui fatti di causa e riportati nella narrativa del presente atto, nonché di essere ammessi a prova diretta e contraria sui capitoli di prova testimoniale eventualmente formulati dalla resistente.

In ogni caso con vittoria di spese e onorari di giudizio

Per *Controparte_1*
Voglia l'Ill.mo Tribunale adito, contrariis rejectis, previa ogni più ampia ed opportuna declaratoria, così giudicare:
IN VIA PRELIMINARE
- accertare e dichiarare l'inammissibilità, improponibilità, improcedibilità del ricorso ex art. 281-undecies c.p.c. per i motivi illustrati in narrativa ovvero accertare e dichiarare che le difese svolte dalle parti richiedono un'istruzione piena per i motivi illustrati in narrativa e, ai sensi dell'art. 281-duodecies c.p.c., disporre con ordinanza non impugnabile la prosecuzione del processo nelle forme del rito ordinario (stante la complessità della causa) fissando l'udienza di cui all'art. 183 c.p.c., rispetto alla quale decorrono i termini previsti dall'art. 171-ter c.p.c.;
NEL MERITO
IN VIA PRINCIPALE
- per tutte le ragioni esposte, respingere le domande tutte ex adverso formulate perché infondate, sia in fatto che in diritto anche alla luce della recentissima Ordinanza n. 7214 del 13 marzo 2023 della Suprema Corte di Cassazione;
- per tutte le ragioni esposte, accertare e dichiarare la colpa grave della sig.ra *Pt_1* e l'assenza di qualsivoglia responsabilità in capo a *CP_1* ;
- per tutte le ragioni esposte ed alla luce della recentissima Decisione ABF del Collegio di Milano 9628 del 6 ottobre 2023, accertare e dichiarare che il sistema di autenticazione forte - SCA in uso presso *CP_1* è conforme alla normativa di riferimento;
IN VIA SUBORDINATA

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

IN VIA ISTRUTTORIA

- rigettare tutte le istanze istruttorie ex adverso formulate per i motivi illustrati in narrativa.

Con ogni riserva di merito e istruttoria.

Con vittoria di spese, competenze e relativi compensi unici, oltre oneri accessori come per legge. Il tutto liquidato ai sensi e per gli effetti D.M. 55/2014, con maggiorazione ex art. 4, comma 1-bis D.M. 55/2014.

MOTIVI DELLA DECISIONE

Parte_1, con ricorso regolarmente depositato ex art. 281 decies c.p.c., ha convenuto in giudizio il *Controparte_1* affinché venisse condannato al pagamento di euro 18.063,00 in suo favore a titolo di risarcimento dei danni subiti per una truffa realizzata ai danni della ricorrente attraverso la tecnica del cd. "spoofing".

A sostegno del ricorso, la ricorrente ha dedotto in fatto le seguenti circostanze:

- di aver ricevuto in data 29.12.2022 sulla propria utenza telefonica cellulare un *sms* riportante il seguente messaggio di testo: "*Nexi informa che ha limitati la sua carta di credito/conto per mancata verifica della sicurezza web; riattivala ora: www. Email_1 .*";
- che mediante collegamento ipertestuale aveva ottenuto l'accesso ad una piattaforma nella quale inserire le credenziali di autenticazione per l'applicazione *CP_1* (cfr. doc. n. 12);
- che subito dopo, aveva ricevuto sulla stessa utenza telefonica una chiamata dal numero di telefono corrispondente alla filiale *CP_1* di Milano (026367901) (cfr. doc. 2);
- che, seguendo quindi le istruzioni impartite dall'operatore telefonico, aveva proceduto al *reset* della password di accesso all'applicazione e all'inserimento della nuova *password* nella piattaforma cui accedeva tramite il *link* ricevuto via *sms*;
- che, seguendo le istruzioni dell'operatore telefonico, aveva successivamente inserito la *password* del proprio account e-mail e aveva quindi ricevuto comunicazione che l'operazione si era conclusa con successo e che avrebbe ottenuto successivamente nuove comunicazioni per verificare lo stato dell'operazione;
- che, decorsi tre giorni dall'accaduto, senza ricevere ulteriori comunicazioni, aveva quindi contattato il servizio clienti di *Controparte_1* e aveva appreso di essere stata truffata attraverso la predisposizione, da parte del truffatore, di n. 5 bonifici sul suo conto corrente;
- che quindi in data 5.01.2023 aveva sporto denuncia del reato patito presso il Comando dei Carabinieri di [redacted] (cfr. doc. 1).

Sulla base di tali allegazioni e sostenendo la responsabilità contrattuale della *CP_3* per non aver adottato le misure idonee a garantire un adeguato livello di sicurezza per l'accesso all'*home banking* e per la predisposizione di pagamenti, aveva inoltrato reclamo per la restituzione delle somme lei sottratte, a cui il *Controparte_1* dava responso negativo (cfr. doc. 3 e 5).

Dopo aver svolto reclamo dinnanzi all'Arbitro Bancario e finanziario e ottenuto un provvedimento favorevole di accoglimento, a cui però il *CP_1* non si era uniformato, la ricorrente ha azionato il presente giudizio (cfr. doc. 7).

Nel costituirsi nel presente giudizio il *Controparte_1* ha contestato l'avversa pretesa, sostenendo di aver adottato un sistema di autenticazione cd. "forte" per la procedura di *login* all'*home banking* e per l'autorizzazione delle disposizioni di pagamento. Ha quindi concluso per l'accertamento della responsabilità per colpa grava della attrice, allegando a sostegno delle proprie deduzioni anche una perizia di parte.

Dopo la concessione dei termini di cui all'art. 281 *duodecies* co. 4 c.p.c. ed il deposito delle relative memorie, la causa, ritenuta matura per la decisione, è stata rinviata ai sensi dell'art. 281 *sexies* c.p.c., all'udienza del 27.06.2024 per la precisazione delle conclusioni e la discussione orale ed infine trattenuta in decisione ai sensi del terzo comma della predetta norma.

***

Preliminarmente, va respinta la richiesta di parte resistente di accertare e dichiarare l'inammissibilità/improponibilità/improcedibilità del ricorso ex art. 281- *undecies* c.p.c., in quanto le difese svolte dalle parti non hanno richiesto un'istruzione piena e i fatti di causa non sono risultati particolarmente controversi. Inoltre, si rileva che la domanda è fondata su prova meramente documentale: le principali risultanze istruttorie emergono dai documenti già in atti. Dunque, il ricorso ai sensi dell'art. 281-*duodecies* c.p.c. è ammissibile in quanto non è stata indispensabile la prosecuzione del processo nelle forme del rito ordinario.

Nel merito la domanda di parte attrice è fondata e deve essere accolta per le ragioni di seguito esposte.
La controversia in esame attiene all'accertamento del diritto della ricorrente ad ottenere il rimborso, da parte dell'intermediario resistente, della somma di € 18.063,00, inerente a cinque operazioni di bonifico eseguite in seguito ad una truffa attuata ai danni della ricorrente tramite la tecnica dello *spoofing*.
È pacifico che si sia concretizzata una truffa ed altrettanto pacifiche sono le modalità di esecuzione dell'evento criminoso nella sua prima parte (in particolare, la comunicazione di nome utente e password al truffatore da parte della ricorrente).
Resta questione dirimente se il comportamento tenuto dalla ricorrente sia stato connotato da colpa grave o meno e se siano state adottate da *Controparte_1* le idonee misure di sicurezza per l'accesso ai sistemi informatici.
A livello normativo, il d.lgs. n. 11/2010 agli artt. 10 e 12, pone a carico dell'intermediario l'onere di dimostrare che le operazioni disconosciute dal cliente e inerenti al conto corrente siano state autenticate, registrate e contabilizzate correttamente; che le stesse non abbiano subito gli effetti pregiudizievoli di un malfunzionamento delle procedure necessarie per la loro esecuzione e che l'utente non abbia impedito la verificazione della transazione illecita in violazione dei doveri comportamentali previsti, operando con dolo o colpa grave.
Spetta, invece, al correntista la prova della fonte del suo diritto e l'allegazione dell'abusiva utilizzazione dello strumento di pagamento in suo danno.
Dunque, anche in virtù del principio del rischio di impresa, opera in questa materia la regola generale di ripartizione dell'onere della prova previsto in materia di responsabilità contrattuale agli artt. 1218 c.c. e 2697 c.c. Tale principio chiede al creditore che agisce per l'adempimento, la risoluzione e/o il risarcimento del danno di provare esclusivamente la fonte del suo diritto e di allegare l'inadempimento di controparte, mentre pone a carico del debitore la prova dell'esatto adempimento ovvero di fatti impeditivi, modificativi o estintivi.
Si richiama una sentenza della Suprema Corte sul tema: "*ne discende che, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (ciò che rappresenta interesse degli stessi operatori), appare del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore di servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici da parte di terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo"*(Cass. civ. n. 2950 del 2017).

Sullo specifico tema delle truffe realizzate tramite la tecnica cd. "*spoofing*" una recentissima sentenza della Suprema Corte di Cassazione ha sancito che: "*La giurisprudenza di questa Corte è [...] consolidata nel senso di ritenere che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, va esclusa se ricorre una situazione di colpa grave dell'utente configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento ma il riparto degli oneri probatori posto a carico delle parti segue il regime della responsabilità contrattuale. Mentre, pertanto, il cliente è tenuto soltanto a provare la fonte del proprio diritto ed il termine di scadenza, il debitore, cioè la banca, deve provare il fatto estintivo dell'altrui pretesa, sicché non può omettere la verifica dell'adozione delle misure atte a garantire la sicurezza del servizio. Ne consegue che, essendo la possibilità della sottrazione dei codici al correntista attraverso tecniche fraudolente una eventualità rientrante nel rischio d'impresa, la banca per liberarsi dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore* (Cass. civ. n. 3738 del 12/02/2024, conf. a Cass. civ. sez. 1, n. 2950 del 3/2/2017; Cass. civ., sez. 3, n. 18045 del 5/7/2019; Cass. civ., sez. 6-3, n. 26916 del 26/11/2020).

Ciò posto, la responsabilità della *CP_3* si esclude o si attenua qualora nel comportamento del cliente sia ravvisabile un profilo di colpa grave. Tale elemento soggettivo deve essere provato dall'intermediario, chiamato in quel caso a fornire anche la dimostrazione di aver adottato ogni misura atta a garantire la sicurezza del servizio offerto.

Nel caso di specie, le questioni contestate da *Controparte_1* sono proprio queste, nel senso che la Banca convenuta ritiene:

i) di aver adottato un sistema di autenticazione forte, annesse tutte le misure idonee e richieste al fine di garantire sicurezza al servizio offerto;

ii) che vi sia responsabilità per colpa grave della cliente che porterebbe all'esclusione e/o all'attenuazione della responsabilità della resistente.

Ciò posto, i punti da affrontare ai fini della risoluzione della controversia sono principalmente due.

Primo punto focale della difesa di *Controparte_1* consta nell'affermare di aver adottato ogni misura idonea a garantire i massimi livelli di sicurezza del servizio offerto, prevedendo la procedura di doppia autenticazione per l'accesso al sistema attraverso l'inserimento dei cd. "codici OTP".

Tale procedura, anche detta *Strong Customer Authentication*, si basa su tre fattori: 1. Conoscenza: qualcosa che solo l'utente conosce, come una *password* o un *pin*; 2. Possesso: qualcosa che solo l'utente possiede, come un dispositivo mobile o una *smart card*; 3. Inerenza: qualcosa che l'utente è, come l'impronta digitale o il riconoscimento facciale.

Conformemente all'art. 98 della direttiva UE 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Al riguardo, nel caso di specie l'intermediario sostiene che le operazioni (truffaldine) sono state

correttamente contabilizzate, registrate e autenticate (con la cd. SCA) e ritiene che l'operatività fraudolenta si sia resa possibile a causa del comportamento tenuto dalla ricorrente, ricostruito come segue:
- alle ore 17:11:51 del 29.12.2022 è stata disinstallata e dunque disattivata la precedente licenza smart OTP dal cellulare della cliente;
- alle ore 17:13:30 del 29.12.2022 è stata attivata una nuova licenza "smart OTP" sul dispositivo mobile Android (presumibilmente) del frodatore;
- il frodatore, per attivare la nuova licenza smart OTP, ha dovuto inserire utenza + password +OTP ricevuto via e-mail dalla cliente + ulteriore OTP ricevuto via sms sul cellulare della cliente;
- la cliente avrebbe fornito al frodatore tali codici per la doppia autenticazione, poi utilizzati per l'accesso truffaldino.
Quanto alla contestata disinstallazione dell'app *Dmobile*, da un'attenta valutazione dei file di log prodotti dalla resistente emerge che, in un momento immediatamente successivo alla disattivazione dell'app dal dispositivo mobile del cliente (cfr. doc. g "ore 17.11.51 del 29.12.2022 Codice evento*: disattivazione licenza smart otp*"), è avvenuta l'attivazione della nuova app (il medesimo Log di cui al doc. g, cit. riporta chiaramente il "ore 17:13:30 del 29.12.2022 Codice Evento: *attivazione licenza smart otp*") in relazione all'utenza *internet banking* della ricorrente. Nei menzionati file di log non vengono, però, riportati gli indirizzi IP dai quali derivano le operazioni di disattivazione licenza smart OTP e attivazione licenza smart OTP.
In questo senso è d'aiuto la perizia di parte convenuta dalla quale emerge che l'operazione corrispondente a quella indicata nei file di log citati - effettuata alle ore 17.11.51 del 29.12.2022 con codice evento "disattivazione licenza smart otp" - è stata realizzata dal dispositivo cellulare realme [redacted] avente codice IP [redacted], pacificamente riconducibile al soggetto frodatore (cfr. relazione tecnica pag. 38).
Controparte_1 dunque, ha dato prova della disinstallazione dell'applicazione, ma non del fatto che tale operazione sia stata compiuta dalla ricorrente, anzi dalle conclusioni della perizia tale operazione risulterebbe compiuta proprio dall'indirizzo IP riconducibile al truffatore.
Dunque, la disinstallazione dell'app e la conseguente disattivazione della licenza sarebbe stata effettuata dal truffatore attraverso l'utilizzo di nome utente e password – che, pacificamente, sono stati comunicati dalla cliente – ma senza l'inserimento di ulteriori codici OTP (i cui invii, come si vedrà di seguito, sono successivi all'orario di disinstallazione).
Occorre evidenziarsi che dai file di log prodotti emerge appunto che la procedura di attivazione della nuova licenza smart OTP (nuova applicazione) è stata portata a compimento alle ore 17:13:30 e solo da questo momento il truffatore avrebbe dovuto avere accesso al sistema. Tuttavia, dalla stessa relazione tecnica di parte convenuta (pag. 32) risulta che già alle ore 17:13:03 l'indirizzo IP del truffatore ha avuto accesso al sistema della cliente, in quanto ha effettuato una "richiesta di bonifico" e ha inserito il nuovo pin [redacted] diverso da quello della ricorrente (21895) per il quale invece non risultano inserimenti. Si deve quindi ritenere che il frodatore abbia generato un nuovo pin dispositivo ([redacted]), senza mai dover inserire quello già esistente.
Pertanto, non solo non è provato che sia stato comunicato il proprio pin dispositivo dalla cliente al frodatore, ma non è nemmeno provato che lo stesso abbia inserito tale pin precedente per poi

modificarlo.
Per quanto concerne i codici OTP inviati alla cliente, l'intermediario ha allegato evidenza dalla quale risulta l'invio di un "sms OTP" al cellulare della cliente alle ore 17:13:03 del 29.12.2022, ma non è provato che tale codice sia stato correttamente inserito per dare seguito alla procedura di accesso. Infatti, in nessuno dei report di log segnalati in perizia si rileva l'inserimento del secondo codice OTP. L'unico inserimento di codice OTP è dimostrato a pag. 33 della relazione "inserimento generica seconda credenziale OTP token" avvenuto alle 17:11:47, che di certo non può essere il codice OTP ricevuto via sms perché il sistema lo consegnava al provider solo alle ore 17:13:03.
L'intermediario ha dedotto che, pochi secondi dopo l'attivazione della nuova licenza "smart OTP", i sistemi hanno registrato un accesso all'home banking tramite app proprio dal medesimo indirizzo IP [redacted], riconducibile al truffatore. Tale accesso, a dire del resistente, risulta possibile solo previo inserimento di nome utente, password e pin dispositivo. Tuttavia, si rileva al riguardo che, dall'esame dei file di log forniti, non vi è evidenza dell'inserimento dei tre elementi richiesti (nome utente, password e pin); seppure il pin possa essere inserito anche mediante credenziali biometriche (ad esempio con il riconoscimento facciale), nel caso di specie, non vi è evidenza nemmeno dell'attivazione di forme di riconoscimento in questo senso.
In conclusione, molteplici sono le incongruenze emergenti dai file di log e dalla perizia prodotta e non risulta evidente la prova dell'avvenuta comunicazione dei codici OTP da parte della ricorrente nei confronti del truffatore. Non per altro, la resistente formula tale tesi difensiva come mera "supposizione" anche all'esito dei risultati della perizia di parte (cfr. memoria ricorrente in cui si legge: "*Da ciò ne consegue che non pare inverosimile credere che così agendo la sig.ra Pt_1 abbia comunicato al terzo frodatore i) le proprie credenziali personali di accesso all'internet banking (cfr. doc. 5, cit.); ii) il codice OTP ricevuto via sms, permettendo così ad un soggetto terzo e sconosciuto di installare l'app Dmobile ed attivare una nuova licenza smart OTP associata alla utenza internet banking della cliente (cfr. doc. 4, 4a, cit.); iii) la propria password personale per accedere al proprio account di posta elettronica, consentendo così al terzo truffatore di disporre (o meglio di "avere sotto controllo e di gestire") anche la corrispondenza in entrata*").
Sul punto giova richiamare una decisione dell'ABF del 10 ottobre 2019, n. 22745 (coll. coordinam.) ove si è affermato che la colpa grave del cliente, nelle frodi online, non è mai in *re ipsa* e la dimostrazione della regolarità formale dell'operazione di pagamento che si assume non autorizzata, in quanto effettuata a seguito di autenticazione c.d. forte, non basta per adempiere l'onere probatorio posto a carico dell'istituto bancario che è tenuto ad indicare le circostanze fattuali, di rilievo indiziario, «che caratterizzano le modalità esecutive dell'operazione» e da cui è possibile desumere «la prova, in via presuntiva, della colpa grave dell'utente» (vd. anche Collegio di Milano, decisione n. 8262/2020).
Dunque, nel caso di specie l'intermediario ha certamente dimostrato la scansione delle operazioni effettuate, ma non ha provato nello specifico che la cd. SCA è stata rispettata attraverso l'inserimento di credenziali in possesso della sola cliente. L'intermediario non ha assolto gli oneri probatori previsti per l'esclusione della responsabilità contrattuale da inadempimento.
Con riferimento, al secondo punto dirimente, ossia la contestata colpa grave della ricorrente, si evidenzia che costante giurisprudenza arbitrale (cfr., Collegio di Milano, decisione n. 5716/2023; Collegio Torino, decisioni n. 3653/2023 e n. 16048/2022) ritiene che l'eventuale negligenza del cliente

può venire in rilievo solo qualora l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di *alert*.
Seppur dunque la questione sarebbe irrilevante, avendo già escluso che l'intermediario sia riuscito a provare di aver adottato le adeguate misure di sicurezza, questo Tribunale ritiene che il *[...] Controparte_1* non abbia fornito neppure la prova di una specifica condotta colposa posta in essere dalla cliente.
Giova evidenziare, innanzitutto, che la fattispecie in esame è qualificabile come un caso di truffa realizzata tramite sms *spoofing*, misto a ID *caller spoofing*. Tale modalità di azione è considerata potenzialmente più decettiva ed insidiosa rispetto al comune *phishing*, che si ritiene possa essere, invece, contrastato con l'uso di una diligenza minima, in considerazione della sua diffusione e della generalmente scarsa idoneità a trarre in inganno i clienti.
Suddetto inquadramento fattuale rileva proprio ai fini della valutazione giuridica del comportamento posto in essere dalla ricorrente. Infatti, si afferma che qualora il truffatore abbia adottato un sistema tecnicamente sofisticato opera una presunzione di assenza della colpa in capo al soggetto truffato, "*a meno che non si rinvengano [...] indici di inattendibilità o anomalia del messaggio; in tale caso potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'atro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario*" (cfr. ABF Roma 1° settembre 2022 n. 12005).
Ancora, nel fenomeno del c.d. *spoofing* il cliente "fisiologicamente" comunica a terzi truffatori le credenziali di accesso al proprio conto *online*, è infatti la modalità *standard* tramite la quale vengono compiute tali truffe (non per altro, la truffa è definita come reato a cooperazione con la vittima). Motivo per cui la comunicazione a terzi delle credenziali di accesso al proprio conto può essere indice di colpa grave del ricorrente solo ove le modalità ed il contesto nel quale la comunicazione viene compiuta rendano la stessa espressiva di manifesta negligenza inescusabile (cfr. sul punto Trib. Milano, sez. VI n. 322 del 18/01/2023).
Questo Tribunale ritiene che la ricorrente abbia tenuto comportamenti diligenti e idonei a evitare azioni truffaldine a suo danno, infatti, la *Pt_1* ha, nello specifico, verificato che il messaggio ricevuto provenisse dal consueto contatto dal quale aveva già ricevuto comunicazioni relative al rapporto in essere con la *CP_3* (infatti dallo *screenshot* allegato emerge come il messaggio fraudolento si sia inserito in una conversazione contenente anche messaggi genuini), ha verificato *online* il numero di telefono dal quale veniva contattata e questo corrispondeva al numero della filiale del *CP_1* di Milano. Inoltre, l'utente che l'ha contattata si è identificato come operatore bancario (fornendo uno specifico codice identificativo) e non ha mai chiesto alla ricorrente di comunicare le credenziali via chiamata, ma l'ha invitata ad inserirle sulla piattaforma (consueta modalità di azione degli operatori bancari), dunque, le circostanze non potevano in alcun modo apparire sospette alla ricorrente.
Nonostante il diligente comportamento della cliente, la truffa ha avuto esito positivo proprio in quanto finemente architettata e particolarmente insidiosa e ciò esclude si tratti di una semplice truffa a cui la ricorrente avrebbe potuto sottrarsi con l'uso della ordinaria diligenza.
Alla luce di quanto esposto, accertato che il *Controparte_1* non ha fornito prova evidente e apprezzabile della corretta autenticazione e del corretto funzionamento del sistema forte

(come richiesto ai sensi del d.lgs. 11/2010) e, nemmeno, la responsabilità per colpa grave della ricorrente, a ciò che consegue che la domanda risarcitoria volta al ristoro del pregiudizio subito per effetto della disposizione dei 5 bonifici va accolta, con conseguente condanna della convenuta a restituire all'attrice la somma pari ad € 18.063,00 oltre interessi legali sull'importo così determinato, dalla pubblicazione presente sentenza e fino al saldo effettivo
Le spese del giudizio seguono la soccombenza e vengono liquidate come da dispositivo.

P.Q.M.

Il Tribunale, definitivamente pronunciando nella causa instaurata da *Parte_1* nei confronti di *Controparte_1* così provvede:
1. in accoglimento della domanda di parte attrice, condanna *Controparte_1* a pagare a *Parte_1*, a titolo di risarcimento del danno, la complessiva somma di euro 18.063,00, oltre interessi legali sull'importo così determinato, dalla pubblicazione presente sentenza e fino al saldo effettivo
2. rigetta ogni ulteriore domanda, eccezione e deduzione delle parti;
3. condanna *Controparte_1* a rifondere a *Parte_1* le spese processuali, che liquida in euro [redacted], per compensi ed € [redacted] per anticipazioni, oltre rimborso forfettario 15%, iva e cpa come per legge.

Monza, 22.07.2024

Il Giudice
Chiara Binetti