N. R.Gen.Aff.Cont.

R E P U B B L I C A I T A L I A N A

IN NOME DEL POPOLO ITALIANO

Tribunale di Napoli

2 SEZIONE CIVILE

Il Giudice, dott. Maria Carolina De Falco, ha pronunziato la seguente

SENTENZA

nella causa iscritta al n. R.Gen.Aff.Cont. assegnata in decisione all'udienza del con la fissazione dei termini previsti dagli artt. 190 c.p.c.

TRA

, elett.te dom.to in presso lo studio dell'Avv. GIANNALAVIGNA LORENZO, c.f.: GNNLNZ78A11F839X, dal quale è rappresentato e difeso in virtù di procura in calce all'atto di citazione

- ATTRICE

E

, elett.te dom.to , presso lo studio dell'Avv. , dal quale è rappresentato/a e difeso/a in virtù di procura in calce alla copia notificata dell'atto di citazione

- CONVENUTA

Oggetto: risarcimento danni contratti bancari

Conclusioni: all'udienza del 05/12/2023, tenutasi mediante la modalità della trattazione scritta, il procuratore dell'attrice ha chiesto, in accoglimento della domanda, accertata la fraudolenza dell'operazione di disposizione bancaria, a mezzo bonifico, compiuta in danno dell'attrice e senza alcuna sua responsabilità, disporre il diritto di ripetizione della somma illecitamente sottrattale e condannare al pagamento la convenuta, con vittoria di spese, diritti ed onorari.

Il procuratore della convenuta ha chiesto il rigetto della domanda poiché infondata in fatto ed in diritto, provata tra l'altro, la colpa grave del cliente nella lamentata sottrazione patrimoniale per cui vi è causa, con vittoria di spese, diritti ed onorari.

RAGIONI DI FATTO E DI DIRITTO DELLA DECISIONE

La domanda è fondata.

con atto di citazione ritualmente notificato a ., a mezzo pec del 09.06.2021 ha chiesto accertare la violazione da parte della convenuta degli obblighi di diligenza tecnica e professionale per tutto quando dedotto nel proprio atto introduttivo e, per l'effetto condannare la stessa, in persona del legale rappresentante p.t., al pagamento di quanto illegittimamente addebitato dal conto corrente a lei intestato, per un totale di euro 11.501,00 (comprensiva di spese di commissione operazione di disposizione), o, comunque, a risarcire i danni subiti dall'attrice nella medesima misura, pari all' importo del bonifico on-line disconosciuto e non autorizzato, con la maggiorazione, in ogni caso, della svalutazione monetaria e degli interessi ex art. 1284 co. 4 cpc, dal dì al soddisfo. Il tutto oltre condanna al pagamento delle spese, diritti ed onorari del presente giudizio con attribuzione al procuratore costituito.

A tal fine premetteva in fatto di essere titolare del conto corrente n. presso la ; che nella mattinata del 19.04.2020, dal numero verde dell'istituto bancario, un operatore contattava uno dei soci accomandanti della correntista – con delega ad operare sul conto - avvertendo che sul conto societario erano in atto delle operazioni anomale e, avuta conferma che le stesse non erano riferibili ad alcun soggetto legittimato ad operarvi, venivano fornite rassicurazioni circa un loro impedimento; che purtroppo, in data 20.04.2020 dal suddetto conto corrente veniva eseguito un bonifico on-line di €. 11.501,00 in favore di tal , giammai disposto né autorizzato dalla correntista; che nel pomeriggio della medesima giornata del 20 aprile, sempre attraverso una chiamata dal numero verde, un operatore della banca confermava la circostanza del bonifico aggiungendo che sospettandone la fraudolenza, sarebbe stata subito bloccata, ma che ad ogni buon conto sarebbe stato opportuno non accedere all'home banking finché non fossero state fornite nuove credenziali; che nella giornata del 21.04.2021, i soci della istante società avviavano una interlocuzione telefonica con la filiale della loro banca, nella persona della dipendente sig.ra , la quale rassicurava che sarebbero state subito attivate le operazioni di "recall" con conseguente annullamento del bonifico; che sempre il 21 aprile, gli stessi soci denunciavano la vicenda alla Questura di , ove si recavano per sporgere formale denuncia/querela contro ignoti; che l'istituto bancario inizialmente riaccreditava effettivamente la somma salvo poi riaddebitarla

nuovamente, affermando al riguardo la totale l'estraneità all'accaduto. L'istante deduceva, quindi, che la verificazione dell'evento lesivo era da ascriversi alla responsabilità esclusiva della banca, non avendo la stessa impedito, attraverso la predisposizione di adeguati strumenti di controllo e di sicurezza, la disposizione di bonifico rivelatasi fraudolenta.

Si costituiva , in persona del suo rapp.te legale pro tempore, la quale resistendo alla domanda, eccepiva preliminarmente la nullità dell'atto di citazione per vizi attinenti l'edictio actionis; nel merito, osservava che nell'ambito della narrazione dei fatti che avevano condotto alla disposizione di bonifico, contestata per truffa dalla parte attrice, emergeva la colpa grave del soggetto che, nelle circostanze di tempo e di luogo riferite, aveva ceduto a terzi i codici per autorizzare l'operazione patrimoniale in uscita, inadempiendo agli accordi a suo tempo sottoscritti con l'istituto che da sempre pubblicizzava, tra l'altro, una compagna informativa per proteggere i clienti da tentativi di phishing e qualsiasi altra forma di raggiro da parte di terzi. Passava, quindi, in rassegna una serie di decisioni dell'arbitro bancario e confermava che i sistemi di sicurezza interna dell'intermediario erano dotati di procedura di autenticazione "forte", a più fattori di identificazione del cliente pertanto, non poteva esservi incertezza sull'identità del soggetto che nel caso in esame aveva disposto il bonifico in uscita verso terzi. Infine, contestava la domanda di risarcimento del danno formulata dalla parte attrice nella parte conclusiva dell'atto di citazione, la quale si deduceva, essere stata posta in maniera generica senza riferire, tra l'altro, la natura dei danni lamentati e la richiesta di rivalutazione monetaria e di interessi ex art. 1284 cc eccependone l'inammissibilità e l'infondatezza in fatto ed in diritto sulla scorta delle motivazioni precisate con l'atto di comparsa di costituzione.

Pertanto, la parte convenuta chiedeva rigettarsi integralmente la domanda e in via subordinata di accertare il concorso di colpa della parte attrice con conseguente esclusione o riduzione proporzionale della responsabilità della banca e dell'eventuale importo dovuto, con vittoria di spese di lite.

Ebbene, alla prima udienza il GU vista la concorde richiesta delle parti concedeva i termini di cui all'art. 183 comma 6 cpc decorrenti dal 17.12.2021 (incluso) e con rinvio della causa ex art. 184 cpc all'udienza del 25.03.2022, laddove veniva ammessa la prova testimoniale nei termini di cui alla relativa ordinanza e disposta l'audizione per l'udienza del 11.10.2022, con riserva, all'esito di CTU informatica.

Conclusa l'escussione dei testi indicati, il GU formulava proposta conciliativa ex art. 185bis cpc la quale veniva rifiutata dalla parte attrice e accettata dalla parte convenuta. Nella medesima udienza insisteva nell'ammissione di CTU informatica, mentre la parte attrice resistendo vi si opponeva deducendone la natura percipiente e non basata su un pregresso impianto

probatorio: la parte attrice, d'altronde, precisava anche che nella fattispecie non si trattava di esaminare documenti originali e che in ogni caso il tutto fosse già stato ampiamente disconosciuto ex art. 2712 cc.

Il GU, pertanto, ritenuta la causa matura per la decisione, fissava per il giorno 05.12.2023 – in modalità di trattazione scritta - l'udienza per la precisazione delle conclusioni e successivamente la tratteneva per la decisione concedendo alle parti i termini di cui all'art. 190 cpc.

Ciò posto, i fatti originanti la vicenda in contestazione vanno esaminati secondo la qualificazione giuridica nei quali vanno sussunti.

Trattasi, di vicenda inerente il fenomeno informatico del "*vishing"*, quale ipotesi a latere del più noto e diffuso phishing.

In particolare, si parla di "vishing", o "phishing vocale", quando una persona o un'azienda utilizza chiamate telefoniche o servizi di messaggistica vocale per indurre le vittime a rivelare informazioni personali. In un attacco di vishing, i truffatori (detti anche "visher") si fingono fonti attendibili (già conosciute dalla vittima – ad esempio il proprio istituto di credito) per ottenere informazioni sensibili, come numeri di carte di credito o altri dati riservati.

I truffatori che ricorrono a tecniche di vishing sono soliti contattare le vittime falsificando un numero telefonico locale o quello di un'azienda affidabile. Talvolta essi sfruttano il vishing per inserire nel dispositivo della vittima "malware" che successivamente potranno utilizzare per recuperare informazioni personali. Si tratta di sofisticate tecniche di ingegneria sociale, molto insidiose e difficilmente inquadrabili nell'immediato dalla vittima, la quale, sensibilizzata rispetto alla possibile aggressione telematica, statisticamente valuta nell'immediato più sicuro fidarsi dell'interlocutore, ancorchè ignoto, che si finge operatore di un'autorità fidata (attraverso l'utilizzo di numeri telefonici civetta e noti alla vittima inconsapevole). A questo punto, senza rendersene conto, perché manipolata psicologicamente, la vittima cede i propri dati sensibili che si riveleranno poi utili alla consumazione della truffa orchestrata.

Alcune delle tecniche di vishing più comuni sono il *wardialing* (inviare messaggi vocali automatici a un gran numero di vittime, di solito per cercare di spaventarle, ad esempio affermando di avere tasse o altre multe non pagate), il *vishing VoIP* (finto operatore che chiama al telefono le possibili vittime dell'attacco mediante un sistema vocale automatizzato, spacciandolo per il call center di una banca o di un istituto di credito), lo *spoofing dell'ID chiamante* (utilizzati per nascondere la posizione reale del truffatore e persino impersonare i numeri di telefono di organizzazioni fidate) e il *dumpster diving* (azione che viene compiuta dagli hacker per cercare nei cestini informatici delle aziende, delle organizzazioni o da semplici utenti comuni, informazioni utili per tentare di hackerare gli account dei clienti).

In tutti i casi citati, la truffa in danno della vittima viene organizzata al fine di creare, nei primissimi momenti del contatto, un senso di urgenza o paura, che prevale su qualsiasi cautela o sospetto naturale che la vittima potrebbe osservare nella normale routine quotidiana.

Ebbene, proprio in riferimento a questa articolata, quanto recentissima, progettazione di truffa informatica a scopo lucrativo, diverse pronunce, sia dell'Autorità giudiziaria che dell'Arbitro Bancario Finanziario (ABF) hanno ravvisato in capo all'istituto finanziario coinvolto, un profilo di colpa cd. "semi oggettiva" (ex art. 10 del Dlgs. 11/2010), con condanna al rimborso della somma sottratta dal truffatore alla vittima.

Più precisamente, nelle cause di tal fatta, oltre alla responsabilità contrattuale sorta dal rapporto con l'utente, l'istituto bancario ha l'onere di provare la negligenza dell'utente, dimostrando, dunque, che la vittima abbia agito con dolo o colpa grave nel fornire le proprie credenziali o dati personali.

Sull'istituto grava anche la dimostrazione che non vi sia stato nessun malfunzionamento dei software, di non aver ricevuto segnalazioni di operazioni sospette e anomale, e, soprattutto, di possedere un sistema di sicurezza "forte", in grado di proteggere le operazioni, i conti e i dati personali dei propri clienti.

Nei casi summenzionati, dunque, le specifiche modalità fraudolente, essendo più difficoltose da riconoscere con la normale diligenza spettante all'utente, possono consentire di alleggerire la vittima dalla colpa "grave" richiesta per imputare alla stessa la responsabilità di quanto avvenuto.

Secondo quanto recentemente esaminato e pronunciato in materia dalla giurisprudenza di merito (cfr. ex multis Tribunale Busto Arsizio, 14/10/2022, n.1434, ma vedi anche Tribunale di Milano sez. VI, 01/12/2022, n.9475), come noto, il d.lgs. n. 11/2010 sancisce l'obbligo del prestatore del servizio di pagamento di assicurare che i dispostivi 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, si vedano gli artt. 8, comma 1, l'art. 10 con riferimento soprattutto al comma 2, l'art. 12 (comma 2 ter, comma 3, comma 4), i quali sostanzialmente prevedono 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 cliente stesso, 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.

Ed invero, "*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 e, da ultimo, Cass. n. 26916/2020).

Non si può dunque addossare al cliente l'onere di provare la propria diligenza nel contegno di utilizzatore del sistema informatico, laddove invece spettava al prestatore del servizio di pagamento provare la riconducibilità dell'operazione al cliente, in base al principio di vicinanza della prova e soprattutto nell'ottica del bilanciamento degli interessi che governa l'ordinamento civile.

Infatti, se così non fosse, il singolo dovrebbe, ad absurdum, essere chiamato ad impiegare settorialmente (in questo caso all'interno di operazioni finanziarie) anche una diligenza superiore a quella normalmente richiesta ex art. 1176 comma 1 cc, in assenza della doverosa natura professionale connessa alla sua persona, nei termini espressamente richiesti dal comma 2 della disposizione citata.

Ciò costituisce, del resto, espressione del principio secondo cui l'impossibilità della prestazione derivante da causa non imputabile al soggetto obbligato (art. 1218 c.c.) richiede la dimostrazione di eventi che si collochino al di là dello sforzo diligente richiesto al debitore (cfr. Cass. n. 2950/2017 cit.; Cass. n. 18045/2019), nel caso di specie di natura particolarmente tecnica, da valutarsi con il parametro dell'accorto banchiere (Cass. n. 806/2016; Cass. n. 13777/2007).

Spetta, pertanto, al prestatore del servizio fornire la prova tanto di avere adottato tutti i migliori accorgimenti della tecnica volti a scongiurare il rischio di impiego fraudolento degli strumenti di pagamento, quanto 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, ma non ha fornito alcuna prova incontrovertibile che l'operazione del relativo inserimento, al fine di confermare l'operazione di bonifico, sia avvenuta inequivocabilmente per volontà e impegno manuale del cliente. Anzi, più elementi di segno contrario depongono proprio a favore della verificabilità immediata dell'operazione anomala e fraudolenta da parte dell'accorto banchiere, tal che non solo la disposizione di bonifico poteva essere immediatamente bloccata da remoto, ma ben poteva essere revocata nell'arco delle 24h, come da allarme mosso immediatamente dal cliente all'operatore bancario conosciuto che addirittura provvedeva ad informare subito il direttore.

Più precisamente, in primo luogo a pag. 4 della comparsa di costituzione e risposta, capo 2, emerge una dichiarazione di natura confessoria dell'intermediario laddove testualmente riferisce: "*Il giorno 20/04/2020 alle ore 16:55:39 da web (foglio tracciatura, riga 53) è tracciato l'inserimento di un bonifico di € 11.500,00 in favore di , IBAN . L'operazione è valutata sospetta dal sistema antifrode (foglio tracciatura, riga 54)*".

L'operazione quindi avrebbe potuto essere nell'immediato bloccata e posta in sospeso e non proseguire, come al contrario è accaduto, con la richiesta di inserimento codici rivolta al cliente per conferma dell'operazione posta in "Allert", ma evidentemente intercettata dal truffatore. E' possibile infatti che per il tramite delle innumerevoli telefonate provenienti dal numero (notoriamente conosciuto anche dalla parte attrice quale numero verde del proprio Istituto bancario e presente sul suo sito istituzionale), sia stato introdotto nell' apparecchio mobile della vittima un *malware* capace di sottrarre tutti i dettagli tecnici necessari e utili a confermare la disposizione di bonifico a favore del truffatore (tant'è che più avanti la dichiarazione confessoria di cui innanzi prosegue nel senso che: "*….L'OTP virtuale non è generata in tempo utile, pertanto è inviato al numero mobile del cliente il messaggio SMS "O-Key SMS - Usa per autorizzare un bonifico europeo a* ").

E', quindi, verosimile che trattenendo la vittima inconsapevole al telefono attraverso le diverse chiamate in rapida successione (cfr. screeshot presenti nel fascicolo di parte attrice), il suo contatto telefonico sia stato clonato al fine di intercettare proprio l'sms autorizzativo del bonifico fraudolento.

In secondo luogo, si vedano i documenti di presa in carico e conferma del bonifico contestato (cfr. doc. contabile bonifico eseguito e presa in carico bonifico allegati alle note ex art. 183 comma 6 II termine del 14.02.2022 della parte convenuta): ebbene, si ponga l'attenzione agli orari impressi sui documenti citati, laddove la presa in carico del bonifico è delle ore 16,58 mentre la contabile del bonifico reca l'indicazione oraria delle 22,48 del medesimo giorno 20.04.2020. I due documenti, posti a confronto poi dell'"estratto bonifico europeo " (depositato dalla parte attrice in uno all'atto di citazione), evidenziano altre anomalie: pur trattandosi di bonifico su territorio nazionale (l'istituto del beneficiario - residente a vedi contabile bonifico), la data della valuta e della contabile coincidono (vedi la diversità degli orari) pur non evidenziando l'istantaneità dell'operazione mentre la data del regolamento è il giorno 21.04.2020.

Questa anomalia è così evidente (notoriamente infatti qualora un bonifico non sia istantaneo, la data della valuta e della contabile non coincidono mai ma divergono sempre di qualche giorno), che l'istituto bancario avrebbe dovuto rilevarla immediatamente, in uno ad un ulteriore dettaglio, di

certo non consono ad un operatore commerciale che lavora nel mercato da anni e che da altrettanti anni si avvale dei servizi dell'intermediario convenuto: all'interno dei documenti "presa in carico del bonifico", "conferma dell'operazione" e "estratto del bonifico" è presente a titolo di causale la locuzione "PAG VOSTRA FATTURA", espressione troppo generica ed insolita per qualsiasi operatore commerciale di esperienza ultradecennale anche in considerazione dell'importo elevato dell'operazione.

Qualsiasi operatore commerciale di media diligenza, che tenga una contabilità mediamente ordinata, ha sempre cura, infatti, di indicare precisamente nella causale il numero di fattura e la data di emissione della stessa, soprattutto se comporti, come nel caso di specie una ingente uscita di liquidità. Anche tale dettaglio rientra nel notorio e non ha bisogno di ulteriori approfondimenti, ma avrebbe potuto anche per tal via indurre l'istituto bancario a procedere a ulteriori controlli, vista la conoscenza risalente e pregressa del cliente (non smentita né contestata ex art. 115 cpc).

In terzo luogo, alcuna prova possono offrire le certificazioni di qualità versate in atti dalla parte convenuta atte a comprovare la tenuta del sistema di sicurezza avverso operazioni fraudolente di terzi in danno del propri clienti.

Così come alcuna prova documentale, tanto più esaminabile a mezzo CTU informatica, può essere offerta dagli allegati "TRACCIATURA COMPLETA" e "TRACCIATURA INFORMATICA" depositate dall'intermediario unitamente alle note ex art. 183 comma 6 II termine cpc, le quali non sono firmate, non possono essere identificate come originali, non contengono informazioni chiare e intellegibili né in favore del cliente che denuncia di essere stato truffato né nei riguardi del GU a cui viene richiesto di compiere un esame a mezzo CTU informatica, la cui domanda per vero è stata formulata in maniera, tra l'altro, generica senza indicazione alcuna degli elementi da sottoporre a perizia e di quali elementi avrebbero dovuto far propendere per la bontà dell'operazione proveniente esattamente dal cliente.

Trattasi di un tipo di esame che per vero non può essere condotto a mezzo esame di supposti documenti probatori ma attraverso la verifica dei file gestionali, atta a disvelare l'ingresso informatico di terzi malfattori all'interno della rete digitale dell'intermediario.

Quanto alle certificazioni di qualità citate e depositate unitamente alla comparsa di costituzione e risposta (cfr. doc. N. 2 CERTIFICATI DI SICUREZZA), restano inconferenti ai fini del presente giudizio e soprattutto al fine di comprovare la solidità del sistema di sicurezza della parte convenuta, poiché non coprono l'ufficio territoriale ove la parte attrice intrattiene il proprio c/c né l'oggetto del certificato dimostra di coprire le criticità sollevate nella presente sede.

La "VIDEATA SITO SU NUMERO VERDE", poi, (cfr. allegato alla comparsa di costituzione e risposta) dimostra, invece, che la parte attrice è stata ragionevolmente indotta in errore

nel ricevere la telefonata proprio dal numero verde chiaramente indicato sul sito istituzionale dell'intermediario, mentre non è assolutamente dirimente e non esenta da responsabilità il documento "SEZIONE SICUREZZA SITO" (cfr. allegato alla comparsa di costituzione e risposta), che non pone il cliente nella condizione di riconoscere agevolmente le ipotesi più diffuse di truffa bancaria.

Nel caso specifico, quindi, non vi è dubbio che il soggetto deputato ad agire sul c/c per il ..., sia incorso in errore di fatto, la cui elencazione di ipotesi lungi dall'essere esaustiva, comprende in maniera inequivoca, l'ipotesi in cui la cattiva rappresentazione della realtà, determinante ai fini della manifestazione del consenso a fornire i propri dati personali, sia caduta sull'identità della controparte, che nella percezione del soggetto in questione non poteva non identificarsi con il proprio intermediario finanziario

Si consideri, infatti, che negli istanti concitati che necessitavano di scelte rapide a tutela del proprio patrimonio, l'agente modello di media diligenza, sarebbe stato senz'altro influenzato in senso negativo nel proprio potere di autodeterminarsi, diviso tra la tempestività della risposta difensiva contro il prospettato attacco informatico al proprio patrimonio e l'urgenza di verificare, mediante altro canale, l'identità dell'interlocutore telefonico che, previe rassicurazioni del caso, lo invitava a restare in linea proprio al fine di garantire la pronta risoluzione del supposto attacco informatico (in realtà lo tratteneva per clonare il dispositivo).

Non vi è dubbio, poi, che la paventata sottrazione patrimoniale esercitata nei riguardi di un soggetto, di media operatività commerciale (vista la lista movimenti depositata in atti), produca una rappresentazione di pericolo, ancorchè eventuale o presunta, di notevole entità, in disparte dalla certa ingiustizia (identificandosi la condotta illecita oggetto di minaccia, e sulla quale si innesta l'atteggiamento psicologico della reazione difensiva immediata, nel reato di furto).

Pertanto, è chiaro che nell'immediatezza della minaccia, il *quisque de populo*, si preoccupi verosimilmente di assicurare la difesa della propria incolumità personale e patrimoniale, rilevando dal punto di vista psicologico prima il pericolo di un danno grave e solo dopo la necessità di verificare se il rischio percepito corrisponda al vero.

Ciò posto, in linea teorica, nella condotta del non sussiste nemmeno una componente di livello medio di imprudenza, laddove come più volte dedotto, egli non abbia mai inserito di sua spontanea volontà e/o iniziativa i codici di autenticazione forte necessari per il buon esito del bonifico fraudolento, limitandosi a trattenersi al telefono con l'interlocutore.

Sul punto è stata svolta anche la prova testimoniale che non pone dubbi sull'assunto; all'udienza del 11.10.2022, infatti, dichiarava: " *E' vero; si trattava del mio numero personale; ADR il mio numero come quello di mia moglie era nell'archivio della banca; il direttore*

all'inizio degli anni 2000 al passaggio dalla banca da ` chiese anche il mio numero; nel 2010 comunicai il mio nuovo numero, forse anche qualche anno prima; ADR la comunicazione delle operazioni anomale avvenne mentre io stavo facendo delle attività di beneficenza in chiesa la domenica, tanto che io riferì all'interlocutore che ero impegnato e l'uomo mi disse solo che doveva riferire tale circostanza e che se c'era necessità di altre comunicazioni mi avrebbe ricontattato; sul capo 2) E' vero; durante la telefonata pomeridiana mi venne confermato il bonifico estero con tutte le indicazioni del beneficiario e mi fu intimato di non aprire il servizio home banking perché c'era il rischio di confermarlo: adr la telefonata durò un po' di tempo perché la linea era disturbata e l'uomo al telefono richiamava; ADR mi disse anche che la banca mi avrebbe richiamato le nuove credenziali di accesso; ADR era la prima volta che vedevo quel numero di telefono; ADR Mi insospettì che fosse domenica ma non ci diedi peso perché ero impegnato; ADR era il numero verde della banca che io conoscevo perché siamo correntisti da . anni e perché è affisso fuori la sede della banca che frequento; sul capo 3) Non è vero; le credenziali non mi furono proprio chieste; sul capo 4) Non è vero; non ho mai ricevuto uno o più sms per completare il bonifico; ADR L'unica cosa che mi chiedevano era di attendere in linea".

Nella medesima udienza, il secondo teste di parte attrice tal precisava: "*sul capo 2) è vero; ero presente alla telefonata a casa di mio fratello anche se non ho visto il numero; la persona che parlava confermava il bonifico e consigliava di non fare niente; ADR ci furono diverse chiamate per disturbo sulla linea; ADR Il contenuto esatto della telefonata mi fu riferito da mio fratello dopo aver chiuso; sul capo 3) No non è vero; sul capo 4) alla mia presenza non è accaduto; ADR il telefono su cui arrivarono le telefonate era il telefono di mio fratello*".

Alle presenti dichiarazioni nulla è stato offerto a titolo di prova contraria dalla parte convenuta.

Orbene, con particolare riferimento, all'utilizzo dei codici identificativi ai fini della corretta esecuzione del bonifico, secondo l'ABF anche ove provata la loro trasmissione a terzi, non può essere sufficiente il solo il codice OTP inviato tramite token o tramite smart phone, (per autenticare in modo sicuro l'identità dell'utente e anche laddove l'operazione risultasse correttamente autorizzata) a dare prova della colpa grave del consumatore, dovendo invero la Banca dimostrare l'elemento soggettivo della colpa grave al fine di rifiutare legittimamente il rimborso.

Nel caso di specie l'intermediario non forniva prova del dolo o della colpa grave dell'utente, ovvero che le operazioni vennero effettuate da terzi per colpa della titolare delle credenziali per averle comunicate o non congruamente custodite, né di aver posto in essere tutte le cautele necessarie ad evitare l'operazione fraudolenta, limitandosi a comunicare all'attrice la legittimità delle operazioni stesse.

Tuttavia, in linea con i recenti orientamenti giurisprudenziali: "*la sottrazione dei codici del correntista, attraverso tecniche fraudolente, rientra nell'area del rischio di impresa, destinato ad essere fronteggiato attraverso l'adozione di misure che consentano di verificare, prima di dare corso all'operazione, se essa sia effettivamente attribuibile al cliente*" (cfr. Cass. Civ. sent. N. 2950 del 3 febbraio 2017n. 2950.), pertanto: "*Ne consegue, anche in virtù del surrichiamato articolo 10, comma 2, del Dlgs n. 11/2010, che non è sufficiente al fine di accertare la legittimità dell'operazione bancaria o postale che risultino inserite le credenziali per attribuire la volontarietà dell'azione al correntista. È necessario, invece, un quid pluris, a carico dell'intermediario, sui cui grava l'onere di accertare l'effettiva volontà del correntista di dar luogo all'operazione in conto corrente prima di dar corso alla stessa, prova non fornita nel caso di specie, non avendo dimostrato la legittimità dell'operazione on line non autorizzata, la violazione, da parte del cliente, degli obblighi nascenti dal contratto, né la condotta dolosa o colposa della danneggiata*". (Tribunale Benevento sez. II, 11/10/2023, (ud. 10/10/2023, dep. 11/10/2023), n.2012 - conforme Tribunale S.Maria Capua V. sez. III, 20/07/2023, n.3022).

Né in senso contrario possono essere invocate dall'istituto di credito le campagne informative asseritamente proposte alla clientela in modo assiduo.

Sul punto, oltre a doversi rilevare che parte convenuta si è limitata a produrre la schermata della home page del sito in cui era presente uno spazio dedicato al riconoscimento del phishing, non indirizzato personalmente al cliente, sicché non è dato comprendere quando lo stesso sia stato pubblicato, deve evidenziarsi che il messaggio in questione non era affatto specifico, non descrivendo il meccanismo con cui vengono perpetrate le truffe più aggressive.

Al riguardo, non può che osservarsi che tanto più i meccanismi di truffa sono sofisticati, tanto più, correlativamente, l'informativa dell'istituto di credito deve essere specifica e puntuale al fine di contrastare efficacemente le manovre truffaldine.

D'altronde, è sempre sul banchiere, e non sul cliente, che per giurisprudenza costante, di merito e di legittimità, grava il maggiore onere di diligenza ex art. 1176 comma 2, rispetto al quale corrisponde la misura della responsabilità di cui all'art. 2236 c.c. cioè la diligenza massima richiesta al *bonus argentarius,* quale protagonista principale della retta circolazione della ricchezza secondo giustizia e in favore e nell'interesse di tutti gli operatori interessati alla sicurezza di traffici economici, secondo il principio della lecita giustificazione causale.

Sul punto, e in estrema sintesi di tutti i principi sin qui espressi si è pronunciata la Suprema Corte di Cassazione, sezione III civile, con la sentenza (data ud. 10/03/2023) 15/05/2023, n. 13204, la quale ha precisato che: "*in caso di truffa informatica cd. phishing incombe sul prestatore dei servizi di pagamento il duplice onere di provare di aver adottato tutte le misure di sicurezza*

necessarie per la protezione del cliente e l'inadempimento doloso o gravemente colposo del cliente medesimo. In tema di responsabilità della banca, ovvero dell'erogatore del corrispondente servizio, 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 un'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".

Mancando, pertanto, qualsiasi prova rispetto alla conformità dei sistemi utilizzati da , e non ravvisando dolo né colpa grave da parte del cliente oggi attore, la responsabilità per il fatto lesivo occorso va posta, in via esclusiva, in capo all'intermediario convenuto, riconoscendo per l'effetto in favore dell'attrice il diritto a ripetere l'intera somma indebitamente ed illecitamente sottrattale.

Per quanto riguarda infine la chiesta rivalutazione monetaria e gli interessi ex art. 1284 cc, stante la natura risarcitoria da responsabilità contrattuale del rimborso dovuto da al , spettano alla parte attrice sulla complessiva somma di € 11.501,00 gli interessi come richiesti.

La incontestata natura contrattuale del rapporto obbligatorio attualmente in essere tra le parti in lite nonché l'obbligazione pecuniaria oggetto del presente giudizio determinano in favore della parte attrice anche il riconoscimento degli interessi ex art. 1284 comma 4 cc, considerando il principio generale posto dalla norma citata e come recentemente espresso da Corte appello Milano sez. III, 19/04/2023, n.1283, secondo la quale: "*La disposizione di cui all'art. 1284, comma 4, c.c., individua un tasso legale degli interessi applicabile, in linea generale, a tutte le obbligazioni pecuniarie (salvo diverso accordo delle parti e salva diversa espressa previsione di legge), per il periodo successivo all'inizio del processo avente ad oggetto il relativo credito, fino al momento del pagamento. La disposizione di cui all'art. 1284, comma 4, c.c. è quindi applicabile, stante il suo carattere generale immediatamente desumibile dalla sua collocazione sistematica e dalla sua ratio, alle obbligazioni di ogni natura, tanto se derivanti da contratti o negozi giuridici, quanto se derivanti da fatti illeciti o altri fatti o atti idonei a produrle*".

Le spese seguono la soccombenza e si liquidano come da dispositivo secondo il valore della lite e la complessità e qualità dell'attività processuale svolta ai sensi e per gli effetti del DM 147/2022.

P.Q.M.

Il Tribunale di Napoli, 2 SEZIONE civile, in composizione monocratica, definitivamente pronunciando sulla domanda proposta da

nei confronti di ., così provvede:

1) Accoglie la domanda e per l'effetto condanna , in persona del legale rapp.te pro tempore al pagamento a titolo di risarcimento dei danni al

. in persona del legale rapp.te pro tempore la somma di €) oltre interessi ex art. 1284 comma 4 cc.

2) per l'effetto condanna in persona del legale rapp.te pro tempore al pagamento in favore di . in persona del legale rapp.te pro tempore delle spese di lite che si liquidano in complessivi € per spese vive ed € per compensi oltre iva, cpa e rimborso forfettario al 15%, con attribuzione all'avv. Lorenzo Giannalavigna dichiaratosi antistatario.

Così deciso in Napoli, il 20/03/2024.

Il Giudice
(dott. Maria Carolina De Falco)