REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

CORTE D'APPELLO DI VENEZIA

Prima Sezione civile

R.G.

La Corte d'Appello di Venezia, riunita in camera di consiglio nelle persone dei Magistrati:

dott. Guido Santoro	Presidente
dott. Federico Bressan	Consigliere
dott. Francesco Petrucco Toffolo	Consigliere rel.

ha pronunciato la seguente

SENTENZA

nella causa civile iscritta al ruolo il , promossa con atto di citazione in appello

da

(C.F.) in persona del procuratore speciale dott.

con sede legale in , rappresentata e difesa dall'avv.

e dall'avv.

appellante

contro

(C.F.

), in persona dei legali rappresentanti *pro tempore*, con sede legale in , Via

, rappresentata e difesa dall'avv. Daniela Ajese;

appellata

Oggetto: "Altri contratti bancari e controversie tra banche"; appello avverso la sentenza n.

; emessa il e pubblicata il a definizione del giudizio iscritto al n. R.G. avanti al Tribunale di

CONCLUSIONI

- per l'appellante:

"in via principale: 1) in riforma del capo 1 della sentenza impugnata, che ha escluso la colpa grave della correntista, valutare tutti i fatti provati e documentati anche da , nonché il contegno processuale e probatorio avversario e per l'effetto accertare e dichiarare la grave negligenza che ha caratterizzato la condotta della , in persona dei legali rappresentanti pro tempore, per omessa adozione di misure idonee a proteggere le credenziali personalizzate ex art. 7, comma 2, D.Lgs. n. 11/2010 e, per l'effetto, l'assenza di ogni onere risarcitorio/restitutorio in capo alla Banca; 2) in riforma del capo 2 della sentenza impugnata, che ha escluso la colpa grave della correntista, valutare tutti i fatti provati e documentati anche da , nonché il contegno processuale e probatorio avversario e per l'effetto accertare e dichiarare la grave negligenza che ha caratterizzato la condotta della in persona dei legali rappresentanti pro tempore, per non tempestiva segnalazione di usi non autorizzati degli strumenti di pagamento ex art. 7, comma 1, lett. b), D.Lgs. n. 11/2010 e, per l'effetto, l'assenza di ogni onere risarcitorio/restitutorio in capo alla Banca; 3) in riforma del capo 3 della sentenza impugnata, che ha escluso la colpa grave della correntista, valutare tutti i fatti provati e documentati anche da , nonché il contegno processuale e probatorio avversario e per l'effetto accertare e dichiarare la grave negligenza che ha caratterizzato la condotta della , in persona dei legali rappresentanti pro tempore, per omessa custodia degli

strumenti di pagamento ex art. 7, comma 1, lett. a), D.Lgs. n. 11/2010 e, per l'effetto, l'assenza di ogni onere risarcitorio/restitutorio in capo alla Banca; 4) in riforma del capo 4 della sentenza impugnata, che ha escluso la colpa grave della correntista, valutare, anche in via indiziaria, tutti i fatti provati e documentati anche da nonché il contegno processuale e probatorio avversario, oltre che tutti i fatti accertati e le gravi, precise e concordanti risultanze processuali emerse nel giudizio di primo grado, e per l'effetto accertare e dichiarare la grave negligenza che ha caratterizzato la condotta della , in persona dei legali rappresentanti pro tempore, nell'utilizzo dei propri strumenti di pagamento ex art. 7, D.Lgs. n. 11/2010 e, per l'effetto, l'assenza di ogni onere risarcitorio/restitutorio in capo alla Banca; 5) in riforma del capo 5 della sentenza impugnata, considerata l'erronea valutazione delle risultanze processuali in relazione alle dotazioni fornite da accertare e dichiarare che il grado di sicurezza dei sistemi della Banca è assolutamente conforme alla normativa applicabile, alla natura del servizio offerto ed agli standard esigibili all'epoca dei fatti contestati e, per l'effetto, accertare e dichiarare l'assenza di qualsivoglia responsabilità in capo a . oltre che ogni onere risarcitorio/restitutorio a carico della stessa come invocato dalla , in persona dei legali rappresentanti pro tempore; 6) in riforma del capo 6 della sentenza impugnata, considerata l'omessa disamina dell'eccezione ex art. 1227, comma 2, c.c. sollevata dalla Banca ed il fatto che i danni contestati sarebbero stati evitati dall'attrice appellata usando anche soltanto una diligenza ordinaria o, in subordine, ridotti ex art. 1227, comma 1, c.c., accertare e dichiarare il concorso colposo della ., in persona dei legali rappresentanti pro tempore, e per l'effetto escludere o ridurre, come risulterà di giustizia, l'onere

risarcitorio posto in capo a . secondo la gravità della colpa dell'appellata e l'entità delle conseguenze che ne sono derivate, anche in termini di compensazione o differente riparto delle spese di lite e di CTU del giudizio di primo grado, nonché di ingiustificato addebito delle spese di CTP sostenute dall'attrice appellata, con conseguente condanna della ., in persona dei legali rappresentanti pro tempore, alla restituzione della somma eccedente, già versata dalla Banca, come liquidata dalla decisione impugnata, oltre interessi e rivalutazione dal 23 novembre 2023 al saldo;

7) per l'effetto, accogliere le domande proposte da formulate nella propria comparsa di costituzione e risposta di cui al giudizio di primo grado, riportate al paragrafo 1 del presente atto e che abbiasi qui integralmente riportate e trascritte; 8) condannare la ., in persona dei legali rappresentanti pro tempore, all'integrale restituzione delle somme già liquidate in proprio favore dal Tribunale di Padova e versate da in esecuzione dell'appellata sentenza, pari a € 141.749,15 (doc. 4) per capitale e spese legali, oltre alle spese ed ai compensi professionali e tecnici del doppio grado di giudizio, nonché rivalutazione e interessi dalla domanda al saldo ed ulteriori spese ed accessori; in ogni caso: con vittoria di spese e compensi professionali e tecnici, ivi inclusi quelli avversari, relativi al presente ed al primo grado di giudizio, come per legge, oltre alle eventuali spese di CTU e CTP del presente giudizio; in via istruttoria: - ai sensi dell'art. 210 c.p.c., ordinare all'attrice appellata, in persona dei legali rappresentanti pro tempore, l'esibizione di ogni documentazione afferente alle somme sottoposte a sequestro su provvedimento del Giudice per le Indagini Preliminari – Tribunale di Venezia, nell'ambito del procedimento penale n. RGNR

e rinvenute sul conto corrente acceso presso , ., intestato a e identificato dal codice IBAN ed al relativo stato, non già esibita nel procedimento di primo grado; - ammettere le istanze istruttorie formulate dall'appellante in primo grado di seguito ritrascritte: - ammettersi la prova testimoniale sui capitoli di prova di seguito formulati, indicando quali testi il signor , domiciliato c/o S.p.A., , nonché il signor , domiciliato c/o : a) "Vero che il flusso informatico prodotto sub doc. 14 dalla Banca, come da documento che si rammostra al teste, corrisponde all'istruzione di bonifico autenticata attraverso le credenziali di home banking della . in data ottobre) in favore di codice IBAN , di € 50.000,00 e inviata alla Banca dal profilo di home banking della correntista"; b) "Vero che il flusso informatico prodotto sub doc. 15 dalla Banca, come da documento che si rammostra al teste, corrisponde all'istruzione di bonifico autenticata attraverso le credenziali di home banking della . di in data ottobre , in favore di , codice IBAN , di € 50.000,00 e inviata alla Banca dal profilo di home banking della correntista"; c) "Vero che il flusso informatico prodotto sub doc. 16 dalla Banca, come da documento che si rammostra al teste, corrisponde alla conferma di inserimento dell'ordine di bonifico, inviata dalla Banca alla e relativa al bonifico disposto e autenticato dalla stessa . in data ottobre , in favore di , codice IBAN , di € 50.000,00"; d) "Vero che il flusso informatico

prodotto sub doc. 17 dalla Banca, come da documento che si rammostra al teste, corrisponde alla conferma di inserimento dell'ordine di bonifico, inviata dalla Banca alla . e relativa al bonifico disposto e autenticato dalla stessa . in data in data ttobre in favore di , codice IBAN , di € 50.000,00"; - disporsi la CTU tecnico-informatica affinché il nominando consulente tecnico, visti ed esaminati gli atti di causa e verificato il sistema informatico dell'attrice, eseguendo gli accertamenti del caso presso gli uffici della : a) verifichi che i bonifici contestati sono stati disposti attraverso i sistemi informatici della stessa attrice ed autenticati mediante gli strumenti di pagamento e le credenziali di home banking rimessi alla custodia della stessa attrice; b) esaminati i sistemi informatici della , in particolare, il computer utilizzato il e ottobre dall'attrice per disporre i bonifici poi contestati, rilevi la presenza di attacchi, fragilità, intromissioni informatiche, infezioni, malware e/o virus intervenuti al momento della disposizione di tali bonifici modificandone gli estremi e generando/alterando le presentazioni di bonifico prodotte dall'attrice sub docc. 3, 4, 12 e 13, escludendo quindi l'ipotesi che qualsivoglia alterazione sia avvenuta nei sistemi di e che le presentazioni in esame siano state generate dai sistemi di c) verifichi che la presenza di attacchi, fragilità, intromissioni informatiche di terzi, infezioni, malware e/o virus nei sistemi informatici della sia conseguenza dell'omessa adozione, da parte di quest'ultima, di misure di sicurezza idonee a salvaguardare i medesimi sistemi da aggressioni di terzi; - ai sensi dell'art. 210 c.p.c., l'Ill.mo Tribunale adito voglia ordinare all'attrice, ., in persona dei legali rappresentanti pro tempore, l'esibizione delle istanze, da questa

già presentate, di restituzione delle somme sottoposte a sequestro su provvedimento del Giudice per le Indagini Preliminari – Tribunale di :ll'ambito del procedimento penale n. RGNR e rinvenute sul conto corrente acceso presso , intestato a e identificato dal codice IBAN , come precisato dalla banca . con propria comunicazione prodotta da ub doc. 12, o qualsivoglia ulteriore documentazione in possesso dell'attrice attestante lo stato della somma ivi indicata e la relativa restituzione; - dichiarare inammissibili le istanze istruttorie avversarie già respinte, qualora riproposte";

- per l'appellata:

"In Via Preliminare: -Accertarsi e dichiararsi l'inammissibilità del quarto motivo d'appello in violazione di quanto disposto dall'art. 345 c.p.c. per tutti i motivi esposti;

In Via Principale: Respingere integralmente l'appello presentato da , rigettando tutte le domande ivi formulate, nessuna esclusa, in quanto inammissibili o comunque assolutamente infondate sia in fatto che in diritto e, per l'effetto, confermare la sentenza impugnata n. emessa dal Tribunale di per tutti i motivi esposti. -In ogni caso spese e compensi di lite di entrambi i gradi di giudizio integralmente rifuse. In Via Istruttoria: Parte appellata si oppone all'ammissione delle istanze istruttorie formulate dalla appellante in primo luogo in quanto inammissibili non essendo state impugnate anche le correlate ordinanze del e con le quali il Tribunale di aveva rigettato le istanze istruttorie dell'appellante ritenendole inammissibili in quanto valutative e/o irrilevanti, e in secondo luogo per i seguenti motivi: -Per quanto concerne la chiesta ammissione di prova testimoniale la stessa è da ritenersi inammissibile essendo tutti i capitoli di prova formulati sub. a), b), c) e d), generici, irrilevanti, comportanti valutazioni da parte del teste ed in ogni caso documentali. In denegata e

non creduta ipotesi venisse ammesso anche solo uno dei suddetti capitoli di prova formulati ex adverso, si chiede di essere ammessi a prova contraria, con gli stessi testi indicati da controparte ossia il Sig. , domiciliato c/o , e il Sig. , domiciliato c/o sui seguenti capitoli di prova: 11) Vero che in data alle ore il Dott. ha eseguito dal conto corrente n. della società attrice, aperto presso la un bonifico bancario on line indicando come beneficiario sé stesso, per la somma di € con causale "bonifico", come da distinta di bonifico che Le si rammostra (Doc. 14)?;

12)Vero che i bonifici bancari effettuati in data , come da tracciature prodotte dalla banca sub. doc. 3 che Le si rammostra, sono stati eseguiti dal conto corrente n. della società attrice a mezzo del profilo di home banking della correntista?

Si chiede di essere ammessi a prova testimoniale sui seguenti capitoli: 1) Vero che in data alle ore 9:12 il ha eseguito dal conto corrente n. della società attrice, aperto presso la un bonifico bancario on line indicando come beneficiario il Dott. , con IBAN per la somma di € 50.000,00 con causale "bonifico", come da distinta di bonifico che Le si rammostra (Doc. 03)?; 2) Vero che in data , alle ore 10:55 il Dott. eseguiva dal conto corrente n. della società attrice, aperto presso la un altro bonifico bancario on line indicando come beneficiario il Dott. questa volta però con IBAN per la somma di € 50.000,00 con causale "bonifico", come da

distinta di bonifico che Le si rammostra (Doc. 04)?; 3) Vero che in data) alle ore 9:14 il Dott. I ha eseguito dal conto corrente n. della società attrice, aperto presso la un bonifico bancario on line indicando come beneficiario sé stesso, per la somma di € 20.000,00 con causale "bonifico", come da distinta di bonifico che Le si rammostra (Doc. 14)?; 4) Vero che i bonifici di cui ai capitoli precedenti sono stati effettuati dal Dott. accedendo al portale di home banking "Inbiz" della banca ?; 5) Vero che le credenziali per accedere al portale di home banking "Inbiz" del conto corrente n. intestato alla società attrice, sono custoditi ed utilizzati solamente dal Dott. ?;

6) Vero che il Dott. nell'effettuare i bonifici di cui ai capitoli 1), 2) e 3) ha utilizzato l'anagrafica registrata nel portale per indicare i dati del beneficiario come da schermate che Le si rammostra sub. docc. 15 e 16?; 7) Vero che i nominativi e risultano sconosciuti nell'anagrafica di cui al capitolo precedente come da schermate che Le si rammostrano sub. docc. 17, 18, 19 e 20, e comunque sconosciuti al

8) Vero che gli accessi al portale di home banking [redacted] del conto corrente n. intestato alla società attrice, vengono effettuati dal Dott. solamente utilizzando il computer aziendale?; 9) Vero che nel computer aziendale utilizzato dal Dott. per accedere al portale di home banking [redacted] del conto corrente n. intestato alla società attrice, è installato il programma antivirus "Norton"?; 10) Vero che il programma Norton antivirus di cui al capitolo precedente è costantemente aggiornato dal sistema essendo impostato in modalità di auto-aggiornamento ed era installato nel computer aziendale anche nei giorni e ottobre)?. Si indica quale testimone la Signora impiegata c/o

-Ci si oppone, poi, alla chiesta CTU informatica in quanto palesemente esplorativa non essendo finalizzata a fornire al giudice uno strumento di valutazione dei fatti, ma a fare entrare, invece, nel processo nuovi fatti inammissibili, che la convenuta avrebbe dovuto invece dedurre e provare. Conseguentemente la chiesta CTU è inammissibile in quanto finalizzata ad aggirare l'onere della prova. - Ci si oppone, infine, al chiesto ordine di esibizione in primo luogo essendo formulato genericamente, ed in secondo luogo essendo assolutamente inammissibile tenuto conto del fatto che viene richiesta la esibizione/produzione di documentazione che controparte avrebbe comunque potuto acquisire direttamente mediante istanza di poter accedere al fascicolo del menzionato procedimento penale.

L'istanza, quindi, è anche in questo caso assolutamente inammissibile in quanto tesa ad aggirare gli oneri probatori gravanti su parte appellante".

RAGIONI DELLA DECISIONE

La conveniva in giudizio la banca , deducendo le seguenti circostanze di fatto: 1) la società aveva intrattenuto con l'istituto di credito il rapporto di conto corrente n. , sul quale era abilitata ad operare anche mediante servizio di *home banking*; 2) il e il il legale rappresentante della correntista aveva eseguito due bonifici bancari *online* della somma di € 50.000,00 ciascuno, indicando come beneficiario , il primo sull'IBAN e il secondo sull'IBAN entrambi con causale "bonifico"; 3) il , avvisata da (accortosi dell'insufficienza di provvista sul proprio conto IBAN , la correntista aveva scoperto che entrambi i predetti bonifici erano stati dirottati in favore di due beneficiari sconosciuti, tali e con modifica delle causali; 4) di

conseguenza, il legale rappresentante, guidato da un'impiegata della filiale, aveva sottoscritto il modulo per il "disconoscimento delle operazioni di pagamento non autorizzate" e aveva sporto querela presso la Questura di ; 5) in un primo momento, la banca aveva riaccreditato la somma di € 100.000,00 in favore della correntista ma, a seguito di controlli interni e ritenendosi estranea ai fatti, aveva stornato il riaccredito.

Sulla base di queste allegazioni, evidenziato di essere caduta nella truffa del c.d. "*man in the browser*", da distinguere rispetto al fenomeno del c.d. *phishing*, e lamentata la inadeguatezza dei sistemi di sicurezza adottati dalla banca, l'attrice chiedeva la condanna della convenuta al risarcimento del danno quantificabile in € 100.000,00 oltre interessi e rivalutazione dalla data delle disposizioni.

Si costituiva in giudizio contestando gli addebiti avanzati dall'attrice, e concludendo per il rigetto delle domande attoree; la convenuta eccepiva altresì il concorso di colpa della correntista ex art. 1227 c.c., deducendo l'omessa custodia delle credenziali di accesso e il mancato controllo del codice SWIFT del beneficiario dei bonifici.

Il Giudice, esperita c.t.u. (avente ad oggetto il seguente quesito: "*Esaminati gli atti e i documenti di causa, eseguiti i necessari sopralluoghi, esperita ogni opportuna indagine anche su apparecchiature informatiche: 1. Descriva il consulente quale la frode informatica, se esistente, di cui è stata vittima l'attrice. 2. Ne individui, da un punto di vista tecnico, le modalità di esecuzione, i luoghi fisici o virtuali presso cui ha avuto esecuzione, le cause. 3. Dica quali le contromisure che possono, di regola, essere adottate da un punto di vista tecnico e dica quali quelle concretamente adottate. 4. Esprima una valutazione tecnica sulla congruità rispetto alla normativa tecnica in vigore delle contromisure adottate dalla convenuta, se esistenti. 5. Riferisca ogni altro utile elemento. 6. Tenti la conciliazione delle parti*", poi integrato sulla base della

seguente richiesta: "*Rilevata la non esaustività della risposta fornita dal consulente tecnico al quesito sottoposto dal giudice, nella misura in cui, da un lato, egli non ha fatto utilizzo del criterio del "più probabile che non", richiamando invece un inapplicabile criterio di "correttezza scientifica", e dall'altro, ha non compiutamente descritto la rispondenza dei sistemi di sicurezza dell'attrice agli standard medi del settore; egli dovrà pertanto rispondere compiutamente al quesito e in particolare al punto numero 3 tenendo in considerazione le argomentazioni di cui sopra*"), tratteneva la causa in decisione e assegnava i termini ex art. 190 c.p.c. per il deposito degli scritti conclusivi.

Con sentenza n. pubblicata il , il Tribunale di in accoglimento della domanda attorea, condannava la banca al pagamento in favore dell'attrice della somma di € 122.150,99 (già rivalutata e aumentata degli interessi legali), oltre interessi ex art. 1284 comma 4 c.c. dalla pubblicazione della sentenza al saldo, ponendo integralmente a carico della convenuta le spese di lite e definitivamente a carico della stessa le spese di c.t.u., sulla base - in sintesi - delle seguenti ragioni: 1) i fatti verificatisi sono inquadrabili nella frode informatica del c.d. "*man in the browser*" (una particolare ipotesi di frode informatica in cui l'*hacker* si mette in mezzo a due entità e, intercettando i messaggi inviati e ricevuti, riesce a modificarli senza provocare alcun malfunzionamento al dispositivo); 2) questa tipologia di frode informatica viene posta in essere utilizzando metodi particolarmente sofisticati, non percepibili da chi non possiede competenze tecniche in materia; 3) l'operato del banchiere dev'essere valutato secondo il parametro della diligenza qualificata di cui all'art. 1176 comma 2 c.c., oltre che alla luce della disciplina speciale di cui al d.lgs. 11/2010 sui servizi di pagamento informatici; 4) in particolare, l'art. 10 del predetto decreto legislativo fa gravare sul prestatore di servizi l'onere della prova del comportamento fraudolento, doloso o gravemente colposo tenuto dall'utente, posto che

l'utilizzazione dei codici di accesso ai servizi bancari da parte di terzi estranei rientra fra i rischi d'impresa tipici del prestatore di servizi di pagamento e, quindi, dev'essere evitato mediante la predisposizione di sistemi di sicurezza idonei; 5) il contenuto dell'onere della prova "liberatoria" non è immutabile, ma si modifica in base alla tecnica di truffa utilizzata e al grado d'insidiosità della stessa; 6) nel caso di specie, la banca non ha assolto al proprio onere probatorio, atteso che si è limitata ad allegare la mancata custodia dei codici di accesso e l'omesso controllo del codice SWIFT da parte della correntista, senza dimostrare che tali inosservanze si siano verificate e/o abbiano determinato o agevolato la buona riuscita della frode; 7) peraltro, il controllo del codice SWIFT da parte del correntista non è esigibile, poiché si tratta di un dato la cui osservazione sfugge all'attenzione e competenza del normale utente, mentre l'asserita mancata custodia dei codici di accesso è smentita dalle conclusioni della c.t.u. (posto che "*Il consulente tecnico ha rilevato che il dispositivo attraverso il quale i bonifici venivano abitualmente disposti era collocato presso lo studio della società, il cui "doppio sistema di allarme utilizzato garantiva un'elevata sicurezza fisica consentendo l'accesso ai locali solamente al personale autorizzato" (cfr. pag. 10 CTU integrativa del 15/5/2023). Tale dispositivo era utilizzato e aggiornato esclusivamente da senza l'ausilio di personale esterno; il che esclude la cessione volontaria o comunque la condivisione negligente delle credenziali a terzi. Inoltre, pur nell'incertezza dei sistemi di sicurezza informatica adottati dall'attrice per la protezione del computer attraverso cui le operazioni di pagamento venivano effettuate (vi è unicamente una "fattura di acquisto di un PC con sistema operativo Windows 10 ed un antivirus preinstallato McAfee LiveSafe" del 5/3/2020, cfr. pag. 16 CTU integrativa), il consulente tecnico d'ufficio non ha evidenziato particolari omissioni nella protezione del sistema operativo della società, tali da agevolare l'intrusione del malware*"); 8) la colpa grave della correntista non può desumersi

nemmeno dalla predisposizione di un sistema di autentificazione forte da parte della banca (a due fattori) che è, comunque, insufficiente ad evitare tipologie di truffe come quella in esame; 9) il disconoscimento delle due operazioni di bonifico è stato fatto in maniera tempestiva, poiché, prima del 1 , non vi era ragione di dubitare del buon esito delle operazioni (alla luce della "finta" schermata apparsa che lo confermava, oltre che dei normali tempi di elaborazione degli ordini di bonifico non istantanei); 10) la somma di € 50.000,00 bonificata il) è bensì stata oggetto di sequestro nell'ambito del procedimento penale instaurato proprio a seguito della querela sporta dal legale rappresentante della correntista ma la stessa potrà essere restituita solo nell'eventualità del dissequestro.

***

Avverso la sentenza ha proposto tempestivo appello

Col primo motivo di gravame, essa ha lamentato che il Tribunale non abbia adeguatamente considerato le risultanze processuali che evidenziavano la colpa grave della correntista per omessa adozione di idonee misure di sicurezza. In particolare, né il giudice di prime cure né il consulente tecnico avrebbero spiegato le precise dinamiche della truffa (interrogandosi, ad esempio, su cosa fosse concretamente apparso sullo schermo del dispositivo infettato dal *virus*), necessarie per valutare il contegno soggettivo, gravemente colposo, della correntista. Nel dettaglio, tale forte negligenza emergerebbe dalle seguenti circostanze: 1) la proprietaria aveva qualche tempo dopo l'accaduto dolosamente formattato e ceduto a terzi il proprio dispositivo, impedendone un'analisi adeguata e fedele; 2) non si era adoperata per mettere in sicurezza i propri dispositivi (come evincibile dalla persistente alterazione dei dati di cui alle ricevute scaricate successivamente); 3) non aveva adottato un sistema di sicurezza idoneo all'utilizzo imprenditoriale del conto corrente, come evidenziato anche dal c.t.u. nella parte in cui questi

aveva rappresentato una gestione "domestica" della *cybersecurity* aziendale, senza l'apporto di tecnici specializzati, anche tenuto conto del fatto che l'attività propria dell'impresa (offerta di servizi medici) imponeva l'adozione di particolari cautele nell'ottica di salvaguardia dei dati sensibili dei pazienti.

Col secondo motivo di gravame l'appellante ha lamentato l'incongruità e illogicità della motivazione per mancata ed erronea valutazione delle risultanze processuali con riguardo alla colpa grave della correntista per intempestivo disconoscimento delle operazioni non autorizzate. Secondo l'appellante, la correntista avrebbe potuto accorgersi della truffa subita (e quindi denunciarla) immediatamente dopo la disposizione del primo ordine di bonifico - evitando, così, di rimanere vittima del secondo – considerate la disponibilità di ricevute in formato PDF (liberamente consultabili, anche dopo la scomparsa della ricevuta "a video") e l'evidente anomalia della sequenza "XXX" in luogo delle ordinarie sequenze "[redacted] e "[redacted]" ("chiaramente" riferibili a banca , quanto alla prima, e a l , quanto alla seconda).

Col terzo motivo di gravame, l'appellante ha lamentato l'incongruità e illogicità della motivazione per mancata ed erronea valutazione delle risultanze processuali con riguardo alla colpa grave della correntista per omessa custodia degli strumenti di pagamento, in quanto, anche alla luce delle conclusioni raggiunte dalla c.t.u., ad una potenziale sicurezza degli ambienti fisici non aveva fatto seguito pari sicurezza degli ambienti informatici.

Col quarto motivo di gravame, l'appellante ha censurato la motivazione di primo grado per non aver ammesso (*recte* valutato come raggiunta) la prova indiziaria circa la colpa grave della correntista.

Col quinto motivo di gravame, l'appellante ha mosso doglianze avverso la sentenza impugnata

nella parte in cui il Tribunale ha ritenuto inidonei i propri sistemi di sicurezza, vagliandoli col parametro (erroneo) di cui all'art. 1176 comma 2 c.c. anziché sulla base degli oneri imposti dalla disciplina speciale (e quindi esclusiva), di derivazione comunitaria, di cui al d.lgs. 11/2010. Secondo l'appellante, il proprio sistema di sicurezza improntato all'autenticazione forte a due fattori rispetterebbe i requisiti di esigibilità previsti dalla suddetta normativa specialistica, come dimostrato dal fatto che esso è munito di certificazione ISO 27001:2013.

Col sesto motivo di gravame, l'appellante ha lamentato la violazione dell'art. 112 c.p.c., in quanto il giudice di prime cure non si sarebbe pronunciato sull'eccezione di concorso di colpa ex art. 1227 c.c. tempestivamente formulata dalla banca in primo grado.

Infine (appello, pag. 35) l'appellante ha evidenziato come "all'accoglimento dell'appello, dovrà seguire la riforma del capo della decisione concernente le spese di lite nonché le spese di CTU e CTP, in quanto accessorio e dipendente da quelli principali, con condanna della alla restituzione della somma di € 141.749,15 pagata da forza della sentenza impugnata (doc. 4), oltre rivalutazione e interessi dal giorno del pagamento (novembre), sino al saldo".

Costituendosi, l'appellata ha eccepito, in via pregiudiziale, la manifesta infondatezza dei primi quattro motivi d'appello e, comunque, l'inammissibilità del quarto motivo (mancato raggiungimento della prova indiziaria sulla colpa grave della correntista) per novità della questione in violazione dell'art. 345 c.p.c. (per non aver mai Intesa avanzato una richiesta, eccezione o argomentazione in tal senso). Nel merito, ha concluso per il rigetto integrale del gravame e per la conferma della sentenza di primo grado.

Con la comparsa conclusionale, l'appellata, sul presupposto del rilevato mancato deposito della nota di precisazione delle conclusioni da parte dell'appellante, ha eccepito l'inammissibilità delle istanze istruttorie dalla stessa formulate, in quanto implicitamente rinunciate.

Con la comparsa conclusionale di replica, l'appellante, negando la fondatezza di quest'ultimo rilievo, ha evidenziato di aver provveduto ad un nuovo deposito della nota di precisazione delle conclusioni (poiché il primo deposito, tempestivo, non era andato a buon fine a causa di un errore informatico), nonché di aver, in ogni caso, precisato le conclusioni nell'atto di citazione in appello, senza che nulla possa far ritenerle anche solo in parte abbandonate.

Con la comparsa conclusionale di replica, l'appellata ha eccepito l'inammissibilità per tardività e irritualità delle conclusioni come precisate con la nota depositata dall'appellante il

Con provvedimento del l'intestata Corte ha fissato udienza di rimessione della causa in decisione, con assegnazione dei termini di cui all'art. 352 c.p.c. e sostituzione dell'udienza con termine fino al per note ex art. 127 ter c.p.c.

***

Le questioni pregiudiziali.

L'eccezione di inammissibilità per manifesta infondatezza dei primi quattro motivi di gravame è infondata e va rigettata, posto che non può escludersi, *a priori* e prima della trattazione, una probabilità di accoglimento dei predetti motivi; la questione è in ogni caso superata, essendo la causa pervenuta alla fase decisionale.

L'eccezione di inammissibilità del quarto motivo d'appello per violazione del divieto di *nova* in appello (art. 345 c.p.c.) non può essere accolta, considerato che tale motivo non introduce una nuova domanda, una nuova eccezione o una nuova richiesta di prova, ma si risolve esclusivamente in una censura nei confronti del ragionamento del giudice di prime cure, il quale – in tesi dell'appellante – avrebbe dovuto ritenere raggiunta la prova della colpa grave della correntista per via presuntiva, in particolare su base indiziaria.

L'eccezione di inammissibilità e decadenza dalle istanze istruttorie formulate dall'appellante (per

l'intempestività o irritualità del deposito della nota di precisazione delle conclusioni) è infondata, atteso che le conclusioni erano già state precisate nei medesimi termini con l'atto introduttivo dell'appello (la cui tempestività non è messa in discussione); in ogni caso, le prove richieste, per quanto si osserverà, non sono suscettibili di recare ad una diversa definizione della lite, così che se ne conferma la mancata ammissione.

I primi quattro motivi d'appello: erroneità della sentenza di primo grado nella parte in cui ha ritenuto insussistente la colpa grave in capo alla correntista.

Con i primi quattro motivi d'appello, che possono essere analizzati congiuntamente in ragione della loro connessione logica, l'appellante ha censurato la sentenza di primo grado nella parte in cui il Tribunale non ha accertato la colpa grave in capo alla correntista, tenuto conto: 1) della mancata adozione da parte della stessa di misure di sicurezza idonee a custodire i propri codici d'accesso (primo e terzo motivo d'appello, nella sostanza sovrapponibili); 2) dell'intempestivo disconoscimento delle operazioni di pagamento non autorizzate (secondo motivo d'appello).

La vicenda occorsa è stata pacificamente ricondotta alla fattispecie di frode informatica, ma le parti sono in disaccordo circa la specifica tipologia di frode occorsa: secondo l'appellante, si tratterebbe del c.d. *phishing*, tipologia meno insidiosa, posta in essere approfittando della "credulità colpevole" della vittima che cede involontariamente i propri dati riscontrando delle comunicazioni (e-mail o messaggi) fraudolenti; secondo l'appellata (oltre che secondo il c.t.u. e il Tribunale), la fattispecie sarebbe inquadrabile nel caso del c.d. *man in the browser*, tipologia più insidiosa, nell'ambito della quale "nella sua massima espressione di efficienza aggressiva, il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una *botnet*, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il *malware* – riconducibile alla più ampia categoria dei cc.dd. *trojan* ("cavalli

di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel *computer* della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il *malware* resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (*targeted banks*). In quel preciso istante il *malware* "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, *Hyper Text Transfer Protocol*) "*http*" e non già "*https*" (dove la "s" finale sta per *secured*, protetto). Ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera" (v. in questi termini il Coll. di coordinamento ABF dec. 34983/2012).

Il quadro normativo di riferimento di entrambe le tipologie di frodi informatiche è comunque recato, principalmente, dal D.lgs. 11/2010, emanato in attuazione della Direttiva 2007/64CE5 e successivamente modificato dal D. Lgs. 218/2017, in attuazione della Direttiva 2015/2366/UE6, in vigore dal 13.1.2018 ed operativa dal 14.9.2019.

In particolare, l'art. 10, comma 1, dispone che, qualora l'utente dei servizi di pagamento (cliente) neghi di aver autorizzato un'operazione di pagamento, è onere del prestatore di servizi (intermediario) provare che l'avvenuta operazione di pagamento: 1) è stata autenticata; 2) è stata correttamente registrata e contabilizzata; 3) non ha subito il malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti. Tale prova – prosegue il 2° comma – non

è tuttavia 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 sul medesimo gravanti di cui all'art. 7 del medesimo decreto legislativo, essendo onere dell'intermediario fornire la prova della frode, del dolo o della colpa grave in capo all'utente.

Più precisamente, "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. (Nella specie, la S.C. in applicazione del detto principio, ha confermato la decisione di merito che aveva ritenuto gravante su . ai fini della non riferibilità al cliente delle operazioni fraudolente eseguite con la sua carta Postepay, la dimostrazione della previa adozione di mezzi di prevenzione dell'uso illecito dei sistemi elettronici di pagamento, quali, ad esempio, l'invio al titolare della carta di appositi sms alert di conferma di ogni singola operazione)" (Cass. n. 3780 del 12/02/2024).

Ne deriva un regime speciale di protezione e di speciale *favor* probatorio a beneficio degli utenti, posto che l'onere di dimostrare la colpa grave (o, nei casi estremi, il comportamento fraudolento) del cliente rimane in capo al prestatore di servizi, coerentemente con il fatto che "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" (v., in motivazione, Cass. n. 13204/2023).

Conseguentemente, qualora la banca dimostri l'autenticazione, la registrazione e la contabilizzazione dell'operazione di pagamento, senza, tuttavia, provare il contegno soggettivo tenuto dal cliente, la "causa ignota" della truffa informatica (e cioè le circostanze che, nonostante il corretto comportamento tenuto dalla banca, abbiano permesso l'esecuzione della frode) rimane a carico della banca.

Tanto premesso, nel caso di specie risulta - in definitiva - irrilevante sussumere i fatti al di sotto della categoria del *phishing* o del *man in the browser*, considerato che difetta, in ogni caso (anche adottando un parametro di diligenza adeguato alla fattispecie meno insidiosa delle due), la prova della colpa grave in capo alla correntista per le ragioni di seguito esposte.

A fondamento della prima censura (mancata adozione da parte della stessa di misure di sicurezza idonee a custodire i propri codici d'accesso), l'appellante contesta alla cliente: a) di aver ceduto a terzi il dispositivo dal quale erano state autorizzate le operazioni di pagamento; b) conseguentemente, di non aver permesso la ricostruzione della precisa dinamica dei fatti; c) di non essersi adoperata tempestivamente per eliminare il *virus* dal dispositivo a distanza di tre mesi dall'attacco di hackeraggio; d) di aver adottato un sistema di sicurezza a "gestione domestica", inadatto ad un contesto aziendale come quello della correntista (anche considerato che l'attività svolta implica il trattamento di dati sensibili dei pazienti-clienti).

Con riferimento ai punti *sub* a) e *sub* b), la c.t.u. resa in primo grado ha condivisibilmente concluso nel senso che "*La mancanza del PC e dei dati di traffico internet rendono impossibile stabilire con certezza scientifica la modalità di esecuzione dei 2 bonifici oggetto di contestazione. Nè le forze dell'ordine nè il personale banca hanno consigliato al dott. . di conservare inalterato il dispositivo con cui sono stati effettuati i bonifici. E' singolare come la parte attorea abbia deciso di disfarsi del computer dopo averlo formattato sapendo che era stato*

utilizzato nella esecuzione di un presunto crimine informatico su cui sono aperti un procedimento civile ed uno penale. L'analisi del PC, accuratamente conservato e custodito (ovvero spento, non più utilizzato e mantenuto in un luogo sicuro) avrebbe potuto fornire informazioni utili a comprendere la dinamica dei fatti, a trovare le traccie di un eventuale virus e a determinarne la modalità di funzionamento. L'assenza del PC preclude anche la possibilità di dare un giudizio certo sulla presenza di antivirus e patch di sicurezza installate sul dispositivo. Non è quindi possibile esprimere un giudizio certo sulle misure di sicurezza adottate dalla azienda" (v. pag. 30 ss. della c.t.u.), evidenziando, inoltre, che "*Riguardo alla mancata conservazione di tale dispositivo risulta singolare come, sia in fase di disconoscimento delle operazioni presso la Banca, sia in sede di denuncia alle Forze dell'Ordine nessuno abbia consigliato di conservarlo inalterato. E' inoltre singolare che la si sia disfatta di tale reperto sapendo che era stato utilizzato per la perpretazione di un illecito su cui erano stati aperti un procedimento civile e uno penale*" (cfr. pag. 12 della c.t.u.).

Sulla base di queste conclusioni, rese all'esito di una c.t.u. che si caratterizza per coerenza, imparzialità e consequenzialità, anche tenuto conto delle repliche alle osservazioni dei c.c.t.t.p.p. e che può – dunque – essere posta alla base della decisione, oltre che sulla base delle circostanze di fatto emerse nel corso del giudizio in parte allegate e non contestate, la scelta della correntista di cedere a terzi il proprio dispositivo elettronico non risulta conseguente ad una volontà dolosa in quanto finalizzata a sottrarre o disperdere la prova o anche solo colposa in considerazione della prevedibile necessità di sottoporre il dispositivo ad accertamenti tecnici.

Più precisamente, deve considerarsi legittimamente sorto nella correntista un affidamento nel senso della non necessità di conservare il proprio dispositivo utilizzato per il servizio di *home banking*, atteso che la diligenza nella conservazione di una prova assume rilevanza solo qualora

essa debba essere utilizzata in un futuro contenzioso la cui instaurazione sia quantomeno prevedibile. Nel caso di specie, il legale rappresentante della correntista si è subito recato in banca denunciando l'ammanco rilevato, ha compilato il modulo per il disconoscimento delle operazioni non autorizzate (che non risulta contenere invito a conservare intatto il dispositivo oggetto di potenziali verifiche future), ha rapidamente ricevuto il riaccredito della somma fraudolentemente distratta dai truffatori senza - ancora una volta - essere stato avvertito che era necessario preservare il dispositivo, ha anche presentato querela senza che ne sia seguito un sequestro o un'informativa circa l'opportunità di consentire accertamenti futuri sugli strumenti utilizzati per le operazioni in regime di *home banking*: è evidente che il cliente non poteva ragionevolmente prevedere (a differenza della banca, che ben conosce il fenomeno cui il singolo episodio *ab initio* poteva apparire riconducibile e le prassi interne) il successivo unilaterale ristorno del riaccredito e il conseguente contenzioso che ne è seguito.

Con riferimento al punto *sub* c), il fatto che la correntista non si sia adoperata – *ex post* (dopo tre mesi dall'attacco di hackeraggio) – per eliminare il *virus* dal proprio dispositivo non incide sulla valutazione della sua diligenza, poiché quest'ultima deve essere vagliata al momento della prima evidenza di operatività del *virus* all'interno del dispositivo stesso, rimanendo le condotte successive del tutto indifferenti ai fini del presente giudizio (nell'ambito del quale l'unico danno di cui la correntista chiede il risarcimento è relativo al danno emergente subito al momento delle operazioni non autorizzate, mentre è assente qualsiasi richiesta risarcitoria di ipotetici danni sopravvenuti).

Per quanto riguarda l'asserita mancata adozione di sistemi di sicurezza adeguati ad un contesto aziendale (*sub* d), occorre richiamare le conclusioni rese dal c.t.u. (che per le ragioni sopra evidenziate, possono essere poste alla base della decisione). Il consulente tecnico ha

rappresentato che "*L'attacco subito dal malware sul dispositivo della* .
non è indicativo di assenza di protezioni e antivirus installati. Il malware potrebbe essere riuscito a eludere i controlli portando a termine l'attacco" (pag. 31 c.t.u.). In altri termini, a causa delle particolari modalità esecutive della truffa, qualsiasi sistema di sicurezza non sarebbe stato idoneo a sventarla: mancherebbe quella che nella teoria generale del reato è definita come "causalità della colpa", nel senso che il comportamento alternativo lecito (adozione di un sistema di sicurezza aziendale, mediante l'assunzione di un esperto di *cybersecurity*) non avrebbe, in ogni caso, impedito agli *hacker* di insinuarsi nel dispositivo.

Del resto, lo stesso c.t.u. riconosce la diffusa prassi di adottare un sistema di sicurezza non professionale, tenuto conto, fra l'altro, delle dimensioni ridotte dell'attività aziendale: "*come tutte le funzioni aziendali, anche la sicurezza informatica è una attività che richiede risorse economiche. E' quindi plausibile che attività imprenditoriali di dimensione contenute possano inserire nei loro budget di spesa importi decisamente inferiori rispetto a multinazionali o aziende di medie 10 dimensioni. Risulta quindi comprensibile che determinate attività economicamente onerose, come security assessment o penetration test non vengano eseguite frequentemente. Oppure che alcune procedure siano definite con minore dettaglio*" (pag. 25 ctu).

Questo ragionamento non può essere inficiato da altre osservazioni, solo apparentemente contrastanti con le precedenti, contenute nella medesima c.t.u. (ad esempio a pag. 10 della relazione integrativa), ove si evidenzia come l'affidamento dei servizi di sicurezza a soggetti qualificati avrebbe impedito la formattazione, la cessione a terzi e quindi la dispersione della prova: in primo luogo, perché, nonostante la segnalazione di questa criticità, il c.t.u. è comunque giunto ad adeguate conclusioni sulla base di altri elementi disponibili e ha risposto in modo esaustivo a tutti i quesiti posti dal Tribunale; in secondo luogo, in quanto tale rilievo non è, in

ogni caso, sufficiente a superare le considerazioni in precedenza esposte con riferimento alle condotte tenute dalle parti successivamente all'accaduto, non essendo risultata prevedibile la futura instaurazione di un contenzioso.

Né, infine, nel caso di specie può assumere rilevanza per l'accertamento della colpa della correntista il fatto che l'azienda appellata offra servizi medici e quindi sia in contatto con i dati sensibili dei pazienti: la norma cautelare che si assume violata (predisporre un idoneo sistema di sicurezza dei dati sensibili) è posta per arginare il rischio della verificazione di un evento (la dispersione dei dati sensibili) diverso da quello verificatosi nel caso di specie (l'appropriazione da parte di terzi dei dati bancari della correntista).

A fondamento della seconda censura (intempestivo disconoscimento delle operazioni di pagamento non autorizzate), l'appellante contesta all'appellata di aver colposamente tardato nel riferire alla banca la mancata autorizzazione delle due operazioni di bonifico. Più precisamente, l'atteggiamento negligente – da apprezzare ai sensi dell'art. 1176 comma 2 c.c., tenuto conto della natura commerciale della correntista - sarebbe rinvenibile nel fatto che, pur avendo essa a disposizione le ricevute di bonifico in formato PDF, la correntista non si sarebbe immediatamente accorta di alcune anomalie riscontrabili nelle diciture contenute nelle due disposizioni di pagamento ("non risulta giustificabile la trascuratezza nell'ignorare l'incompletezza della presentazione riportante la generica sequenza "XXX" piuttosto che la dicitura [redacted]" chiaramente riferibile a l . e differente dalla sequenza[redacted] chiaramente riferibile a l ' cfr. pag. 20 dell'atto di citazione in appello, aggiungendo l'appellante che "è notoria, infatti, l'operazione societaria che nel porto . ad acquisire il controllo della _ (, con iniziali, appunto BCI": cfr. nota 44 pag. 20 dell'atto di citazione in appello).

Il motivo è infondato e va rigettato.

Sul punto, il Tribunale ha correttamente osservato che "*nemmeno dal riepilogo dell'operazione di pagamento è possibile, per l'utente, evincere l'avvenuta frode, atteso che, come anche documentato dalle ricevute di bonifico effettuate dalla , il beneficiario e la causale del bonifico appaiono essere quelli selezionati originariamente dal disponente (cfr. doc. 3 e 4 citazione). In tal senso, è infondata la contestazione della convenuta circa il mancato controllo, da parte della società attrice, del codice SWIFT del beneficiario dei bonifici. Pretendere, infatti, che l'utilizzatore dei servizi di pagamento verifichi tale codice, peraltro relativo a bonifici internazionali (ipotesi non ricorrente nel caso in esame), implicherebbe attribuire a tale soggetto, privo di competenze tecniche specifiche, una responsabilità che esula dalle normali capacità informatiche di un utente di media diligenza. Il controllo, cioè, su una particolare sequenza alfanumerica, quale quella del codice SWIFT, è un'attività che non rientra nella gamma di accorgimenti diligenti che normalmente l'utilizzatore di servizi di pagamento compie. L'affidamento dell'utente nella sicurezza del servizio di pagamento informatico è invero generato dalla serie di credenziali e codici di verifica richiesti dalla banca prima di effettuare un'operazione di pagamento. In tale contesto, il codice SWIFT non è elemento che riveste carattere determinante al fine di verificare la diligenza dell'utente nell'utilizzo corretto dello strumento di pagamento, posto che tale codice viene automaticamente associato al conto corrente del beneficiario selezionato. Da quanto sopra, emerge altresì l'infondatezza della contestazione di parte convenuta in punto a ritardo della società attrice nell'effettuare il "disconoscimento" delle operazioni di pagamento. La banca ha affermato che, se l'attrice avesse controllato l'estratto conto subito dopo le disposizioni di pagamento, i bonifici avrebbero potuto essere revocati entro le ore 17.30 del medesimo giorno dell'operazione. Tale assunto è*

infondato. Data l'impercettibilità, da parte dell'utilizzatore, dell'interposizione della schermata del software malevolo con quella autentica del sistema di home banking, non è stato possibile per l'attrice avvedersi del dirottamento dei bonifici sino al momento in cui tali somme non sono confluite nel conto corrente del beneficiario originario. L'interposizione fittizia della schermata del malware nel sistema di home banking ha generato una schermata di buon esito dell'operazione di pagamento; il che non induce e non ha indotto, nel caso di specie, il disponente a controllare l'estratto conto per verificare la correttezza del pagamento. Inoltre, dal momento che non si tratta di bonifici istantanei, e dunque con accredito immediato della somma di denaro, i bonifici ordinari (come quelli di specie) richiedono un periodo di elaborazione da parte della banca normalmente di due giorni, pari al tempo trascorso tra la disposizione dei bonifici e il disconoscimento delle operazioni di pagamento da parte della . In altri termini, non sussisteva alcun motivo per il quale l'attrice dovesse rivolgersi alla banca prima del 16/10/2020, allorquando, scoperto il mancato accredito dal beneficiario originario, la si è recata prontamente presso la filiale del proprio istituto di credito per denunciare l'accaduto, assolvendo agli obblighi imposti a suo carico dall'art. 7, comma 1, lett. b) del D. Lgs. 11/2010" (pp. 14 e seguenti della sentenza di primo grado).

Tale ragionamento è condivisibile e va, quindi, confermato.

Da un lato, l'arco temporale di un solo giorno fra il momento di esecuzione del pagamento non autorizzato e il momento del disconoscimento rende senza dubbio qualificabile la condotta della correntista come tempestiva. Del resto, il legislatore non ha ipotizzato un termine massimo, tantomeno inferiore ad un giorno, entro il quale effettuare il disconoscimento, limitandosi a prevedere che lo stesso debba essere eseguito "senza indugio" (con una formulazione elastica, indicativa della necessità di valutazione secondo le circostanze del caso concreto); né risulta che

il contratto che disciplinava i servizi di pagamento elettronici tra le parti contenesse previsioni in tal senso.

Dall'altro lato, come coerentemente osservato dal giudice di prime cure, la comprensione dei codici alfanumerici utilizzati nell'ambito delle operazioni bancarie richiede competenze tecniche superiori a quelle esigibili da un operatore medio, ancorché esercente un'impresa commerciale. In questa prospettiva, non può accogliersi la ricostruzione proposta dall'appellante secondo cui le diciture "[redacted]" e "[redacted]" sarebbero "chiaramente" riferibili ad una banca piuttosto che ad un'altra.

Tutte le considerazioni che precedono ostano ad un accertamento, anche per via presuntiva (come richiesto dal quarto motivo d'appello), della colpa grave in capo alla correntista, essendo carenti - a monte - gli indizi da cui desumerla. Peraltro, l'appellante non indica nemmeno quali sarebbero gli elementi di gravità, precisione e concordanza da prendere in considerazione per la efficace formazione di una sufficiente presunzione ai sensi dell'art. 2729 c.c.

Quinto motivo d'appello: erroneità della sentenza di primo grado nella parte in cui ha ritenuto inidoneo il sistema di sicurezza adottato dalla banca.

Con il quinto motivo di gravame, l'appellante censura la sentenza di primo grado nella parte in cui il Tribunale ha ritenuto inidonei i sistemi di sicurezza dell'istituto di credito, vagliandoli sulla base di un parametro generale (art. 1176 comma 2 c.c.), anziché sulla base della disciplina speciale (e quindi esclusiva) di derivazione comunitaria (d.lgs. 11/2010). Secondo l'appellante, il proprio sistema di sicurezza improntato all'autenticazione forte a due fattori rispetterebbe i requisiti di esigibilità previsti dalla suddetta normativa di settore, godendo anche di certificazione ISO 27001:2013.

Innanzitutto, è priva di rilievo la censura rivolta all'utilizzo del – in tesi erroneo - parametro della

diligenza qualificata in capo al prestatore di servizi (art. 1176 comma 2 c.c.), considerato che tale parametro non si pone in antitesi (come sembrerebbe sostenere l'appellante) bensì in coerenza rispetto alla normativa di settore.

Va premesso che l'idoneità di un sistema di sicurezza adottato da un prestatore di servizi per i pagamenti elettronici dev'essere apprezzata non solo in astratto, ma anche in concreto, tenendo conto della sua capacità di resistenza a specifici attacchi di hackeraggio (i quali assumono connotati sempre più insidiosi, anche a seconda delle modalità con cui vengono posti in essere): in questo senso, secondo recente giurisprudenza di diversi collegi arbitrali bancari e finanziari, pur dovendosi confermare la capacità protettiva del sistema OTP (*one time password*), deve escludersi che alla predisposizione di un sistema di autenticazione a doppio fattore corrisponda, per ciò solo, una presunzione di colpa grave in capo al cliente, imponendosi, al massimo, una valutazione maggiormente rigorosa del comportamento tenuto dal cliente stesso (Coll. ABF Napoli, Dec. 3192/2012; vd. anche Coll. ABF Roma, Dec. n. 1910/2012) e occorrendo, comunque, tenere conto dell'intero sistema di controlli approntato dall'intermediario (Coll. ABF Roma, Decc. nn. 2264/2012; 2660/2012; 1910/2012).

In tale quadro s'inserisce anche il concetto di c.d. autenticazione forte del cliente (*strong customer authentication*, con acronimo SCA) di cui all'art. 10 *bis* D.lgs. 10/2011 secondo cui i prestatori di servizi di pagamento devono disporne l'applicazione quando l'utente, mediante l'accesso ad un conto di pagamento *online*, richieda un'operazione di pagamento effettuando azioni che possano comportare un rischio di frode o altri abusi (cioè che evidenziano indici di anomalia). L'autenticazione forte si basa su due o più elementi che sono classificati nelle seguenti categorie: 1) conoscenza, cioè qualcosa che solo l'utente conosce (*password*); 2) possesso, cioè qualcosa di personale e di esclusivo possesso (*smartphone* o *token*); 3) inerenza, cioè qualcosa

di riconducibile esclusivamente alla persona interessata (impronta digitale o riconoscimento facciale).

Nel caso di specie, sul presupposto della riconducibilità della frode allo schema del *man in the browser*, il c.t.u. ha osservato che:

- "*a differenza di altri tipi di attacchi, come per esempio nel phising, l'utente interagisce sempre con i web server del sito legittimo, per tale motivo l'utilizzo della autenticazione a 2 fattori non consente di bloccare questi tipi di malware*" (pag. 19 CTU);
- "*l'uso della autenticazione a 2 fattori e della crittografia non riescono a contrastare questi tipi di malware. Anche il controllo della localizzazione dell'utente attraverso l'indirizzo IP sorgente fa supporre la connessione come genuina in quanto le richieste sono effettivamente originate dal browser della macchina che l'utente abitualmente usa. Nel caso di transazioni finanziarie è possibile effettuare controlli sull'importo delle operazioni e sui destinatari, chiedendo conferma, per esempio quando vengono effettuate a beneficiari nuovi. Un meccanismo di difesa che può essere la presenza di un secondo fattore di autenticazione che non risieda nel browser, così da poter validare l'operazione su un canale che non è stato infettato (out of band communication). La richiesta di conferma potrebbe contenere i dettagli della operazione (es. Importo, IBAN accredito e Beneficiario). In questo modo la vittima potrebbe accorgersi che la operazione originaria è stata modificata*" (pag. 22 ctu);
- "*Nel portale inBiz il canale di comunicazione out of band viene attivato quando il controllo antifrode individua l'operazione come sospetta (vedi pag. 14 e 15 della presente relazione e pag. 4 del documento "Allegato_13_Intesa_Risposte a domande.pdf"). L'operazione sospetta viene bloccata, viene contattato il cliente su un cellulare*

"certificato", se ne verifica l'identità con una serie di domande segrete, dopodichè si chiede la conferma della disposizione da sottomettere. Il controllo antifrode non ha classificato i bonifici oggetto della presente relazione come sospetti. L'indirizzo IP da cui si era collegato l'utente era noto, l'autenticazione effettuata con il controllo a 2 fattori e gli importi in linea con altri trasferimenti di denaro richiesti precedentemente" (pag. 22 ctu).

In definitiva, quindi, il sistema adottato dalla banca non si è dimostrato, in concreto, utile a prevenire ed evitare la consumazione della truffa ai danni dei clienti: la mancata attivazione del controllo antifrode, dovuta all'apparente assenza di quelli che vengono classificati secondo il sistema come indici sospetti, non ha attivato l'invio dell'*alert* che avrebbe preventivamente informato la correntista dell'operazione anomala in corso di esecuzione.

Come più sopra evidenziato, la possibilità che alcune truffe siano, nella sostanza, assai difficilmente sventabili con gli strumenti difensivi messi a disposizione dallo sviluppo tecnologico del momento non può ripercuotersi negativamente sui risparmiatori, ma, al più, sull'intermediario (banca) che ha considerato, o avrebbe dovuto considerare, quest'alea all'interno del più generale rischio d'impresa.

In ogni caso, in applicazione dei principi giurisprudenziali sopra richiamati, la bontà astratta del modello di sicurezza non manleva la banca dal proprio onere di provare la colpa grave del cliente che, come già osservato, non è stato assolto.

Sesto motivo d'appello: violazione dell'art. 112 c.p.c. per omessa pronuncia sull'eccezione di colpa della correntista ex art. 1227 c.c.

Il sesto motivo d'appello, volto a far valere l'omessa pronuncia del Tribunale sull'eccezione di concorso di colpa della correntista ex art. 1227 c.c., è infondato e va rigettato, posto che la

omissione non sussiste, essendosi il giudice di grado espressamente pronunciato sul punto: "*In mancanza di prova sulla condotta colposa dell'attrice, non sussiste conseguentemente concorso di colpa della stessa, ai sensi dell'art. 1227 c.c., per la negligente custodia delle credenziali di accesso e il mancato controllo del codice SWIFT*" (pag. 18).

Nel merito, le osservazioni espresse da questa Corte in ordine agli altri motivi di gravame evidenziano come condivisibilmente sia stata ritenuta assente o comunque non provata la colpa della correntista, con l'effetto di rendere infondata anche l'eccezione di cui all'art. 1227 c.c. sollevata dalla banca.

Esito dell'appello e regolamentazione delle spese di lite.

L'appello deve, quindi, essere integralmente rigettato.

Le spese di lite del presente grado di giudizio seguono la soccombenza e vanno quindi poste a carico dell'appellante, come liquidate in dispositivo, tenuto conto del valore della causa (€ 100.000,00), secondo importi medi di cui al DM 55/2014 come aggiornato con DM 147/2022 per le fasi di studio, introduttiva e decisionale e con esclusione della fase di istruttoria e trattazione (il compenso per tale fase non è contemplato nella nota spese depositata dall'appellata il 29.10.2025).

Ai sensi dell'art. 13, comma 1 *quater*, del d.P.R. n. 115 del 2002, dev'essere dichiarata la sussistenza dei presupposti per il versamento dell'ulteriore importo a titolo di contributo unificato pari a quello dovuto per l'introduzione del presente giudizio, a norma del comma 1 *bis* dello stesso art. 13.

P. Q. M.

La Corte d'Appello di Venezia, ogni diversa domanda ed eccezione reiette ed ogni ulteriore deduzione disattesa, definitivamente pronunciando, così provvede:

1) rigetta l'appello e per l'effetto conferma la sentenza n. : emessa dal Tribunale di Padova;
2) condanna l'appellante .. alla rifusione in favore di . delle spese di lite del presente giudizio, che liquida in € per compenso di avvocato, oltre a rimborso forfetario 15% per spese generali ed oltre Iva e cpa se ed in quanto dovute per legge;
3) dà atto che sussistono i presupposti di cui all'art. 13, comma 1 *quater* del DPR n. 115/02 a carico di parte appellante.

Così deciso in Venezia, nella camera di consiglio del 27 novembre 2025.

Il Consigliere Estensore — Il Presidente

Francesco Petrucco Toffolo — Guido Santoro