N. R.G. 800/2024

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

CORTE DI APPELLO DI FIRENZE

SEZIONE SECONDA CIVILE – IMPRESE

* * * * *

La Corte di Appello di Firenze, Seconda Sezione, in persona dei Magistrati:

- Anna Primavera — Presidente
- Carmine Capozzi — Consigliere relatore
- Nicola Mario Condemi — Consigliere

ha pronunciato la seguente

SENTENZA

nella causa civile d'appello iscritta al n. r.g. **800/2024**, promossa

DA

APPELLANTI

CONTRO

in Roma, Via dei Barbieri, 6, giusta procura speciale allegata telematicamente alla comparsa di costituzione.

APPELLATA

PROVVEDIMENTO IMPUGNATO:

Sentenza n. 214/2024 del Tribunale di Prato pubblicata il 12/03/2024.

CONCLUSIONI

Per la parte appellante: "*Voglia la Corte adita, contrariis reiectis, previo accoglimento dei motivi di cui al presente atto di appello, in riforma della gravata sentenza: A) ritenere e dichiarare che le operazioni di bonifico e di prelievo di cui in premessa mai autorizzate dagli attori, sono riconducibili all'uso illecito di terzi delle credenziali di accesso al conto on line; e per l'effetto ritenere e dichiarare responsabile per l'indebito utilizzo del conto da parte di terzi, per non avere predisposto un sistema di protezione dei dati informatici adeguato all'effettiva tutela della sicurezza dei correntisti, e conseguentemente, B) in tesi, stante la sussistenza della responsabilità contrattuale della medesima, condannarla a rimborsare gli attori della perdita subita tramite la corresponsione in loro favore della somma di euro 44.974,00=, o quella minore o maggior somma che sarà ritenuta di giustizia, pari agli importi dei due bonifici on line non autorizzati eseguiti sul conto corrente n. 05601 005025 in data 29 e 30 marzo 2022; oltre rivalutazione monetaria ed interessi legali sulla somma rivalutata dal dì del dovuto fino al saldo effettivo; C) in ipotesi, previo accertamento dell'inesatto adempimento della banca convenuta, stante la violazione del limite operativo pari ad euro 250,00= per operazione di bonifico (P2P), condannare a pagare in favore degli attori la somma di euro 44.474,00=, o quella minore o maggiore di giustizia, relativa ai due bonifici non autorizzati effettuati in data 29 e 30 marzo 2022, detratto l'importo di euro 500,00= corrispondente al limite operativo vigente; oltre rivalutazione monetaria ed interessi sulla somma rivalutata dal dì del dovuto fino al saldo effettivo; D) con vittoria delle spese legali di entrambi i gradi di giudizio*".

Per la parte appellata: "*Voglia l'On.le Corte di Appello di Firenze, respinta ogni contraria istanza ed eccezione, così giudicare: - in via preliminare in rito, dichiarare inammissibile, ai sensi dell'art. 342 c.p.c., l'appello proposto dai Sig.ri per carenza di specificità dei motivi di impugnazione; - in via principale, nel merito, accertare l'inammissibilità ex art. 348-bis c.p.c. dell'appello proposto dai Sig. e e, per l'effetto, confermare la sentenza n. 214/2024 resa*

dal Tribunale di Prato, Sezione Unica Civile, Giudice Dott.ssa Raffaella Brogi, ex adverso impugnata; - in via subordinata, nel merito, rigettare, in quanto inammissibile e infondato, o in subordine con la miglior formula, l'appello proposto dai Sig.ri Pt_1 e Pt_2 e, per l'effetto, confermare integralmente la sentenza n. 214/2024 resa dal Tribunale di Prato, Sezione Unica Civile, Giudice Dott.ssa Raffaella Brogi, ex adverso impugnata per le ragioni dedotte nella comparsa di costituzione in appello e nei precedenti scritti difensivi di primo grado; - sempre nel merito, condannare l'appellante al risarcimento di tutti i danni patrimoniali per responsabilità aggravata ai sensi dell'art. 96 c.p.c. per le ragioni dedotte nella comparsa di costituzione in appello, nella misura che l'Ecc.ma Corte d'Appello riterrà opportuna; - in ogni caso, con vittoria di spese, competenze ed onorari di entrambi i gradi di giudizio".

Fatti di causa - svolgimento del giudizio

1. e hanno impugnato la sentenza del tribunale di Prato n.214/24, che ha respinto l'azione di risarcimento danni da loro proposta nei confronti della , fondata sull'asserita violazione da parte della banca degli obblighi gravanti, ex d.lgs.11/2010, sul prestatore dei servizi di pagamento per aver consentito in data 29 e 30 marzo 2022 l'effettuazione di n.2 operazioni di bonifico non autorizzate, che avevano, in sostanza, svuotato il loro conto corrente.

Il Tribunale, ricostruito il quadro normativo di riferimento e gli obblighi gravanti sulle parti con richiamo al d.lgs. n.11/2010, come successivamente integrato, ha ritenuto, in sintesi, dimostrata la colpa grave dell'utilizzatore del servizio di pagamento, per avere questi – vittima di una truffa ad opera di ignoti – consegnato il PIN dispositivo, consentendo l'attivazione (da parte dei terzi truffatori) del mobile token e per non essersi attivato per bloccare le operazioni dispositive (due bonifici, eseguiti in data 29.3.2022 e 30.3.2022), nonostante che avesse ricevuto i messaggi di allert, la cui ricezione doveva ritenersi dimostrata in via presuntiva.

Secondo il Tribunale l'incontestata ricezione del messaggio della banca, con il quale veniva segnalata l'attivazione del mobile token era tale da consentire al cliente di avere la piena conoscenza della truffa in atto. Inoltre, il messaggio SMS relativo all'esecuzione del primo bonifico, in data 29 marzo 2022, rendeva edotto il cliente circa il compimento di un'operazione da lui non autorizzata. Infine, difformemente da quanto

allegato dagli attori, non sussistendo un limite giornaliero di euro 250,00 per i bonifici on line (il limite era di euro 50.000,00), andava esclusa la responsabilità della banca per avere consentito operazioni oltre il limite consentito.

Gli appellanti hanno gravato la sentenza articolando plurime censure che possono essere così raggruppate.

Un primo gruppo di censure (§§ 1.1., 1.2., 2, 2.1., 3., 3.1. della citazione) investe il primo capo decisorio della sentenza.

Con queste censure – variamente rubricate – gli appellanti assumono, in sintesi:

a) che, diversamente da quanto ritenuto dal tribunale, essi avevano sin dall'atto di citazione contestato la ricezione degli SMS relativi ai bonifici e la contestazione era stata poi reiterata con la memoria ex art.183, co.6 cpc. La mancata ricezione degli ultimi due SMS era stata rappresentata anche nella denuncia querela presentata ai Carabinieri. Essi avevano, ancora, tempestivamente contestato la valenza probatoria del documento prodotto da con la comparsa di costituzione e risposta, circa l'inoltro e l'asserito ricevimento degli da parte del cliente sul proprio cellulare.

Pertanto, il giudizio probatorio inferenziale del tribunale era errato tenuto conto che:

i) la banca non aveva contestato che il suo sistema informatico risultava già vulnerato (al momento dell'invio degli SMS), poiché i malfattori si erano già introdotti in esso avendo carpito il primo codice statico (codice cliente) di che mai era stato da lui inserito nella pagina Home Banking;

ii) la banca non aveva fornito la prova positiva che il proprio sistema informatico fosse esente da qualsiasi malfunzionamento: non aveva chiesto di provare se il suo sistema di fosse funzionante e se lo stesso avesse regolarmente recapitato gli sms sul cellulare del cliente, limitandosi a produrre il documento contestato recante la registrazione degli sms di allerta asseritamente inviati, per i quali tuttavia non è stata minimamente provata l'avvenuta ricezione;

iii) che la banca convenuta, anziché chiedere, come avviene solitamente nell'istruzione probatoria di casi uguali, l'ammissione di una CTU informatica volta a verificare, al di là dell'adozione di un sistema di autenticazione forte, se il servizio di fosse funzionante e congegnato secondo le soluzioni tecnologiche migliori a disposizione degli operatori del settore, si era difesa con la contestata produzione limitandosi semplicemente ad affermare che il detto documento faceva prova fino a querela di falso, ovviamente senza motivare il perché ed in base a quale norma, visto che,

come puntualmente contestato da essi appellanti, non risulta che un atto interno della banca, neppure digitalmente firmato, abbia il valore e l'efficacia probatoria di un atto pubblico;

iv) che, a fronte della sofisticata frode informatica qualificata come "spoofing" anche da controparte, non solo la banca non aveva fornito prova alcuna circa l'efficienza e l'adeguatezza del sistema di alert, ma nemmeno era stato provato che la frode non era stata resa possibile dal mancato funzionamento del detto servizio di sicurezza, che "utilizza lo stesso canale potenzialmente compromesso dai malfattori, sul quale questi ricevono non solo le otp dispositive tramite le quali effettuano le operazioni in realtà mai autorizzate dall'ignaro correntista, ma anche i messaggi di allerta che quindi non vengono mai ricevuti e letti da quest'ultimo";

v) che, in altre parole, essi avevano allegato che il sistema adottato da era stato bypassato dall'autore della truffa in quanto esso utilizzava "presumibilmente lo stesso canale già compromesso e non un canale autonomo, così violando il requisito di indipendenza dei diversi fattori imposta dalla normativa europea (regulatory technical standards dell'European Banking Autority)"; la banca convenuta non aveva dato prova del fatto che il suo sistema di alert utilizzasse all'epoca delle operazioni di bonifico non autorizzate dai comparenti due canali autonomi;

vi) che il Tribunale aveva ritenuto che la banca avesse fornito la prova positiva della piena efficienza sotto il profilo tecnologico del servizio di pagamento dalla stessa prestato non in quanto all'esito di una CTU fosse stato accertato che gli sms asseritamente inviati erano stati effettivamente ricevuti dal cellulare di bensì sic et simpliciter, sulla scorta di un ragionamento presuntivo siffatto: siccome il cellulare del cliente funzionava, tant'è che tramite le otp il medesimo aveva autorizzato i due bonifici per cui è causa, allora era presumibile che il medesimo avesse ricevuto i messaggi di allerta;

vii) che, in questo modo decidendo, il tribunale aveva invertito l'onere della prova gravante sulla banca, presumendo che il cellulare del fosse funzionante e che, pertanto, il medesimo avesse ricevuto gli sms di allerta asseritamente inviati da sms che, ancor prima di attivare il contenzioso, già nella denucia-querela sporta ai Carabinieri di Pistoia, aveva rappresentato di non aver mai ricevuto; il Tribunale aveva finito per gravare sull'utente del servizio di pagamento "la fattispecie del rischio da ignoto tecnologico", che, invece, è a carico del prestatore dei servizi di pagamento.

Un secondo gruppo di censure investe, invece, l'altro capo decisorio, relativo al limite giornaliero alle disposizioni on line mediante bonifico.

Assumono, anzitutto, gli appellanti che a pag.18 della gravata sentenza sul punto in esame si legge "la seguente laconica affermazione": "*Anche con riferimento al limite di pagamento quello di euro 250,00 indicato da parte attrice è riferito a diverse operazioni di pagamento eseguite con il sistema P2P*".

Secondo gli appellanti siamo di fronte ad una motivazione apparente, visto che niente si dice circa l'interpretazione delle clausole contrattuali proposta da essi attori che nega, appunto, che il detto limite non sia applicabile alle due operazioni di pagamento per cui è causa.

Aggiungono che "*la banca convenuta risulta palesemente inadempiente alle obbligazioni contrattualmente assunte anche per la mancata osservanza del disposto dell'art. 3 Sez. IV – C rubricato "Trasferimento e ricezione di somme mediante smartphone" il quale recita: "In ogni caso, l'importo trasferito non può essere superiore a quello previsto dai massimali, giornalieri, mensili, per transazione, indicati nel predetto Documento di Sintesi". Il detto Documento di Sintesi relativo al contratto canali diretti evoluti per cui è causa, oltre a prevedere le voci di costo per i vari tipi di operazione, che per i contestati bonifici effettuati in favore di persona fisica, classificati con la sigla P2P, è pari ad 0,30 centesimi, prevede altresì un limite di utilizzo per singola operazione di invio denaro P2P che è pari ad euro 250,00 (cfr. doc. 5 pag. 15). Pertanto la condotta pienamente negligente di che prima non ha prontamente avvisato delle due operazioni di bonifico nessuno dei due correntisti, e poi ha eseguito i due indebiti pagamenti disattendendo per ciascuno di essi il limite di euro 250,00, è causa esclusiva del danno per la perdita complessiva subita dai propri clienti, che anziché ammontare a complessivi euro 44.974,00, in caso di esatto adempimento della banca sarebbe stata contenuta nell'importo di euro 500,00. Priva di pregio in quanto documentalmente smentita risulta l'eccezione sollevata da controparte a pagina 13 della comparsa di costituzione, circa l'asserita inoperatività del limite giornaliero di euro 250,00 per ciascuna operazione non autorizzata di pagamento allegata dai comparenti. Detto limite non è riservato al solo servizio digitale BANCOMAT Pay come dedotto da ma appunto come testualmente riportato dal documento di sintesi in atti, si estende a tutte le modalità di pagamento. Il doc. 5 a pagina 15 riporta testualmente quanto segue: "LIMITI DI UTILIZZO DEL SERVIZIO INVIO DENARO P2P E PAGAMENTI P2B/P2G BANCOMAT PAY", dove la sigla P2P sta per invio di denaro tramite bonifico a*

favore di privati, P2B per pagamenti in favore di esercenti abilitati e P2G pagamenti in favore di enti pubblici abilitati. Contrariamente a quanto ex adverso sostenuto è pertanto del tutto evidente che per il bonifico di denaro tra privati sussiste sicuramente il detto limite giornaliero, che la congiunzione "E" estende anche alle altre operazioni di pagamento con modalità BANCOMAT PAY. Quanto al massimale di euro 50.000 asseritamente operante per i bonifici effettuati da home banking, nel contratto del 26.01.2021 sottoscritto dai comparenti non vi è traccia di simile pattuizione, e comunque la stessa sarebbe inapplicabile al caso che ci occupa, poiché i non autorizzati bonifici sono stati eseguiti tramite smartphone, e risultano regolati, come detto, dalla SEZIONE IV – C del Documento di Sintesi prodotto che non prevedono il detto massimale. Anzi l'art. 3.4 rinvia espressamente ai detti limiti giornalieri poiché testualmente recita : "In ogni caso l'importo trasferito non può essere superiore a : quello previsto dai massimali giornalieri, mensili, per transazione, indicati nel predetto Documento di Sintesi nonché al saldo massimo disponibile dello strumento associato al servizio" (cfr. pag. 47 doc. 5). Pertanto anche sotto tale rilevante profilo sussiste un grave inadempimento della banca convenuta dal quale consegue la responsabilità contrattuale della stessa ed il conseguente obbligo risarcitorio.

2.- Si è costituita in giudizio parte appellata, eccependo preliminarmente l'inammissibilità dell'appello e contestando, poi, nel merito i singoli motivi, di cui ha chiesto il rigetto.

3. Acquisito il fascicolo di ufficio del procedimento di primo grado, la causa, senza attività istruttoria, è stata trattenuta in decisione in data 10.6.2026, sulle conclusioni delle parti, precisate come in epigrafe trascritte, a seguito di trattazione scritta.

Motivi della decisione

4. L'eccezione d'inammissibilità dell'appello è infondata e va respinta, i motivi d'appello, come sopra sintetizzati, permettendo di individuare i capi della decisione impugnati e le violazioni di legge denunciate.

5. Prima di esaminare le doglianze degli appellanti, pare opportuno riportare, ai fini di una migliore intellegibilità della sentenza, la ricostruzione in fatto della vicenda, come compiuta dal giudice di primo grado.

Si riporta, di seguito, testualmente la parte della sentenza del tribunale di rilievo: *"La presente causa ha per oggetto il risarcimento dei danni conseguente all'inadempimento della gestione del servizio di home banking da parte della banca convenuta. In particolare, sono contestate due operazioni di bonifico per l'importo complessivo di € 44.474. La parte attrice espone (pag. 1 dell'atto di citazione) di aver ricevuto sulla propria utenza mobile, alle ore 15:07 del giorno 29.03.2022 un sms proveniente dal numero 060060 di in coda alla cronologia di sms risalente alla data di accensione del rapporto (26 gennaio 2021), del tutto identico agli altri precedenti sms, che lo avvisava della necessità di migliorare la sicurezza web con invito a cliccare su di un link sottostante. Nella denuncia querela prodotta sub doc. 1 risulta che tale SMS fu ricevuto alle ore 14:44 (e non alle 15:07) del 29 marzo 2022). Seguendo tale invito la parte attrice entrò su una pagina web identica a quella del cd. Home Banking di BNL (dal numero 060060) nella quale, tuttavia, risultava già inserito il proprio codice cliente, e veniva chiesto l'inserimento del codice PIN. Dalla denuncia querela prodotta sub doc. 1 di parte attrice risulta che per ben due volte l'attore provò a inserire il PIN, ma veniva segnalato che il codice inserito era errato e, infine, pervenne un messaggio con il quale il sig. veniva avvisato che sarebbe stato contattato dal personale della banca. La parte attrice fu, infatti, chiamata da un sedicente operatore di alle ore 15:07 del giorno 29 marzo 2022. Tale operatore invitava il sig. a fare un'attivazione guidata del sistema di sicurezza, inviando due link sui quale l'attore avrebbe dovuto cliccare. Seguite le istruzioni del sedicente operatore l'installazione andò a buon fine e fu comunicato all'attore che sarebbe stato ricontattato il giorno dopo. Dalla lista delle operazioni della banca (doc. 3) e dai messaggi prodotti sempre dalla parte convenuta (doc. 2) risultano, nella giornata del 29 marzo 2022, i seguenti accadimenti, secondo la sequenza cronologica temporale di seguito riportata: - alle ore 15:21:39 fu eseguito a nome del sig. il log-in mediante inserimento di PIN con verifica a 2 fattori, utilizzando l'OTP (029***36) generato dal mobile token; - alle ore 15:26:45, risultano correttamente trasmessi dalla e consegnati al cliente un sms e una notifica push del seguente tenore: "Stai attivando il Mobile Token. Ricordati che il personale non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ********." - alle ore 15:27:01 è stato attivato il mobile token mediante inserimento di PIN e utilizzando l'OTP (234***58) ricevuto via sms, con verifica a 2 fattori, utilizzando l'OTP (310***89) generato dal mobile token; - alle ore 15:29:45 è stato inserito il bonifico di importo pari ad € 24.986,00 verso il beneficiario*

*con IBAN IT78Z3608105138212976912986 e causale "pagamento per ditta edile", firmato con Strong Customer Authentication, in particolare con PIN e OTP (924***02) generato da mobile token; - alle ore 15:29:46, risultano correttamente trasmessi dalla e consegnati al cliente un sms e una notifica push del seguente tenore: "E' stato inserito un ordine di Bonifico dal c/c 21501***025, importo 24986,00 Euro, in data 29/03/2022, da Mobile BNL. Info: 060060.". Ricostruendo gli accadimenti della giornata del 29 marzo 2022 risulta, quindi, che tramite un SMS proveniente da un soggetto diverso dalla banca la parte attrice abbia installato non un sistema di sicurezza, ma abbia piuttosto determinato l'installazione (ad opera di terzi) di un Mobile Token, come risulta dalla messaggistica trasmessa dalla banca (sulla quale, v. infra). Per fare ciò è stato necessario l'inserimento non solo del codice utente e della password, ma anche della cd. one time password, generata al momento del compimento dell'operazione. È pertanto verosimile ritenere, dai documenti in atti, che grazie all'attivazione del Mobile Token sia stata resa possibile l'esecuzione del primo bonifico. Il sig. fu, poi, ricontattato alle ore 12.58 del 30.03.2022 dallo stesso interlocutore, tramite il medesimo numero Anche in tale occasione il sedicente operatore chiese di cliccare sui link trasmessi con le stesse modalità del giorno avanti e riferì alla parte attrice che però il tentativo non era andato a buon fine e che sarebbe stato ricontattato. Dalla lista delle operazioni (doc. 3) e dai messaggi prodotti dalla banca (doc. 2) in data 30 marzo 2022 risultano le seguenti operazioni sul conto corrente intestato agli odierni attori: - alle ore 12:56:56 fu eseguito il log-in mediante inserimento di PIN con verifica a 2 fattori, utilizzando l'OTP (627***91) generato dal mobile token; alle ore 13:01:51 fu inserito il bonifico di importo pari ad € 19.988,00 il beneficiario con IBAN IT78Z3608105138212976912986 e causale "saldo pagamento ditta edile", firmato con Strong Customer Authentication, in particolare con PIN e OTP (405***27) generato da mobile token. - alle ore 13:01:52, risultano correttamente trasmessi dalla e consegnati al cliente un sms e una notifica push del seguente tenore: "E' stato inserito un ordine di Bonifico dal c/c 21501***025, importo 19988,00 Euro, in data 30/03/2022, da Mobile BNL. Info: 060060." Anche in tale occasione l'esecuzione del secondo bonifico fu resa possibile grazie alla cd. one time password generata dal mobile token".*

6. Ciò premesso, le censure riconducibili al primo motivo d'appello sono infondate e vanno respinte.

Le questioni si riducono, nella concreta vicenda, a questo, e cioè se la condotta del come ricostruita in primo grado, e non oggetto di specifica censura, sia connotata da colpa grave ai fini del combinato disposto degli art.7 e 10 del d.lgs. 11/2010, come novellato dal d.lgs. 218/17, entrato in vigore in data 13.1.2018.

Ai sensi dell'art.7, che disciplina gli obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate, l'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di:

a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati;

b) comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza.

Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.

L'art.10, che disciplina la prova di autenticazione ed esecuzione delle operazioni di pagamento, prevede invece che:

1. qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

1-bis. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, questi ha l'onere di provare che, nell'ambito delle proprie competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato.

2. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di di-

sposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente.

Pertanto, in base al combinato disposto di tali disposizioni:

- l'utente è tenuto ad una serie di obblighi, tra cui quello di adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate;

- il solo utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7;

- la banca è onerata della prova del dolo o della colpa grave dell'utente.

Tali disposizioni, come rilevato dagli appellanti, invertendo l'onere della prova, pongono a carico del prestatore di servizi anche il c.d. rischio da ignoto tecnologico.

Tuttavia, il generico richiamo al rischio dell'ignoto tecnologico non è conferente nella concreta fattispecie, nella quale, per stessa ammissione del contenuta già nella denuncia-querela, viene in rilievo una sua condotta gravemente negligente consistita nel consegnare i pin dispositivi della Home banking e le OTP generate dal sistema di autenticazione a terzi truffatori e, in questo modo, nel consentire l'attivazione di un mobile token, con il quale poi, assieme ai codici dispositivi, i truffatori hanno eseguito i due bonifici oggetto di causa.

In simile fattispecie di ignoto non c'è nulla se non il nome dei truffatori: l'utilizzo dello strumento di pagamento, da parte di terzi, è stato possibile soltanto a causa della condotta colposa del che ha consegnato a terzi, ancorché qualificatisi come operatori di i PIN dispositivi e le OTP, in violazione di minimali norme di prudenza e di specifici obblighi di legge (art.7 d.lgs.11/2010) e di contratto (le condizioni generali di contratto prevedendo, tanto con riferimento ai PIN della carta di debito, quanto ai PIN e agli strumenti di sicurezza (per generare l'OTP) previsti per i canali diretti e diretti evoluti (smartphone), che essi siano strettamente personali e che non possano essere comunicati a terzi), e ciò nonostante le informazioni fornire dagli istituti bancari e dalla stessa (v. documento n.1 prodotto in primo grado), che raccomandano la

massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nella pagina di accesso al portale, sulle proprie app e sugli schermi degli ATM, dando specifico avviso alla clientela che le credenziali di sicurezza sono strettamente personali e non saranno mai richieste da alcun dipendente della Banca.

Su tale condotta di per sé gravemente negligente si è innestato l'ulteriore condotta del consistita nel non allertare la banca una volta ricevuto l'SMS, con cui veniva informato dell'attivazione del nuovo dispositivo (mobile token). Questo il testo dell'SMS: "*Stai attivando il Mobile Token. Ricordati che il personale non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ********".*

La ricezione di questo messaggio non è stata contestata ed è stata anzi implicitamente ammessa nella integrazione della denuncia-querela in atti, in cui il fa riferimento alla mancata ricezione soltanto dei due SMS relativi ai bonifici (v. integrazione querela del 31.5.2022).

Questo messaggio, se mai il avesse potuto avere un qualche dubbio, rendeva evidente che i codici riservati non sono richiesti dai funzionari bancari e non sono comunicabili a nessuno. Giusta, pertanto, la valutazione compiuta dal giudice di primo grado, secondo cui tale messaggio rendeva al chiaro che egli era stato vittima di una truffa, sicché avrebbe dovuto immediatamente segnalare la circostanza alla banca e revocare/bloccare ogni ordine dispositivo che fosse stato nel frattempo dato.

Questi elementi provano la colpa grave dell'utente, rilevante ai fini dell'art.10 del d.lgs. 11/2010, e la sua correlazione causale con gli ordini dispositivi. Nesso causale che, a questo punto, avrebbe potuto far apprezzare un concorso della banca soltanto nel caso in cui questa, in violazione degli obblighi assunti con il servizio "allert", obbligatorio per il cliente in caso di Home banking, non avesse dimostrato di avere avvertito il cliente degli ordini dispositivi, mettendolo, quindi, in condizione, di nuovo, di comprendere la truffa di cui era rimasto vittima.

Sul punto va tuttavia, ancora una volta, condiviso il giudizio probatorio svolto dal giudice di prima istanza, secondo cui può presumersi, ex art.2729 c.c., che tali messaggi siano stati effettivamente ricevuti dal cliente.

L'inferenza probatoria è stata argomentata dal tribunale sulla base di questi fatti:

a) non risulta allegata alcuna disfunzione nel funzionamento della linea telefonica intestata a parte attrice, come dimostrato dal fatto che, sia dall'esposizione dell'atto

di citazione che dalla denuncia querela sub doc. 1 di parte attrice, i contatti con il sedicente operatore della banca sono stati tenuti in via telefonica nei giorni e nelle ore in cui sono state eseguite le operazioni di bonifico non autorizzate;

b) parte attrice ha dichiarato di aver cliccato sul link inviato tramite SMS, circostanza che dimostra sia il funzionamento della linea telefonica che la connessione attraverso internet;

c) l'attivazione del Mobile Token, di cui al messaggio del 29 marzo 2022 (sopra riportato, e la cui ricezione non è contestata), ha richiesto l'inserimento della OTP (one time password) necessariamente generata al momento della richiesta dell'operazione, in possesso del solo utente ed evidentemente da questi comunicata per telefono al truffatore.

In base a questi elementi, il giudice di prima istanza, ha ritenuto "*non è comprensibile come il cliente abbia potuto ricevere l'OTP che ha consentito l'attivazione del mobile token (circostanza provata non solo dal messaggio trasmesso, ma anche dell'effettiva attivazione di quest'ultimo) e non abbia, invece, ricevuto gli altri messaggi (relativi ai bonifici, n.d.r.). Tale credenziale poteva essere in possesso solamente della parte attrice ed è ragionevole ritenere – alla luce del quadro fattuale ricostruito supra - che la stessa sia stata o comunicata al sedicente operatore o inserita nei link apocrifi inviati da questo*".

A questi elementi indiziari possono aggiungersi i seguenti:

- l'utente non ha contestato di aver ricevuto, prima o dopo i fatti di causa, SMS relativi alle operazioni compiute;

- dai documenti interni prodotti dalla banca risulta che l'SMS, tanto quello che ha consentito l'attivazione del Mobile Token (la cui ricezione non è contestata), quanto dei successivi (relativi ai bonifici), sono stati spediti proprio all'utenza cellulare del (cell.3464945306, come indicata nella denuncia-querela);

- nella denuncia querela del 1.4.2022 non vi è alcun accenno alla mancata ricezione degli SMS di cui sopra, che compare invece nella denuncia integrativa depositata in data 31.5.2022;

- nella denuncia querela del 1.4.2022 il riferisce, fra l'altro, di avere disattivato l'APP della home banking su richiesta del terzo truffatore che egli aveva ritenuto essere un operatore di così testualmente mediante riproduzione screenshot della parte di interesse:

a cliccare. Io quindi convinto dal fatto che l'uomo stesse chiamando da un canale ufficiale BNL (del quale ribadisco già in passato avevo utilizzato con esito positivo) e che l'uomo mi avesse edotto in modo esaustivo sulle motivazioni delle azioni che stavo andando a compiere, sempre restando in linea con lo stesso, così facevo ma dopo i fari click la fantomatica installazione non andava a buon fine e l'interlocutore allora asseriva che ci saremmo dovuti risentire il giorno seguente. Preciso che durante il colloquio guidato, il fantomatico operatore BNL mi invitava a disinstallare l'App dell'home banking della BNL appunto installata sul mio smartphone (esortandomi ad eseguire tale operazione anche su quello di mia moglie) e così facevo.

- il avrebbe potuto produrre (in applicazione del principio di vicinanza della prova) quantomeno lo screenshot della messaggistica ricevuta dalla banca per dimostrare di non avere ricevuto i due SMS relativi ai bonifici.

Né era necessario, in presenza di tali elementi indiziari, come invece assumono gli appellanti, che parte appellata chiedesse l'ammissione di una CTU per dimostrare che il proprio sistema di allert funzionasse correttamente e non fosse in qualche modo "corrotto" dai truffatori.

Deve pertanto conclusivamente condividersi il giudizio del tribunale, secondo cui "*il regime di responsabilità semi-oggettiva delineato dal combinato disposto degli artt. 7, 10, 10-bis d.lgs. n. 10 del 2011 in capo al prestatore di servizi bancari in via telematica comporta un parziale ribaltamento del rischio in capo a quest'ultimo, che trova il proprio limite nella colpa grave del cliente. Quest'ultima deve essere parametrata anche al carattere tecnologicamente sofisticato della condotta truffaldina posta in essere da terzi, tanto più se attuata con modalità informatiche. Nel caso di specie, tuttavia, la banca ha trasmesso ben tre messaggi – la cui lettura non implicava una prestazione di diligenza inesigibile da parte di chi usa un telefono cellulare sul quale sia attivata anche la connessione internet – da cui la parte attrice avrebbe ben potuto rendersi conto che il sedicente operatore della banca, con il quale ha interloquito per due giorni era, in realtà, un truffatore. La perpetrazione della truffa in danno della parte attrice è avvenuta attraverso una cooperazione di quest'ultima qualificabile in termini di colpa grave, essendo state comunicate a terzi le chiavi necessarie a perfezionare le operazioni dispositive delle somme presenti sul conto corrente, nonostante gli avvisi contestualmente inviati dalla banca. La semplice lettura di questi ultimi avrebbe, infatti, consentito al cliente di avvisare immediatamente la banca, ai sensi di quanto previsto nell'art. 7, comma 1, lett. b) d.lgs. n. 10 del 2011, in ordine all'appropriazione indebita e all'uso non autorizzato delle proprie credenziali e dei codici generati per le singole operazioni*".

Le conclusioni del giudice di primo grado non sono infine inficiate:

a) dal fatto che il conto corrente fosse cointestato e gli SMS sono stati spediti soltanto al e non alla corretta e condivisibile essendo sul punto la difesa della banca, secondo cui "anche in presenza di un conto cointestato, ciascun contitolare conserva la propria autonomia, disponendo non solo di proprie personali credenziali di autenticazione riservate, ma anche di un proprio numero certificato associato ai propri strumenti di sicurezza, utilizzato esclusivamente per gli sms e le notifiche push relative alle operazioni eseguite e disposte per mezzo di dette credenziali". Pertanto, non vi era ragione di informare la per operazioni dispositive compiute dall'altro cointestatario.

b) dal riferimento contenuto negli scritti conclusionali alla mancata attivazione da parte della banca, in violazione dei doveri gravanti sull'accorto banchiere, di un sistema di controllo e di segnalazione/blocco delle operazioni anomale o sospette per importo rispetto alla normale operatività del conto, sistema aggiuntivo rispetto a quello di adottato dalla banca.

La deduzione, oltre che tardiva in fatto, è anche inconferente in diritto, come dimostrato dal richiamo al D.M. 30 aprile 2007, n. 112, Regolamento di attuazione della L. 17 agosto 2005, n. 166, che ha istituito un sistema di prevenzione delle frodi sulle carte di pagamento. Questo articolato normativo è relativo unicamente alle operazioni dispositive eseguite tramite carte di pagamento/credito e non tramite conto corrente online come quelle per cui è causa. Peraltro, il contratto in atti, in relazione alle operazioni compiute con le carte di pagamento e con l'equivalente forma evoluta (smartphone abilitato a funzioni di pagamento) contiene disposizioni in linea con il DM 112/07. Ma, come detto, queste disposizioni riguardano diverso servizio di pagamento e non quello che viene in rilievo nel caso di specie (bonifici eseguiti tramite il canale home banking).

7. Anche il secondo motivo d'appello è infondato.

La sentenza non incorre nel vizio di motivazione apparente, in quanto sia pure sinteticamente spiega la ragione del rigetto dell'azione di danni fondata sul diverso assunto che la banca avesse eseguito bonifici oltre il limite giornaliero di euro 250,00, e non è errata nel merito.

Al riguardo, ad integrazione della decisione di primo grado, può osservarsi che il limite di euro 250,00 al giorno opera soltanto per i pagamenti eseguiti mediante i "canali diretti evoluti". Di seguito lo screenshot del documento di sintesi con la parte di rilievo ai fini de quibus.

DOCUMENTO DI SINTESI
DEL CONTRATTO CANALI DIRETTI EVOLUTI

Intestato a
Documento di Sintesi n. 0 del 26.01.2021

Il servizio Canali Diretti Evoluti regolamenta il servizio di canalità diretta, il servizio di pagamenti in mobilità e i servizi di Account Aggegator/Personal Finance Management (PFM):

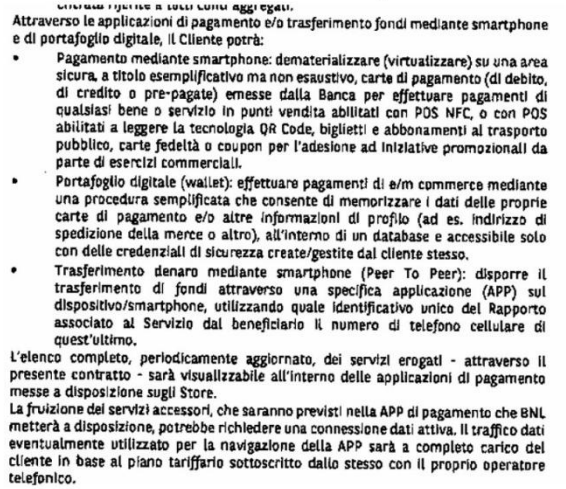
- il servizio di canalità diretta consente al Cliente di effettuare operazioni informative, dispositive e di acquisto sui canali diretti internet, Mobile e Telefonico, nonché a sportello o tramite gli sportelli automatici BNL ovvero attraverso gli altri servizi che potranno essere resi disponibili anche in futuro;
- il servizio di pagamento in mobilità (c.d. Mobile Payment) mette a disposizione del Cliente, tramite l'app dedicata, nuove ed innovative modalità di pagamento e controllo delle proprie carte di credito;
- il servizio di Account Aggregator e il servizio di Personal Finance Management (PFM) consentono, rispettivamente, di aggregare le informazioni relative ad uno o più conti correnti di cui il Cliente è titolare presso una o più banche per una gestione accentrata degli stessi, e di operare approfondimenti personalizzati per controllare la propria vita finanziaria, categorizzando le voci di spesa e di entrata riferite a tutti conti aggregati.

0,00 €

LIMITI DI UTILIZZO DEL SERVIZIO INVIO DENARO P2P E PAGAMENTI P2B/P2G BANCOMAT PAY®	
Importo massimo per singola operazione di invio Denaro P2P	250,00 €
Importo massimo giornaliero	250,00 €
Importo massimo cumulato mensile	1.500,00 €
Numero massimo di operazioni mensili effettuabili in invio	100
Numero massimo di operazioni mensili ricevibili	100
Importo massimo per singola operazione di pagamento P2B/P2G	2.000,00 €
Importo massimo cumulato mensile per operazioni di pagamento P2B/P2G	2.000,00 €

VALUTE E DISPONIBILITA' DEL SERVIZIO BANCOMAT PAY

Come risulta dalle condizioni di contratto relative ai predetti "canali evoluti", essi consentono servizi di pagamento equivalenti (ma più evoluti rispetto) a quelli che un tempo si facevano soltanto mediante carta di debito. Di seguito si riporta mediante screenshot una parte del testo delle condizioni generali di contratto:



[illegible] aggregati.

Attraverso le applicazioni di pagamento e/o trasferimento fondi mediante smartphone e di portafoglio digitale, il Cliente potrà:

- Pagamento mediante smartphone: dematerializzare (virtualizzare) su una area sicura, a titolo esemplificativo ma non esaustivo, carte di pagamento (di debito, di credito o pre-pagate) emesse dalla Banca per effettuare pagamenti di qualsiasi bene o servizio in punti vendita abilitati con POS NFC, o con POS abilitati a leggere la tecnologia QR Code, biglietti e abbonamenti al trasporto pubblico, carte fedeltà o coupon per l'adesione ad iniziative promozionali da parte di esercizi commerciali.
- Portafoglio digitale (wallet): effettuare pagamenti di e/m commerce mediante una procedura semplificata che consente di memorizzare i dati delle proprie carte di pagamento e/o altre informazioni di profilo (ad es. indirizzo di spedizione della merce o altro), all'interno di un database e accessibile solo con delle credenziali di sicurezza create/gestite dal cliente stesso.
- Trasferimento denaro mediante smartphone (Peer To Peer): disporre il trasferimento di fondi attraverso una specifica applicazione (APP) sul dispositivo/smartphone, utilizzando quale identificativo unico del Rapporto associato al Servizio dal beneficiario il numero di telefono cellulare di quest'ultimo.

L'elenco completo, periodicamente aggiornato, dei servizi erogati - attraverso il presente contratto - sarà visualizzabile all'interno delle applicazioni di pagamento messe a disposizione sugli Store.
La fruizione dei servizi accessori, che saranno previsti nella APP di pagamento che BNL metterà a disposizione, potrebbe richiedere una connessione dati attiva. Il traffico dati eventualmente utilizzato per la navigazione della APP sarà a completo carico del cliente in base al piano tariffario sottoscritto dallo stesso con il proprio operatore telefonico.

Sempre nelle condizioni generali è precisato quanto segue:

BANCOMAT Pay®: Sistema di pagamento al dettaglio gestito da Bancomat S.p.A., che consente di effettuare le operazioni tra privat (P2P) e verso esercenti con POS abilitati a BANCOMAT Pay® (P2B) con altri soggetti titolari del Servizio Mobile Payment ovvero titolari di analoghi servizi forniti da altri prestatori di servizi di incasso o pagamento, operanti sempre sul detto Circuito BANCOMAT Pay®.
PARTI: indistintamente. Il Cliente e la Banca.

E' chiaro quindi che il documento di sintesi richiamato dagli appellanti si correla a tali diversi servizi di pagamento evoluti, effettuati mediante smartphone, equivalenti, in parte, a quelli che si fanno mediante carta di debito.

Nel caso di specie, invece, vengono in rilievo bonifici effettuati mediante home banking: il cliente accede tramite sito web al proprio conto corrente e dà direttamente disposizioni alla banca con modalità on line. In tal caso, vengono in rilievo le condizioni generali di contratto relative al rapporto di conto corrente e il relativo documento di sintesi, dai quali non è dato desumere un limite giornaliero diverso da quello indicato dalla banca nel proprio documento n.6 (ovvero euro 50.000,00).

In conclusione, l'appello va integralmente respinto, con conferma della sentenza impugnata anche in ordine alle spese.

Le ulteriori spese del giudizio di appello seguono la soccombenza e si liquidano, in difetto di notula, tenuto conto del valore e della complessità della lite, in € 6.946,00, oltre 15% spese generali, IVA e CPA come per legge (DM 55/14 e ss. mod.; causa di valore compreso tra euro 26.001,00 ed euro 52.000,00; parametri medi per le fasi 1, 2, 4, nulla per la fase 3 non effittavamente tenutasi).

L'istanza ex art.96 cpc formulata dalla banca è infondata e va respinta, non potendosi sostenere che gli appellanti abbiano agito nel giudizio d'appello con dolo o colpa grave.

Deve darsi atto dei presupposti per il raddoppio a carico dell'appellante del contributo unificato ex art. 13 DPR n. 115/2002, come modificato dall'art. 17 legge n. 228/2012.

P.Q.M.

La Corte di Appello di Firenze, definitivamente pronunciando, così provvede:

- rigetta l'appello e, per l'effetto, conferma la sentenza impugnata;
- respinge l'istanza ex art.96 cpc formulata da parte appellata;
- condanna parte appellante a rimborsare all'appellata le spese di lite che liquida in complessivi euro € 6.946,00, oltre 15% spese generali, IVA e CPA come per legge.

Dà atto che sussistono a carico degli appellanti i presupposti per il raddoppio del contributo unificato.

Così deciso nella camera di consiglio del 16-6-2026.

Il Consigliere relatore – estensore

Carmine Capozzi

Il Presidente

Anna Primavera

Nota

La divulgazione del presente provvedimento, al di fuori dell'ambito strettamente processuale, è condizionata all'eliminazione di tutti i dati personali in esso contenuti ai sensi dell'art. 52 D. Lgs 30 giugno 2003 n. 196 e successive modificazioni e integrazioni.