REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

IL TRIBUNALE DI LANCIANO

in composizione monocratica, nella persona del giudice Giovanni Nappi, all'esito dell'udienza sostituita dal deposito di note scritte *ex* art. 127-*ter* c.p.c. del 16 gennaio 2024, ha pronunciato ai sensi dell'art. 281-*sexies* c.p.c. la seguente

SENTENZA

nella causa civile iscritta al n. [redacted] R.G. e vertente

TRA

Parte_1 (*C.F._1* , *Parte_2* *[...]* (*C.F._2* , elettivamente domiciliati in [redacted], presso lo studio dell'avv. [redacted], che li rappresenta e difende, anche disgiuntamente, con l'avv. [redacted], come da mandato in calce all'atto di citazione;

ATTORI

E

Controparte_1 *P.IVA_1* , in persona del procuratore speciale *CP_2* *[...]* (notaio *Per* in [redacted]), rappresentata e difesa dall'avv. [redacted], come da mandato in atti;

CONVENUTO

E

CP_3 (*P.IVA_2* , in persona del direttore generale *CP_4* rappresentata e difesa dall'avv. [redacted], come da mandato in atti;

TERZO CHIAMATO IN CAUSA

avente a oggetto: contratti bancari

conclusioni delle parti: come da note d'udienza

Fatto e diritto

1. *Parte_1* e *Parte_2* hanno convenuto in giudizio *Controparte_1* (d'ora in avanti, *CP_1*) domandandone la condanna al pagamento della somma di euro [redacted], "oltre rivalutazione monetaria[e] interessi legali", oggetto di "illecita sottrazione di fondi" "dal loro conto corrente *CP_1* " "subita il 20.04.2021", allorché a mezzo di due carte di pagamento (carta di credito e carta prepagata) sono state eseguite operazioni di pagamento *on-line* non autorizzate a valere sul predetto conto corrente, per l'importo totale indicato; e al risarcimento del "danno non patrimoniale" conseguente al medesimo fatto, "quantificato in € 1.500,00 per ciascun attore".

CP_1 si è costituita deducendo che entrambe le carte, "pur collocate da *CP_1* [...], venivano emesse da *CP_3* (d'ora in avanti, *CP_3* ; chiamando pertanto in causa quale vera obbligata *CP_3* in ogni caso, chiedendo il rigetto delle domande, anche in subordine nel *quantum* per "concorso di colpa degli attori", per avere *CP_1* "introdotto, nel pieno rispetto delle normative europee, dei

rigidi sistemi di sicurezza in forza dei quali l'autenticazione al conto online richiede l'utilizzo di codici che solo l'utente è in grado di conoscere ed inserire".

CP_3 si è costituita chiedendo, "in adesione alle richieste di *CP_1* ", di "rigettare integralmente la domanda principale articolata [...] nei confronti di *CP_1* " e, in subordine, deducendo il concorso di colpa degli attori.

Il Tribunale ha concesso i termini *ex* art. 183, c. 6, c.p.c.; all'esito, ha fissato udienza di precisazione delle conclusioni, discussione e decisione *ex* art. 281-*sexies* c.p.c.

2. Le domande sono fondate nei limiti e nei sensi di cui a seguire.

2.1. Ai sensi degli artt. 7, 8, 10, 10-*bis*, 11 e 12 del d.lgs. 11/2010, nel testo risultante dalle modifiche del 2017, "L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di[...] 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" e, "non appena riceve uno strumento di pagamento, *adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate*" (art. 7); "Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di[...] assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7" (art. 8); "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. [...] 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. [...] 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 disposizione 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*" (art. 10); "Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'*autenticazione forte* del cliente quando l'utente: [...] a) accede al suo conto di pagamento on-line; [...] b) dispone un'operazione di pagamento elettronico; [...] effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi" (art. 10-*bis*); "nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata, il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in

cui prende atto dell'operazione o riceve una comunicazione in merito. *Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo*, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo. [...] Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, *il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo. In caso di operazione di pagamento non autorizzata, se il relativo ordine di pagamento è disposto mediante un prestatore di servizi di disposizione di ordine di pagamento, quest'ultimo è tenuto a rimborsare immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, senza che sia necessaria la costituzione in mora, al prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo, gli importi rimborsati al pagatore*. Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente e, in ogni caso, entro la fine della giornata operativa successiva senza che sia necessaria la costituzione in mora il prestatore di servizi di pagamento di radicamento del conto, su richiesta di quest'ultimo, anche per le perdite subite. In entrambi i casi è fatta salva la facoltà del prestatore di servizi di disposizione di ordine di pagamento di dimostrare, in conformità a quanto disposto dall'articolo 10, comma 1-*bis*, che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato, con conseguente diritto in questi casi alla

restituzione delle somme da quest'ultimo versate al prestatore di servizi di pagamento di radicamento del conto ai sensi del presente comma" (art. 11); "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'*autenticazione forte* del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente. [S]alvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita. [c. 3] Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3" (art. 12).

Ai sensi dell'art. 1, c. 1, lett. b-*bis*, del d.lgs. 11/2010, *servizio di disposizione di ordine di pagamento* è "un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento".

La disciplina di cui sopra è ricostruibile nei sensi di cui a seguire.

Innanzitutto, le obbligazioni del prestatore di servizi di pagamento si conformano nell'oggetto (prestazione) a un modello di diligenza qualificata professionale o *perizia*, nel caso di specie la perizia dell'"accorto banchiere" (C. 20543/2009; con

riferimento a carta bancomat, C. 806/2016; con riferimento a *home banking*, C. 2950/2017); le obbligazioni dell'utilizzatore ("utente") si conformano a un modello di diligenza media, come diligenza del buon padre di famiglia (art. 1176, c. 1, c.c.).

In secondo luogo, ove non venga dimostrata l'autorizzazione dell'operazione di pagamento (e "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente"), l'operazione stessa, contestata (ai sensi dell'art. 9 del d.lgs. 11/2010), è da considerare non autorizzata.

In tal caso, la normativa disciplina la responsabilità (contrattuale) e i conseguenti obblighi risarcitori (aventi a contenuto principalmente la somma pagata senza autorizzazione) derivanti dall'inadempimento delle parti alle obbligazioni discendenti dal "contratto quadro" di prestazione di servizi di pagamento; e inoltre prevede una ripartizione della perdita economica nel caso in cui l'operazione non autorizzata non discenda da un inadempimento imputabile a una delle parti, e rientri pertanto nei *rischi* connessi all'attività di prestazione di servizi di pagamento (rischio è l'evento non imputabile ad alcuna delle parti).

In caso di utilizzo *fraudolento*, da parte del pagatore, dello strumento di pagamento, questi non ha alcun diritto, ed è irrilevante l'eventuale concorrente inadempimento del prestatore di servizi di pagamento alle obbligazioni e agli obblighi derivanti a suo carico dal contratto quadro e dalla normativa che lo integra.

In caso di inadempimento, *anche per colpa lieve*, del prestatore di servizi di pagamento alle sue obbligazioni (come detto, conformate alla diligenza dell'accorto banchiere), l'utente/pagatore ha diritto all'integrale rimborso dell'importo dell'operazione di pagamento non autorizzata; può ipotizzarsi un suo concorso di colpa, ai sensi dell'art. 1227, c. 1, c.c.; e, in tal caso, si avrà una riduzione del *quantum* del rimborso dovuto dall'intermediario, secondo la gravità della colpa dell'utente e l'entità delle conseguenze che ne sono derivate. Il concorso colposo dell'utente, però, dovrebbe rilevare, ai fini della riduzione del *quantum* del rimborso, solo se la sua colpa può essere qualificata come colpa grave; nei casi di concorso per colpa lieve, la riduzione o è da escludersi, oppure può aversi solo entro il limite di 50 euro, che è il limite di rilevanza posto dalla normativa sopra richiamata alla colpa lieve dell'utente.

Trattandosi di responsabilità contrattuale, la colpa del debitore prestatore di servizi di pagamento è normalmente presunta nell'inadempimento; e sarà quindi il prestatore di servizi di pagamento a dover provare la non imputabilità del suo inadempimento (art. 1218 c.c.); inoltre, l'art. 10, c. 1, d.lgs. 11/2010, lì dove prevede che "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita [...], è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che *non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*", pone a carico del prestatore di servizi di pagamento, a monte, la *prova dell'esatto adempimento delle sue obbligazioni*, ossia pone una presunzione semplice di suo inadempimento; il che, a ben vedere, si allinea alle conclusioni cui è pervenuta la giurisprudenza in tema di prova dell'inadempimento, soprattutto con riferimento a obbligazioni il cui con-

tenuto deve conformarsi ai modelli della perizia professionale, per cui il creditore (qui utente) che pone a fondamento delle sue domande (a esempio risolutorie, restitutorie, risarcitorie) o eccezioni l'inadempimento, anche corrispettivo, del debitore (qui prestatore di servizi di pagamento), deve provare il titolo contrattuale del proprio diritto, ma può limitarsi ad allegare *specificamente* l'inadempimento del debitore, *essendo a carico di questo la prova dell'(esatto) adempimento*.

In caso di inadempimento, da parte dell'utente, per colpa grave o per dolo, delle sue obbligazioni, non vi è alcun diritto al rimborso. Ma l'onere della prova della condotta gravemente colposa dell'utente è a carico del prestatore di servizi di pagamento (art. 10, c. 2, d.lgs. 11/2010); tale prova può però darsi anche "in via presuntiva" (ABF Collegio di coordinamento, 22745/2019).

In caso di inadempimento, da parte dell'utente, per colpa lieve, delle sue obbligazioni; o nel caso in cui non vi sia alcun inadempimento imputabile ad alcuna delle parti (rischio), l'utente ha diritto al rimborso (solo) delle somme superiori a 50 euro. Secondo le regole generali, la colpa (lieve) dell'utente è presunta (*iuris tantum*) nell'inadempimento dei suoi obblighi conformati alla diligenza media.

Su controversie del tipo di quella oggetto del presente giudizio vi sono numerose pronunce dell'ABF. Le più recenti ricostruiscono in dettaglio la disciplina nei sensi di cui a seguire.

Il quadro normativo di riferimento è dato dalla "direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015[...] (c.d. *PSD 2 - Payment Services Directive 2*), recepita con il d.lgs. n. 218[/]2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010[; e dal] Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede [...] che 'le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366'. In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'*autenticazione forte* del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. [...] Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019" (ABF Roma, 11261/2023).

"L'art. 12 del d. lgs. n. 11/2010 regola il regime della responsabilità a fronte dell'utilizzo non autorizzato di strumenti e servizi di pagamento. La disposizione, con un evidente *favor* nei confronti dell'utilizzatore, opera *uno spostamento della responsabilità in capo al prestatore dei servizi di pagamento* in caso di utilizzo fraudolento, estendendola a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non [qualificate] da frode, dolo o colpa grave. [L]'art. 7, comma 3 del d.lgs. n. 11/2010 [prevede che] l'utente 'adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate'. [...] Ai sensi del 2° comma dell'art. 10 del d. lgs. n. 11/2010, l'onere della prova che l'utilizzatore abbia agito

con dolo o colpa grave incombe sull'intermediario, il quale, ai sensi del primo comma della norma, nel caso di un'operazione di pagamento disconosciuta è tenuto a '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'. [...] Deve ancora richiamarsi l'art. 10 bis, comma 1, del d. lgs. n. 11/2010, il quale, recependo l'art. 98 della direttiva UE 2015/2399, sancisce l'obbligo per i prestatori di servizi di pagamento di applicare 'l'autenticazione forte del cliente' nei casi in cui questi acceda al proprio conto di pagamento on line, effettui un'operazione o 'qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi'".

In virtù di quanto sopra, la "prova della corretta autenticazione a doppio fattore da parte della banca, come necessario ai sensi de[gli] art. 10, comma 1 ed art. 10bis, comma 1[,] del d. lgs. n. 11/2010[,] *non è di per sé sufficiente* per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento [dovendosi] valutare la sussistenza o meno della colpa grave del[...] titolare dello strumento" (ABF Bologna, 4868/2024); al contrario, "la mancata prova, da parte dell'intermediario, dell'autenticazione forte è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al[l'utente, sicché] l'operazione di pagamento disconosciuta [...] dovrà essere rimborsata per intero dall'intermediario" (ABF Milano, 9152/2024).

Peraltro, i "Collegi ABF hanno [...] escluso l'applicazione del regime di protezione previsto dal d.lgs. n. 11 del 2010 e, di conseguenza, ritenuto irrilevante l'eventuale prova fornita dall'intermediario in ordine all'autenticazione, nel caso di operazioni disposte ed autorizzate personalmente dal titolare dello strumento

di pagamento, sebbene sulla base di un consenso viziato dagli artifizi e raggiri posti in essere da un truffatore anche per mezzo di sms o chiamate 'civetta' apparentemente provenienti dall'intermediario[, ma] l'inapplicabilità alle fattispecie di *social hacking* degli artt. 10 e ss. del d.lgs. n. 11 del 2010 in materia di operazioni non autorizzate non vale ad escludere in modo automatico ogni responsabilità dell'intermediario, la cui condotta deve essere valutata alla luce degli obblighi di protezione previsti dal d.lgs. n. 11 del 2010 e tenuto conto delle regole generali del codice civile in materia di obbligazioni" (ABF Bologna, *P.IVA_3* .

"I Collegi di quest'Arbitro sono ormai da tempo orientati nel senso di ritenere il *phishing* un tipo di truffa molto nota e, quindi – data, appunto, la sua notorietà – evitabile utilizzando una diligenza minima ed elementare generalmente osservata da tutti. Questo salvo che la stessa truffa [...] sia consistita in un'intrusione talmente insidiosa da rendere la medesima particolarmente sofisticata. [Ne discende una] presunzione di colpa grave [dell'utente], soprattutto nel caso in cui l'intermediario provi la regolare e corretta autenticazione delle operazioni disconosciute prive[...] di indici di anomalia (come gli indici di rischio frode di cui all'art. 8 del DM 112/07)"; anche in caso di "*phishing* telefonico (o *vishing*), realizzatosi mediante l'intervento telefonico di un truffatore, spacciatosi per operatore dell'intermediario[,] deve escludersi che l'operazione avrebbe potuto realizzarsi senza la decisiva collaborazione involontaria dell'utilizzatore" con comunicazione dei "codici OTP e OTS pervenutigli sul proprio *token* e *device* telefonico"; "malgrado la truffa tramite *vishing* rappresenti una tipologia potenzialmente insidiosa, [...] non assume rilevanza il fatto che le chiamate ricevute apparissero provenire dal numero verde del servizio clienti dell'intermediario. Infatti, il carattere anoma-

lo delle richieste rivolte [all'utente] avrebbe[...] dovuto indurre quest'ultimo a non seguire le indicazioni del falso operatore" (ABF Bologna, 12450/2022).

Il "fenomeno del c.d. '*phishing* attraverso *vishing*/*spoofing* misto a *smishing*'[si] realizza[...] mediante iniziale telefonata di un ignoto truffatore, che si qualifica[...] come un operatore dell'intermediario [...] e induce[...] il cliente ad attivare la procedura di aggiornamento dell'AppToken installata sul proprio cellulare. Conseguentemente, il cliente scarica[...] la nuova versione dell'App strumentale all'utilizzo dei servizi di *home banking* [...] tramite smartphone, la quale evidenzia[...] un'icona del tutto riconducibile all'intermediario, così come del resto [è] riconducibile all'intermediario anche il numero di telefono utilizzato dal truffatore" (ABF Milano, 9152/2024); si ha un "fenomeno di *spoofing* seguito da *vishing* [allorché si] ricev[a] un sms apparentemente proveniente dall'intermediario[e poi] una chiamata da numero non specificato, che [...] avvisa[...] della necessità di effettuare uno storno, [mentre l'utente si] limita[...] a digitare [...] i codici per controllare i movimenti nell'App dell'intermediario"; perché sia provato lo *spoofing*, però, è necessario produrre l'sms: infatti, "la mancata allegazione, da parte del cliente, del messaggio civetta, determin[a] il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto vi sia un legittimo affidamento dell'utente circa la genuinità del messaggi" (ABF Torino, 9095/2024).

Quando "il cliente è vittima di *spoofing* non può essere in genere ravvisata una sua colpa grave, salvo che il messaggio civetta presenti indici di evidente inattendibilità o anomalia che dovrebbero allertare l'utente avveduto; in quest'ultimo caso può essere riconosciuto un concorso di colpa per l'utente a causa della sua grave negligenza che agevola la truffa. [...] L'eventuale colpa grave del cliente è desumi-

bile, ad esempio, [...] dall'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta [o dall'aver il cliente] ricevuto ben 59 mail che l[o] informavano dell'effettuazione di altrettanti bonifici[. Per altro verso,] la numerosità delle operazioni[...] configur[a chiaramente un] *indicatore di anomalia* di cui alla lettera b), punto n. 1), del DM 112/2007 [in tema di "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento"], [...] le [cui] previsioni [...] rappresentano un parametro per la formulazione di un giudizio in concreto della negligenza tecnica dell'intermediario" (ABF Bologna, 4868/2024).

La "nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. 'sistema di autenticazione forte' (in inglese *strong customer authentication* o *SCA*). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, 'salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente'. [I]l concetto di 'autenticazione forte' trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): 'un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente

conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione'. [...] Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019. [...] L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della *strong customer authentication*" (ABF Roma, 11261/2023), in particolare "il codice OTP inviato tramite sms ovvero generato tramite token o *push notification* rientra nella categoria 'possesso'[,] il codice PIN rientra nella categoria 'conoscenza'" (ABF Bologna, 12450/2022), "mentre l'impronta digitale e il *face* ID appartengono alla categoria 'inerenza'" (ABF Bologna, 9791/2022), "i dati riportati sulla carta (numero, scadenza e CVV)[...] non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33)": al "par. 43 d[el] documento [EBA] si legge[...] che '*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with* Contr . *This includes approaches in which card details printed in full on the card are used as stand alone elements or used in combination with a communication protocol such as* [redacted] *or with only one compliant SCA element (such as SMS OTP)*'. [...] Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione[.] Nel caso di specie, le operazioni disconosciute consistono in due pagamenti online a favore di esercente tramite piattaforma online, che

l'intermediario deduce essere 'sito sicuro'. [...] L'intermediario deduce che le operazioni sono state autorizzate tramite un sistema SCA *compliant*: nell'accesso all'*home banking* da App, per effettuare il login e le operazioni di *inquiry*, il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (*One Time Password*) per disporre le operazioni; dopo avere effettuato la login e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP (*One Time Password*), generato da Mobile Token. [...] Deduce, inoltre, che le notifiche push generate da app riportano i dettagli delle operazioni dispositive, motivo per cui ritiene integrata la responsabilità del ricorrente che le avrebbe, dunque, consapevolmente approvate. [...] I Collegi ABF ritengono *compliant* alla SCA tale modalità autorizzativa. [...] Si rileva che, a differenza delle ipotesi 'classiche' e più frequenti di SMS-*spoofing*, nel primo messaggio ricevuto dal ricorrente e presumibilmente opera dei truffatori, non è rinvenibile un link, ma semplicemente l'informazione relativa ad un prossimo contatto da parte dell'intermediario. [...] Ad avviso del Collegio, nel caso in esame, si tratta di ipotesi di *smishing* [*phishing* tramite SMS] in cui il messaggio reca, quale mittente, la denominazione riferibile all'intermediario, tanto che il testo si è inserito nella visualizzazione dello smartphone all'interno della conversazione contenente messaggi genuini, effettivamente provenienti dall'intermediario (*spoofing*). [I]l Collegio ritiene che sussistano profili di colpa grave del cliente - consistente nell'avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa posta in essere dall'intermediario - e che essi siano tali da contribuire alla causazione dell'evento dannoso; tuttavia, ritiene altresì che la loro efficienza causale non sia esclusiva. Il caso di specie si discosta, infatti, dallo *smishing* perpetrato at-

traverso modalità tipiche e ampiamente note, dove la colpa grave del cliente è causa sufficiente dell'evento dannoso[.] Nel caso in esame[...] il truffatore ha adottato un sistema tecnicamente più sofisticato, *tale da concretare un'ipotesi di malfunzionamento del servizio di pagamento o altro inconveniente connesso al servizio di disposizione di ordine di pagamento*[...] destinato a ricadere nella sfera del rischio di impresa dell'intermediario. [...] Non è dubbio, infatti, che le operazioni siano un effetto di tale malfunzionamento, sul quale si innesta la colpa grave del cliente" (ABF Roma, 11261/2023).

2.2. Ebbene, nel caso di specie, innanzitutto, *CP_1* è il "prestatore di servizi di pagamento" ("di radicamento del conto"); mentre *CP_3* è prestatore del "servizio di disposizione di ordine di pagamento".

Gli attori deducono di aver ricevuto una chiamata sul proprio cellulare da numero cellulare; che l'interlocutore "si qualificava come operatore *CP_1* " e chiedeva di "ripetere l'operazione di impostazione del codice di sicurezza 'KEY 6' [...] utile ad abbinare la carta al conto corrente"; che il "supposto operatore" "invitava ad aprire un sms che di lì a poco sarebbe sopraggiunto sul telefono cellulare" di *[...] Per_2* ; che, giunto dopo qualche minuto tale sms, "nella chat *CP_1* ", "comunemente utilizzata dalla Banca per le comunicazioni di servizio", con "titolo" "impostazioni [redacted]", *Pt_1* "apriva il messaggio ma non appena terminata tale operazione, il telefono, pur a batteria carica, si spegneva, per riaccendersi solo dopo tre quarti d'ora"; che beneficiario è stata "l'azienda" [redacted]", "con sede in [redacted]", "società produttrice e distributrice di Gift *CP_6* .

CP_1 e *CP_3* deducono che il sistema adottato (servizio "3D Secure a due fattori") è pienamente SCA *compliant*; per il criterio del "possesso", è previsto il

codice OTP "ricevuto via notifica push"; per il criterio della "conoscenza", "l'operazione veniva autorizzata anche mediante codice key6"; che *Pt_1*, "comunicando i codici al truffatore, lo ha posto in condizione di [...] operare all'interno del portale del suo home banking": *Pt_1* "comunicava [...] i propri dati riservati, [...] mettendo il truffatore nella condizione di accedere all'area riservata, di modificare il numero di telefono collegato al servizio 3D Secure e di ricevere direttamente sul proprio cellulare i codici OTP necessari alla ratifica degli acquisti on line": "il cambio numero di telefono collegato al servizio 3D secure ha costituito l'antecedente necessario per la conclusione delle operazioni di acquisto, autorizzate dal truffatore, che ha così potuto ricevere sul proprio cellulare i codici OTP e recuperare il codice Key6".

Peraltro, gli attori hanno prodotto lo *screenshot* dei messaggi ricevuti, che li colloca nella *chat* "[redacted]"; e gli intermediari convenuti deducono che l'essere il messaggio "pervenuto sulla stessa chat dove la banca è solita inviare i codici di accesso OTP nulla aggiunge", a nulla "rileva", "atteso che il fenomeno dei c.d. alias, che appunto consentono ai truffatori di inserirsi, camuffandosi, anche nella messaggistica, non implica la violazione del sistema di sicurezza informatico delle banche".

Il Tribunale ritiene che il caso di specie sia sovrapponibile a quello di cui alla pronuncia dell'ABF Roma (11261/2023) sopra riportata, e che la relativa decisione sia condivisibile; ossia, non sufficiente all'intermediario la prova (che anche qui può ritenersi raggiunta) della "corretta autenticazione a doppio fattore"; e peraltro predicabile (anche per prova "in via presuntiva") di colpa grave il comportamento dell'utente (per "avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa" ormai generalizzata), anche consideran-

do che la inziale telefonata (nella quale è stato fornito il codice " *C.F._3*) proveniva da numero mobile non riferibile all'intermediario, così collocandola nel c.d. *vishing* senza c.d. *spoofing*; residua però il difetto di prova, da parte dell'intermediario, dell'esatto adempimento di *tutte* le obbligazioni a suo carico le cui prestazioni si conformano alla perizia professionale, ossia il difetto di prova che l'operazione di pagamento "non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti", prova di cui l'intermediario è onerato, come detto *sub* 2.1, *a maggior ragione* ove, come nel caso di specie risulta specificamente allegato e anzi sostanzialmente provato anche per non specifica contestazione, con riferimento al successivo (alla telefonata-*vishing*) sms (*smishing*), sia riscontrabile un caso di *spoofing*, per apparente riconducibilità del messaggio all'intermediario e assenza di indici evidenti di "contraffazione".

Il Tribunale determina nella misura della metà l'incidenza del concorso (gravemente) colposo dell'utente; anche sulla considerazione che se non vi fosse stato l'allegato spegnimento del cellulare conseguito allo *smishing-spoofing* si sarebbe verosimilmente potuto avvedersi prima dell'uso non autorizzato in corso e quindi comunicarlo prima all'intermediario.

In virtù di quanto detto *sub* 2.1, e a prescindere da previsioni contrattuali diverse (che non possono derogare alla normativa sopra richiamata, imperativa), è *CP_1* ("prestatore di servizi di pagamento" "di radicamento del conto") che (art. 11, cc. 1 e 2-*bis*, d.lgs. 11/2010) dovrà provvedere a "riporta[re] il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo" (per la misura della metà dell'importo delle operazioni non autoriz-

zate, ossia *nella misura di euro 2.905,00*); mentre i rapporti tra CP_1 e CP_3 ("prestatore di servizi di disposizione di ordine di pagamento"), di cui al medesimo art. 11, c. 2-*bis*, non sono oggetto del presente giudizio perché CP_1 ha chiamato in causa CP_3 quale "vero obbligato" e non in garanzia processuale (per rivalsa contrattuale), sicché nessuna domanda autonoma CP_1 ha formulato nei confronti di CP_3

È invece totalmente infondata, anche per difetto di qualsiasi allegazione specifica a supporto, la domanda degli attori di condanna al risarcimento del danno "non patrimoniale".

3. Le spese di lite seguono la soccombenza; il Tribunale le liquida come da dispositivo in base ai parametri *ex* d.m. 147/2022 e considerando sia la parziale soccombenza reciproca degli attori (domanda di condanna al risarcimento del danno), sia la distanza tra *petitum* e *decisum* quanto alla domanda accolta.

P.Q.M.

Il Tribunale di Lanciano, definitivamente pronunciando, così provvede:

a) condanna Controparte_1 in persona del rappresentante legale *pro tempore*, a riaccreditare in favore di Parte_1 e Parte_2 , su conto corrente bancario ad almeno uno degli stessi riferibile e con data valuta 20 aprile 2021, la somma di euro[redacted];

b) condanna Controparte_1 in persona del rappresentante legale *pro tempore*, e CP_3 in persona del rappresentante legale *pro tempore*, in solido, al rimborso, in favore di Parte_1 e Parte_2 , delle spese

di lite, che liquida in euro [redacted] per compensi, euro [redacted] per spese documentate, oltre rimborso forfettario spese generali al [redacted] e accessori di legge.

Lanciano, 11 novembre 2024.

Il giudice

Giovanni Nappi