# TRIBUNALE DI ROMA

**Sentenza n. 16588/2023 del 15-11-2023**

## REPUBBLICA ITALIANA IN NOME DEL POPOLO ITALIANO

IL TRIBUNALE DI ROMA ### civile Il Tribunale, in persona del Giudice Unico, dott. ### ha emesso la seguente

## SENTENZA

nella causa civile di I grado iscritta al n. 62434 del ruolo generale per gli affari contenziosi dell'anno 2021, trattenuta in decisione all'udienza del 23-05-2023 e vertente TRA ### C.F. ###, elettivamente domiciliat ###, presso lo studio dell'avv. ### che lo rappresenta e difende, giusta delega depositata in via telematica unitamente all'atto di citazione E ### S.P.A., C.F. ###, con sede ###### in persona del legaleATTORE rappresentante pro-tempore, elettivamente domiciliat ###, presso lo studio dell'avv. ### che la rappresenta e difende, giusta procura depositata in via telematica unitamente alla comparsa di costituzione e risposta ###

## CONCLUSIONI

All'udienza di precisazione delle conclusioni del 23-05-2023, le parti concludevano come da verbale in atti e la causa veniva trattenuta in decisione, con assegnazione dei termini ex art. 190 c.p.c.

## SVOLGIMENTO DEL PROCESSO

: Con atto di citazione ritualmente notificato, ### conveniva in giudizio ### S.p.A., chiedendo l'accoglimento delle seguenti conclusioni: "Voglia l'###mo Tribunale adito, contrariis reiectis: - in via principale accertare e dichiarare il diritto ai sensi del D.Lgs. n. 11/2010 in capo al ### ### al rimborso della complessiva somma di ### (ottomilaseicentottantotto/00), ovvero alla diversa maggiore o minore somma ritenuta di giustizia, anche mediante applicazione del criterio equitativo, in conseguenza dell'utilizzo fraudolento e prontamente disconosciuto dal Cliente della carta prepagata come meglio argomentato ed esposto nella narrativa e, per l'effetto, condannare ### S.p.a., (C.F.:

### e P.iva: ###) in persona del legale rappresentante pro tempore nella sede ###### ### alla ### 156 a corrispondere all'attore la complessiva somma di ### (ottomilaseicentottantotto/00), ovvero alla diversa maggiore o minore somma ritenuta di giusti-zia, anche mediante applicazione del criterio equitativo. Con espressa riserva di ulteriormente argomentare, precisare e modificare la domanda nonché di articolare istanze istruttorie, anche all'esito della costituzione della convenuta. Si depositano documenti come da separato indice a dimostrazione della propria domanda. Con vittoria di spese, competenze e onorari di lite da distrarsi a favore del procuratore antistatario, ivi compreso il rimborso delle spese generali e della C.P.A.". A sostegno delle proprie ragioni l'attore esponeva: - di essere titolare della carta di debito prepagata denominata "### PayPass", avente n. ### e ### n.

IT50I###, emessa in data ### presso ### S.p.A., filiale di ### n. ###; - che, in data ###, aveva ricevuto sul numero telefonico associato alla carta prepagata un messaggio all'apparenza proveniente da ### S.p.A., con cui era stato invitato a verificare la sospensione del contratto intrattenuto con la banca, collegandosi all'indirizzo htpps indicato nell'### - che, ricevuto analogo messaggio in data ###, si era collegato al link contenuto nell'SMS e così era stato automaticamente reindirizzato ad una pagina web avente veste grafica e denominazione identiche a quelle dell'applicazione ufficiale della banca; - che, subito dopo, un soggetto qualificatosi come un operatore di banca ### lo aveva contattato telefonicamente ribadendo l'imminente blocco del conto, qualora non avesse confermato i dati della carta inserendoli all'interno dell'applicazione; - che, pertanto, aveva inserito i dati della carta nella pagina web a cui era stato reindirizzato, e subito dopo, aveva ricevuto da ### un primo messaggio avente ad oggetto l'attivazione del servizio O-### (necessario per i pagamenti online) su ###A202F e un secondo messaggio avente ad oggetto la modifica del PIN abbinato al proprio profilo; - che, al fine di verificare la provenienza dei suddetti messaggi, nonché la propria posizione personale e lo stato del conto, aveva tentato di accedere sul sito della banca tramite PC, tuttavia, non riuscendo ad

entrare, aveva contattato la banca per bloccare la carta prepagata; - che, nel frattempo, era stato illecitamente effettuato un bonifico in favore di "### Bill" per l'importo di ### che la banca aveva omesso di bloccare; - che, in data ###, aveva sporto denuncia presso il commissariato di polizia di ### (### e, successivamente, aveva disconosciuto presso la filiale l'operazione contestata; - che, la banca aveva respinto ogni richiesta di rimborso, rifiutando altresì il tentativo di mediazione avviato ex art. 5 del D.lgs. n. 28/2010. ### evidenziava che, a fronte dell'operazione di pagamento non autorizzata, aveva immediatamente richiesto il blocco della carta telefonando al numero comunicato dalla banca, nonché, entro le 48 ore dall'accaduto, aveva sporto denuncia alle autorità di polizia e aveva confermato la segnalazione telefonica presso la filiale di appartenenza, ottemperando perciò alle previsioni contrattuali e alle prescrizioni del d.lgs. 11/2010. ### riteneva, invece, che la banca, omettendo i dovuti controlli e le cautele richieste dalla normativa di settore, fosse responsabile del fraudolento accesso di soggetti non abilitati al proprio conto online e, pertanto, domandava all'istituto di credito il rimborso della somma illecitamente bonificata. Si costituiva in giudizio ### S.p.A., in persona del legale rappresentante pro tempore, contestando quanto ex adverso dedotto poiché infondato in fatto ed in diritto e chiedendo l'accoglimento delle seguenti conclusioni: "Piaccia all'###mo Tribunale civile di ### contrariis rejectis, rigettare le avverse domande siccome totalmente infondate in fatto e in diritto e non provate. In via meramente subordinata e salvo gravame, nella denegata ipotesi di riconoscimento di qualsivoglia sia pur minima responsabilità della ### atteso l'esclusivo e comunque prevalente concorso colposo del signor ### escludere -o quantomeno ridurre in proporzione ad essoex art. 1227 c.c. le somme da restituire all'attore. In ogni caso con vittoria di spese e compensi professionali del giudizio, maggiorati di spese generali e di iva e cpa." La convenuta, innanzitutto, specificava che ### era titolare di due carte di credito "SUPERFLASH", nonché di una "PAY CARTA" avente n. ###, in essere presso la filiale ### di ### 82 B/C/D (###; che, l'attore, in data ###, aveva sottoscritto il contratto ### n. 20664397, per poter utilizzare le carte a sé intestate tramite ###

installata sul proprio cellulare, abbinata al numero di telefono certificato ###082. La convenuta, a sostegno delle proprie ragioni, da un lato rilevava che il sistema di sicurezza adottato per il servizio di home banking, articolato in vari meccanismi protettivi dell'infrastruttura tecnologica, era conforme allo stato dell'arte, tanto da essere certificato ### 27001, cioè era tale da soddisfare lo standard internazionale per la sicurezza delle informazioni. Dall'altro, sosteneva che la conclusione dell'operazione fraudolenta, ossia il bonifico di ### disposto in data 5-11-2020 in favore dell'esercente "### Birmingham", non era imputabile a difetti strutturali o al malfunzionamento contingente del sistema di internet banking utilizzato (come dimostrava il fatto che l'operazione contestata era stata regolarmente autenticata tramite l'inserimento delle credenziali statiche e dinamiche, nonché correttamente registrata e contabilizzata), ma alla negligenza e mancanza di cautela dell'attore, che, per sua stessa ammissione, nel corso dell'accesso al link fraudolento e nelle telefonate intercorse con il sedicente operatore di banca ### aveva fornito ai truffatori le proprie credenziali statiche (codice cliente e ### e dinamiche (OTP e ###, nonché i propri dati personali e quelli della carta di credito, in tal modo vanificando il sistema di autenticazione forte adottato a tutela del servizio di pagamento elettronico; che, inoltre, aveva incautamente ignorato gli allert inviati tramite SMS e notifiche push sul numero di telefono certificato, tramite cui era stato tempestivamente avvisato dell'accesso all'home banking da dispositivo diverso da quello in uso, del cambio del ### nonché, dell'esecuzione dell'operazione poi contestata. La convenuta, pertanto, riteneva che la condotta gravemente colposa di ### violativa degli obblighi di custodia e di comunicazione sullo stesso gravanti in base all'art. 7 D.lgs. 11/2010 e alle norme contrattuali, integrasse un inadempimento tale da comportare l'addebitabilità al cliente stesso della perdita subita a causa del bonifico fraudolento, ex art. 12 c. 4 D.lgs. n. 11/2010, o almeno, il riconoscimento del concorso dell'attore alla causazione dell'evento lesivo, ex art. 1227 c.c., dovendosi optare, in ogni caso, per il rigetto della domanda attorea o, in subordine, per la riduzione del rimborso eventualmente dovuto al cliente, nella misura ritenuta di giustizia. La

causa veniva istruita sulla base della documentazione versata in atti dalle parti; all'udienza del 23-05-2023 queste precisavano le conclusioni come da relativo verbale e la causa veniva trattenuta in decisione con i termini per il deposito delle conclusionali e delle repliche.

## MOTIVI DELLA DECISIONE

Le domande formulate da ### sono infondate, pertanto, devono essere respinte. Giova evidenziare, ai fini della delimitazione del thema decidendum, che l'attore nel presente giudizio ha chiesto accertarsi la responsabilità di ### S.p.A. nell'effettuazione, ad opera di soggetti ignoti, dell'operazione di bonifico di ### disposta, in data ###, in favore del beneficiario "### Birmingham", dalla "PAY CARTA" a sé intestata avente n. ###. In conseguenza, l'attore ha domandato all'istituto di credito il rimborso della somma corrispondente alla perdita subita, dichiarando il proprio incolpevole coinvolgimento nella frode bancaria informatica di cui trattasi. Per parte propria, ### S.p.A. ha contestato le domande attoree ed ha domandato il loro integrale rigetto, sostenendo il concorso colposo di ### nella causazione dell'evento lesivo e, pertanto, l'insussistenza del diritto dell'attore al rimborso della perdita subita a causa del bonifico fraudolento. Orbene, preliminarmente, deve darsi atto che in data 25-2- 2019, ### ha stipulato con ### S.p.A. il contratto ### n. 20664397 (cfr. doc. 4 allegato alla memoria ex art. 183 c. 6 n. 2 di parte attrice; doc. 2 allegato alla comparsa di costituzione e risposta della banca) avente ad oggetto il servizio di home banking, ossia l'esercizio di servizi bancari a distanza tramite il sistema di autenticazione forte del cliente denominato "a due fattori", che prevede l'utilizzo congiunto di credenziali statiche (delle quali fa parte, per espressa previsione dell'art. 1 del citato contratto, anche il cellulare certificato - nel caso di specie abbinato al numero ###082) e di credenziali dinamiche inviate tramite SMS o notifica push nell'App scaricata sul cellulare, consistenti in codici temporanei, generati per completare l'accesso al servizio e per autorizzare le disposizioni sui rapporti connessi (nel caso di specie il rapporto relativo alla "PAY CARTA" n. ### intestata a ### conformemente a quanto stabilito dall'art. 10 bis del d.lgs. n. 11/2010. Tale provvedimento normativo, attuativo della

direttiva 2007/64/CE (c.d. PSD1), da ultimo novellato con il d.lgs. n. 218/2017, emanato per recepire la nuova direttiva relativa ai servizi di pagamento 2015/2366/UE in vigore dal 13 gennaio 2018 (c.d. PSD2), individua in relazione all'utilizzo degli strumenti di pagamento elettronici e/o tramite canali a distanza che possano comportare un rischio di frode o di altri abusi, gli obblighi posti a carico del prestatore dei servizi e quelli gravanti sull'utente. Quest'ultimo, ai sensi dell'art. 7, è tenuto: ad utilizzare gli strumenti di pagamento secondo i termini d'uso pattuiti con il prestatore dei servizi ed esplicitati nel contratto quadro; a comunicare allo stesso, non appena ne venga a conoscenza, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento di pagamento, al fine di consentirne il blocco; ad adottare tutte le misure idonee a proteggere dall'altrui ingerenza i dispositivi di accesso personalizzati, tra cui le credenziali di sicurezza personalizzate. In base al successivo art. 12 c. 3, qualora l'utente dei servizi di pagamento violi uno dei suddetti obblighi con dolo o colpa grave o agisca in modo fraudolento, assume la responsabilità delle perdite relative all'utilizzo abusivo dello strumento di pagamento, per intero; diversamente, ha diritto di ottenere dal prestatore dei servizi il rimborso della somma illecitamente sottrattagli, al netto di una franchigia di 50 ### da applicarsi in caso "di operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Quindi, come espressamente previsto dall'art 10 c. 2 d.lgs. 11/2010, il prestatore di servizi di pagamento può escludere la propria responsabilità per l'utilizzo non autorizzato dello strumento di pagamento ad opera di terzi, provando la frode dell'utilizzatore o il suo inadempimento per dolo o colpa grave, che costituiscono fatti impeditivi del risarcimento del danno ex art. 2697 c. 2 c.c. Del resto, anche la giurisprudenza di legittimità ha affermato che "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 se ricorre una situazione di colpa grave

dell'utente" (cfr. Cass. 05/07/2019, n. 18045). Specularmente, il d.lgs. n. 11/2010 pone anche a carico del gestore dei servizi di pagamento il rispetto di obblighi determinati, tra i quali rientrano: l'obbligo di assicurare, tramite l'adozione delle misure più idonee alla luce dello sviluppo tecnologico, che i dispositivi personalizzati per l'utilizzo dello strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato (art. 8 c. 1 lett. a); l'obbligo di assicurare che siano sempre disponibili gratuitamente strumenti adeguati affinché l'utilizzatore possa effettuare la comunicazione di cui all'art. 7 c. 1 lett. b (art. 8 c. 1 lett. c); l'obbligo di impedire l'utilizzo dello strumento di pagamento in seguito al blocco (art. 8 c. 1 lett. d); l'obbligo di attuare l'autenticazione forte del cliente, quando l'utente accede al suo conto di pagamento online, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione tramite un canale di pagamento a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi (art. 10 bis c. 1). Di talché, per far sì che l'utilizzatore sopporti le perdite derivate da un uso illegittimo dello strumento di pagamento ad opera di terzi, non è sufficiente che il prestatore del servizio dia prova di una condotta fraudolenta o dell'inadempimento degli obblighi ex art 7 d.lgs. 11/2010 sorretto da dolo o colpa grave del cliente, dovendo altresì dimostrare, preventivamente, di aver adempiuto i doveri di tutela del consumatore prescritti a suo carico dal decreto (cfr. Cass. 26/11/2020, n. 26916). ###. 10 c. 1 d.lgs. 11/2010 afferma infatti che, qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione 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 altri inconvenienti". In conclusione, è possibile affermare che l'imputazione di responsabilità all'utilizzatore dello strumento di pagamento, ex art. 12 c. 3 d.lgs 11/2010, presuppone che l'istituto di credito raggiunga una duplice prova, ossia: quella di aver usato un elevato grado di diligenza nell'adempimento dei propri oneri e quella che dimostri, con sufficiente grado di attendibilità giuridica, l'inadempimento degli obblighi del cliente

dovuto a frode, dolo o colpa grave. Nel caso di specie, ### a sostegno della asserita regolarità formale dell'operazione in contestazione, ritenuta correttamente autenticata, registrata e contabilizzata, nonché eseguita secondo un sistema di autenticazione a due fattori, supportato dalla certificazione UNI CEI ISO IEC 27001:2017, da cui evincere l'elevato livello di sicurezza dello strumento di pagamento (cfr. doc. 9 all. a comparsa di costituzione e risposta della banca), ha prodotto in atti i file log contenenti la tracciatura dell'operazione di bonifico svolta sul portale home banking della banca, nonché i file log da cui evincere specificamente gli accessi, gli ### le notifiche push, le caratteristiche degli IP unici relativi agli accessi, concernenti il bonifico in oggetto (cfr. docc. 14/15 all. alla memoria 183 c. 6 n. 2 di ###. Analizzata tale documentazione informatica, da ritenersi valida ed efficace nonostante le contestazioni di parte attrice, del tutto generiche e non esplicative dei motivi della pretesa inattendibilità della stessa, è stato accertato che, in data 5-11- 2020 alle ore 18:45:47, l'utenza n. 20664397 intestata a ### ha completato la procedura di login all'### banking di ### tramite inserimento delle credenziali statiche (### e ### e ha poi avviato un'operazione di enrollment dell'App della banca sul dispositivo mobile ###A202F (dispositivo diverso da quello in uso all'attore), che, grazie al corretto inserimento del codice di attivazione (### 831209, inviato tramite SMS sul numero di telefono certificato, si è conclusa positivamente. ### di enrollment ha quindi comportato l'invio sul medesimo cellulare, alle ore 18:58:04, dell'SMS di allert: "E' appena stato attivato O-### su ###A202F con cui è possibile effettuare pagamenti online. Non sei stato tu? ### la ### Online", nonché, della notifica push: "E' stato eseguito il ### alle 18.58 un Accesso all'### da un nuovo dispositivo: SM-A202F. Non sei stato tu? ### la filiale online dalla sezione ### con Noi". Risulta poi che, alle ore 18:59:20, l'utenza n. 20664397 ha provveduto al cambio del ### il che è stato debitamente segnalato dal sistema di sicurezza antifrode di banca ### tramite invio di apposito SMS al numero di telefono certificato, nonché, tramite notifica push del seguente tenore: "### del tuo profilo è stato modificato. Visita la sezione il mio ### per i dettagli. Non sei stato tu?

### la ### dalla sezione ### con Noi". Infine, emerge dalla documentazione in atti che, alle ore 19:00:56, l'utenza n. 20664397 ha disposto un bonifico online di ### in favore di "### Birmingham" utilizzando la carta n. ###; che, in relazione all'operazione di pagamento non sono state rilevate anomalie, posto che la stessa è stata eseguita previo il corretto inserimento da parte dell'ordinante del PIN (come modificato) e la successiva verifica sul device ###A202F dell'OTP virtuale generato dall'APP di banca ### (### anche doc. 8 all. alla comparsa di costituzione e risposta). Inoltre, è stato riscontrato che, anche in questo caso, l'istituto di credito ha comunicato all'utente l'avvenuta richiesta di bonifico tramite immediato invio sul cellulare certificato di notifica push di allarme, indicante tutti i dati dell'operazione di pagamento: "### autorizzando il pagamento di 8688,00 ### presso ### del 05.11.2020 19:00 con la carta 534207******2148". Orbene, esaminata la condotta dell'istituto di credito convenuto alla luce della ricostruzione fattuale emergente dall'istruttoria, tenuto conto altresì della circostanza incontestata per cui i codici statici e dinamici, indispensabili all'enrollment dell'APP della banca su un cellulare diverso da quello normalmente in uso al ### e necessari all'utilizzo dello strumento di pagamento, sono stati comunicati agli autori della truffa, in tempo reale, dallo stesso attore, secondo la dinamica fraudolenta più volte esposta dal ### negli atti di causa, nonché, nella denuncia contro ignoti presentata in data ### (Cfr. doc. 6 allegato all'atto di citazione), si deve affermare che ### ha consentito l'operatività da remoto della carta di debito n. ### a seguito del corretto inserimento delle credenziali (statiche e dinamiche) teoricamente riconducibili all'intestatario ### e che ha regolarmente inviato sul cellulare certificato del cliente le dovute comunicazioni di allerta, dovendosi perciò concludere per la regolarità formale del sistema di sicurezza approntato dalla banca, le cui procedure non hanno sofferto alcun malfunzionamento. Alla luce di quanto sopra, deve rilevarsi che ### ha adempiuto con la dovuta diligenza gli obblighi imposti agli istituti di credito dal d.lgs. n. 11/2010 (nel caso di specie ribaditi dal contratto ### in essere tra le parti), tutelando adeguatamente l'interesse del cliente ad un uso sicuro ed efficiente dello

strumento elettronico di pagamento, tramite: l'adozione e regolare attuazione di un sistema di autenticazione del cliente a più fattori (come richiesto dall' art. 10 bis c. 1 del d.lgs. n. 11/2010); l'impiego di strumenti comunicativi idonei a segnalare tempestivamente al cliente le operazioni gestorie e le movimentazioni eseguite sul conto online e, dunque, un eventuale utilizzo abusivo dello strumento di pagamento da parte di terzi. Nel caso di specie, infatti, non vi è dubbio che le cautele attuate dalla banca, potenzialmente in grado di prevenire e/o evitare il perfezionamento delle più comuni truffe informatiche bancarie (quale quella in oggetto), sono state di fatto neutralizzate dalla condotta fortemente imprudente del ### che, per sua stessa ammissione, ha comunicato al frodatore le password statiche (### e codice ### e le password dinamiche e temporizzate (OTP e ###, consentendo allo stesso di operare sull'home banking nel pieno rispetto delle procedure finalizzate a garantire la puntuale esecuzione da parte della banca degli ordini gestori e dispositivi impartiti dal cliente debitamente autenticato. Di talché, valutata la documentazione prodotta dall'istituto di credito alla luce delle allegazioni dell'attore, deve ritenersi che ### abbia dato prova, non solo di aver predisposto le misure più idonee a garantire la tutela del cliente e ad evitare l'utilizzo abusivo dello strumento di pagamento da parte di terzi non autorizzati, ma anche dell'inadempimento sorretto da colpa grave, da parte del ### dell'onere di custodia delle credenziali di sicurezza personalizzate, posto a carico dello stesso dall'art. 7 del d.lgs. 11/2010 e dalle norme contrattuali. Infatti, a fronte della enorme diffusione di truffe informatiche bancarie della stessa tipologia di quella in oggetto, dell'attenzione dedicata al fenomeno da parte di molteplici campagne informative volte a prevenire la vittimizzazione degli utenti e, soprattutto, dinanzi alla specifica campagna antifrode posta in essere da ### S.p.A., diretta a sensibilizzare la clientela sulle dinamiche del phishing e sui i rischi derivanti dal riscontrare anomale richieste di cessione di dati e codici personali pervenute tramite e-mail/###contatti telefonici apparentemente riconducibili all'istituto di credito (### doc. 10 all. alla comparsa di costituzione e risposta; doc. 16 all. alla memoria ex art.

183 c. 6 n. 2 di parte convenuta), deve ritenersi che l'imprudenza del ### nel fornire le proprie credenziali (nonché gli altri fattori di autenticazione/autorizzazione delle operazioni) a terzi nel contesto della truffa organizzata in suo danno, del tutto riconoscibile, non sia scusabile, giacché l'impiego di una media diligenza da parte dell'attore sarebbe stata sufficiente ad evitare il verificarsi dell'illecito. Del resto, a pag. 2 dell'atto di citazione si riscontra che il ### "conscio dell'importante rilevanza dei dati richiesti considerava attentamente se digitare o meno tali informazioni", il che equivale a dire che l'attore aveva percezione dell'ambiguità della richiesta pervenutagli, per cui, nel dubbio circa l'effettiva riconducibilità della stessa ad ### prima di fornire i codici avrebbe dovuto accertare la legittimità della richiesta, contattando l'istituto di credito al numero verde indicato nel sito ufficiale della banca. In ogni caso, deve rilevarsi che la condotta gravemente colposa di ### non consiste solo nell'aver incautamente fornito le proprie credenziali di accesso all'home banking al phisher, nonostante la massiccia campagna antifrode realizzata da ### a tutela dei propri clienti, risultando altresì dal fatto che lo stesso non ha valutato con la dovuta perizia gli allert inviati dalla banca. In particolar modo: l'SMS e la notifica push aventi ad oggetto la comunicazione circa l'avvenuta installazione dell'APP O-### su un dispositivo diverso dal proprio; l'SMS e la notifica push aventi ad oggetto la comunicazione circa l'avvenuta modifica del ### la notifica push avente ad oggetto la comunicazione circa l'autorizzazione dell'operazione di pagamento, poi contestata, contenente tutti i dati del bonifico. Tali comunicazioni, infatti, certamente idonee a rendere edotto l'attore della frode in corso, avrebbero dovuto condurre lo stesso a non persistere nella propria negligente condotta e a rendere immediatamente noto alla banca l'accaduto, consentendo all'istituto di credito di intervenire tempestivamente e di sventare il perfezionamento della truffa con l'adozione di ulteriori misure cautelative a tutela del rapporto bancario colpito, prima del trasferimento della somma bonificata all'esercente "### Birmingham" a fronte dell'acquisto e-commerce effettuato dal frodatore (posto che, data la regolarità dell'operazione di pagamento e la natura di corrispettivo di una compravendita della

somma bonificata, la banca non ha potuto effettuare il recall dell'operazione ormai perfezionatasi, in assenza del consenso del beneficiario). Per i motivi sopra esposti, la responsabilità di ### S.p.A. per la perdita derivata dalla disposizione di pagamento in contestazione deve essere esclusa, giacché dal quadro probatorio risulta che l'utilizzo abusivo dello strumento di pagamento da parte di terzi sia riconducibile alla condotta gravemente colposa dell'attore ### il quale, dunque, non ha diritto al rimborso richiesto, ai sensi e per gli effetti dell'art. 12 c. 3 d.lgs 11/2010. Le spese di lite, liquidate come da dispositivo, seguono la soccombenza e, pertanto, sono poste a carico dell'attore ###

## P.Q.M

Il Giudice Unico del Tribunale di ### definitivamente pronunciando, ogni contraria istanza, eccezione e deduzione disattesa, nel contraddittorio tra le parti, così provvede: respinge le domande formulate da ### nei confronti di ### S.p.A. per le ragioni di cui in motivazione; condanna ### al pagamento in favore di ### S.p.A. delle spese di lite che liquida in complessivi ### per compensi professionali, oltre spese generali come da tariffa forense, IVA e CPA come per legge. Così deciso in ### in data 30 ottobre 2023

il Giudice
Unico dott. ###