Sentenza, Tribunale di Palermo, Giudice Andrea Illuminati, n. 3438, dell'11/07/2023

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
TRIBUNALE DI PALERMO

Il Giudice nella persona del dr. Andrea Illuminati, nella causa di primo grado iscritta al N. xxxx/2021 RG, ha pronunciato la presente

SENTENZA

tra

SOCIETA', in persona del legale rappresentante pro - tempore (avv.to omissis)

- attrice -

e

BANCA, in persona del legale rappresentante pro - tempore (avv. omissis)

- convenuta -

oggetto: <<rapporti di c/c e altri contratti bancari>>
CONCLUSIONI
v. verbale del 17.4.23

MOTIVI DELLA DECISIONE

Con atto di citazione ritualmente notificato, SOCIETA' ha convenuto in giudizio, innanzi a questo Tribunale, BANCA per sentirla condannare a titolo risarcitorio al pagamento della somma di € 23.501,00 in dipendenza di una truffa informatica perpetrata in suo danno.
L'attrice lamenta che terzi soggetti avrebbero posto in essere un'attività fraudolenta consistente nell'avere effettuato un bonifico non autorizzato per complessivi € 23.501,00 utilizzando le somme giacenti sul suo conto corrente, sebbene questa non avesse mai autorizzato tale disposizione di bonifico.
Stando alla ricostruzione di parte attrice, la responsabilità di tale attività fraudolenta sarebbe addebitabile alla convenuta ai sensi degli artt. 11 e 12 del D. Lgs. n. 11/2010, non avendo l'intermediario predisposto idonee garanzie atte a fronteggiare indebite intromissioni di terzi soggetti nel sistema informatico della banca utilizzato per effettuare l'operazione contestata.
Radicatasi la lite, si è costituita in giudizio BANCA la quale ha chiesto il rigetto delle avverse domande in ragione della loro ritenuta infondatezza.
Una volta assunte le prove orali ed espletata CTU, la causa è stata trattenuta per la decisione all'udienza in epigrafe indicata, con concessione dei termini ex art. 190 c.p.c.

***

Ciò posto, la domanda di risarcimento danni proposta dall'attrice è fondata per le ragioni appresso spiegate.
Il giudizio de quo verte sull'accertamento della responsabilità del prestatore di servizi di pagamento nel caso in cui il cliente abbia disconosciuto un'operazione eseguita tramite home banking, da terzi ignoti, con mezzi fraudolenti.
Pertanto, la normativa di riferimento è quella che regola le operazioni di pagamento a distanza di cui al d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore del d.lgs. 15 dicembre 2017, n. 218 (di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno).
Con riferimento all'ipotesi — verificatasi nel caso che ci occupa — in cui il cliente neghi di aver autorizzato un'operazione di pagamento già eseguita, l'art. 10 del citato d.lgs. stabilisce che sia onere dell'intermediario dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute; e, a norma del successivo art. 12, co. 4, è altresì onere dell'intermediario fornire la prova di tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore. In mancanza di tale duplice prova, la Banca sopporta integralmente le conseguenze delle operazioni disconosciute, senza alcuna limitazione o franchigia.
L'intenzione del legislatore è all'evidenza quella di sollecitare la fissazione - da parte del prestatore di servizi - di elevati standard di trasparenza e sicurezza e di riversare su di esso, almeno in linea di principio, le conseguenze sfavorevoli dell'uso fraudolento o non autorizzato degli strumenti di pagamento, tanto in base alla logica per cui la Banca, quale operatore professionale che gestisce il servizio di pagamento, è il soggetto più idoneo a sopportare il rischio delle operazioni non autorizzate.
La lettura nei termini sopra precisati del sistema delineato dal d.lgs. 11/10 trova diretta conferma nella giurisprudenza della SC, alla cui condivisibile stregua, "In tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo" (citata in massima Cassazione civile sez. I, 20/05/2022, n. 16417; conformi: Cassazione civile sez. I, 03/02/2017, n. 2950).

Sotto il profilo della prova del dolo o della colpa grave del cliente, la medesima giurisprudenza ha inoltre chiarito che la stessa debba essere fornita positivamente dal prestatore di servizi, non potendo presumersi in ragione dell'idoneità delle protezioni adottate dalla banca, al fine di evitare l'esecuzione di operazioni fraudolente. Così ha statuito in proposito Cassazione civile sez. VI, 26/11/2020, n. 26916: "La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente. (Nella specie, la S.C. ha cassato con rinvio la decisione di merito che, disattendendo il principio di cui in massima, aveva ritenuto che, essendo stata raggiunta la prova presuntiva dell'idoneità delle protezioni adottate dal prestatore dei servizi di pagamento contro l'uso non autorizzato della carta cd. prepagata "postepay", gravasse sul cliente l'onere di dimostrare di avere tenuto un comportamento esente da colpa nella custodia della carta e dei codici, in modo da evitare furti o smarrimenti)".

Ciò debitamente premesso in punto di diritto, con specifico riferimento al caso in esame l'intermediario ha dato prova di aver adottato un sistema di autenticazione multifattoriale consistente nell'inserimento delle credenziali statiche di accesso al canale di home banking, di un codice OTP inviato tramite notifica push, e una ulteriore password - c.d. codice OTS - inoltrata tramite sms sul cellulare certificato dell'attrice; nonché di avere correttamente registrato e contabilizzato l'operazione oggetto di giudizio.

Le suddette evenienze emergono dai disposti accertamenti peritali, che danno conto delle operazioni svolte dal conto corrente dell'attrice sul portale home banking della banca e consentono di ricostruire lo svolgimento del bonifico in contestazione.

Le operazioni peritali espletate comprovano che l'operazione disconosciuta - del 25.02.21 - è stata correttamente autenticata con l'inserimento della OTP e della OTS ed escludono un'anomalia operativa o un malfunzionamento del servizio predisposto dall'intermediario, secondo quanto previsto dall'art. 10 del d.lgs. 11/10. Infatti, le credenziali "statiche" (nome utente e codice PIN) sono state opportunamente digitate per effettuare l'accesso alla Home Banking, e le credenziali dinamiche (OTP e OTS) sono state correttamente generate e inserite ai fini dell'operazione di bonifico, con conseguente obbligo della banca di darne esecuzione.

Sebbene BANCA abbia provato che il bonifico disconosciuto sia stato autenticato nel rispetto della normativa vigente e attraverso strumenti di sicurezza idonei a garantire elevati standard di sicurezza (c.d. sistema di autenticazione c.d. forte), la circostanza non vale di per sé ad escludere la responsabilità della convenuta, essendo necessario che l'intermediario - alla stregua dell'art. 12, co. 4 d.lgs. 11/2010 e della giurisprudenza sopra richiamati - dimostri elementi fattuali caratterizzanti le modalità esecutive dell'operazione dai quali possa ricavarsi la colpa grave dell'utente.

Sotto tale aspetto si osserva che per quanto emerso in sede di accertamenti tecnici l'operazione bancaria in contestazione - bonifico del 25.02.21 - è frutto di una attività fraudolenta perpetrata da terzi truffatori nell'ambito di una "campagna malevola denominata BRATA che mira a ottenere i dati bancari degli ignari utenti". Come in particolare spiegato dal Ctu nominato, "Tutto parte da un messaggio contenente un link malevolo (in cui usualmente i truffatori si fingono la banca o comunque qualche realtà "autorevole", si fa dunque riferimento alla truffa dello smishing). Quest'ultimo rimanda poi a un portale che invita l'utente a scaricare una falsa app "antispam" cercando persino di rassicurare l'utente dicendo che potrà contattare un dipendente della banca per discutere tutti i dettagli legati al software" (p.11 CTU).

Come inoltre illustrato nel successivo grafico a pagina 12 della CTU, dopo l'effettuazione del download dell'applicazione, questa chiede al cliente della banca una serie di permessi, compresi quelli sugli SMS e sulla gestione delle chiamate vocali. Successivamente, il malweare Brata entra in attività ed è in grado di prendere possesso dei codici di accesso all'account bancario ed intercettare gli SMS inviati sul numero telefonico della vittima per carpire il codice di autenticazione a due fattori inviato dalla banca.

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

Deve pertanto ritenersi che l'attrice sia rimasta vittima di una truffa informatica, essendo i truffatori riusciti — attraverso l'invio sullo smartphone della cliente di un link malevolo apparentemente riconducibile alla BANCA e il successivo download da parte di questa della applicazione "BANCA.apk" — a capire le credenziali statiche e dinamiche di accesso al conto on - line della SOCIETA' e a compiere con esse da remoto il bonifico di €. 23.501,00 in favore del conto intestato a tale omissis.

Ebbene, in relazione a tale truffa non può ritenersi sussistente la colpa grave della vittima, che in questo tipo di frodi confida nella riconducibilità alla banca del messaggio contenente il link malevolo. Al riguardo, il fatto che l'applicazione utilizzata per realizzare la truffa sia stata istallata dalla cliente al di fuori dello store ufficiale di Google Play (come rilevato dal perito a pag. 8 della CTU) è un elemento in sé neutro ove si consideri che molte applicazioni scaricabili on - line tramite android non transitano neppure per tale servizio, di talché la circostanza non era sufficiente a rendere sospetta l'operazione per un soggetto mediamente avveduto.

Risultano inoltre non pertinenti rispetto al caso in esame i precedenti citati dalla banca a sostegno della dedotta colpa grave del cliente (cfr. Cass. n. 7217/2023; n. 9158/2018; n. 9721/2020; n. 10638/2016) riferendosi gli stessi a casi in cui il cliente, violando gli obblighi di custodia dei codici di accesso al conto corrente on -line posti a suo carico dalle previsioni contrattuali, aveva colposamente fornito tali dati ai truffatori, cosi permettendo il compimento della frode informatica in suo danno. Di contro, nel caso in esame l'attrice non ha fornito alcun dato sensibile agli autori della truffa, essendosi limitata ad effettuare il download di un programma apparentemente riconducibile ad IS; pertanto nella fattispecie alcun obbligo di custodia può ritenersi violato.

Alla stregua delle considerazioni che precedono, non potendo dunque ritenersi raggiunta la prova liberatoria posta a carico della banca dall'art. 12, co. 4 d.lgs. 11/10, la domanda risarcitoria proposta dall'attrice va senz'altro accolta nella misura dell'importo indebitamente sottrattole, di €. 23.501,00.

Il superiore importo, siccome debito di valore non determinato all'attualità, deve essere rivalutato secondo gli indici istat dalla data del fatto lesivo – da individuarsi in quella di effettuazione dell'operazione contestata del 25.5.21 - alla pubblicazione della presente decisione, così che alla data odierna ascende ad €.26.908,65. Sulla sorte capitale progressivamente rivalutata sono pure dovuti, per il corrispondente periodo, gli interessi compensativi al saggio legale al fine di liquidare il danno per il ritardato pagamento, pari ad €. 885,49, il tutto per complessivi €. 27.794,14 (di cui € 26.908,65 per sorte rivalutata ed €. 885,49 per interessi compensativi).

***

Le spese di lite – che si liquidano in dispositivo ex DM 55/14 (e succ. mod.) – seguono la soccombenza della parte convenuta. Alla luce dei relativi esiti, i costi della CTU, liquidata con separato decreto, vanno posti a carico della medesima parte.

p.q.m.

Il Tribunale, definitivamente pronunciando sulla presente controversia, ogni altra istanza ed eccezione disattesa, così provvede:

- condanna la convenuta a corrispondere all'attrice l'importo di € 27.794,14, oltre ad interessi al saggio legale dalla pubblicazione della sentenza al saldo effettivo;
- condanna la convenuta a rifondere alla attrice le spese di lite che si quantificano in €. 3.809,00 per compensi di avvocato, oltre ad oneri e accessori di legge;
- pone i costi della CTU, liquidata con separato decreto, a carico della convenuta.

Così deciso a Palermo il 10.7.23

Il Giudice Unico
dr. Andrea Illuminati

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano