Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) FERRARI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) TENELLA SILLANI

Seduta del 02/09/2021

Esame del ricorso n. 482146 del 25/03/2021

proposto da

nei confronti di 3069 - INTESA SANPAOLO S.P.A.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) FERRARI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) TENELLA SILLANI

Seduta del 02/09/2021

FATTO

Il ricorrente, premesso di essere contitolare con la moglie di due conti correnti presso l'intermediario convenuto, riferisce quanto segue. "*In data 4 luglio 2020 […] riceveva un messaggio di testo sul suo telefono cellulare dal [la Banca], con cui veniva avvisato della necessità di collegarsi al link contenuto nello stesso SMS, per ragioni di sicurezza bancaria. Atteso che la comunicazione di testo proveniva proprio dal[la Banca], mittente dal quale solevano giungere ai ricorrenti, quando necessario, le altre comunicazioni da parte di Banca … (tanto che il messaggio de quo si accodava agli altri, già presenti nella cartella […]) non dubitava di alcunché e accedeva alla pagina Internet mediante il link*". Riceveva quindi, poco dopo, una telefonata dal numero verde della Banca e l'operatore "*lo invitava ad eseguire determinati passaggi per bloccare alcune disposizioni di pagamento … Al termine delle operazioni effettuate seguendo quanto suggerito dall'interlocutore, … riceveva un SMS con cui veniva invitato ad utilizzare il codice contenuto nel messaggio per attivare*" il servizio di autenticazione della Banca. Di seguito, accedendo all'estratto conto riscontrava l'effettuazione: sul conto *888 di n. 3 ricariche di importo pari ad Euro 2.490,00 ciascuna e n. 1 bonifico istantaneo per l'importo di Euro 1.499,60; sul conto *132 di n. 1 ricarica di importo pari ad Euro 2.490,00. Chiedevano immediatamente il blocco della carta ed il giorno 6 luglio 2020 sporgevano denuncia. Precisa che "*trattasi di sms spoofing, tecnica evoluta, che differisce dallo smishing perché mentre nella prima il*

soggetto estraneo rimpiazza il numero originario con un testo alfanumerico e fa apparire all'esterno ciò che non è, di talché la comunicazione si dimostra giungere dal numero di telefono riferibile alla banca, nello smishing il testo del messaggio mira ad estorcere informazioni personali ma non appare provenire direttamente dall'usuale indirizzo dell'istituto bancario". Presentato infruttuosamente ricorso, chiede, per tutto quanto suesposto, il rimborso di Euro 11.459,00 pari alle somme indebitamente sottratte.

L'intermediario, nelle controdeduzioni, precisato che il conto *132 è intestato alla sola cointestataria del ricorso, afferma che le operazioni sono state correttamente autenticate con l'inserimento di OTP e OTS, registrate e contabilizzate, senza il verificarsi di malfunzionamenti e/o inconvenienti. Rileva, inoltre, che il cliente ha ammesso di aver inserito i propri codici nel link contenuto in un messaggio civetta e di aver comunicato i codici OTP e OTS a un finto operatore della Banca. Sottolinea, infine, che la banca ha allertato il cliente con "11 *sms/Push*" dell'accesso e dell'inserimento delle operazioni, pur senza ottenere alcuna reazione da parte dello stesso. In considerazione di quanto sopra esposto, chiede in via principale, il rigetto della domanda restitutoria, in quanto immotivata ed infondata; in subordine, laddove si ritengano di ravvisare suoi profili di responsabilità nell'accaduto, di "*definire la ripartizione fra le parti del danno in esame, in misura proporzionale elle rispettive effettive responsabilità e, in particolare, ai sensi dell'art. 1227, 1 e 2 comma c.c.*".

Il ricorrente, in sede di repliche, premesso che i log in formato *Excel*, allegati dall'intermediario, sono modificabili e quindi "*non hanno alcun valore probatorio*"; sostiene che "*Potrebbe essere verosimile che le notifiche che la banca sostiene di aver inviato al ricorrente, in realtà, non siano mai giunte al cellulare … a causa di mancanza di copertura temporanea di rete oppure che tali notifiche non si siano generate a causa della manipolazione operata dai truffatori durante l'incursione nel sistema informatico della Banca. Manca, pertanto, la prova dell'effettiva ricezione dei mentovati alert da parte dei ricorrenti*"; e inoltre che "*gli odierni ricorrenti hanno inserito le proprie credenziali nella schermata falsa pagina internet e fornito i codici di sicurezza via filo all'interlocutore in quanto comprensibilmente persuasi che vi fosse in essere una comunicazione diretta con la propria banca di fiducia, in considerazione del fatto che l'utenza che li aveva contattati corrispondeva al numero verde*" della banca, per è ipotizzabile un caso di "*Man in the browser*".

L'intermediario, nelle controrepliche, ribadisce che i tracciati prodotti "*riportano pedissequamente le risultanze a sistema e l'operatività registrata per il periodo*"; precisa inoltre che, "*contrariamente a quanto affermato dai ricorrenti,* [essi] *sono allegati in formato non editabile*". Evidenzia altresì che il ricorrente ha rilasciato dichiarazioni confessorie posto che "*è lo stesso cliente a dichiarare nell'integrazione alla denuncia … di aver inserito i propri codici personali a seguito della ricezione di un messaggio sms contenente un link e di una telefonata, che dichiara provenire dalla Banca, ma in merito alle quali non fornisce alcuna prova di quanto affermato. Ed è parimenti lo stesso cliente nella medesima integrazione a confermare la ricezione dei messaggi inoltrati dalla scrivente. Messaggi che contenevano i codici necessari alla conferma delle operazioni chiaramente ivi dettagliate, che sono stati inseriti per confermare le operazioni poi disconosciute*".

DIRITTO

Il Collegio, rilevato che alle operazioni contestate, effettuate nel luglio 2020, si applica il D.lgs. n. 11/2010, come modificato dal D.lgs. n. 218/2017, di attuazione della Direttiva 2015/2366/EU (PSD II), richiama l'art. 8 del suddetto decreto, secondo il quale il prestatore dei servizi di pagamento che emette uno strumento di pagamento ha, tra gli altri, "*l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo dall'art. 7*"; l'art. 10, comma 1, a tenore del quale, in caso di disconoscimento di un'operazione da parte dell'utente, è onere del prestatore di tali servizi "*provare che, nell'ambito delle proprie competenze, 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 […]*"; l'art. 10 *bis*, comma 1, secondo cui "*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; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*"; gli artt. 11, comma 1, e 12, comma 4, i quali, rispettivamente, dispongono che quando l'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento deve rimborsarla immediatamente fatto salva l'ipotesi in cui l'utente "*abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave*", nel qual caso, questi "*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*".
Sulla base della normativa sopra riportata è l'intermediario a dover provare l'insussistenza di malfunzionamenti dei dispositivi di pagamento, nonché l'autenticazione, la corretta registrazione e contabilizzazione della operazione disconosciuta, prova comunque di per sé non sufficiente a dimostrare il dolo o la colpa grave dell'utente. Il Collegio di Coordinamento, nella decisione n. 22745/19, ha infatti affermato il seguente principio di diritto: *"la previsione di cui all'art. 10, comma 2, del d.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l''autenticazione' e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*".
Con riguardo alla fattispecie in esame, premesso che il ricorrente chiede il rimborso della complessiva somma di € 11.459,00, a valere su due conti diversi (esso fa, infatti, riferimento alle seguenti operazioni: conto *888: n. 3 ricariche di importo pari ad Euro 2.490,00 ciascuna e n. 1 bonifico istantaneo per l'importo di Euro 1.499,60; conto *132: n. 1 ricarica di importo pari ad Euro 2.490,00), si rileva preliminarmente che nei moduli di disconoscimento allegati risulta presente evidenza solo delle operazioni effettuate a valere sul conto *888, ossia tre ricariche e il bonifico istantaneo; sul punto si segnala altresì che l'intermediario, nelle controdeduzioni, afferma che il conto *132 è intestato unicamente alla moglie del ricorrente, cointestataria del ricorso. La questione viene quindi esaminata solo con riguardo alle contestate operazioni relative al conto *888. In proposito, parte resistente ha prodotto evidenze delle operazioni disconosciute, volte a fornire la prova dell'insussistenza di malfunzionamenti nei dispositivi di pagamento nonché della corretta

registrazione e autenticazione delle stesse. Sulla base di tale documentazione esso fornisce l'analitica descrizione dell'iter che ha portato al perfezionarsi degli addebiti. Accertato che il file *Excel* allegato dall'intermediario non è modificabile, si evince che le tre ricariche ed il bonifico istantaneo sono stati validati mediante inserimento corretto dei relativi *OTP push* e *OTS sms*, anche se dopo una serie di annullamenti e di inutili invii.
Relativamente alla diligenza del cliente, l'intermediario sostiene che il suo comportamento sia stato improntato a colpa grave avendo fornito a terzi estranei i propri codici personali e le *password* dinamiche inviate tramite notifica *push* sul *device* o via sms (OTP e OTS). In proposito, si constata che è lo stesso ricorrente a dichiarare di aver scaricato un'applicazione cliccando su un *link* indicatogli in un sms, di avere poi seguito le istruzioni impartitegli via telefono da un sedicente operatore dell'intermediario, comunicando i codici pervenuti via sms, ritenendo trattarsi dei codici necessari a bloccare le segnalate transazioni fraudolente. A sua discolpa sostiene, tra l'altro, che il sms civetta risultava in apparenza proveniente dall'intermediario, analogamente alla successiva telefonata, ma non produce evidenze in proposito, il che impedisce di verificare l'attendibilità del mittente e del contenuto del messaggio e, quindi, di valutare se sia o meno creato un possibile affidamento dell'utente circa la genuinità del messaggio e della telefonata. Quanto alla comunicazione dei codici al sedicente operatore, afferma che aveva ritenuto trattarsi dei numeri necessari a bloccare le transazioni fraudolente, come segnalatole dall'interlocutore, nonostante la diversa informazione contenuta nelle notifiche *push* e negli sms che contenevano una chiara descrizione delle attività e della natura delle operazioni da autorizzare.
Dalla ricostruzione dei fatti sopra esposta si deve concludere che il ricorrente sia stato vittima di un *smishing* misto a *vishing*, ovvero di *phishing* perpetrato a mezzo chiamata telefonica realizzata con tecnica *spoofing*, schemi ormai tradizionali di frode, consistenti nell'indurre il titolare dello strumento di pagamento, tramite chiamate o sms apparentemente riconducibili all'intermediario, a comunicare o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza.
Accertata la colpa grave del ricorrente, ad attenuare la palese violazione da parte dello stesso degli obblighi - previsti negozialmente ed imposti dalle disposizioni sopra richiamate - di custodia dei dispositivi statici e dinamici ad esso affidati per l'uso dello strumento di pagamento, può rilevare la circostanza che le quattro operazioni contestate (le tre ricariche ed il bonifico istantaneo) sono state poste in essere in un lasso di tempo brevissimo, considerando che richiedevano anche l'inserimento di codici autorizzativi in sequenza trasmessi con notifica *push* sul *device* e via sms e che tutte le notifiche push inviate sono state precedute da almeno una notifica *push* annullata e relativa alla medesima operazione poi autorizzata. Trattandosi di una tempistica alquanto anomala, ciò avrebbe dovuto comportare da parte dell'intermediario, oltre all'avvenuto invio dei codici OTS (essendo le attività state considerate dal sistema come sospette), ulteriori misure "protettive" per assicurare un effettivo controllo circa l'identità dell'autore dei pagamenti, indipendenti da quelle già utilizzate per l'autenticazione, come ad esempio predisporre cautelativamente l'immediato blocco delle operazioni valutate come sospette e, di seguito, contattare direttamente il cliente.
Ravvisandosi, quindi, un concorso di colpa da parte dell'intermediario, si ritiene che la domanda del ricorrente, con riguardo alle operazioni disconosciute poste in essere sul conto *888 possa essere accolta in modo parziale nella misura del 50%, con conseguente riconoscimento di un rimborso pari ad € 4.485,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.485,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese di procedura, e alla parte ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA