COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 28/09/2023

FATTO

Il cliente nel ricorso afferma che/di:
- alle ore 14.00 del 14/03/2023 riceveva un sms che sembrava provenire dall'intermediario;
- con l'sms gli veniva comunicato che risultava un accesso anomalo all'*home banking* e veniva invitato a cliccare su un *link*;
- cliccava sul link e veniva indirizzato ad una pagina in cui inseriva il numero di cellulare;
- successivamente, riceveva una chiamata proveniente da un'utenza fissa, da un soggetto che si qualificava come operatore dell'intermediario;
- il sedicente operatore invitava il cliente a scaricare un'applicazione sul cellulare;
- dopo aver installato la predetta applicazione, il cellulare sembrava essere oggetto di scansione e il cliente non era più nelle condizioni di gestire lo stesso;
- durante questa presunta scansione, il cliente riceveva una notifica relativa all'effettuazione di un bonifico;
- veniva tuttavia rassicurato dall'operatore che spiegava la notifica ricollegandola alle verifiche che stava effettuando la banca; un successivo sms confermava quanto detto dall'operatore;

- terminata la scansione, il cellulare tornava di nuovo utilizzabile e l'operatore fissava un appuntamento per il giorno successivo al fine di terminare la procedura iniziata, invitando il cliente a non utilizzare l'applicazione della banca;
- il giorno successivo veniva contattato dallo stesso operatore, il quale fissava un ulteriore appuntamento;
- non avendo ricevuto ulteriori telefonate, il cliente contattava il numero verde dell'intermediario e scopriva di essere stato vittima di una truffa;
- procedeva a presentare denuncia presso le Autorità;
- presentava reclamo all'intermediario che rispondeva negativamente.

In conclusione il Cliente chiede il rimborso della somma relativa all'operazione contestata.

L'intermediario, riportato il fatto, afferma che:
- il ricorrente è intestatario di un conto corrente cui è collegato il servizio di cd. *home banking*;
- il ricorrente aveva aderito al servizio SMS alert;
- l'accesso alle citate funzioni di *inquiry* e dispositive prevede un sistema di autenticazione forte;
- in presenza di un sistema in astratto valutabile come sicuro, si deve presumere la negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento;
- dalle dichiarazioni di natura confessoria del ricorrente, si evince che lo stesso abbia di fatto consegnato il suo strumento di pagamento al truffatore;
- è risaputo che il caller ID non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul *display*;
- la nuova app scaricata dal ricorrente non è palesemente riconducibile all'intermediario;
- è plausibile ritenere che per scaricare l'app sia stato necessario digitare le credenziali di sicurezza dell'*home banking*;
- il cliente è stato vittima di *phishing*, tramite *vishing*: assecondando acriticamente le richieste del suo interlocutore, il ricorrente ha vanificato qualsiasi presidio di sicurezza posto in essere dalla Banca;
- sussiste la colpa grave del cliente per non aver monitorato il proprio conto corrente subito dopo la prima telefonata;
- l'operazione è stata correttamente contabilizzata, registrata e autenticata;
- la notifica push e l'sms alert risultano regolarmente consegnati;
- la banca è intervenuta ad inviare la richiesta di restituzione alla banca corrispondente;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

In conclusione, l'Intermediario chiede il rigetto del ricorso.

DIRITTO

La questione in oggetto riguarda un'operazione contestata per un importo di € 17.500,00 effettuata in data 14/03/2023. Si tratta di un bonifico online.

Si osserva innanzitutto che l'operazione contestata è stata effettuata in vigenza del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D. Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).

Sulla base della normativa sopra indicata, in primo luogo è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore (cfr. art. 10, comma 2 del decreto legislativo n. 11/2010, secondo cui *"l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento …. non è di per sé necessariamente*

sufficiente a dimostrare che (...) questi [il cliente] 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"). In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo e alla frode, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. Si fa presente che - sulla materia in esame - si è recentemente pronunciato il Collegio di Coordinamento (Decisione n. 22745/19 del 10.10.2019), ove viene enunciato il seguente principio interpretativo: "*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".*

Sotto il primo profilo, l'Intermediario non produce adeguata prova della contabilizzazione, registrazione e autenticazione dell'operazione contestata.

Dalle evidenze prodotte si rileva che:

- l'id utente riportato nel log corrisponde al numero cliente riferito dall'intermediario nelle controdeduzioni (numero cliente 23*****536) e risulta essere identico in tutte le varie fasi;
- si evidenziano 3 distinti log in, di cui gli ultimi due (effettuati alle 15:29 e alle 15:43) risultano realizzati da un indirizzo IP diverso da quello del primo log in, avvenuto prima della ricezione dell'sms civetta;
- tutti e 3 gli accessi risultano effettuati dallo stesso device indentificato col nome "m32" (compatibile con l'ipotesi di utilizzo da remoto del device del cliente da parte dei truffatori, a seguito dell'installazione di app malevole);
- i 2 accessi delle ore 15:29 e 15.43 risulterebbero realizzati tramite PIN e OTP da *mobile token*;
- risulta evidenza dei codici OTP utilizzi.

Quanto invece all'inserimento del PIN, nei log prodotti non vi è evidenza del relativo inserimento; il suo impiego è infatti descritto unicamente nella colonna "attività utente".

In mancanza della prova dell'inserimento del PIN questo Collegio accoglie il ricorso, reputando non provata l'effettiva adozione di un sistema di autenticazione forte.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 17.500,00.

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 della 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