COLLEGIO DI MILANO

composto dai signori:

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

Relatore MARINA SANTARELLI

Seduta del 05/09/2024

FATTO

Parte ricorrente agisce per ottenere il rimborso di € 20.000,00 oggetto di operazioni fraudolente a suo danno prospettando la seguente ricostruzione dei fatti e argomenti.
Alle ore 16.38 del 22/11/2023 parte ricorrente riceveva un sms che la informava di un accesso da un dispositivo non riconosciuto e la invitava a cliccare su un link.
Parte ricorrente, nonostante il messaggio sembrasse provenire dall'intermediario, non vi dava seguito. Dopo circa mezz'ora, riceveva una telefonata da un soggetto qualificatosi operatore dell'intermediario, che gli chiedeva se avesse ricevuto o meno un SMS di disconoscimento. Parte ricorrente confermava al sedicente operatore di non aver effettuato alcun bonifico di € 10.000,00 e riceveva un ulteriore SMS che comunicava che il pagamento era stato cancellato correttamente e ne avrebbe ricevuto il riaccredito entro 24 ore.
Durante la medesima telefonata a parte ricorrente pervenivano altri messaggi contenenti codici autorizzativi di operazioni dispositive; tali sms gli venivano preannunciati dal sedicente operatore, che chiedeva conferma della relativa ricezione e annunciava che l'operazione di annullamento si sarebbe chiusa entro le ore 8.00 del giorno successivo.
Il giorno dopo, il 23/11/2023 alle ore 8.00, riceveva un altro sms apparentemente proveniente dall'intermediario, con un codice relativo ad un bonifico di € 10.000,00: secondo l'operatore, tale codice era necessario per il riaccredito dei 10.000,00 €

precedentemente sottratti. Tuttavia, emergeva in seguito che detto codice serviva per un altro bonifico fraudolento. Sempre il 23/11/2023 parte ricorrente effettuava altre telefonate all'intermediario, per rimarcare di non aver effettuato bonifici dal proprio conto corrente, Parte ricorrente riusciva infine ad accedere al conto, a verificare il saldo e ad effettuare il disconoscimento dei due bonifici fraudolenti.
Deduce parte ricorrente di essere stato vittima di una truffa informatica particolarmente raffinata, realizzata mediante l'invio di messaggi (che comparivano nella stessa chat in cui abitualmente si collocavano le comunicazioni della banca) e telefonate da canali apparentemente ufficiali e che non ha posto in essere nessun tipo di protezione o tentativo di recupero delle somme sottratte (nonostante il conto di destinazione dei bonifici fraudolenti fosse aperto presso l'intermediario stesso).
L'intermediario chiede il rigetto del ricorso in quanto: (a) le operazioni sono state correttamente contabilizzate, registrate e autenticate con il corretto inserimento delle credenziali; (b) sussiste la colpa grave di parte ricorrente, che ha condiviso con i truffatori username e password per accedere all'area riservata e i codici OTP necessari ad autorizzare gli ordini di bonifico; (c) l'intermediario mette a disposizione dei propri clienti numerosi contenuti in materia di sicurezza informatica, ivi incluso un contenuto dedicato alle frodi perpetrate mediante la tecnica del c.d. *vishing*; (d) gli SMS contenenti le OTP riportavano con chiarezza la finalità di utilizzo di ciascun codice; (e) il testo dell'SMS truffaldino ricevuto, incluso il link di cui si richiedeva l'apertura, risultava evidentemente sospetto.
Parte ricorrente ha replicato per osservare che: (i) il proprio comportamento non può essere considerato gravemente colposo: proprio perché, edotto dalle campagne informative dell'intermediario, non ha cliccato sul link del primo messaggio ricevuto; (ii) ha dato credito ad una telefonata pervenuta dagli stessi contatti telefonici che di solito utilizza la banca, in cui si paventava un accesso indebito da parte di terzi nel proprio conto corrente; (iii) non ha fornito codici PIN per l'accesso all'*homebanking*; (iv) non si è in presenza di *vishing*, ma del più sofisticato *caller id spoofing*; (v) l'intermediario non ha inviato alcun avviso relativo all'accesso da un dispositivo non autorizzato e diverso da quelli usuali, né alcun messaggio di *alert* in tempo utile ad evitare la truffa.
L'intermediario ha a sua volta controreplicato quanto segue: (a) gli ordini di bonifico sono stati disposti in favore di un altro conto corrente aperto presso la banca convenuta e dunque non richiedendo la trasmissione dell'ordine di pagamento ad un prestatore di servizi di pagamento terzo; pertanto le operazioni sono state eseguite istantaneamente con l'effetto che non potevano più essere revocate al momento della segnalazione del cliente; (b) peraltro, una volta accreditati sul conto corrente del beneficiario, gli importi sono stati distratti mediante pagamenti con carta e bonifici nel medesimo giorno di accredito, impedendo alla banca di recuperare le somme oggetto di frode.

DIRITTO

I principi che regolano la materia delle operazioni fraudolente, ormai noti e reiteratamente richiamati da questo Arbitro, sono racchiusi nelle disposizioni del D. Lgs. 27.1.2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011. Disposizioni che fissano due passaggi ineludibili che attengono al piano degli oneri probatori: (a) è l'intermediario a dover provare (oltre alla l'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute; (b) 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, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
In particolare, per quanto concerne la SCA, è bene ricordare che, ai sensi delle disposizioni che disciplinano la materia (cfr. artt. 97 e 98 della PDS2, art. 10 bis del D. Lgs. 11/2010, norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché criteri interpretativi forniti dal parere dell'EBA del 21 giugno 2019), la SCA è richiesta quando il cliente (a) accede al suo conto di pagamento online; (b) dispone un'operazione di pagamento elettronico; (c) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi (ad esempio, *l'enrollment* di un diverso *device*).
Dunque, la prova dovuta dall'intermediario – con adeguata spiegazione dei log e della ulteriore documentazione prodotta (cfr. Collegio di coordinamento, decisione n. 22745/2019) deve essere fornita per tutti i passaggi che hanno reso possibile l'operazione disconosciuta.
Venendo al caso di specie, la materia del contendere si incentra su due bonifici per l'importo complessivo di € 20.000,00 effettuati il 22/11/2023 alle ore 17.28 ed il 23/11/2023 alle ore 8.07. Con riferimento alla fase di accesso all'area riservata, l'intermediario afferma che l'autenticazione forte avviene mediante inserimento delle credenziali statiche scelte dal cliente ed OTP trasmesso via SMS, validato la prima volta che il cliente accede e successivamente solo qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha effettuato l'accesso al conto con autenticazione forte. In aderenza a tale premessa, quanto ai due accessi antecedenti all'esecuzione delle operazioni contestate, l'intermediario produce documentazione da cui si apprende che: (a) il primo accesso all'area riservata del 22/11/2023 alle ore 17:23 è stato effettuato da un indirizzo IP diverso da quello ordinariamente utilizzato dal cliente ed è avvenuto mediante inserimento di username e password scelti dal cliente in fase di apertura del conto corrente (cfr. riga 61, colonna "*Medio de autentificación*" = "*02*" e colonna "*Tipo Trans.*" = "*solicitarTicketConsumoAPI*"); (b) il secondo accesso al conto corrente del 23/11/2023, quando è stato disposto il secondo ordine di bonifico, è stato effettuato alle ore 07:52 mediante inserimento di username e password (cfr. riga 51, colonna "*Medio de autentificación*" = "*02*" e colonna "*Tipo Trans.*" = "*solicitarTicketConsumoAPI*"). In entrambi i casi, dunque, non risulta l'inserimento dell'OTP (elemento di possesso), ma solo quello di *username* e *password* (elemento di conoscenza), in quanto l'ultimo accesso all'area riservata mediante autenticazione forte (e quindi inserimento di OTP inviata via SMS al numero di telefono validato dal cliente) è avvenuto in data 06/09/2023 alle ore 18:58, e cioè meno di 180 giorni prima della frode. Sostiene, in proposito, l'intermediario che l'art. 10 del Regolamento delegato (UE) 2018/839 disporrebbe una deroga consentendo, all'interno di un arco temporale di 180 giorni, l'accesso senza autenticazione forte per le "*seguenti informazioni: saldo del conto; operazioni di pagamento eseguite negli ultimi 180 giorni*". Tuttavia, tale interpretazione dell'art. 10 della PSD2 non può essere condivisa: la disposizione in esame, infatti, limita l'esenzione della SCA solo ad accessi di tipo meramente informativo (e non dispositivo come nella specie) e, comunque, quanto alle operazioni di pagamento "*eseguite negli ultimi 90 giorni*".
Essendo provato (ed anzi dichiarato dallo stesso intermediario) che gli accessi prodromici alle operazioni disconosciute non sono stati effettuati mediante SCA (cfr. sul punto anche Collegio di Milano, decisione n. 8151/2024, in cui è stata prodotta la medesima documentazione), il ricorso non può che essere accolto, essendo principio pacifico, in aderenza al dato normativo, che la prova dell'autenticazione forte rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente. Il che, appunto, esime

sia dall'esame della prova della sussistenza della SCA in relazione alle due operazioni disconosciute sia di quella relativa all'eventuale colpa grave di parte ricorrente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 20.000,00.
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