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) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CETRA

Seduta del 23/09/2024

FATTO

Con ricorso dell'11 maggio 2024, parte ricorrente, esponeva di avere ricevuto, in data 28.11.2023, alle ore 16.11, due messaggi di testo apparentemente provenienti dall'intermediario convenuto, uno in spagnolo e uno in italiano, che la informavano di un accesso insolito al proprio account e la invitavano a cliccare su un link al fine di compilare un modulo di disconoscimento; di aver ignorato i due messaggi, ma contestualmente riceveva una chiamata dal numero 02***081: l'interlocutore, presentandosi quale dipendente dell'intermediario, la invitava a cliccare sul link, ad inserire i propri dati bancari – inclusa la password – e a disinstallare l'applicazione della banca; insospettitasi, contattava immediatamente la stessa banca al numero verde, per riferire quanto accaduto; l'operatore le comunicava di aver bloccato il conto corrente e le garantiva che, in questo modo, non poteva essere eseguita nessuna operazione correlata al medesimo. Nonostante le rassicurazioni, in data 1.12.2023 - a seguito della procedura di sblocco del conto - constatava che il 28.11.2023 erano stati effettuati un bonifico dell'importo di € 900,00 ed un pagamento di € 2.900,00 tramite carta di debito; lamentava che l'importo del pagamento fosse superiore al limite giornaliero di spesa di € 2.000,00 previsto nel contratto della carta di debito e di non aver ricevuto alcun messaggio di alert dopo la prima operazione; rappresentava di aver ottenuto già il rimborso del bonifico di € 900,00, ma non

dell'altra operazione di € 2.900,00. Rappresentava di aver presentato denuncia alle autorità di pubblica sicurezza e reclamo all'intermediario, che veniva riscontrato negativamente. Pur ammettendo di avere cliccato sul link inviatole nella chat sms della banca in buona fede e di aver segnalato tempestivamente a quest'ultima quanto le era successo, riteneva che l'operatività non autorizzata fosse stata conseguenza di una perdita di dati personali imputabile all'intermediario e all'evidente inadeguatezza del suo sistema informatico. La ricorrente, pertanto, attivava il presente procedimento per chiedere all'Arbitro di condannare l'intermediario a restituire gli importi illegittimamente sottratti pari ad euro 2.900,00. Chiedeva, inoltre, il rimborso delle spese legali anche in via equitativa.

L'intermediario, nelle controdeduzioni, eccepiva che le operazioni erano state correttamente contabilizzate, registrate e autenticate in quanto realizzate con il corretto inserimento delle credenziali; che sussisteva la colpa grave della cliente, per aver violato l'obbligo di adottare tutte le ragionevoli misure idonee a proteggere le proprie credenziali di sicurezza. Aggiungeva, poi, che la banca aveva messo a disposizione dei propri clienti numerose informazioni in materia di sicurezza informatica e, nello specifico, avvertimenti relativi alle frodi perpetrate mediante la tecnica del c.d. vishing; aggiungeva che, il giorno della frode, avrebbe inviato alla cliente via e-mail e via notifica push in app diverse segnalazioni di accesso all'area riservata da una posizione insolita, di accesso mediante un nuovo dispositivo e di avvio del processo per l'attivazione della conferma tramite token. L'intermediario, per tutto questo, chiedeva di non accogliere il ricorso.

La ricorrente, nelle repliche, rilevava che l'intermediario non avrebbe provato la sua colpa grave; ribadiva di non essere stata informata dall'operatore su tutti i rischi ai quali era potenzialmente esposta a seguito dell'accesso ai dati sensibili del proprio conto da parte di terzi, ivi inclusi quelli relativi alla carta di debito; negava di aver mai ricevuto le e-mail contenenti avvertimenti e consigli sull'utilizzo del proprio conto corrente e della propria carta di debito; sosteneva che l'intermediario non aveva provato di aver adottato idonee misure di sicurezza, come l'invio di SMS alert per le singole operazioni compiute.

L'intermediario, nelle controrepliche, precisava che le operazioni di pagamento oggetto di frode erano state realizzate prima che la cliente provvedesse a contattare il servizio clienti della banca: il pagamento con carta di € 2.900,00, veniva autorizzato alle ore 16.44 del (del 28.11.2023), mentre il bonifico di € 900,00 alle ore 16.48 (sempre del 28.11.2023), il contatto con il servizio clienti si verificava, invece, alle ore 16.49 (dello stesso giorno). E successivamente alla chiamata della cliente, la banca provvedeva in via cautelativa a bloccare il conto corrente, cosa avvenuta alle ore 17.03.

DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte attraverso un pagamento avvenuto mediante carta di debito appoggiata sul conto corrente intestato alla ricorrente. L'operazione contestata, di importo pari ad euro 2.900,00, è avvenuta il 28.11.2023 alle ore 16.44. Essa è stata disconosciuta dalla ricorrente, sicché deve soddisfare l'onere probatorio previsto dal d. lgs. 27.1.2010, n. 11 di recepimento della Direttiva 2007/64/CE sui servizi di pagamento (PSSD), come modificata dal d. lgs. 15 dicembre 2017, n. 218, di recepimento della Direttiva 2015/2366/UE (PSSD-II).

Il Collegio ricorda che, per la normativa appena richiamata, la corretta esecuzione di un'operazione di pagamento è subordinata al consenso del pagatore (art. 5 d. lgs. 11/2010), prestato nella forma e secondo la procedura contrattualmente prevista. Qualora

l'utente neghi di aver autorizzato l'operazione o sostenga che questa non sia stata correttamente eseguita, lo stesso può ottenerne il rimborso dell'importo (art. 11 d. lgs. 11/2010), a meno che il prestatore dei servizi di pagamento non riesca a provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10, comma 1, d. lgs. 11/2010). Il prestatore dei servizi, peraltro, assolto con successo questo primo onere, necessario ma di per sé insufficiente a dimostrare che l'operazione sia stata autorizzata dal titolare, deve ancora provare, al fine dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento, fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010, trattandosi primariamente di obblighi di custodia del dispositivo e delle chiavi di accesso al servizio. La valutazione della condotta dell'utilizzatore, ai fini dell'eventuale giudizio di colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.

Il Collegio ricorda, inoltre, che la suddetta autenticazione si deve realizzare in forma di autenticazione forte (c.d. strong customer authentication in acronimo SCA), secondo quanto stabilito dagli artt. 97 e 98 della PDS2, dall'art 10-bis del d. lgs. 10/2011 e nelle 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 nei criteri interpretativi forniti dallo stesso EBA. E questo sia nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni: l'autenticazione, in tutti questi casi, richiede almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso; gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Il Collegio, venendo allo specifico caso oggetto di decisione, rileva che l'intermediario sostiene che il primo accesso all'area riservata sia avvenuto da un indirizzo IP e da un dispositivo diversi da quelli ordinariamente utilizzati dalla cliente e che il dispositivo sia stato registrato alle ore 16.38 del 28.11.2023 mediante inserimento di username e password scelti dalla cliente in fase di apertura del conto corrente. Aggiunge che l'ultimo accesso all'area riservata mediante autenticazione forte precedente a quello controverso sia avvenuto in data 06.11.2023 alle ore 17.18, realizzato mediante inserimento di username e password e inserimento di OTP inviata via SMS al numero di telefono validato dal cliente. Di quest'ultimo accesso allega evidenze. L'intermediario asserisce che poiché tale accesso era stato eseguito da meno di 180 giorni, gli accessi registrati il 28.11.2023 non avevano richiesto l'applicazione del secondo fattore di autenticazione ai sensi della deroga prevista dall'art. 10 del Regolamento delegato (UE) 2018/839; sicché, sulla base delle allegazioni e delle affermazioni dell'intermediario, risulta che il primo accesso dal dispositivo dei truffatori sia stato autorizzato con il solo inserimento di username e password (elemento di conoscenza). L'intermediario compie una non condivisibile interpretazione dell'art. 10 del Reg. Delegato UE 2018/839, secondo la quale l'autenticazione forte sarebbe necessaria soltanto qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha fatto accesso al conto mediante SCA. Si tratta, infatti, di una interpretazione che confligge con quanto stabilito dagli artt. 97 e 98 della PDS2, dall'art 10-bis del d. lgs. 10/2011 e nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Reg. Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dallo stesso EBA che, come sopra ricordato, esigono il doppio fattore anche in fase di accesso/enrollment nel caso in cui, come quello in esame, a questa segua un'attività

dispositiva (l'eccezione consentita dall'art. 10 del Reg. Delegato UE 2018/839 si riferisce all'accesso successivo ad uno già avvenuto nei 90 giorni precedenti ma solo per fini conoscitivi e non dispositivi).

Ne consegue che, nel caso di specie, a nulla rileva che in data 6.11.2023 la cliente aveva autorizzato l'accesso con doppio fattore, mediante inserimento delle credenziali statiche (elemento di conoscenza) e dell'OTP (elemento di possesso), poiché la doppia autenticazione avrebbe dovuto essere richiesta anche nell'accesso del 28.11.2023, in quanto prodromico ad un'attività dispositiva (quella, cioè, rilevatasi fraudolenta). La mancata evidenza dell'ulteriore fattore di autenticazione (oltre a quello di possesso) non consente, pertanto, di ritenere raggiunta la prova della SCA con riguardo alla fase di login: prova che, in aderenza al dato normativo più sopra descritto, rappresenta un antecedente logico rispetto alla colpa grave dell'utente, sulla quale, pertanto, ai fini della presente decisione, non è necessario soffermarsi.

Il Collegio, in definitiva, non può che rilevare, alla luce della documentazione prodotta dall'intermediario, come non sia stata provata la SCA (nello stesso senso, si veda Coll. Milano, decisione n. 8151/24 del 13/07/2024). E in assenza di SCA l'intermediario è tenuto a sopportare l'intero costo dell'operazione, con la conseguente restituzione al ricorrente dell'importo indebitamente sottratto e dallo stesso domandato, che nel caso specifico ammonta ad euro 2.900,00.

Non può trovare, invece, accoglimento la richiesta di refusione di spese legali, poiché dinanzi a questo Arbitro non è richiesto il patrocinio di un difensore: là dove il ricorrente decida di avvalersene, quindi, non può che restare a suo carico la relativa spesa; a ciò si aggiunga, nel caso di specie, la natura seriale della questione, che contribuisce a rendere ancor meno necessario il ricorso all'assistenza tecnica.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.900,00.
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