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) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CETRA

Seduta del 23/07/2024

FATTO

Con ricorso del 5 maggio 2024, parte ricorrente rappresentava quanto segue: in data 20 febbraio 2024, nel primo pomeriggio, riceveva una chiamata, avente il logo figurativo dell'intermediario convenuto, dal numero "ufficio frodi" dello stesso; l'interlocutore, qualificatosi come operatore dell'intermediario, conosceva già i dati personali del cliente e ne chiedeva la solo conferma; ricevuta la quale, l'interlocutore proseguiva ad informarlo circa l'emissione di un bonifico dal valore di € 4.900,00, partito dal conto corrente del cliente che presentava indici di anomalia; pertanto, il sedicente interlocutore chiedeva conferma ed autenticità dell'operazione, che il cliente si apprestava a disconoscere.

A quel punto, il sedicente operatore informava il cliente della presenza di un virus informatico nel suo telefono ed era pertanto necessario, per tutelarsi, scaricare un'applicazione per debellarlo; lo invitava per tanto a scaricare detta applicazione attraverso un link, che, però, nonostante i diversi tentativi fatti, non riusciva ad installare poiché fermata dall'antivirus.

Il sedicente interlocutore tranquillizzava il cliente informandolo che avrebbe provato lui a scaricare l'applicativo da remoto e lo informava che l'applicazione principale dell'intermediario sarebbe stata bloccata perché quest'ultima veniva sottoposta a pulizia dai virus; prima di far partire le operazioni di pulizia da remoto, il sedicente interlocutore

invitava a confermare l'ultimo movimento autorizzato dal cliente stesso. Il cliente accedendo dal cellulare, che riporta codice cliente e password oscurato, seguiva le istruzioni impartite dall'interlocutore senza fornire le proprie credenziali; il sedicente interlocutore, a questo punto lo invitava a non accedere all'applicazione principale dell'intermediario per 24 ore e lo rassicurava che lo avrebbero tenuto informato ed aggiornato attraverso molteplici chiamate durante la giornata.

Le chiamate, ricevute effettivamente durante la giornata, rassicuravano il cliente circa la buona riuscita di installazione dell'applicazione antivirus; in serata, probabilmente verso le ore 17:00, il cliente veniva ricontattato per essere rassicurato che le operazioni di pulizia erano ancora in corso. Queste chiamate seguitavano anche il girono successivo, il 21 febbraio 2024, in più momenti della giornata, circostanza che ingenerava affidamento in capo al cliente; il giorno successivo, ossia il 22 febbraio 2024, non riuscendo nuovamente ad accedere all'applicazione principale dell'intermediario, il cliente ricontattava il numero dell'intermediario e veniva a conoscenza della truffa subita consistente nell'emissione di un bonifico dal valore di € 49.801,00, senza ricevere alcun dettaglio, in merito alla causale o al beneficiario.

L'operatore allo sportello invitava il cliente a denunciare il fatto alle autorità e ad esporre reclamo agli uffici competenti; nessun aiuto o collaborazione perveniva dall'operatore dell'intermediario; sottolineava di non aver ricevuto alcun SMS di conferma di esecuzione bonifico sul suo numero telefonico e che nel corso degli oltre quarant'anni di rapporto con la filiale non aveva mai effettuato bonifici di tale importo oltremodo a beneficio di soggetti collocati a oltre duemila km di distanza e non era in alcun modo a conoscenza di avere un massimale giornaliero così elevato: il suo abituale utilizzo della remote banking si esauriva con l'esecuzione di pochi bonifici all'anno di modici importi.

Rappresentava l'anomalia dell'operazione effettuata, soprattutto tenendo in considerazione lo storico dell'entità delle operazioni e l'ammontare dello stipendio percepito dal cliente. In ragione di ciò, l'operazione potrebbe essere qualificata come operazione sospetta ai sensi dell'art. 35 del d. lgs 231/2007; segnalava, inoltre, che da fine febbraio 2024 erano comparse in rete molteplici notizie riguardanti questa metodologia nuova di attacco informatico o malware e solo nel mese di marzo gli istituti di credito avevano palesato sulla propria home page specifici messaggi di allerta, indicando in dettaglio il tipo di truffa che stava emergendo.

Lamentava, infine, la scarsa stabilità e sicurezza del sistema informatico dell'intermediario. Il ricorrente, per tutto questo, attivava il presente procedimento per chiedere all'Arbitro di condannare l'intermediario a restituire gli importi illegittimamente sottratti pari ad Euro 49.801,00.

L'intermediario, nelle controdeduzioni, eccepiva la colpa grave del ricorrente per aver confidato nella genuinità di una telefonata da parte di persona a lui sconosciuta e per averne seguito le istruzioni, affidandosi a quanto veniva riferito al telefono, senza avere ricevuto alcuna comunicazione ufficiale e preventiva; precisava che le operazioni, sia di attivazione del mobile token, sia di *login*, che di bonifico, risultavano correttamente autenticate, registrate ed eseguite mediante un sistema di autenticazione "forte", senza che fosse emerso alcun malfunzionamento o compromissione dei sistemi, in linea con la normativa Europea PSD2.

Proseguiva che la colpa grave del ricorrente era idonea a spezzare il nesso di causalità tra l'evento dannoso e la condotta dell'autore dell'attività pericolosa poiché, seguendo acriticamente e colpevolmente le richieste del suo interlocutore, egli aveva vanificato qualsiasi presidio di sicurezza, diventando, così, l'unico responsabile del danno; contestava che il ricorrente non avesse allegato alcuna evidenza probatoria né dell'eventuale SMS civetta né dell'eventuale link malevolo né della cronologia delle possibili conversazioni telefoniche a dimostrazione dei fatti sommariamente narrati, con ciò venendo meno all'onere probatorio ex lege; che a fronte dell'operatività disconosciuta l'intermediario aveva inviato sul cellulare del ricorrente le notifiche *push* e gli SMS alert che risultavano regolarmente consegnati e aveva avviato tempestivamente l'azione di recall verso la banca del beneficiario, che purtroppo aveva avuto esito negativo. L'intermediario, per tutto quanto precede, chiedeva di non accogliere il ricorso.

Parte ricorrente, con le repliche, eccepiva che, dalle controdeduzioni non si comprendeva chiaramente il sistema di autenticazione definito forte; il codice OTP generato, in un primo momento veniva definito silente e poi si negava tale caratteristica; per effettuare le transazioni nell'applicazione era sufficiente immettere il solo PIN.

Nei *log*, erano riportati accessi da lui effettuati in data 16.2.2024 per una ricarica di una carta prepagata in cui si citavano OTP da lui mai digitati personalmente, probabilmente perché silenti; in data 20.2.2024 venivano segnalati accessi con IP diversi dai suoi e alle ore 16:35 sembrava essere stato effettuato il bonifico fraudolento. Aggiungeva, inoltre, che in data 3 marzo 2024 si era anche attivato per avere evidenza degli SMS dal proprio operatore telefonico, ma stante la necessità di avere supporto legale, che in quel momento di estrema difficolta economica non si poteva permettere, aveva infine desistito; in merito al recall del bonifico, si richiedeva di avere evidenza di quanto affermato dall'intermediario. Insisteva nella domanda espressa nel ricorso.

DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte attraverso un bonifico istantaneo che ha interessato il conto corrente intestato al ricorrente. L'operazione contestata, di importo pari ad Euro 49.800,00 (più 1 Euro di commissioni), è avvenuta il 20.2.2024, alle ore 16.40. Non è, peraltro, chiaro se detta operazione sia stata interamente compiuta dalla parte ricorrente o se sia stata realizzata solo in parte da questa (e, dunque, per altra parte dal truffatore). Nel dubbio, pertanto, l'operazione deve essere qualificata come "disconosciuta" e deve sottostare all'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 regolamenta-zione 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 le operazioni siano state correttamente registrate, autenticate e contabilizzate ed eseguite dall'APP installata sul device del cliente con il doppio fattore di autenticazione: Token + PIN e autorizzate con OTP silente generato dall'applicazione a seguito di "*tap*" sulla notifica apparsa sul device e contenente gli estremi dell'operazione inserita. Il Collegio, a questo proposito, rileva che, quanto al *login* prodromico all'operazione disconosciuta, l'intermediario ha affermato che l'accesso all'home banking è stato eseguito alle ore 16:35:06 del 20.2.2024 con ID utente e Pin e generazione in app dell'OTP c.d. silente. Non produce, tuttavia, diretta evidenza dell'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione attività dell'utente, mentre la colonna "esito operazione" non risulta in alcun modo valorizzata. Il Collegio ha rilevato, inoltre, la mancanza di prova dell'inserimento del PIN pure nella fase dispositiva dell'operazione: lacuna assai significativa, là dove si consideri che il ricorrente, in sede di ricorso, ha affermato di non aver fornito al sedicente incaricato alcun codice OTP e/o *password*.

La mancata evidenza dell'effettivo inserimento del codice PIN e, quindi, di un fattore di autenticazione (fattore di conoscenza), non consente di ritenere raggiunta la prova della SCA: prova che, in aderenza al dato normativo più sopra descritto, rappresenta un antecedente logico rispetto alla colpa grave dell'utente, sulla quale non è, dunque, necessario soffermarsi. Va, comunque, rilevato che, dalla documentazione in atti, non si comprende come sia stato possibile disporre un'operazione di un importo così tanto elevato, posto che i massimali giornalieri (oltreché mensili) risultanti dalle pattuizioni contrattuali si attestano ben al di sotto.

Ne consegue, in definitiva, che, 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, che nel caso specifico ammonta ad Euro 49.800,00 oltre 1 Euro per commissioni.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 49.801,00.
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