Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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) ANTONIO CETRA

Seduta del 23/09/2024

FATTO

Con ricorso del 30 maggio 2024, parte ricorrente riferiva che, in data 02.11.2023, alle ore 10:32, riceveva un messaggio apparentemente riconducibile all'intermediario convenuto, contenente un link; controllava l'applicazione di home banking e questa risultava bloccata: per tale motivo apriva il link che gli era stato inviato. Telefonava, a quel punto, alla filiale dell'intermediario per riferire l'accaduto e si avvedeva che dal proprio conto era stata sottratta la cifra di € 37.414,56: erano stati, in particolare, realizzati n. 40 pagamenti tutti allo stesso beneficiario. Riferiva di avere subito disconosciuto le operazioni, ma l'intermediario aveva dato riscontro negativo, come pure, in seguito, aveva rigettato il reclamo. Lamentava che le operazioni contestate si differenziassero notevolmente dalla sua abituale operatività - ben conosciuta dall'intermediario - che di regola realizzava solo due o tre bonifici all'anno: uno dei pagamenti, dell'importo di € 5.329,00, superava, peraltro, i massimali relativi alla singola operazione (€ 5.000,00), come pure l'ammontare complessivo, pari, come detto, a € 37.414,56, superava i massimali giornalieri (€ 25.000,00). Il ricorrente, pertanto, attivava il presente procedimento per chiedere all'Arbitro di condannare l'intermediario a riconoscere la propria responsabilità e di rimediare al danno causato.

L'intermediario, nelle controdeduzioni, eccepiva preliminarmente l'inammissibilità del ricorso in quanto del tutto lacunoso, dal momento che il ricorrente non aveva allegato alcun documento sostegno di quanto affermato, limitandosi a mere enunciazioni prive di riscontro. Nel merito, riteneva che il ricorrente fosse stato vittima di mero phishing e che le operazioni erano state correttamente contabilizzate, registrate e autenticate, in quanto disposte previo corretto inserimento delle credenziali. Affermava di aver diffuso una campagna informativa, con cui venivano fornite ai clienti specifiche indicazioni per difendersi da simili tentativi di truffa, aggiungendo che, nel caso di specie, sussistesse la colpa grave del ricorrente, per aver ceduto le proprie credenziali, inserendo i propri codici personali in un link contenuto in un messaggio sms, a seguito della ricezione di una telefonata. Rilevava che non si trattava di una truffa particolarmente sofisticata, in quanto il messaggio ricevuto dal cliente, per quanto desumibile dalla denuncia, presentava un link non riconducibile alla banca; il numero di telefono utilizzato dall'interlocutore, anch'esso desunto dalla denuncia, era riconducibile ad un'utenza svedese e non era in alcun modo riferibile all'intermediario. Il cliente aveva, peraltro, ricevuto un messaggio recante lo specifico invito a non divulgare il codice ricevuto: nonostante l'alert di una possibile frode, il ricorrente dava seguito a quanto gli veniva chiesto di effettuare da parte del suo ignoto interlocutore. L'intermediario, per tutto quanto precede, chiedeva di dichiarare il ricorso inammissibile ovvero, nel merito, di non accoglierlo o in via di ulteriore subordine, di tenere conto del concorso di colpa della ricorrente, comunque con applicazione della franchigia.

DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte attraverso quaranta operazioni di pagamento addebitate sul conto corrente del ricorrente. Le operazioni contestate, di importo complessivo pari ad € 37.414,56, sono avvenute tutte il 2.11.2023 tra le ore 10.45 e le 11.14. Le operazioni sono state disconosciute e devono, quindi, 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 afferma che le operazioni controverse sono state correttamente contabilizzate, registrate e autenticate. In particolare, prova che tali operazioni sono state preceduta dall'installazione dell'app sullo smartphone in uso ai truffatori, tramite inserimento del PIN (fattore di conoscenza) e dell'OTS inviato via SMS all'utenza del cliente (fattore di possesso), nonché da un accesso via web prodromico alla variazione dei massimali giornalieri, tramite inserimento del PIN (fattore di conoscenza) e codice OTP generato sul dispositivo certificato (fattore di possesso). Le operazioni dispositive risultano autorizzate mediante l'inserimento del PIN (fattore di conoscenza) e del codice OTP generato sul nuovo dispositivo certificato (fattore di possesso). Le evidenze versate dall'intermediario, opportunamente verificate, consentono, dunque, di ritenere provata la SCA. È possibile, pertanto, procedere con la valutazione della condotta del ricorrente.

In quest'ottica, giova osservare che sul ricorrente si può presumere la colpa grave, lo stesso non producendo alcuna evidenza in merito allo SMS civetta e/o alla successiva telefonata truffaldina: non allega alcun documento al ricorso, neppure la denuncia, prodotta invece dall'intermediario, nell'ambito della quale il ricorrente riferisce che la chiamata proveniva dal numero +46***186, utenza che, da verifiche svolte, non è riconducibile all'intermediario convenuto.
Il Collegio, però, sotto altro profilo, rileva che non vi è evidenza dell'attivazione di un servizio di alert con riferimento alle operazioni contestate: e già questo rappresenta un profilo di responsabilità dell'intermediario. E, inoltre, vi è, soprattutto, l'integrazione di uno degli indici di anomalia/rischio frode di cui al D.M. 112/2007, rappresentato, nello specifico, da sette o più richieste di autorizzazione sullo stesso strumento di pagamento, nell'arco di 24 ore (art. 8, lett. b, punto 1): infatti le quaranta operazioni contestate, che si sostanziano in pagamenti ad enti pubblici (C-BILL, Pagopa) sono state eseguite in circa mezz'ora, ossia tra le 10:45 e le 11:14, del 02.11.2023.
Il Collegio ricorda che gli indici di frode contenuti del D.M. richiamato, sebbene facciano riferimento alla prevenzione delle frodi sulle carte di pagamento, possono costituire un parametro di valutazione del comportamento del PSP anche con riguardo ad operazioni eseguite con strumenti di pagamento diversi (ad es. bonifici o ricariche online), in ragione della *ratio* sottesa agli stessi. Sicché, nel caso in esame, l'intermediario deve essere considerato responsabile per non avere impedito il verificarsi di un'operatività fraudolenta davvero anomala, con conseguente obbligo di rimborsare al ricorrente l'importo corrispondente alle operazioni che vanno dall'ottava alla quarantesima, il tutto – con gli arrotondamenti di legge – per complessivi € 31.159,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 31.159,00.
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