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) CAPIZZI

Seduta del 23/07/2024

FATTO

Il ricorrente riferisce di avere denunciato in data 9 febbraio 2024 di essere stato oggetto, il giorno precedente, di frode informatica – asseritamente riconducibile al fenomeno c.d. *phishing* tramite telefonata truffaldina (*vishing/spoofing*) e successivi messaggi SMS fraudolenti (*smishing*) – che si sarebbe concretizzata nell'addebito sul rapporto di conto corrente intrattenuto presso l'intermediario convenuto di un bonifico on-line, di importo pari a Euro 49.800,75 (inclusivo di Euro 0,75 a titolo di commissioni), disposto tramite AppToken precedentemente installata sul *device* certificato dell'utilizzatore. Di conseguenza, disconoscendo l'addebito registrato sul proprio conto corrente sopra evidenziato, in quanto frutto di frode informatica, e inputando la responsabilità della suddetta frode all'intermediario, che non avrebbe saputo impedire una violazione al proprio sistema informatico da parte dei truffatori, il ricorrente ha chiesto il rimborso della somma complessiva di Euro 49.800,75 relativa alla menzionata operazione di pagamento on-line contestata e disconosciuta.

L'intermediario, con le controdeduzioni, dimostra la sua regolare esecuzione dell'operazione in oggetto a seguito del corretto inserimento delle credenziali previste nell'ambito del sistema adottato di autenticazione forte (SCA) ai fini sia dell'accesso ai servizi di home banking della banca tramite App, sia dell'inserimento della disposizione di pagamento contestata, e chiede dunque il rigetto del ricorso.

DIRITTO

La questione sottoposta al Collegio concerne la rimborsabilità o meno in favore di parte ricorrente della somma fraudolentemente sottratta mediante svolgimento di una operazione disconosciuta. Si tratta, in particolare, di un bonifico on-line, di importo pari a Euro 49.800,75 (inclusivo di Euro 0,75 a titolo di commissioni bancarie), eseguito alle ore 13:55 del giorno 8 febbraio 2024 tramite accesso in App ai servizi di home banking dell'intermediario convenuto.

Alla data di effettuazione delle operazioni contestate era vigente il D. Lgs. n. 11/2010, modificato a seguito dell'entrata in vigore del D. Lgs. n. 218/2017 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD II). Pertanto, la sussistenza delle responsabilità che le parti della controversia odierna vicendevolmente si addebitano dovrà essere valutata in base a quanto previsto da tale decreto con riferimento a entrambi i profili caratterizzanti l'onere probatorio, ossia l'accertamento della regolare autenticazione ed esecuzione delle operazioni di pagamento, nonché l'accertamento dell'eventuale colpa grave dell'utilizzatore dei servizi di pagamento.

Con riferimento al primo profilo, il Collegio osserva che l'art. 8, comma 1, lett. a) del D. Lgs. 11/2010, come novellato dal D. Lgs. 218/2017, prevede che "*il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7 […]*". L'art. 10, comma 1, del medesimo Decreto prescrive che "*qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*".

L'art. 10, comma 2, prevede che "*quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, […] è onere del prestatore di servizi di pagamento […] fornire la prova della frode, del dolo o della colpa grave dell'utente*". Inoltre, con riferimento alle modalità di autenticazione di una operazione di pagamento, ai sensi dell'art. 10 bis, comma 1, "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*". L'art. 1, comma 1, lett. q-*bis*, del summenzionato testo normativo definisce l' "*autenticazione forte del cliente" quale "basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".

Vale comunque la pena ribadire che, già prima dell'entrata in vigore delle citate modifiche normative, l'orientamento consolidato dei Collegi ABF era nel senso di richiedere all'intermediario la prova dell'avvenuta autenticazione delle operazioni tramite sistema a

due o più fattori (cfr. *ex multis* Collegio di Milano, Decisioni n. 6936/2016 e n. 7131/2017). Quanto al secondo profilo dell'onere probatorio, l'orientamento consolidato dell'Arbitro è nel senso conformarsi al principio interpretativo statuito dal Collegio di Coordinamento (Decisione n. 22745/2019), secondo cui "*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*". Tuttavia, il Collegio di Coordinamento ha al contempo evidenziato che, anche "*nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio [può] comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso*".

Venendo ora al caso di specie, si rileva, innanzitutto, che dalla ricostruzione dei fatti parrebbe che il cliente sia caduto vittima del noto fenomeno del c.d. "*phishing attraverso vishing/spoofing misto a smishing*", realizzato mediante iniziale telefonata di un ignoto truffatore, che si qualificava come un operatore dell'intermediario convenuto e induceva il cliente ad attivare la procedura di aggiornamento dell'AppToken installata sul proprio cellulare. Conseguentemente, il cliente scaricava la nuova versione dell'App strumentale all'utilizzo dei servizi di home banking del convento tramite smartphone, la quale evidenziava un'icona del tutto riconducibile all'intermediario, così come del resto era riconducibile all'intermediario anche il numero di telefono utilizzato dal truffatore.

Il sedicente interlocutore concludeva la telefonata fissando un appuntamento per il giorno successivo con la finalità di verificare la corretta installazione dell'AppToken ed inoltre informava il cliente che fino al giorno seguente non avrebbe dovuto utilizzare il conto corrente; subito dopo aver concluso la chiamata, il cliente ricontattava il numero dell'intermediario e riceveva conferma dal medesimo operatore truffaldino che era in corso l'aggiornamento dei sistemi e la verifica dell'aggiornamento della App.

L'intermediario, attraverso le evidenze versate in atti, riferisce che sia l'accesso all'area riservata dei servizi di home banking del cliente sia la successiva esecuzione dell'operazione di pagamento contestata sarebbero avvenute nel rispetto del sistema di autenticazione forte a due fattori (Strong Customer Authentication – SCA) con corretta applicazione della tecnologia 3D Secure ("3DS"), che prevede l'inserimento delle credenziali statiche, ossia userid e PIN (fattore della conoscenza), unitamente all'utilizzo della password dinamica, ossia il codice monouso OTP generato dal MobileToken integrato nell'App installata sul device certificato dell'utilizzatore.

Senonché, il Collegio osserva che, con riferimento alla fase di accesso all'area riservata per la fruizione dei servizi di home banking, dall'analisi della documentazione prodotta dall'intermediario, si ha evidenza soltanto del fattore di possesso (invio del codice OTP), ma non di quello di conoscenza (utilizzo del PIN), cui lo stesso ha fatto riferimento. Tenendo conto di quanto previsto, in tema di SCA, dalle "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*", si deve concludere che l'intermediario intervenuto ha fallito nell'offrire prova di corretta autenticazione forte con riferimento alla fase di login prodromica all'esecuzione dell'operazione contestata, in quanto non è stata prodotta chiara e completa evidenza in

merito ai requisiti di autenticazione previsti dal richiamato D. Lgs.11/2010 (cfr. *ex multis* Collegio di Milano, Decisioni n. 7792/2024, n. 4951/2023 e n. 6642/2023). Con riferimento poi all'esecuzione dell'operazione di bonifico on-line in questa sede contestata, pur essendo la stessa valorizzata, nei *log* prodotti dall'intermediario resistente, nella colonna "esito operazione" come eseguita, risulta evidenza soltanto dell'inserimento del codice dinamico OTP (fattore del possesso), ma non del codice PIN (fattore della conoscenza).

Sembra pertanto da escludere, nel caso di specie, il pieno assolvimento dell'onere probatorio relativo alla SCA. Ne consegue che questo Collegio, in conformità all'orientamento consolidato dell'Arbitro, da cui non vi è ragione di discostarsi, non può che evidenziare come l'intermediario convenuto non abbia adottato, quantomeno nell'operazione di pagamento di cui è ricorso, gli standard di sicurezza corrispondenti alla disciplina oggi applicabile, funzionali ad evitare il verificarsi di questo particolare tipo di frode (cfr. *ex multis* Collegio di Milano, Decisioni n. 4760/2024, n. 2478/2023 e n. 9854/2022). Tenuto conto che la mancata prova, da parte dell'intermediario, dell'autenticazione forte è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al ricorrente, ne consegue che l'operazione di pagamento disconosciuta al centro della presente controversia dovrà essere rimborsata per intero dall'intermediario convenuto, nei limiti già precisati dell'importo chiesto dal cliente in sede di ricorso.

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