COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) MODICA	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 28/04/2025

FATTO

Il ricorrente riferisce di avere denunciato in data 14 dicembre 2024 di essere stato oggetto, il giorno precedente, di frode informatica – asseritamente riconducibile al fenomeno c.d. *phishing* tramite telefonata truffaldina (*vishing*) e successivo invio di SMS (*smishing*) – che si sarebbe concretizzata nell'addebito sul rapporto di conto corrente intrattenuto presso l'intermediario convenuto di un pagamento online tramite carta di debito intestata al cliente, di importo pari a € 2.000,00. La menzionata operazione di pagamento è stata disposta tramite accesso in App sul device certificato del cliente all'area riservata dei servizi di internet banking dell'intermediario. Di conseguenza, disconoscendo l'addebito registrato sul proprio conto corrente sopra evidenziato in quanto frutto di frode informatica, e imputando 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 € 2.000,00 relativa alla menzionata operazione di pagamento online contestata e disconosciuta.

L'intermediario, con le controdeduzioni, sostiene la 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 all'area riservata per l'utilizzo dei servizi di internet banking del convenuto, 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 pagamento online tramite carta di debito intestata al cliente ed emessa dall'intermediario convenuto, di importo pari a € 2.000,00. L'operazione contestata a state eseguita alle ore 16:55 del 13 dicembre 2024 tramite accesso in App sul device certificato del cliente all'area riservata dei servizi di internet banking dell'intermediario resistente.

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 la cliente sia caduta vittima del noto fenomeno del c.d. "*phishing attraverso vishing misto a smishing*", realizzato mediante iniziale telefonata di un ignoto truffatore, che si qualificava come un operatore dell'intermediario convenuto e induceva il ricorrente ad attivare una procedura di sicurezza aggiuntiva alla propria carta di debito, allo scopo di bloccare due transazioni anomale effettuate con la menzionata carta di pagamento. Conseguentemente, il cliente, seguendo le istruzioni del sedicente operatore, provvedeva, come evidenziato nella denuncia versata in atti, a comunicare i codici ricevuti via SMS sulla propria utenza telefonica ai truffatori, nell'erronea convinzione che servissero all'ignoto truffatore per eseguire il blocco delle suddette transazioni anomale e recuperare i relativi importi.

L'intermediario, attraverso le evidenze versate in atti, afferma che l'esecuzione dell'operazione contestata ha richiesto una serie di passaggi autorizzativi precedenti, tra cui l'accesso all'area riservata, la consultazione del codice PIN associato allo strumento di pagamento e il cambio password, tutti avvenuti 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 username e password (fattore della conoscenza), unitamente all'utilizzo delle credenziali dinamiche, ossia il codice monouso OTP inviato tramite SMS sul device certificato dell'utilizzatore (fattore del possesso) o, in alternativa, l'attivazione tramite riconoscimento biometrico di un token generato in App su smartphone precedentemente registrato (fattore della inerenza).

In effetti, dall'analisi dei log prodotti dall'intermediario, il Collegio appura che, per l'accesso su web all'area riservata dei servizi di internet banking, i fattori di autenticazione utilizzati siano la digitazione del codice monouso OTP inviato tramite SMS sullo smartphone del cliente (elemento di possesso) e l'inserimento delle credenziali statiche, tra cui la password (elemento di conoscenza). Con riferimento alla successiva fase di consultazione del PIN associato alla carta di debito contestata – strumentale al cambio password – i fattori di autenticazione utilizzati, come desumibile dai log prodotti, sono la conferma tramite Token (elemento di possesso) e l'inserimento del fattore biometrico sullo smartphone (elemento di inerenza). Nella fase di cambio password, i fattori di

autenticazione sono il codice PIN e le credenziali statiche (elemento di conoscenza) e il codice monouso OTP inviato tramite SMS sullo smartphone del cliente (elemento di possesso)

Con riferimento, invece, all'esecuzione dell'operazione di pagamento contestata, l'applicazione della SCA, secondo il convenuto, sarebbe garantita dalla digitazione di un "CVV dinamico", a sua volta generato mediante inserimento di username e password (elemento di conoscenza), e dal riconoscimento biometrico di un token generato in App su smartphone precedentemente registrato (elemento di inerenza). Senonché, il Collegio osserva che, con riferimento al suddetto CVV dinamico, si pone il problema di stabilirne la valenza, in virtù della sua composita modalità di generazione, in cui il fattore della conoscenza è, ad evidenza, un input.

Alla luce della Opinion EBA del 21 giugno 2019, questo Collegio si uniforma all'orientamento consolidato dell'ABF secondo cui il CVV dinamico è da qualificarsi come elemento di possesso (cfr. *ex multis* Collegio di Milano, Decisioni n. 8153/2024 e n. 3554/2024; Collegio di Torino, Decisione n. 7207/2024). Non si può che dedurne che l'intermediario convenuto ha fallito nell'offrire prova di SCA, dato che l'operazione di pagamento di cui è ricorso è stata autenticata sulla base di un doppio fattore di possesso, invece che sulla base di due fattori di autenticazioni appartenenti a categorie diverse.

Tenuto conto che la mancanza anche parziale, da parte dell'intermediario, della prova di 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 € 2.000,00.
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
ANDREA TINA