COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) MANENTE	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) ACHILLE

Seduta del 22/09/2022

FATTO

Con ricorso presentato in data 16 maggio 2022, preceduto dal reclamo, la parte ricorrente chiede il rimborso di € 29.547,43, o in subordine della metà dello stesso importo, relativo a una transazione effettuata in data 4 aprile 2022 con lo strumento di pagamento di cui è titolare e dalla stessa disconosciuta. A tal fine deduce, anche secondo quanto risulta dalla denuncia depositata agli atti della procedura, che: i) il 4 aprile 2022 riceveva un SMS dalla stessa utenza dalla quale l'intermediario inviava normalmente gli OTP e le comunicazioni ufficiali; ii) nel messaggio le veniva comunicato l'apposizione di limiti sul suo conto per "mancata verifica della sicurezza web"; iii) nello stesso messaggio era presente un link sul quale veniva invitata a cliccare per aggiornare la password di accesso; iv) cliccando sul link si apriva una pagina identica a quella del sito dell'intermediario dove si eseguono le operazioni on-line; v) veniva quindi contattata dal numero del servizio clienti dell'intermediario e il sedicente operatore la guidava nell'installazione di una nuova applicazione; vi) un nuovo messaggio la informava che la richiesta era stata presa in carico e sarebbe stata ricontattata il giorno successivo; vii) poiché non riceveva alcuna chiamata, contattava il servizio clienti e si avvedeva di essere stata vittima di una truffa in quanto, a sua insaputa, era stato disposto un bonifico di € 29.547,23 a valere sul proprio conto; viii) bloccava il conto e presentava denuncia presso le autorità competenti in data 5 aprile 2022; ix) l'8 aprile 2022 presentava reclamo all'intermediario, che rispondeva negativamente in data 21 aprile 2022.

Con le proprie controdeduzioni, l'intermediario resistente chiede il rigetto del ricorso. Deduce a tal fine che: i) la cliente è stata vittima di smishing e vishing; ii) le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risultano avvenute con il corretto inserimento delle credenziali; ii) sussiste la colpa grave del cliente in quanto, aprendo un link non a sé riconducibile ed installando un'applicazione non ufficiale, ha fornito a terzi le credenziali necessarie ad operare con il proprio profilo di internet banking; iii) è presumibile che l'installazione dell'applicazione suggerita dal sedicente operatore abbia fornito al truffatore il controllo del proprio telefono, consentendogli di autorizzare l'operazione contestata; iv) non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.
Con le repliche alle controdeduzioni, la parte ricorrente eccepisce che: i) la riconducibilità all'intermediario del numero da cui è provenuta la chiamata truffaldina le ha ingenerato fiducia; ii) non è pertanto connotabile come gravemente colpevole il fatto che abbia seguito le istruzioni del sedicente operatore; iii) non vi è comunque alcuna prova che abbia comunicato le proprie credenziali all'interlocutore; iv) non ha ricevuto gli SMS Alert che l'intermediario afferma di aver inviato; v) l''importo dell'operazione truffaldina è anomalo rispetto alla propria normale operatività e l'intermediario avrebbe dovuto rilevare l'anomalia e impedire o limitare l'esecuzione di una simile transazione; vi) non è provato che le comunicazioni di informazione e sensibilizzazione sui rischi di truffa indicate dall'intermediario nelle controdeduzioni siano effettivamente pervenute alla cliente.
Con le controrepliche, l'intermediario resistente eccepisce che: i) la cliente avrebbe dovuto accorgersi della truffa perché il link presente nel messaggio truffaldino non è assimilabile a quelli autentici e riporta in modo errato il proprio nome; ii) dalle stesse dichiarazioni della cliente si può presumere che abbia fornito i propri dati personali al sedicente operatore; iii) l'evidenza in atti dimostra che gli SMS Alert sono stati correttamente inviati all'utenza della cliente; iv) l'importo di un'operazione non può essere assunto come elemento anomalo di per sé; v) se la cliente avesse ritenuto fuori norma una simile cifra avrebbe dovuto modificare il plafond dei bonifici; vi) secondo l'interpretazione dell'EBA all'art. 2 del regolamento delegato (UE) n. 2018/389 della Commissione Europea non è necessario che i sistemi di monitoraggio delle operazioni predisposti dagli intermediari operino in tempo reale; vii) le informazioni di sensibilizzazione al rischio frodi sono pubblicate nel proprio sito nella pagina di accesso ai servizi di home banking, pertanto sono facilmente accessibili da tutti i clienti.

DIRITTO

Il ricorso, avente ad oggetto la richiesta di rimborso di € 29.547,43 pari all'importo di una transazione effettuata in data 4 aprile 2022 con lo strumento di pagamento di cui è titolare la parte ricorrente e dalla stessa disconosciuta deducendo di essere stata vittima di frode, deve essere deciso facendo applicazione delle disposizioni del d. lgs. n. 11 del 27 gennaio 2010, come modificate in seguito al recepimento della seconda Direttiva sui servizi di pagamento (Direttiva 2015/2366/UE del 13 novembre 2007), applicabile ratione temporis a decorrere dal 13 gennaio 2018.
In base a tali disposizioni, come applicate da questo Arbitro (da ultimo, ABF-Coll. Coord. n. 22745 del 10 ottobre 2019, al § 8), due sono i passaggi ineludibili in materia. In primo luogo, è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza che le operazioni disconosciute siano state autenticate con un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA), posto

che ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente". In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
In tale contesto e con riguardo al caso di specie è possibile rilevare, quanto al primo dei suddetti passaggi, che dalle evidenze fornite agli atti della procedura non risulta che l'intermediario resistente abbia richiesto un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA) conformemente a quanto previsto dalla normativa di riferimento. Occorre al riguardo ricordare che in base al disposto dell'art. 12-bis, d.lgs. n. 11/2010, comma 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente…". Tale autenticazione, secondo quanto prevede l'art. 97 della Direttiva 2015/2366/UE e conformemente l'art. 10 bis, comma 1, d.lgs. n. 11/2010, deve trovare applicazione quanto 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".
La definizione di autenticazione forte si rinviene nell'art. 1, d.lgs. n. 11/2010, ove si prevede che per autenticazione forte del cliente si intende: "un'autenticazione 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 (...)". Giova al riguardo ricordare che in base alle determinazioni dell'EBA (Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 del 21 giugno 2019) l'autenticazione forte del cliente "consiste in una procedura basata sull'impiego di due o più dei seguenti elementi - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: i) qualcosa che solo l'utente conosce, per esempio una password statica, un codice, un numero di identificazione personale; ii) qualcosa che solo l'utente possiede, per esempio un token, una smart card, un cellulare; iii) qualcosa che caratterizza l'utente, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione".
Nel caso di specie, dai log prodotti dall'intermediario non si evince il corretto inserimento del secondo fattore di autenticazione quanto all'accesso al profilo cliente; secondo fattore che in base a quanto prospettato dall'intermediario resistente sarebbe stato il codice OTP generato tramite mobile token, il cui utilizzo avrebbe dovuto comportare la valorizzazione nel log della colonna denominata "OneTimePSD" che tuttavia non risulta in concreto valorizzata.
Da ciò consegue che, ad avviso del Collegio (in senso analogo vd. ABF-Coll. Napoli n. 17207 del 5 ottobre 2020 e Coll. Roma nn. 8493 dell'11 maggio 2020 e 11271 del 24 giugno 2020), l'intermediario resistente non ha provato di aver adottato gli standard di

sicurezza corrispondenti alla disciplina oggi applicabile come sopra individuata, non avendo adottato – in particolare – un sistema di autenticazione forte quanto all'accesso al profilo cliente, dovendosi quindi disporre che l'intermediario resistente corrisponda alla parte ricorrente la somma di € 29.547,00, in ciò facendo applicazione di quanto previsto dalla Sez. VI § 3 delle nuove Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari in vigore dal 1° ottobre 2020 ove alla nota a piè di pagina n. 3 si prevede che "Gli importi contenuti nelle pronunce di accoglimento sono arrotondati all'unità di euro (per eccesso se la prima cifra dopo la virgola è uguale o superiore a 5; per difetto, se la prima cifra dopo la virgola è inferiore a 5)".

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 29.547,00.
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