COLLEGIO DI ROMA

composto dai signori:

(RM) PATTI	Presidente
(RM) PORTA	Membro designato dalla Banca d'Italia
(RM) MEZZACAPO	Membro designato dalla Banca d'Italia
(RM) GULLO	Membro di designazione rappresentativa degli intermediari
(RM) COEN	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ROBERTO COEN

Seduta del 05/07/2022

FATTO

In data 20.07.2021, la ricorrente, titolare di un conto corrente presso l'intermediario convenuto, riferiva di aver ricevuto una chiamata da un sedicente operatore dell'intermediario, che le riferiva la necessità di aggiornare la propria carta di pagamento.
Pertanto, la ricorrente comunicava i codici OTP pervenuti sul suo cellulare.
Successivamente, parte ricorrente veniva contattata da un operatore che le chiedeva conferma per tre operazioni sospette e, quindi, si avvedeva di essere rimasta vittima di una truffa e, scopriva tre operazioni e-commerce, per l'importo complessivo di € 1.400,00.
Immediatamente, chiamava il numero verde della banca, provvedeva a bloccare il conto e sporgeva formale querela avanti alle autorità competenti.
In data 23.07.2021, la ricorrente presentava reclamo alla resistente per il rimborso della somma di € 1.400,00, indebitamente prelevata dal conto corrente, e, in considerazione dell'esito negativo del reclamo esperito, le medesime doglianze venivano riproposte dal ricorrente innanzi all'A.B.F. in data 11.01.2022.
Si costituiva l'intermediario, il quale chiedeva il rigetto del ricorso, sostenendo la piena responsabilità in capo alla parte ricorrente.
Secondo l'intermediario, le operazioni contestate non presentavano alcuna anomalia in quanto, dalle verifiche effettuate, era stata accertata la legittima esecuzione e sostanziale regolarità delle operazioni, eseguite con un sistema dinamico di autenticazione.

Le operazioni disconosciute dalla ricorrente erano state eseguite tramite la digitazione delle credenziali statiche della carta (fattore di conoscenza) e conseguente generazione del codice OTP (fattore di possesso).
Questa tipologia di autenticazione rientrante nella modalità di autenticazione in 3DS dinamico, oltre a rispondere alla necessità di protezione del cliente, rende impossibile qualsivoglia tentativo di forzatura.
L'intermediario chiede, quindi, il rigetto del ricorso, in quanto infondato.

DIRITTO

Il Collegio osserva che, nel caso di specie, la parte ricorrente ha subito la truffa, successivamente all'entrata in vigore del D.lgs. n. 218/2017(di recepimento della PSD 2), ovvero successivamente al 14 settembre 2019, data di applicazione del Regolamento delegato (UE) della Commissione 2018/389, che stabilisce i requisiti dell'autenticazione forte ai sensi della PSD 2.
Ciò posto, la questione relativa alla fattispecie del *phishing* impone di valutare sia l'adeguatezza del sistema di protezione adottato dall'Intermediario, che l'adempimento del corretto obbligo di custodia dello strumento di pagamento da parte dell'utente (ex artt. 7 e 8 del D. Lgs. 11/2010, così come modificati alla luce del nuovo decreto precedentemente citato).
Per quanto riguarda il primo profilo, una delle più significative novità introdotte dalla suddetta normativa è il concetto della c.d. "autenticazione forte" (strong customer authentication – SCA, nella direttiva), di cui all'art. 1, c.1, lett. q-bis del D.lgs. 11/2010 (così come modificato dal D.lgs. 218/2017), secondo cui: "*q -bis) "autenticazione forte del cliente": 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, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".
Orbene, l'avere o meno offerto al cliente un sistema di autenticazione forte assume rilevanza sostanziale con riferimento al caso di specie, soprattutto in considerazione dell'ulteriore novità introdotta dall'art. 12 commi 2 bis e 4 del D. Lgs. 11/2010 (così come modificato dal D. Lgs. 218/2017) ai sensi del quale: "*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. 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. (…)*
4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3."
È notorio che il sistema delineato dal legislatore comunitario in materia di strumenti di pagamento è di particolare favore per il cliente soprattutto per quel che concerne l'onere probatorio. Ciò in quanto, per un verso limita la responsabilità del cliente alle sole ipotesi di dolo e colpa grave e, per altro verso, pone in capo all'intermediario l'onere di provare che l'operazione di pagamento sia stata eseguita correttamente e non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.
Nel caso di specie, l'intermediario produce documentazione tratta dai propri sistemi informatici, dalla quale si desume che l'operazione contestata è stata eseguita in

ambiente 3-D Secure, previo utilizzo di un sistema di autenticazione dinamico, basato sull'inserimento dei dati della carta e del codice OTP ricevuto tramite SMS.
Sulla base di quanto rilevato in relazione alle norme tecniche di regolamentazione per l'autenticazione forte del cliente e alle linee interpretative fornite dall'EBA nella sua Opinion del 2019, deve ritenersi che l'intermediario, riferendosi unicamente all'esecuzione dell'operazione in ambiente 3-D Secure e tramite inserimento dell'OTP e dei dati della carta, non abbia dato prova dell'utilizzo, per la transazione contestata, di un sistema di autenticazione forte.
Ai sensi del già richiamato comma 2-*bis* dell'art. 12 D.Lgs. n. 11/2010: *"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*".
Ne consegue che parte ricorrente ha diritto ad ottenere il rimborso dell'importo corrispondente all'operazione fraudolenta effettuata mediante la sua carta di pagamento.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.400,00.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FRANCESCO PAOLO PATTI