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 - FABIO GIROLAMO PORTA

Seduta del 05/07/2022

FATTO

I ricorrenti, cointestatari di un rapporto di conto corrente abilitato ai servizi on-line intrattenuto con la banca convenuta, chiedono il rimborso della somma di euro 2.542,90 fraudolentemente sottratta da terzi non autorizzati. All'uopo gli istanti hanno allegato la denuncia sporta, da ultimo, in data 31 maggio 2021, presso le Forze dell'ordine, a mezzo della quale i medesimi hanno dichiarato di essersi avveduti (in data 30 maggio 2021) che circa un anno prima, tra il 28 febbraio e il 27 maggio 2020, sul proprio conto corrente erano state addebitati n. 5 bonifici europei per l'importo complessivo di euro 2.542,90.
Ritenendo di essere rimasti vittima di una frode informatica, i ricorrenti hanno disconosciuto formalmente le transazioni controverse chiedendone la restituzione all'intermediario, che ha negato il rimborso.
Insoddisfatti dell'esito del reclamo, i ricorrenti si sono rivolti all'Arbitro al quale hanno chiesto di disporre, a carico della convenuta, il riaccredito di tutti gli importi prelevati illecitamente, oltre interessi legali, rivalutazione monetaria e spese per la presentazione del ricorso.
Costituitasi parte del presente procedimento, la banca convenuta si è opposta alle richieste dei ricorrenti sollevando le seguenti eccezioni.
Sotto un primo profilo la resistente ha eccepito che l'art. 9, comma 1, d.lgs. n.11/2010, richiamato dal contratto, impone all'utilizzatore del servizio di pagamento di comunicare l'effettuazione di un'operazione non autorizzata entro tredici mesi da quando la stessa è

avvenuta. Pertanto nella fattispecie le uniche due operazioni disconosciute tempestivamente sono le ultime due, per un importo totale di euro 597,23; viceversa le precedenti operazioni effettuate dal 28 febbraio 2020 al 29 febbraio 2020 risultano denunciate oltre i termini di legge.
In ogni caso, dagli accertamenti informatici condotti con riguardo a tutte le operazioni disconosciute è emerso che le stesse sono risultate regolarmente autorizzate con l'utilizzo di un sistema di autenticazione certificato (ISO/IEC 27001) che prevede massimi livelli di sicurezza e protezione dei sistemi di pagamento elettronici e dei servizi on line erogati.
In proposito, la banca ha precisato che per l'accesso al sistema di home banking occorre digitare il codice titolare e il PIN (credenziali statiche) e una password dinamica (OTP). Dopo l'accesso al sistema, per autorizzare le operazioni dispositive è necessario conoscere un codice dinamico (OTP), che viene comunicato via SMS sul numero di telefono certificato dal cliente, allorquando si opti per il servizio "*O-K** SMS",* oppure generato dall'applicazione della banca per i clienti che attivano il servizio "*O-K** Smart"*. In tal caso il cliente seleziona la notifica che perviene sul proprio *device*, digita il PIN oppure esegue il riconoscimento biometrico con impronta digitale o riconoscimento facciale, onde ottenere il codice O-K** dinamico. Nel caso il cliente utilizzi uno smartphone o un tablet con connessione dati assente o momentaneamente non funzionante, il codice O-K** dinamico viene inviato tramite SMS al numero di cellulare certificato. Inoltre, per aumentare ulteriormente il livello di sicurezza di alcune disposizioni di pagamento, si richiede al cliente di rispondere alle domande di sicurezza precedentemente censite e/o l'inserimento di un secondo codice inviato via SMS.

Ciò rilevato, nella fattispecie, all'esito delle verifiche svolte, sulla scorta dei tracciati elettronici registrati in occasione delle operazioni disconosciute, dai quali emerge che tutte le transazioni sono state autorizzate mediante regolare autenticazione, registrazione e contabilizzazione, in assenza di malfunzionamenti delle procedure necessarie per la loro esecuzione, la banca ha escluso profili di responsabilità alla medesima ascrivibili.
La resistente ha chiesto pertanto all'Arbitro di pronunciarsi per il rigetto della domanda restitutoria da ritenersi infondata e, in ogni caso, da limitare agli importi di cui alle operazioni effettuate in data 25 e 26 maggio 2020.

DIRITTO

La materia trova specifica regolamentazione nelle disposizioni del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). Le operazioni controverse risultano inoltre poste in essere sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione, che definisce i requisiti per l'autenticazione *forte* previsti dalla citata direttiva.
Come evidenziato in narrativa, i ricorrenti agiscono per il rimborso dell'importo complessivo di euro 2.542,90, a fronte di cinque operazioni di bonifico effettuate in data 28 febbraio (€ 577,38), 3 marzo (€ 527,79; € 835,50), 25 e 26 maggio 2020 (rispettivamente di € 378,21 ed € 219,02), non autorizzate.
Con riguardo ai tre bonifici eseguiti in data 28 febbraio (€ 577,38) e 2 marzo 2020 (€ 527,79 e € 835,50), la convenuta ha eccepito la tardività della contestazione rispetto al termine di tredici mesi imposto dalla richiamata normativa di riferimento. In proposito è stato chiarito che "*Il termine di 13 mesi previsto dall'articolo 9 del d.lgs. n. 11/2010 ha natura di termine di decadenza, tale per cui, in assenza della richiesta di rettifica e/o di una*

contestazione del cliente del sistema bancario entro 13 mesi dal compimento dell'operazione inesatta o non autorizzata, è preclusa al medesimo la possibilità di contestarla e di ottenerne il rimborso in un tempo successivo alla inutile scadenza di detto termine. L'inutile scadenza del suddetto termine non può essere rilevata d'ufficio, ma deve formare oggetto di espressa eccezione di parte" (ABF, Coll. Coordinamento, Dec. n. 11676/2021).

Nel caso di specie il disconoscimento delle operazioni in parola è avvenuto in data 11 giugno 2021, sicché la contestazione si palesa tempestiva – come in effetti eccepito dalla resistente – esclusivamente in relazione ai due bonifici europei non autorizzati disposti il 25 e 26 maggio 2020 per gli importi di euro 378,21 ed euro 219,02.

Appurato ciò, la normativa *de quo* introduce una serie di obblighi in capo agli utilizzatori e ai fornitori dei servizi di pagamento (cfr. artt. 7 e ss.) al fine di presidiarne la sicurezza: ai primi è imposto di non rendere noti i codici personalizzati per l'utilizzo degli strumenti; ai secondi di predisporre meccanismi di sicurezza adeguati per impedire l'accesso da parte di terzi diversi dall'utilizzatore. Contestualmente, al fine di bilanciare le differenti posizioni e in ragione del rischio d'impresa che grava sul prestatore dei servizi di pagamento, le disposizioni in rassegna prevedono una diversa distribuzione degli oneri probatori, con l'obiettivo di attribuire all'impresa la responsabilità degli utilizzi fraudolenti nel caso in cui essi non siano stati cagionati da dolo o colpa grave del cliente. Ne deriva che per sottrarsi alla richiesta di rimborso del cliente, che neghi di aver compiuto o autorizzato operazioni usufruendo dei servizi di internet banking, grava sull'intermediario l'onere di provare, in primo luogo, di aver adottato un sistema di autenticazione multifattoriale forte, atto a garantire un elevato livello di sicurezza dei servizi di pagamento prestati, in conformità alla vigente legislazione in materia di autenticazione e agli standard (SCA), come definiti dagli orientamenti dell'European Banking Authority del 21 giugno 2019; in secondo luogo, la colpa grave o il dolo del cliente titolare di strumenti abilitati all'operatività on line.

Nella fattispecie, dalla documentazione agli atti emerge che le operazioni disconosciute sono state effettuate con l'impiego delle credenziali personali e dei codici dispositivi conosciuti unicamente dai contitolari del rapporto di conto corrente, all'interno di un sistema di autenticazione multifattoriale. Tale sistema, secondo l'attuale stato della tecnica, appare idoneo a garantire un elevato livello di sicurezza, in conformità agli standard definiti dagli orientamenti dell'European Banking Authority del 21 giugno 2019, in materia di autenticazione forte (cfr. ABF Roma, Dec. nn. 8534/2021; 9215/2021). Consta, infatti, che per effettuare bonifici a distanza, l'utilizzatore debba essere in possesso delle credenziali di accesso al sistema di home banking necessarie per installare l'OTP software sul proprio *device,* in modo da ottenere le password dinamiche indispensabili per autorizzare le operazioni dispositive.

Orbene, a sostegno della regolarità formale delle operazioni controverse, la resistente ha prodotto i tracciati informatici da cui può evincersi che le due transazioni all'esame del Collegio sono state processate in data 25 e 26 maggio 2020 con un sistema a più fattori.

In particolare, quanto al bonifico europeo di € 378,21 del 25 maggio 2020, risulta un accesso alle ore 12:30 tramite browser, autenticato con le credenziali statiche del ricorrente (elemento di conoscenza) e l'OTP generato dallo smartphone del ricorrente (elemento di possesso), previa ricezione della notifica push e digitazione del PIN (elemento di conoscenza). Consta inoltre che alle 12:31 è stato inserito un bonifico europeo da browser, autenticato tramite l'OTP generato in via silente dallo smartphone del ricorrente (elemento di possesso) previa digitazione del PIN (elemento di conoscenza). L'operazione appare confermata mediante digitazione del codice OTS trasmesso via SMS al ricorrente e risposta alla domanda di sicurezza.

Dai log SMS prodotti risulta, altresì, l'invio del messaggio OTS al numero di cellulare indicato dal ricorrente anche nel modulo di ricorso.
In ordine al bonifico europeo addebitato per l'importo di € 219,02, in data 26 maggio 2020, alle ore 17:43, risulta un accesso tramite browser autenticato con le credenziali statiche del ricorrente e l'OTP generato in via silente dallo smartphone della medesima, previa ricezione della notifica push e digitazione del PIN. Alle 17:44 risulta inserito un bonifico europeo da browser, autenticato tramite OTP generato in via silente dallo smartphone della ricorrente (elemento di possesso) previa digitazione del PIN (elemento di conoscenza). L'operazione appare confermata mediante digitazione del codice OTS trasmesso via SMS al ricorrente e risposta alla domanda di sicurezza. Consta altresì l'invio del massaggio OTS al numero di cellulare certificato dal ricorrente.
Si precisa che, nel caso in esame, i due codici dinamici OTP e OTS appaiono generati e trasmessi su canali distinti. Dagli stessi log risulta ancora che ciascuna operazione è stata preceduta da diverse notifiche push inviate allo smartphone del ricorrente, contenenti i dati delle operazioni.
Dal canto suo parte ricorrente, tanto nella denuncia presentata alle forze dell'ordine, quanto nel ricorso, non ha ricostruito le modalità della truffa, limitandosi ad affermare di essersi avveduto solo il 31 maggio 2021 di aver subito i cinque addebiti fraudolenti.
In questo contesto è ragionevole presumere che le operazioni effettuate avvalendosi del sistema di autenticazione a più fattori - in assenza di elementi di prova o quanto meno di indizi di segno contrario - non possano che essere ricondotte ai titolari del conto di pagamento, ancorché compiute da terzi non autorizzati ai quali i medesimi hanno reso accessibili i codici segreti per grave imprudenza. In tal modo l'utilizzatore ha violato l'obbligo di custodia sul medesimo gravante (ai sensi dell'art. 7 della normativa sopra citata) delle credenziali di accesso ai servizi di internet banking e delle password dispositive dinamiche, OTP e OTS, necessarie per la finalizzazione delle transazioni oggetto di vertenza.
Pertanto, in linea con l'indirizzo interpretativo di questo Collegio (cfr. ABF Roma, Dec. n. 17334/2021), le perdite subite nella sfera patrimoniale dei ricorrenti non possono ricevere alcun ristoro da parte dell'intermediario; di conseguenza il ricorso non può trovare accoglimento.

P.Q.M.

Il Collegio respinge il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FRANCESCO PAOLO PATTI