COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) GENOVESE	Membro di designazione rappresentativa degli intermediari
(BO) D ATRI	Membro di designazione rappresentativa dei clienti

Relatore ANDREA GENOVESE

Seduta del 04/06/2024

FATTO

Insoddisfatta dell'interlocuzione intercorsa con l'intermediario nella fase del reclamo, con ricorso n. 2177754 del 16.12.2023 la parte ricorrente si rivolge all'Arbitro al quale chiede disporsi il rimborso della somma di euro 1.500,00 relativa ad un'operazione di pagamento fraudolenta. A sostegno della domanda, deduce che: i) in data 6.11.2023 alle ore 20:00 circa riceveva una telefonata da parte di un numero apparentemente riconducibile all'intermediario. Un presunto operatore della banca, che era a conoscenza delle sue generalità e del numero del suo bancomat, la informava che era in atto una transazione fraudolenta sulla sua carta di debito n. ***812 di euro 1.500,00, per evitare la quale avrebbe dovuto seguire una data procedura sull'home banking; ii) durante la telefonata, l'interlocutore dimostrava una perfetta conoscenza delle funzionalità del sito home banking della banca; iii) durante la stessa, riceveva inoltre alcuni messaggi, sempre apparentemente riconducibili alla banca resistente; iv) terminate le operazioni frattanto eseguite, il sedicente operatore bancario lo rassicurava sul blocco dell'operazione, dandogli appuntamento telefonico per le ore 09:00 del giorno seguente per la verifica della situazione; v) non avendo ricevuto la telefonata promessa, alle ore 10:00 del giorno seguente contattava la banca e nell'occasione scopriva di essere stato vittima di una frode; vi) il giorno dell'operazione disconosciuta, il ricorrente non si trovava nel luogo ove la stessa veniva eseguita; vi) la banca resistente non ha filiali e l'unico contatto telefonico

è rappresentato dal numero ***107 da cui ha ricevuto la telefonata il giorno 06.11.2023.

Costituitosi in giudizio, l'intermediario contesta l'avversa domanda della quale chiede il rigetto perché infondata, sul rilievo che: a) l'operazione contestata è stata correttamente autenticata tramite verifica a doppio fattore. Nel dettaglio, alle ore 20:07 del 06.11.2023 il cliente ha eseguito l'accesso all'app della banca mediante inserimento del codice segreto; in seguito, ha autorizzato l'attivazione del "Master Card Identity Check" con un secondo codice segreto e con codice B*** generato in modo silente dall'app (tale attivazione veniva comunicata tramite apposite notifiche *push*); alle ore 20:14, veniva autorizzata l'operazione contestata mediante l'inserimento dei dati identificativi della carta, del Master Card Identity Check e del codice OTP ricevuto via sms; b) dalle tracciature informatiche risulta che il codice OTP è stato correttamente recapitato sul numero di cellulare del cliente; c) l'operazione è stata prontamente comunicata tramite l'invio di un sms alert; d) il cliente ha creduto al malfattore nonostante l'ampia informativa antifrode effettuata dalla banca, nella quale viene anche precisato che il numero ***107 non è abilitato ad eseguire telefonate in uscita; e) l'attivazione del Master Card Identity Check avrebbe dovuto insospettire il cliente, data la finalità puramente autorizzativa di detto codice; f) il cliente ha colposamente cooperato con il malfattore, nonostante fosse accertabile mediante impiego della normale diligenza che si aveva a che fare con una frode riconducibile nello schema del vishing; g) la ricorrente ha ammesso di avere eseguito l'accesso all'applicazione e di avere seguito pedissequamente le istruzioni impartite dal malfattore; h) la frode non si sarebbe verificata se solo il cliente non avesse comunicato al sedicente operatore tutti i codici segreti necessari.

In sede di repliche, la parte ricorrente contesta di essere stato informato del fatto che il numero ***107 non è abilitato alle chiamate in uscita. Assume che nella specie la frode sarebbe stata particolarmente insidiosa in quanto riconducibile nello schema dello spoofing.

L'intermediario in sede di controrepliche insiste nei precedenti assunti

DIRITTO

L'operazione contestata è stata posta in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

In particolare, si osserva che la parte ricorrente lamenta l'esecuzione fraudolenta in data 06.11.2023, alle ore 20:14, di un pagamento online di euro 1.500,00.

Le parti non riferiscono alcunché in ordine al blocco dello strumento di pagamento.

Tanto premesso, le allegazioni offerte dalle parti e l'esame delle tracciature informatiche prodotte dalla banca permettono di porre in rilievo che:

i) l'intermediario assume che il login è stato autenticato mediante inserimento di un "primo codice segreto" (fattore di conoscenza) e del codice B*** generato in

modo silente dall'applicazione installata sul device del cliente (fattore di possesso).

ii) Dalla documentazione prodotta, parrebbe evincersi che: a) la legenda esplicativa chiarisce il significato delle voci "login secondo livello" e "login terzo livello", ma non anche della voce "login primo livello"; b) ad ogni modo, in corrispondenza dell'operazione "login primo livello" risulta la voce "codice corretto" (cfr. all. 3 controdeduzioni, voci evidenziate all'interno dei riquadri rossi nella colonna "dati operativi"); c) non si ha un'esplicita evidenza del secondo fattore di autenticazione, cioè del codice B*** generato in modo silente dall'applicazione; d) tuttavia, risulta che l'accesso all'area riservata sia avvenuto tramite l'applicazione installata sul device del cliente (cfr. all. 3 controdeduzioni, colonna "canale accesso", voce "MOBILE APP"); e) la sessione di login è individuata dal numero ***250 (cfr. all. 3 controdeduzioni, colonna "ID sessione").

iii) Per ciò che attiene al Master Card Identity Check, che consiste in una password statica di cinque cifre scelta direttamente dal cliente all'interno della sua area riservata e che serve ad autorizzare le operazioni online eseguite su siti convenzionati (cfr. all. 16), la banca resistente assume che l'attivazione della suddetta password sia avvenuta mediante l'inserimento di un "secondo codice segreto" (fattore di conoscenza) e del codice B*** generato in modo silente dall'applicazione installata sul device del cliente (fattore di possesso).

Dalla documentazione prodotta, si evince che: a) "la label login di secondo livello fa riferimento alla validazione di secondo livello (secondo codice segreto)" (cfr. all. 3 controdeduzioni, foglio "Legenda"); b) in corrispondenza dell'operazione "login secondo livello" risulta la voce "codice corretto" (cfr. all. 3 controdeduzioni, voci evidenziate all'interno dei riquadri rossi nella colonna "dati operativi"); c) non si rinviene invece un'esplicita evidenza del secondo fattore di autenticazione, cioè del codice B*** generato in modo silente dall'applicazione.

Inoltre, nonostante quanto allegato dalla banca resistente, dalle evidenze prodotte si evince che: 1) il tipo di transazione "01" (cfr. all. 6 Controdeduzioni, colonna "tipo transazione") corrisponde ad un pagamento autenticato (cfr. la legenda di cui all'allegato n. 5 alle controdeduzioni); 2) l'esito "Y" (cfr. all. 6 Controdeduzioni, colonna "esito") sta ad indicare che il titolare della carta è stato correttamente autenticato (cfr. la legenda di cui all'allegato n. 5 alle controdeduzioni); 3) il codice "02" (cfr. all. 6 Controdeduzioni, colonna "tipo autenticazione") indica che l'operazione è stata autorizzata mediante l'inserimento di un codice OTP (cfr. legenda di cui all'allegato n. 5 alle controdeduzioni); 4) il codice OTP risulta inviato via sms al numero di cellulare del cliente (cfr. all. 7 Controdeduzioni e denuncia); 5) non risulta invece evidenza diretta del secondo fattore di autenticazione, ossia dell'inserimento della password Mastercard identitiy check.

Tanto premesso, in un precedente analogo, il Collegio di Milano, con decisione scevra da vizi e oggettivamente condivisibile, ha ritenuto l'inidoneità del materiale versato in atti dalla banca in atti al fine della prova della corretta autenticazione, esecuzione e contabilizzazione dell'operazione disconosciuta dal cliente, deducendo al riguardo che "… *Difatti, se risulta comprovata l'effettuazione di un accesso da app, la descrizione del «login primo livello», ossia la validazione del primo codice segreto (elemento di*

conoscenza), e la descrizione del «login terzo livello», ossia la validazione del codice OTP (elemento di possesso) nonché, nell'ambito della sessione così aperta, l'attivazione del Mastercard Identity Check, ossia «la password statica di 5 cifre necessaria per l'utilizzo online dello strumento di pagamento», una preiscrizione con richiesta di password, la conferma di attivazione con touch Id ulteriormente confermata dall'SMS inviato all'utenza di parte ricorrente alle ore 18:02, tutto ciò ai fini dell'accesso all'app (circostanze che concordano con quanto dichiarato dalla stessa parte ricorrente), con riferimento all'esecuzione delle operazioni contestate manca evidenza dell' inserimento della password Mastercard Identitiy Check quale secondo fattore di autenticazione (risultando, invece, l'invio dei codici OTP autorizzativi via SMS." (così, Collegio di Milano, decisione n. 2803 del 4/03/2024).

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 1.500,00 (millecinquecento/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
MARCELLO MARINARI