COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MAIMERI	Membro designato dalla Banca d'Italia
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) PASQUARIELLO	Membro di designazione rappresentativa degli intermediari
(BO) PETRAZZINI	Membro di designazione rappresentativa dei clienti

Relatore FEDERICA PASQUARIELLO

Seduta del 31/01/2023

FATTO

Parte ricorrente è titolare del conto corrente *250 acceso con l'intermediario A cui è collegata la carta bancomat n. *050. Espone che:

- il giorno 06/04/2022, alle ore 15:17 circa, riceveva sul cellulare due messaggi dall'intermediario A, con cui veniva informata che un altro dispositivo era stato associato alla sua App e che per bloccare l'operatività fraudolenta bisognava cliccare su un link;
- la ricorrente cliccava sul link e veniva reindirizzata sulla pagina web ufficiale dall'intermediario A, ove inseriva i propri dati credendo così di bloccare le operazioni sospette;
- subito dopo, alle ore 15:18, riceveva una telefonata da un sedicente agente della polizia postale che la informava che il suddetto intermediario aveva segnalato la violazione di alcuni conti correnti, tra cui il suo, e che la polizia postale era stata allertata per fornire supporto ai correntisti interessati;

- la ricorrente riferiva dell'sms ricevuto e quindi seguiva le istruzioni del falso agente fornendogli i dati statici della carta;
- riceveva quindi tre notifiche da parte dell'intermediario con cui veniva segnalata l'esecuzione di tre operazioni: una da 370,00 e altre due da 100,00 euro. L'agente le riferiva che per bloccare le stesse necessitava dell'autorizzazione della ricorrente, che quindi cliccava sui link presenti negli sms nel frattempo ricevuti;
- il falso agente le riferiva che i truffatori erano probabilmente riusciti anche a impossessarsi dei codici del conto corrente e quindi, per effettuare ulteriori verifiche, si faceva dare dalla ricorrente anche i dati di altro conto acceso con l'odierna resistente (*i.e.* Intermediario B), invitandola a trasferire, mediante bonifico istantaneo di euro 1.900, il saldo residuo su quest'ultimo conto, in modo da mettere al sicuro i propri risparmi;
- dopo l'esecuzione del bonifico, il falso addetto suggeriva alla ricorrente di disinstallare la app relativa al conto detenuto presso l'Intermediario B, quindi la stessa riceveva poi degli sms dalla chat ufficiale della resistente che servivano a *certificare la App*;
- poco dopo il falso agente chiedeva alla ricorrente conferma della ricezione dei tre codici necessari alla certificazione del conto e della App che servivano, a dire del truffatore, a reinstallare la App in questione;
- successivamente si avvedeva che il conto acceso con la resistente risultava essere stato svuotato tramite tre bonifici istantanei dell'importo, rispettivamente, di euro 990,00, 2.990,00 e 1.900,00, e che erano stati effettivamente addebitati i tre pagamenti effettuati tramite la carta bancomat accesa con l'intermediario A.

Quindi domanda il rimborso della somma di euro 5.880,00.

L'intermediario contesta che:

- come descritto nella denuncia, seguendo pedissequamente le istruzioni del messaggio e dopo aver cliccato sul *link* contenuto nel testo dell'SMS, la ricorrente procedeva ad inserire i propri dati all'interno di una non precisata pagina *web* che riportava un logo apparentemente simile a quello dell'intermediario A;
- contattata successivamente sulla medesima utenza telefonica da una persona che si presentava come un Ispettore della Polizia Postale, la signora ha informato telefonicamente quest'ultimo di intrattenere anche un rapporto di conto corrente presso la resistente e ha altresì comunicato allo stesso tutte le credenziali di accesso di tale rapporto;
- l'interlocutore chiedeva alla ricorrente di trasferire la liquidità presente sul conto dell'intermediario A in favore del conto radicato presso la convenuta e poi, seguendo, ancora una volta, tutte le istruzioni del truffatore, la ricorrente trasferiva, con un bonifico istantaneo, la somma di euro 1.900,00 in favore del conto corrente radicato presso la resistente, disinstallava la App relativa a quest'ultimo conto e forniva il codice per certificare l'applicazione che nel frattempo aveva ricevuto via SMS;
- dopo aver fornito all'interlocutore tutti i codici di accesso del proprio internet banking nonché, per ben tre volte, quelli necessari per certificare l'applicazione che nel frattempo il truffatore aveva provveduto ad installare sul proprio dispositivo (e che la signora aveva disinstallato), venivano disposte tre transazioni tramite le quali tutti i fondi presenti sul conto in esame, i.e. euro 5.880,00, venivano trasferiti in favore di due conti correnti bancari esteri riconducibili a terze persone;

- resasi conto del raggiro, in data 11 aprile 2022 (cinque giorni dopo il fatto) ha presentato formale denuncia – querela;
- si eccepisce preliminarmente il difetto di legittimazione passiva della Banca resistente, poiché la ricorrente avrebbe dovuto rivolgere le proprie domande, in sede giudiziale, ai beneficiari dei bonifici in contestazione, o, tuttalpiù, avrebbero potuto eccepire una responsabilità dell'Intermediario A e chiedere a quest'ultimo la restituzione della somma di euro 5.880,00;
- la banca dati eventualmente violata sarebbe quella di un intermediario terzo, non certo quella della convenuta, posto che il messaggio truffaldino era inserito nella chat ufficiale di quest'ultimo;
- l'esistenza del conto corrente presso la resistente è stata comunicata telefonicamente dalla cliente al suo interlocutore, il quale, a sua volta, si è introdotto nella pagina personale del conto della resistente con le credenziali di accesso fornite dalla stessa ricorrente;
- non meno dirompente del precedente motivo è la improcedibilità del ricorso, in quanto, per la medesima vicenda, i Ricorrenti hanno già adito l'autorità giudiziaria penale mediante denuncia – querela;
- nel merito, il ricorso sarebbe comunque infondato, poiché la truffa è stata perpetrata solo ed unicamente per colpa grave della ricorrente;
- per converso, è evidente come la resistente abbia adottato un sistema di autenticazione c.d. "forte", declinato secondo le caratteristiche della conoscenza (le credenziali statiche di accesso), del possesso (il dispositivo mobile) e dell'inerenza (il pin dispositivo), la cui efficacia, tuttavia, è stata completamente neutralizzata dalla condotta gravemente colpevole e negligente della ricorrente.

Conclude pertanto per il rigetto del ricorso.

In sede di replica il ricorrente afferma che:

- il ricorso presentato nei confronti della resistente è del tutto legittimo ed ammissibile in quanto sussiste la legittimazione passiva della banca, che ha permesso la realizzazione della truffa di cui si discute;
- i sistemi di sicurezza adottati dalla predetta Banca non sono risultati idonei: allorquando i malviventi hanno disposto i tre bonifici istantanei non è arrivato nessun "alert" che avvisasse di ciò che stava accadendo;
- dal tenore dei tre messaggi ricevuti, la ricorrente non poteva certo immaginare che comunicando quei tre codici avrebbe autorizzato i bonifici istantanei;
- risulta palese la responsabilità dell'istituto di credito, perchè se la ricorrente avesse ricevuto gli SMS alert non avrebbe mai comunicato quei codici;
- si ritiene del tutto infondata oltre che inconferente l'eccezione sollevata da controparte circa l'irricevibilità del ricorso presentato, in quanto l'azione esercitata in sede penale e quella esercitata in questa sede hanno presupposti e finalità differenti. L'azione penale ha come scopo quella di vedere condannati gli eventuali responsabili per il compimento di condotte penalmente rilevanti. L'azione esercitata in questa sede ha invece unicamente finalità risarcitorie.

DIRITTO

Il Collegio osserva che la controversia riguarda il disconoscimento di tre operazioni di bonifico eseguite il 6.04.2022 rispettivamente per euro 990,00; 2.990,00; 1900,00.

In via preliminare, il Collegio prende in esame l'eccezione sulla asserita litispendenza, per l'apertura di procedimento penale, a seguito di denuncia querela, nei confronti del beneficiario dei bonifici disconosciuti. Il Collegio rileva che la mancanza di identità soggettiva tra le parti, rispettivamente, del procedimento penale e del procedimento radicato avanti questo arbitro conduce a ritenere insussistente la litispendenza (come affermato dal Coll. Coord. 5265/2014); l'eccezione va quindi respinta.

Altrettanto va respinta l'eccezione sulla carenza di legittimazione passiva dell'odierno convenuto: egli eccepisce che le doglianze di parte ricorrente andrebbero rivolte verso i beneficiari dei bonifici in contestazione o verso l'Intermediario A, dal quale è stata tratta la provvista, in seguito versata sul conto acceso presso l'intermediario oggi convenuto, necessaria per poi effettuale i bonifici a favore di soggetti terzi. In particolare, la eventuale legittimazione passiva dell'intermediario A deriverebbe dal fatto che il messaggio che ha dato origine alla truffa in esame sarebbe stato ricevuto sulla chat ufficiale di tale banca, e quindi le falle nei sistemi di sicurezza sarebbero da imputare solo a tale istituto di credito.

Il Collegio reputa correttamente radicato il ricorso in punto di legittimazione, a considerare che il ricorso ha ad oggetto il rimborso della somma di 5.880,00 euro, corrispondente all'importo dei bonifici disposti dai truffatori a valere sul conto corrente acceso con la odierna resistente.

Il Collegio rileva poi che le operazioni contestate sono state poste 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.
A fronte del disconoscimento delle operazioni di pagamento da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, del D.Lgs. 11/2010, che così statuisce: *"Qualora l'utilizzatore 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"*.
Con riguardo alla modalità di autenticazione delle operazioni, l'art. 10 bis del medesimo D.Lgs. n. 11/2010 prevede: *"Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, 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, lettera q bis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in *"un'autenticazione basata sull'uso di due o piu' 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"*.
Sul punto, è intervenuta l'EBA con la "Opinion" del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27.11.2017), nella quale sono stati passati in rassegna alcuni dei più comuni sistemi di autenticazione predisposti dagli intermediari per valutare se possano o meno annoverarsi tra i presidi di autenticazione forte.
Occorre dunque verificare se, nel caso di specie, le operazioni contestate siano state autenticate mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".

Nello specifico, al fine di dimostrare la corretta autenticazione dei bonifici istantanei disconosciuti, l'intermediario afferma e documenta, depositando log informatici esplicativi, che per l'enrollment della App sul *device* del frodatore è stato necessario inserire credenziali statiche, e a seguire, PIN e codice OTP inviato per sms. Se questa procedura risulta coerente con un sistema di autenticazione multifattoriale, invece quanto alla autenticazione di ciascuna delle operazioni disconosciute, risulta documentata la applicazione di un solo fattore di autenticazione, cioè, l'inserimento dei codici ricevuti direttamente dal frodatore sul proprio *device*.

Tanto rilevato in punto di mancata prova circa la corretta autenticazione delle operazioni disconosciute, il ricorso merita accoglimento, esonerando il Collegio dalla disamina degli ulteriori profili, connessi alla valutazione del grado di colpa nella condotta del ricorrente.

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 5.880,00 (cinquemila ottocento ottanta/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