

COLLEGIO DI ROMA

composto dai signori:

(RM) GRECO	Presidente
(RM) PAGLIETTI	Membro designato dalla Banca d'Italia
(RM) POZZOLO	Membro designato dalla Banca d'Italia
(RM) CAPPIELLO	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore CHERTI STEFANO

Seduta del 05/10/2021

FATTO

1) Il ricorrente in data 24 ottobre 2020, si recava presso la banca per effettuare un prelievo bancomat; in tale occasione, tuttavia, apprendeva che nel conto corrente non vi era alcuna disponibilità di danaro. Provvedeva dunque ad effettuare un estratto conto dal quale emergevano due transazioni in favore di un soggetto sconosciuto e non avente con lui alcun rapporto; in particolare si trattava di due bonifici on-line di € 9.871,00 e di € 1.601,00 effettuati rispettivamente in data 20/10/2020 e 21/10/2020.

2) Segnalava l'accaduto all'intermediario, il quale provvedeva al blocco delle operazioni sul conto corrente e lo invitava ad attendere un successivo contatto per maggiori informazioni. Non avendo più ricevuto alcun successivo riscontro, in data 26 ottobre 2020, sporgeva denuncia dell'accaduto che veniva subito trasmessa anche agli Uffici della banca (in questa occasione è stata formulata la richiesta di rimborso degli importi relativi alle operazioni disconosciute).

3) Tuttavia, in data 6 novembre 2020, l'intermediario riscontrava negando la richiesta di rimborso. In tale sede, l'intermediario ignorava completamente la circostanza relativa all'avvenuto blocco della SIM CARD nelle date in cui in cui venivano disposte le operazioni poi disconosciute. Successivamente, in data 17 novembre 2020 diffidava parte convenuta a provvedere alla restituzione della somma di Euro 11.472,00, indebitamente sottratta dal conto corrente.

4) L'intermediario, costituendosi, ha confermato che il è titolare del conto corrente al quale è collegato il servizio "*Rapporti a distanza tra Banca e Cliente*" c.d. home banking, che consente ai clienti di effettuare le operazioni di *inquiry* e dispositive sui conti correnti personali a loro riferibili, utilizzando il telefono cellulare o Internet (il ricorrente aveva altresì attivato il servizio SMS Alert collegato al suo numero di telefono cellulare certificato). Il servizio fornito "*Rapporti a distanza tra Banca e Cliente*" prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte", in linea con la normativa europea PSD2.

5) Nel caso specifico, come dimostrato nel dettaglio degli SMS, la Banca alle ore 15:45 del 20/10/2020 ha inoltrato al ricorrente, sul proprio cellulare un SMS alert, avente il seguente contenuto: "*Stai attivando il Mobile Token. Ricordati che il personale B** non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ***** Info ******". Di fronte a tale comunicazione il ricorrente, oltre a non dover comunicare a nessuno il codice OTP contenuto nel messaggio, sapendo di non essere stato lui a richiederlo, avrebbe dovuto contattare subito il personale della banca così da evitare ogni danno a suo carico.

6) La sostituzione della sim card, non consente l'aggiornamento del sistema di autenticazione a doppio fattore adottato in quanto non si può giungere alla fase di generazione del codice OTP necessario per attivare il *Mobile Token* se non si conoscono le credenziali di sicurezza, Id Cliente e codice PIN noto solo al cliente e che neppure il personale della Banca conosce.

7) Secondo l'intermediario nel caso di specie è plausibile presumere che il cliente non abbia adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del suo strumento di pagamento, rivelandole a terzi non autorizzati.

DIRITTO

Come emerge dalla documentazione in atti, il ricorrente è stato vittima di una frode informatica che ha consentito l'effettuazione di due bonifici on-line di € 9.871,00 e di € 1.601,00; detta frode, come emerge da quanto allegato, sembra essere stata perpetrata tramite la c.d. *SIM Swap Fraud*.

Giova inoltre ricordare che le operazioni fraudolente sono state poste in essere successivamente all'entrata in vigore della normativa di recepimento della PSD 2. Ebbene, secondo l'orientamento condiviso dei Collegi ABF in materia di *sim swap fraud*, la sostituzione della sim card deve essere equiparata alla mancanza di autenticazione dell'operazione di pagamento, ai sensi dell'art. 10 del d.lgs. 11/2010. Infatti, mentre nei casi di *man-in-the-browser* la valutazione della vicenda rientra nell'ambito dell'art. 12 del D.lgs. 11/2010, riguardando i profili di colpa del cliente, nelle fattispecie di *sim swap fraud* l'operazione non può ritenersi "regolarmente autenticata" in conseguenza della sostituzione della sim dell'utenza telefonica associata al servizio di home banking, venendo quindi in questione l'applicazione dell'art. 10 del menzionato decreto.

Dunque, nel caso di specie il ricorso non può che essere accolto nella sua interezza, posto che in tale fattispecie la sostituzione della sim card va equiparata alla mancanza di autenticazione dell'operazione di pagamento.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 11.472,00.

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
FERNANDO GRECO