

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CETRA

Seduta del 21/03/2024

FATTO

Con ricorso del 7 novembre 2023, parte ricorrente riferiva di aver ricevuto in data 8.9.2023, alle ore 16:03, un SMS apparentemente proveniente dall'intermediario N** con il quale veniva chiesta la conferma di un'operazione di bonifico pari a € 382,00, con possibilità di negare la predetta operazione cliccando sul link contenuto nel predetto SMS; di avere quindi seguito la procedura indicata e di avere ricevuto, alle ore 16:46, una telefonata dal numero 05***180 corrispondente all'utenza dell'intermediario convenuto presso il quale insisteva il rapporto di c/c ***141; di avere continuato a seguire la procedura indicata dal presunto operatore per bloccare i bonifici, quindi di avere tentato di mettersi in contatto con il proprio consulente finanziario nonché dipendente della banca per chiedere chiarimenti immediatamente dopo la predetta telefonata senza ottenere alcun riscontro; di avere ricevuto in data 11.9.2023 un'altra telefonata sempre dall'utenza 05**180, apparentemente riconducibile all'intermediario, con la quale il sedicente operatore esponeva la necessità di conservare le ricevute dei tentativi dei bonifici per sporgere denuncia; di aver ricevuto una terza telefonata in data 14.9.2023, nel corso della quale la cliente capiva che si trattava di una truffa e quindi chiamava il suo consulente finanziario per bloccare il c/c. Presentato, senza esito, il reclamo nei confronti



dell'intermediario, attivava, quindi, il presente procedimento per richiedere a quest'ultimo la restituzione della somma sottratta pari ad euro 10.000,00.

L'intermediario, nelle controdeduzioni, eccepiva la legittima esecuzione e sostanziale regolarità delle operazioni disconosciute; affermava la colpa grave della ricorrente per aver cliccato sul link contenuto nell'SMS ed inserito le proprie credenziali di accesso al proprio internet banking, consegnandole in questo modo ai truffatori; per non avere bloccato immediatamente il suo c/c e il relativo servizio di internet banking dell'Area Clienti, nonostante i sospetti ingenerati dalla chiamata del venerdì 8.9.2023; per avere colpevolmente ignorato tutte le comunicazioni che venivano inoltrate a far data dal 8.9.2023 via mail con le quali veniva informata dei vari accessi al suo internet banking e delle avvenute esecuzioni dei bonifici e che, nonostante la ricezione delle predette comunicazioni, solamente in data 14.9.2023 aveva preso contatti con la filiale. Eccepiva che il consulente finanziario non avesse risposto alla chiamata nonché al successivo vocale whatsapp perché in ferie. Chiedeva, per tutto quanto precede, il rigetto del ricorso.

La ricorrente, con le repliche, insisteva nella domanda, e ribadiva l'ingannevolezza del messaggio truffaldini; negava di aver immesso le proprie credenziali personali sul link truffaldino né di avere condiviso alcuna user_id o password, ma di aver effettuato il proprio accesso alla propria Area Clienti tramite il riconoscimento facciale; precisava che il fatto che il consulente leggesse il messaggio senza darne seguito rassicurava la cliente che nulla di anomalo fosse successo; contestava l'inadeguatezza dei sistemi di sicurezza della banca. L'intermediario, con controrepliche, insisteva nel rigetto del ricorso sostenendo, tra l'altro che la tipologia di truffa in cui era incorsa la cliente era molto nota e non particolarmente sofisticata; che la schermata prodotta in atti con le repliche non provava la riconducibilità delle telefonate ricevute al numero della banca; che l'SMS civetta presentava evidenti indizi di anomalia; che la vicenda truffaldina descritta dalla cliente era poco chiara e che l'utilizzo del riconoscimento facciale era stato utilizzato per lo sblocco del telefono, mentre per l'accesso all'area riservata la cliente aveva utilizzato le proprie credenziali personali.

DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte al ricorrente attraverso due operazioni di bonifico dell'importo complessivo di euro 10.000,00. Le operazioni contestate sono avvenute lo 11 settembre 2023: esse, pertanto, in quanto operazioni disconosciute, rientrano nell'ambito di applicazione della disciplina del d. lgs. 27.1.2010, n. 11 di recepimento della Direttiva 2007/64/CE sui servizi di pagamento, come modificata dal d. lgs. 15 dicembre 2017, n. 218, di recepimento della Direttiva 2015/2366/UE.

Il Collegio ricorda che, per la normativa appena richiamata, la corretta esecuzione di un'operazione di pagamento è subordinata al consenso del pagatore (art. 5 d. lgs. 11/2010), prestato nella forma e secondo la procedura contrattualmente prevista. Qualora l'utente neghi di aver autorizzato l'operazione o sostenga che questa non sia stata correttamente eseguita, lo stesso può ottenerne il rimborso dell'importo (art. 11 d. lgs.



11/2010), a meno che il prestatore dei servizi di pagamento non riesca a provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10, comma 1, d. lgs. 11/2010). Il prestatore dei servizi, peraltro, assolto con successo questo primo onere, necessario ma di per sé insufficiente a dimostrare che l'operazione sia stata autorizzata dal titolare, deve ancora provare, al fine dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento, fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010, trattandosi primariamente di obblighi di custodia del dispositivo e delle chiavi di accesso al servizio. La valutazione della condotta dell'utilizzatore, ai fini dell'eventuale giudizio di colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.

Il Collegio ricorda, inoltre, che la suddetta autenticazione si deve realizzare in forma di autenticazione forte (c.d. strong customer authentication in acronimo SCA), secondo quanto stabilito dagli artt. 97 e 98 della PDS2, dall'art 10-bis del d. lgs. 10/2011 e nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dallo stesso EBA. E questo sia nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni: l'autenticazione, in tutti questi casi, richiede almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso; gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Il Collegio, passando allo specifico caso oggetto di decisione, rileva che l'intermediario afferma che le operazioni contestate siano state correttamente contabilizzate, registrate e autenticate documentando l'esecuzione di tre bonifici in date diverse a seguito di inserimento di PIN [***60] (elemento di conoscenza) e OTP [162011; 719921 e 029663] (elemento di possesso) da APP (cfr. dispositivo mobile); tuttavia l'intermediario non produce evidenza relativamente all'accesso all'home banking propedeutico all'esecuzione dei bonifici, sebbene affermi che un accesso vi sia stato mediante inserimento delle credenziali di accesso della cliente. Per costante orientamento dell'Arbitro, in tali casi il ricorso deve essere accolto integralmente, posto che la mancanza della prova di autenticazione, in questo caso nella fase di accesso al servizio *on line*, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili alla ricorrente: la prova di autenticazione rappresenta, infatti, in aderenza al quadro normativo innanzi esposto, un *prius* logico rispetto alla prova di colpa grave dell'utente. Ne consegue l'accoglimento della domanda per mancata prova della corretta autenticazione delle operazioni disconosciute.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 10.000,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

della procedura e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA