

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SANTARELLI

Seduta del 30/04/2024

FATTO

Parte ricorrente agisce per ottenere il rimborso di “€ 9.001,00 oltre le spese di procedura sostenute” oggetto di truffa. Questi i fatti posti a fondamento della domanda. In data 15/09/2023 parte ricorrente riceveva un SMS, in cronologia ad altri messaggi dell'intermediario, che la avvisavano della presenza di anomalie sul proprio conto e della conseguente necessità di accreditare tutti i suoi risparmi su una nuova carta. Parte ricorrente cliccava, quindi, su un *link* presente nell'SMS e successivamente veniva contattata da un sedicente operatore dell'intermediario che carpiva la sua fiducia, essendo a conoscenza dei suoi dati personali e del suo conto. Il truffatore faceva, quindi, eseguire a parte ricorrente alcune operazioni per smobilizzare i suoi risparmi dal proprio libretto e dalla carta, ad esso associata, n. ***616 verso la ricaricabile n. ***379. A conferma di tali operazioni parte ricorrente riceveva un SMS. Il sedicente operatore la invitava a questo punto a recarsi presso lo sportello dell'intermediario per eseguire un bonifico a favore della carta n. ***407, per un importo di € 9.001,00, così azzerando totalmente il proprio conto corrente ed i propri investimenti. In proposito parte ricorrente si lamenta del fatto che nessuno degli operatori presenti allo sportello dell'intermediario la allertava circa la truffa che stava subendo, di cui si avvedeva solo dopo essere rientrata a casa. Recatasi nuovamente allo sportello dell'intermediario per il blocco di tutte le carte, le veniva riferito che l'addebito non era più revocabile.

L'intermediario convenuto non ha depositato controdeduzioni, mentre è intervenuto nel procedimento il secondo intermediario in qualità di effettivo titolare del rapporto giuridico oggetto del contendere, chiedendo il rigetto del ricorso. Questa la sintesi delle argomentazioni svolte: (a) parte ricorrente, titolare della carta n. ***379, chiede il rimborso dell'importo di una operazione di ricarica di prepagata disposta presso lo sportello dell'intermediario in data 15/09/2023; (b) l'operazione è stata interamente eseguita da parte ricorrente senza comunicare alcunché all'addetto dello sportello e in costante contatto telefonico con il truffatore e, pertanto, il relativo addebito è esclusivamente ascrivibile alla sua condotta; (c) tale tipologia di frodi non rientra nell'ambito di applicazione della disciplina di cui agli artt. 10 e 5 del d.lgs.11/2010; (d) l'operazione risulta effettuata in assenza di anomalie, previa corretta lettura del *microchip* della carta n. ***379 e autorizzazione della titolare tramite riconoscimento informatico avvenuto con digitazione del codice segreto PIN; (e) parte ricorrente ha contribuito in maniera determinante alla compromissione del suo dispositivo di pagamento, fornendo incautamente a terzi i dati che invece era tenuta a custodire gelosamente; (f) la frode oggetto del contendere è riconducibile un classico *phishing*, da tempo oggetto di campagne informative antifrode sul proprio sito, nell'apposita sezione Sicurezza; (g) la frode sembrerebbe essersi perfezionata attraverso il c.d. SMS *spoofing*, seguito dalla telefonata del finto operatore, c.d. *vishing*; (h) l'intermediario interloquisce con i propri clienti solo tramite canali ufficiali e mai richiedendo la comunicazione di dati relativi agli strumenti di pagamento forniti; non allega *link*, non minaccia la chiusura del conto o dell'*home banking* con SMS o *e-mail*, non invia *e-mail ultimatum*; (h) non sussiste alcun *vulnus* nel sistema di autorizzazione alla operazione adottato dall'intermediario.

Parte ricorrente ha replicato per osservare che: (i) non ha mai ceduto a nessuno le proprie credenziali di accesso; (ii) nell'app dell'intermediario sussiste un'anomalia di sicurezza, che ha permesso al truffatore di entrare in possesso dei suoi dati personali, inducendola a ritenere di essere in contatto con l'intermediario; (iii) la richiesta del malfattore di recarsi presso lo sportello dell'intermediario la ha indotta a ritenere di poter ricevere assistenza dal personale presente; (iv) il personale dell'intermediario avrebbe dovuto accorgersi che era vittima di truffa informatica, a fronte dell'operazione che andava ad azzerare tutti i suoi risparmi; (v) l'assenza di causale dell'operazione eseguita allo sportello avrebbe dovuto altresì allarmare gli operatori dell'intermediario, tenuti a operare secondo la diligenza posta a carico del professionista; (vi) nello stesso giorno – il 15/09/2023 - sono state effettuate tre operazioni di carattere anomalo, per le quali l'intermediario avrebbe dovuto rilevare un rischio di frode e cioè due disinvestimenti per € 3.242,24 e € 3.800,00 e, a pochi minuti di distanza, il bonifico di € 9.001,00, lasciando sul deposito della carta della cliente soltanto € 75,05. Parte ricorrente insiste quindi nella domanda formulata.

L'intermediario ha a sua volta controreplicato, contestando in fatto ed in diritto tutto quanto dedotto ed eccepito ed insistendo nel rigetto del ricorso.

DIRITTO

Materia del contendere è un'operazione di ricarica di carta prepagata per € 9.901,00 (di cui €1,00 per commissioni) effettuata personalmente da parte ricorrente presso uno sportello dell'intermediario il 15/09/2023, alle ore 14.55. Operazione preceduta da due giroconti sulla carta prepagata di parte ricorrente (n. ***379), successivamente utilizzata

per l'esecuzione dell'operazione e in particolare: (a) un'operazione di bonifico istantaneo sulla carta prepagata n. ***379, per € 3.242,21 (questo l'importo che risulta dalla documentazione prodotta); (b) un'operazione di ricarica della carta prepagata n. ***379 dal libretto di titolarità della cliente stessa, pari a € 3.800,00.

Lo svolgersi degli eventi, che attesta il fatto che l'operazione disconosciuta è stata effettuata dalla stessa ricorrente, è descritto nella denuncia da cui si apprende che, come indicato anche nel ricorso, parte ricorrente ha ricevuto il primo messaggio truffaldino in data 15/09/2023, alle ore 12.00 circa, seguito da un secondo messaggio, in cui veniva avvisata che sarebbe stata contattata da un operatore dell'intermediario. Quindi, a distanza di pochi minuti, parte ricorrente ha dichiarato di aver ricevuto una chiamata dal numero 329****258, nel corso della quale il sedicente operatore la informava di alcune frodi riscontrate nel sistema dell'intermediario e la invitava a proteggere il proprio conto. A tal fine, dichiara parte ricorrente, essa veniva indotta a comunicare al sedicente operatore il numero e tutti i dati della propria carta prepagata, cosa che essa faceva. Quindi, il truffatore la invitava a recarsi presso lo sportello dell'intermediario e ad accreditare la somma di € 9.000,00 su una carta da lui indicata, il cui numero e la cui intestazione le erano state comunicate. Quindi, parte ricorrente effettuava l'operazione contestata alle ore 15.30 circa del 15/09/2023. Nella denuncia parte ricorrente precisa di essere rimasta in contatto telefonico con il truffatore per tutto il tempo necessario a recarsi presso lo sportello, ad eseguire l'operazione e ad inviarne conferma tramite messaggistica WhatsApp.

Essendo pacifico che l'operazione oggetto del ricorso è stata disposta direttamente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione) da parte ricorrente, sia pure per effetto di un raggio, seguendo le istruzioni impartite dal frodatore, l'operazione non può che essere considerata autorizzata. Pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D. Lgs n. 11/2010 e quindi l'intermediario è esonerato dalla prova di autenticazione ai sensi degli artt. 10 ss. del decreto citato.

Ai fini della valutazione della sussistenza, comunque, di un eventuale apporto causale dell'intermediario alla frode (ad esempio, per la mancata disponibilità, anche temporanea, del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore; ovvero per la mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore, etc.) vanno esaminati gli ulteriori fatti che risultano dalle rappresentazioni rese e dai documenti disponibili in merito alla modalità della truffa e alla condotta delle parti. Rileva in proposito ed in primo luogo il fatto che parte ricorrente ammette (a) di aver cliccato sul *link* contenuto nel messaggio ricevuto in data 15/09/2023, con cui veniva informata di un accesso anomalo al proprio conto; (b) di avere inserito i propri dati nella propria area personale *dell'home banking* accedendovi; (c) di aver seguito le istruzioni ricevute dal sedicente operatore per effettuare operazioni che pensava fossero volte a mettere al sicuro i propri risparmi; (d) di aver effettuato le operazioni, di cui riceveva conferma tramite SMS. Agli atti risultano, poi, i vari SMS truffaldini, tra cui quello civetta, da cui risulta che: (i) il *link* contenuto nel messaggio civetta non è riconducibile al dominio dell'intermediario, anche se la denominazione della *chat* in cui è inserito il messaggio è riferibile all'intermediario; (ii) il messaggio civetta contiene anomalie lessicali (si passa dal registro del "lei" a quello del "tu"); (iii) nella *chat* sono presenti messaggi genuini dell'intermediario, in particolare quelli contenenti i codici per disporre le operazioni che parte ricorrente stava eseguendo dietro direttive del truffatore. Non risulta, invece, agli atti lo *screenshot* della chiamata che parte ricorrente afferma di aver ricevuto dal numero

329****258 che, comunque, non pare riconducibile all'intermediario convenuto. Infine, risulta agli atti che l'operazione contestata è stata effettuata dalla cliente presso lo sportello dell'intermediario. A tal proposito, parte ricorrente si lamenta che l'operatore dell'intermediario presente allo sportello non ha identificato il tentativo di frode in corso ai suoi danni. Tuttavia, il Collegio non può in proposito non tenere conto, tra l'altro, del fatto che risulta agli atti come parte ricorrente sia rimasta in collegamento con il truffatore anche mentre era presso gli uffici dell'intermediario e che in uno degli SMS prodotti parte ricorrente è stata invitata *“per motivi di indagine” “a non divulgare informazioni”*: il che porta ad escludere che essa si sia rivolta all'addetto esponendo le richieste del frodatore o fornendo dettagli dai quali l'addetto allo sportello avrebbe potuto desumere il compimento di un tentativo di frode in atto. Né, quanto alla condotta dell'intermediario, rilevano indici di anomalia dell'operazione. Da un lato, le prime due operazioni (non oggetto di disconoscimento e comunque del presente procedimento) costituiscono, sì, atti preparatori dell'operazione fraudolenta per costituire provvista, tuttavia, sono operazioni effettuate a favore della carta prepagata della stessa ricorrente e come tali, ai fini degli indici di anomalia irrilevanti. Dall'altro, non vi è agli atti copia del contratto e non è quindi possibile stabilire i limiti operativi eventualmente previsti. Infine, la mera sussistenza di un indice di rischio di frode – e nella specie non risulta la sussistenza degli indici di anomalia/rischio frode di cui al D.M. 112/2007, che vengono valorizzati da questo Arbitro - non determina di per sé responsabilità per l'intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA