## COLLEGIO DI ROMA

composto dai signori:

| | |
|---|---|
| (RM) SIRENA | Presidente |
| (RM) MARINARO | Membro designato dalla Banca d'Italia |
| (RM) PATTI | Membro designato dalla Banca d'Italia |
| (RM) SICA | Membro di designazione rappresentativa degli intermediari |
| (RM) SARZANA DI S. IPPOLITO | Membro di designazione rappresentativa dei clienti |

Relatore FRANCESCO PAOLO PATTI

Seduta del 13/04/2023

## FATTO

Parte ricorrente afferma che, in data 22/09/2022, riceveva un sms da un numero con cui la banca comunicava normalmente con la cliente; cliccava sul messaggio mentre era in macchina e immediatamente veniva contattata da un sedicente operatore della banca, che l'avrebbe aiutata a impedire una frode in atto; il primo sms ricevuto, che avrebbe indotto la ricorrente in errore, escluderebbe la responsabilità o la colpa della stessa nella vicenda in esame; per converso, i sistemi della banca sarebbero risultati carenti e insufficienti a impedire le truffe. Per l'effetto, chiede la restituzione della somma di € 523,12, corrispondente a tre transazioni online disposte da terzi ignoti.

L'intermediario resiste al ricorso eccependo che la cliente sporgeva denuncia in data 26/09/2022 indicando le tre operazioni disconosciute; da quanto descritto in tale occasione la ricorrente, per sua stessa ammissione, sarebbe stata vittima di una truffa realizzata attraverso *smishing* misto a *vishing*, consistente nell'invio di sms fraudolenti che sembrano provenire dalla propria banca (cd. *sms spoofing*) e mirano a carpire dati riservati per poter effettuare operazioni dispositive; la cliente avrebbe inizialmente cliccato sul link contenuto nel testo di un sms civetta, inserendo i dati di accesso al proprio *internet banking* e il numero di cellulare; successivamente, ricevuta una telefonata da parte di un sedicente

operatore della banca (*vishing* semplice), avrebbe comunicato tutti i dati necessari per poter operare sul proprio *digital banking* e compiere le operazioni in questione. Riferisce altresì che le operazioni disconosciute sarebbero state effettuate previo accesso al *digital banking* della ricorrente; tale accesso avviene attraverso credenziali personali che garantiscono la riconoscibilità della cliente e la massima sicurezza (digitazione di un codice utente; digitazione di una password, composta da 8 cifre e di esclusiva conoscenza della cliente); avendo optato per la modalità di autenticazione tramite sms, la stessa riceveva sul proprio *smartphone* un messaggio contenente una password temporanea (OTP), a sei cifre, univoca dell'operazione da autorizzare, la cui scadenza è impostata a dieci minuti. Inoltre, dall'analisi della operatività, come certificato dai relativi *log* informatici, si evincerebbe che tutti gli accessi all'*internet banking* sarebbero avvenuti mediante la corretta autenticazione prevista dall'intermediario in ottemperanza agli attuali protocolli di sicurezza e basata sui principi dell'autentificazione c.d. "*forte*"; gli accessi all'*internet banking*, infatti, sarebbero avvenuti mediante la modalità di autenticazione forte e digitazione di codice utente, password e codice di conferma temporaneo inviato per sms sull'utenza telefonica della cliente; tutte le operazioni contestate sarebbero avvenute durante il primo accesso, nel quale veniva modificato il della carta prepagata (tramite OTP specifico pervenuto sul numero telefonico della ricorrente); in seguito, veniva inserita la carta prepagata nella rubrica del *digital banking*, così da rendere più veloce la ricarica essendo sufficiente selezionarla, senza dover digitare nuovamente il numero; venivano effettuate le ricariche, alcune delle quali non andavano a buon fine in quanto realizzate su un conto non capiente; alle ore 18:29 veniva effettuato il blocco dell'utenza per frode. Eccepisce altresì che la ricorrente avrebbe potuto accorgersi facilmente dell'anomalia e dell'inattendibilità nel messaggio ricevuto; la cliente avrebbe ricevuto per ogni operazione di pagamento un messaggio contenente il codice OTP autorizzativo composto da uno standard specifico atto a non lasciare dubbi in merito al tipo di operazione da autorizzare. Alla luce di quanto esposto, chiede il rigetto del ricorso.

## DIRITTO

1. Parte ricorrente chiede la restituzione della somma di € 523,12, corrispondente a tre transazioni online disposte da terzi ignoti all'esito di una truffa perpetrata tramite la tecnica del c.d. sms *spoofed* seguito da *vishing*. L'intermediario chiede di rigettare il ricorso.
2. Il ricorso merita accoglimento entro i limiti di seguito indicati.
3. Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).
4. Sulla base della ricostruzione dei fatti presentata dalle parti, risulta che la ricorrente ha cliccato sul *link* contenuto nel messaggio esca ed è stata reindirizzata su un sito clone di accesso all'area riservata della banca, dove ha inserito nome utente e password, nonché il numero di cellulare; contattata dal frodatore, che nel frattempo effettuava il login con le predette credenziali, riferiva a quest'ultimo il codice (OTP) necessario per l'accesso all'*home banking*; alle ore 18.00, il frodatore ha modificato il codice per effettuare gli acquisti on-line con la carta prepagata, operazione autorizzata dalla ricorrente con notifica *push* inviata sulla sua applicazione; una volta memorizzata nell'*home banking*, la carta prepagata è stata ricaricata con due addebiti effettuati sul conto della ricorrente (rispettivamente di € 250,00 e € 2.000,00), per poter disporre gli acquisti on-line; per ogni operazione di pagamento sono stati inviati i codici dispositivi

sul cellulare della ricorrente, comunicati per sua stessa ammissione al sedicente operatore; sulla base delle evidenze prodotte, gli acquisti risultano autorizzati tramite l'uso dell'OTP pervenuto sul cellulare della cliente (elemento di possesso) e il pin (elemento di conoscenza), in possesso del frodatore.

5. Orbene, la prima fase della frode è ascrivibile all'ipotesi di *smishing* con sms *spoofed*, in cui il messaggio civetta si mescola alle comunicazioni genuine correntemente trasmesse dall'intermediario. Sul punto, questo Arbitro ha chiarito che "*ciò è possibile in quanto, attraverso l'utilizzo di appositi software in grado di modificare l'ID del mittente, i frodatori possono far sì che un sms appaia con il nome dell'intermediario. In sostanza, il messaggio truffaldino viene visualizzato sullo smartphone insieme a precedenti messaggi provenienti dall'intermediario, ingenerando nella vittima la convinzione della sua genuinità*" (cfr. Collegio di Roma, decisione n. 3750/2021).
6. Alla luce della documentazione in atti, la seconda fase della frode appare riconducibile al modello del *vishing*, effettuato tramite un numero di telefono non riconducibile alla banca. Secondo l'orientamento condiviso di questo Arbitro, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario) del messaggio civetta. In tale caso, può essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa – similmente a quanto avviene negli episodi di *phishing* – e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario. Alla luce di quanto esposto, parte ricorrente ha diritto alla restituzione della somma di € 300,00 determinata in via equitativa.

## PER QUESTI MOTIVI

**Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 300,00, determinata in via equitativa.**

**Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di € 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA