COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) BARTOLINI	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SALVATORE SICA

Seduta del 26/10/2023

FATTO

La ricorrente riferisce che, in data 07.03.2022, mentre era impegnata ad effettuare un bonifico in favore del figlio, appariva una finestra in cui la si invitava a fornire un recapito telefonico al fine di aggiornare il questionario MIFID. Dopo aver inserito il proprio numero di cellulare e aver tentato inutilmente di disporre il bonifico, riceveva una telefonata dal numero della banca da parte di un sedicente operatore dell'intermediario, il quale le rappresentava che avrebbe sbloccato il pagamento mediante l'invio via *mail* di un QR *code* che avrebbe generato un OTP che la ricorrente avrebbe dovuto poi comunicargli. Ella, pertanto, provvedeva a seguire le indicazioni fornite. Soltanto in seguito si accorgeva della presenza di due bonifici istantanei di € 15.000 (già restituiti a seguito di *recall*) e di € 14.000.
Insoddisfatta dell'interlocuzione con la resistente, si rivolge all'Arbitro per ottenere il rimborso di € 14.000.
L'intermediario, costituitosi, rileva che l'operazione contestata è stata eseguita, senza anomalie, tramite un sistema di autenticazione forte. Evidenzia, pertanto, la colpa grave della ricorrente nella custodia delle credenziali e chiede che il ricorso sia rigettato.

DIRITTO

L'odierna controversia ha ad oggetto il rimborso di € 14.000,00, fraudolentemente sottratti alla ricorrente mediante l'esecuzione di un bonifico effettuata da terzi ignoti e non autorizzato.
La predetta operazione è stata eseguita in data 07.03.2022 e, pertanto, ricadono nell'ambito della vigenza temporale del d.lgs. n. 11/2010, così come modificato dal d.lgs. n. 218/2017 che ha recepito la c.d. PSD2 (Direttiva 2015/2366/UE).
Come è noto, l'art. 10, d.lgs. n. 11/2010, nella formulazione ratione temporis applicabile al caso in esame, pone in capo al prestatore di servizi l'onere di provare che l'operazione «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». La richiamata normativa impone al prestatore di servizi di pagamento anche l'onere di dimostrare che l'utente abbia agito con dolo o colpa grave o, addirittura, mediante un comportamento fraudolento.
Nel caso in esame, per quanto riguarda il profilo della SCA, così come innanzi delineato, dalla documentazione prodotta dall'intermediario è possibile rilevare che l'operazione è stata eseguita a seguito di *login* effettuato sull'*home banking* da *desktop*, mediante inserimento delle credenziali statiche (codice utente e *password*) e dell'OTP. Inoltre, essa è stata autorizzata attraverso l'inquadramento del QR *Code* (inviato alla ricorrente dai malfattori via *mail*) dall'*app* dell'intermediario, digitazione del PIN e del codice OTP generato dall'applicazione.
Da ciò si ricava che le operazioni sono state compiute grazie al comportamento della ricorrente, che ha comunicato le credenziali statiche e dinamiche ai malfattori. Sul punto, tuttavia, va evidenziato che la ella è stata vittima di una truffa sofisticata e particolarmente insidiosa: nel momento in cui stava eseguendo un bonifico in favore del figlio, non andato a buon fine, le è apparsa sullo schermo una finestra in apparenza riferibile alla banca resistente relativa all'aggiornamento del questionario MIFID e, subito dopo aver inserito il proprio numero di cellulare, è stata contattata telefonicamente dal truffatore che, per camuffare la propria utenza, ha utilizzato una tecnica che gli ha consentito di far apparire un numero riconducibile a quello dell'intermediario (*vishing caller id spoofing*). Peraltro, ciò ha fatto sì che la ricorrente, confidando nella genuinità delle comunicazioni, desse seguito alle indicazioni del sedicente operatore, scansionando i codici QR pervenuti tramite *mail*, da un indirizzo sostanzialmente analogo a quello della banca (l'unica differenza, infatti, va rinvenuta esclusivamente nell'estensione impiegata nelle *mail* truffaldine – ".com" in luogo di quella ".it" dell'intermediario –) e comunicando le credenziali statiche e dinamiche.
L'analisi dello svolgimento complessivo della vicenda, dunque, consente a questo Collegio di escludere che la ricorrente abbia agito con colpa grave e, di conseguenza, determina l'accoglimento della domanda di rimborso, al netto della franchigia.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 13.950,00 con interessi legali dalla richiesta al saldo.
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
PIETRO SIRENA