COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore - CONSIGLIA SILVIA PANZARINO

Seduta del 11/09/2023

FATTO

Il ricorrente afferma di esser stato di vittima di frode a mezzo sms e chiamate telefoniche provenienti dall'intermediario. Precisa che in tali messaggi e chiamate gli veniva comunicato del "blocco del servizio Home Banking", oltre al fatto che l'operatore telefonico conosceva i suoi dati personali, compreso il nome utente per l'accesso ai servizi di home banking.
Soggiunge che l'operatore lo invitava a proseguire digitando la propria password, rilevando in quel momento che "la procedura risultava bloccata"; pertanto, questi lo invitava a recarsi personalmente in banca per aggiornare il "documento di sicurezza".
In data 24/03/2023 si recava in banca ove l'operatore di sportello gli comunicava il blocco del conto corrente e che occorreva aggiornare il documento di riconoscimento.
In data 27/03/2023 riceveva una telefonata dalla banca in cui gli veniva richiesto di recarsi presso i suoi sportelli, ove gli veniva comunicato che dal suo conto corrente era stata fraudolentemente prelevata "la quasi totalità della somma in giacenza", pari ad € 6.500,00.
Sostiene che la banca non gli aveva mai comunicato la necessità i documenti di riconoscimento "scaduti da mesi", tantomeno aveva ricevuto informazioni su varie tipologie di truffe.
Evidenzia che, contrariamente a quanto affermato dall'intermediario in sede di riscontro al reclamo, il sistema di sicurezza informatico sarebbe stato violato, considerate le informazioni in possesso dell'operatore che lo aveva contattato telefonicamente.
L'intermediario ricostruisce le modalità di accesso, disposizione di un bonifico, enrollment del Token Software su un nuovo device e modifica dei dati personali, precisando che la

password ed il PIN sono scelti dai clienti e non sono noti a nessuno, e che il PIN è configurato dal cliente in fase di installazione del Token Software.
Ritiene che un sistema di autenticazione basato sull'utilizzo di un codice statico e di un codice dinamico (OTP), è notoriamente ritenuto dai Collegi ABF e dall'EBA conforme ai requisiti previsti dalla direttiva comunitaria PSD2 per l'autenticazione forte del cliente (SCA) basata sull'uso di almeno due elementi di autenticazione tra loro indipendenti.
Nel ricostruire i fatti oggetto di controversia esposti dal ricorrente in sede di reclamo, denuncia e ricorso, rappresenta che: in data 23/03/2023, alle ore 12:39, questi riceveva due s.m.s. recanti l'intestazione di altro intermediario; alle successive ore 13:57 questi riceveva due chiamate da un numero che coincide con quello di una delle sue filiali, in quanto i criminali "avevano evidentemente manipolato il numero telefonico del chiamante"; i criminali avevano posto in essere la truffa dal falso numero chiamante (c.d. "call ID spoofing") e che nel corso delle telefonate l'operatore induceva il cliente ad accedere a quello che quest'ultimo credeva essere il sito della banca tramite il link riportato negli S.m.s. fraudolenti e ad inserire la propria password; sempre nel corso delle telefonate il ricorrente era invitato ad accedere all'App, ovvero ad utilizzare il Token Software per generare l'OTP; i truffatori avevano potuto scaricare l'App sul proprio smartphone ed attivare il Token Software, impostando il relativo PIN, utilizzando il codice OTP inviato alle ore 14:13 via e-mail all'indirizzo del ricorrente (cfr. all. 1); i truffatori, una volta completata l'installazione del Token Software sul loro device, avevano effettuato l'accesso tramite App alle ore 14:13 al servizio di internet banking, visionando il messaggio di alert della banca con cui si informavano i clienti "dell'avvenuto blocco dell'operatività on line del servizio causa intervenuta scadenza dell'Adeguata Verifica"; i truffatori avevano concluso la telefonata col ricorrente invitandolo a recarsi in filiale per aggiornare l'ADV; in data 24/03/2023, il ricorrente si era recato in filiale dove aveva fornito copia dei documenti di riconoscimento e compilato il nuovo modulo ADV, consentendo il ripristino della normale operatività del servizio di internet banking; alle successive ore 14:06 riceveva una nuova telefonata dai truffatori, nel corso della quale era stato modificato l'indirizzo e-mail collegato al servizio di internet banking, cui seguiva alle 14:07 un Alert a mezzo e-mail in cui si dava atto di tale modifica; alle ore 15:23 i truffatori avevano potuto autorizzare il bonifico in questione.
Ritiene, pertanto, che dalla ricostruzione dei fatti si evinca che l'operazione disconosciuta era stata autenticata, correttamente registrata e contabilizzata con un sistema a doppio fattore e senza alcuna anomalia, come confermato dai log informatici allegati (cfr. all. 2).
Soggiunge che nel caso in esame sussiste la colpa grave del ricorrente che con il suo comportamento imprudente aveva consentito ai truffati di poter perpetrare la frode. Precisa che le modalità utilizzata dai truffatori per ottenere le informazioni sono riconducibili al c.d. "smishing", variante ormai nota e priva di particolare "sofisticazione" rispetto al fenomeno del phishing tradizionale via e-mail.
Evidenza, inoltre, che: gli s.m.s. ricevuti sembravano provenire da altro intermediario (soggetto terzo, emittente di carte di credito/debito), mentre il ricorrente era stato invitato a digitare la password del servizio di internet banking della banca convenuta; il ricorrente aveva avuto a disposizione oltre 24 ore di tempo per riflettere su tale "macroscopica incongruenza" e sul fatto che, da un lato, credevano di parlare con un operatore della banca, e dall'altra continuavano a ricevere S.m.s. da altro intermediario; l'e-mail di Alert, con cui il ricorrente era stato avvisato dell'avvenuto cambio di indirizzo e-mail, era stata "colpevolmente" ignorata dal ricorrente (cita plurimi Precedenti ABF, nonché Collegio di Coordinamento, decisioni nn. 3498/2012 e 1820/2013).
Il ricorrente, in sede di repliche, ribadisce di esser stato contattato telefonicamente da un'utenza telefonica riconducibile alla banca. Precisa che l'operatore, confermando il

blocco del servizio di home banking, era a conoscenza del suo codice utente e pertanto, quest'ultimo aveva avuto accesso "in qualche modo" al sistema informatico della banca.
Sostiene che non può essergli imputata alcuna colpa grave, stante la manipolazione del numero di telefono della banca, la quale non ha sistemi di protezione adeguati. Inoltre, non può essergli addebitata alcuna "leggerezza", in quanto il truffatore era già a conoscenza dei suoi dati personali e del codice utente.
Conclude insistendo per l'accoglimento della domanda di rimborso formulata nel ricorso, pari ad € 6.500,00.
L'intermediario, con le controrepliche, evidenzia che la truffa subita dal ricorrente è purtroppo diffusa e ben nota nelle sue modalità di funzionamento, precisando che tutto era partito dall'S.m.s. fraudolento contenente il link truffaldino, ricevuto il 23/03/2023 alle ore 11:50, e che solamente chi segue tali link e digita le relative credenziali, è destinatario della successiva fase della truffa, condotta mediante telefonata da parte del falso operatore. Soggiunge che il secondo S.m.s., delle ore 12:39, veniva inviato a coloro che avevano "cliccato" il link e che, pertanto, al momento della telefonata il truffatore era già in possesso dei dati inseriti precedentemente, seppur il ricorrente affermi "maliziosamente" di non averlo fatto prima.
Ribadisce, altresì, che: la frode era stata portata a termine solo grazie alla totale, seppur inconsapevole, collaborazione del ricorrente che aveva condiviso con i truffatori le sue credenziali personali di accesso al servizio di internet banking ed anche il codice OTP necessario per l'attivazione dell'App sul device dei truffatori; nessuna manipolazione era avvenuta ai danni del numero telefonico della banca, poiché i truffatori, con la tecnica del "call ID spoofing", avevano manipolato il loro numero telefonico.
Conclude insistendo nel rigetto della domanda formulata nel ricorso, in quanto completamente infondata.

DIRITTO

La questione sottoposta all'attenzione del Collegio riguarda la richiesta avanzata dal ricorrente di rimborso di una somma di denaro sottratta dal proprio conto corrente in maniera fraudolenta.
L'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018.
Il ricorrente ricostruisce le modalità della truffa subita: riceveva un primo s.m.s. in cui era invitato ad accedere all'area clienti, a cui non rispondeva; successivamente, riceveva un secondo s.m.s., a cui non rispondeva, con cui gli veniva comunicato che sarebbe stato contattato nelle successive ore da un operatore "in merito alla nuova sicurezza web"; riceveva due chiamate sul suo cellulare da un numero identico a quello della banca, e nel corso di tali chiamate un operatore lo informava del "blocco delle procedure home banking del conto on-line", invitandolo a collegarsi al sito web della banca e ad accedere all'App; la mattina successiva si recava presso lo sportello della banca ove l'operatore di sportello gli confermava che era "necessario procedere ad aggiornare i documenti di identità associati al conto corrente"; sempre nello stesso giorno riceveva un'e-mail dalla banca in cui veniva informato della sostituzione dell'indirizzo di posta elettronica presente nei dati dell'internet banking"; in data 27/03/2023 si recava nuovamente in filiale ed apprendeva che dal suo conto corrente, in data 24/03/2023, era stata prelevata la somma di € 6.500,00 a mezzo bonifico bancario.

L'intermediario da parte sua riferisce che la operazione di bonifico contestata è stata validata attraverso un sistema di autenticazione forte a due fattori, con codice di accesso statico e password dinamica inviata sull'utenza registrata del ricorrente e produce a supporto di quanto affermato, i log del proprio sistema informatico relativi al periodo 23/03/2023 – 24/03/2023.

Il Collegio rileva che dall'esame dei predetti log, si evince solamente l'autorizzazione avvenuta il 24/03/2023 per le operazioni di modifica dei dati personali e di predisposizione del bonifico in questione, mancando qualsiasi riferimento all'operazione di enrollment del Token Software sul device dei truffatori (cfr. Collegio di Roma, dec. n. 688/22), pertanto, non è stato provato da parte dell'intermediario l'impiego della SCA nella fase di onboarding.

Alla luce di queste evidenze, il Collegio reputa che l'intermediario non abbia provato la regolare autenticazione delle operazioni contestate e che, di conseguenza, il ricorso merita accoglimento.

Da ultimo, con riferimento all'applicazione della franchigia invocata dall'intermediario in caso di accoglimento del ricorso, il Collegio rileva che l'art. 12, comma 3, del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218, prevede una franchigia a carico del cliente di € 50,00 soltanto in caso di "operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita", dovendosi dunque ritenere esclusa in fattispecie diverse di utilizzo illecito, come quella oggetto del presente ricorso (cfr. Collegio di Bari, dec. nn. 4040/2022 e 5298/2020).

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 6.500,00 oltre gli interessi legali dalla data del reclamo al saldo.

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

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI