COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) MAZZU'	Membro di designazione rappresentativa degli intermediari
(PA) CAMBOA	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 19/01/2023

FATTO

Con ricorso pervenuto il 26.07.2022, il ricorrente espone che in data 23.03.2022 riceveva un SMS apparentemente proveniente dalla banca, nel quale si richiedeva di cliccare un link. Dopo aver fatto ciò, si apriva una schermata apparentemente riconducibile al sito internet dell'intermediario. Il ricorrente provvedeva quindi ad inserire il proprio numero cliente e il PIN. Dopo aver inserito le credenziali, gli veniva comunicato che il suo conto era stato bloccato e che avrebbe dovuto cliccare sull'ulteriore link "*chiama ora*" per sbloccarlo. Operato in tal senso, veniva contattato da un sedicente operatore dell'intermediario, il quale lo guidava nell'installazione di un'app denominata "*Banca Sicura*" e nella disinstallazione di quella utilizzata sino a quel momento per effettuare l'accesso alla *home banking*. In data 24.03.2022 egli chiamava un operatore della banca, il quale gli comunicava che erano stati disposti due bonifici, per un totale di € 43.767,84, da due conti correnti a lui cointestati, a favore di tale R****** P******. In particolare, si tratta di

due operazioni, effettuate su due diversi conti, una il 23.03.2022, per un importo di € 29.772,21, e l'altra il 24.03.2022, per un importo di € 13.995,63.

Né lui né i cointestatari del conto ricevevano alcun SMS relativi alle transazioni contestate. Nessuna anomalia veniva ravvisata dall'intermediario, a seguito delle operazioni effettuate. Il ricorrente afferma che le due operazioni di pagamento contestate superano l'importo massimo trasferibile con un unico bonifico, fissato in € 10.000,00. Non sono state fornite risposte ai quesiti posti via e-mail all'intermediario dal ricorrente.

Chiede all'Arbitro di pronunciarsi in merito:

- alla validità della richiesta di restituzione dell'intero importo truffato, con i relativi interessi maturati,
- alla effettiva completezza e correttezza delle modalità adottate dall'Intermediario nell'assisterlo: segnala che nel mese di giugno un Funzionario lo ha telefonicamente contattato per chiedere se volevo attivare un prestito personale, in quanto persona potenzialmente interessata, così come da segnalazione interna
- all'esistenza di inadempienze contrattuali, con particolare riferimento ai limiti per singolo bonifico (€ 10.000)
- alla presenza di carenze, inosservanze, nel sistema home banking proposto dalla banca: evidenzio il supporto del servizio via e-mail di relazioni con il cliente privo di effettiva utilità con allungamento dei tempi
- all'uso di tecniche, ufficiose, volte a dissuadere il Cliente in caso di richieste di restituzione, piuttosto che in accordo ai dettami di buon governo e trasparenza, così come da codice etico o comunque rapporto di mutua fiducia e rispetto: ovvero gestione del rischio del servizio home banking verso la gestione del rischio per il Cliente, evidenziando gli obblighi di buona custodia dati, da qui la conseguente e scontata colpa grave, senza fornire un reale supporto per limitare/annullare i possibili/probabili errori umani
- alla presenza di carenze della banca relative alle modalità attuate nella fase di proposta dell'home banking, che appare, volutamente, orientata a non verificare/indagare sulle conoscenze informatiche e di pirateria informatica, da parte del Cliente, prima di suggerirgli l'utilizzo dello home banking; non è inoltre illustrato il rischio che si corre di subire una truffa che lo possa portare in una condizione economica particolarmente esposta, per assenza di liquidità anche per le spese correnti.

Con controdeduzioni pervenute il 10.10.2022, l'intermediario chiede il rigetto del ricorso. Dopo avere illustrato il sistema di autenticazione "forte" al sito della banca, e avere

precisato che risulta attivo il sistema di SMS alert e che questo ha regolarmente operato nel caso di specie, espone che

- il giorno 23.03.2022, alle ore 12:50, ha inviato al cellulare del ricorrente, un SMS (e notifica push) contenente il codice OTP necessario per l'attivazione del Mobile Token, di cui il ricorrente non fa menzione, avente il seguente contenuto: "*Stai attivando il Mobile Token. Ricordati che il personale B* non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ******** Info ******"*;
- In merito ai link ricevuti via sms dal ricorrente, rileva che essi non riportano nella loro estensione nulla di riconducibile all'intermediario, bensì ad un portale sconosciuto: http://link.**********, per accedere al quale il cliente dichiara di aver inserito le proprie credenziali di sicurezza dell'home banking, rendendole così note al terzo non autorizzato.
- Inoltre ha utilizzato il link "chiama ora" e in ultimo il link http://app.********* per scaricare l'app "Banca sicura", tutti estranei all'intermediario resistente;
- dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, l'operazione risulta correttamente autenticata, registrata e contabilizzata (così come previsto dall'art. 10 del D. Lgs. n. 11/2010);
- a fronte di ciascuna dispositiva la Banca ha inviato al cellulare del ricorrente la relativa notifica push e sms alert;
- in linea generale, utilizzare le proprie credenziali per accedere a Link di cui non si sia preventivamente verificata l'attendibilità del mittente, configura un incauto comportamento del titolare degli strumenti di pagamento e una condotta gravemente colposa, laddove il ricorrente ha fornito le proprie credenziali.

Alle controdeduzioni ha replicato parte ricorrente, esponendo:

- di non aver mai ricevuto sul proprio cellulare alcun SMS relativo all'inserimento dei bonifici oggetto di contestazione;
- di non aver mai ricevuto una richiesta di inserimento di un codice OTP per poter effettuare bonifici;
- di non aver mai ricevuto, per lo specifico caso oggetto di contestazione ma anche per bonifici precedenti e successivi alla frode, un SMS da parte dell'intermediario avente il seguente contenuto: "Stai attivando il Mobile Token. Ricordati che il personale B* non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato ******** info ******";
- di non aver mai comunicato le proprie credenziali a terzi;

- che i log informatici forniti dall'intermediario sono incompleti, in quanto non evidenziano che la prima fase della truffa ha avuto inizio con la disinstallazione dall'app dell'intermediario e la contestuale installazione dell'app "*banca sicura*" fornita dal sedicente operatore. Per questo motivo il ricorrente sostiene di non aver mai ricevuto le comunicazioni da parte della banca relative ai bonifici e alle operazioni effettuate sul proprio conto;
- l'intermediario è comunque responsabile sia della mancata sorveglianza sulle chiamate telefoniche provenienti dal numero ascrivibile all'utenza dell'intermediario, sia del mancato riscontro ai quesiti posti via mail dal ricorrente;

In sede di controrepliche, l'intermediario ha ribadito quanto già sostenuto in sede di controdeduzioni.

Le parti hanno presentato replica e controreplica, con le quali hanno sostanzialmente ribadito le proprie posizioni.

DIRITTO

La controversia verte sulla richiesta di restituzione dell'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.

Le operazioni contestate sono state poste in essere 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), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

In particolare, le fonti normative che regolano la Strong Customer Authentication (SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del d.lgs. n. 10/2011, 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 dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

In base a quanto emerge dalla denuncia e dalle ulteriori evidenze, la fattispecie oggetto del presente ricorso appare rientrare nelle fattispecie di *smishing* e di *vishing*.

I Collegi dell'ABF si sono in più occasioni occupati di casi simili. Per consolidata giurisprudenza dell'Arbitro, l'accertamento della eventuale sussistenza di un profilo di

colpa grave del cliente che comunica le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario, a seguito della ricezione di un messaggio ingannevole che indirizza ad una data pagina web (*phishing* operato tramite semplice email o *smishing*, attuato mediante SMS) può intervenire solamente se l'intermediario dimostra che l'operazione è stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/10). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute. Altro profilo da considerare è se il sistema di accesso al conto del titolare dello strumento di pagamento e di effettuazione delle operazioni dispositive sia adeguatamente presidiato, attraverso un'autenticazione a due fattori (username + PIN e successiva generazione dell'OTP), con ciò configurandosi l'adozione di un sistema di SCA.

Nel caso di specie, i bonifici disconosciuti sono stati disposti mediante l'inserimento del PIN (primo fattore di conoscenza) e dell'OTP generato dal Mobile Token (secondo fattore di possesso). Ne ha dato prova l'intermediario, producendo i log (si veda, da ultimo, per l'idoneità di tale prova, la decisione n. 13855/22 di questo Collegio).

Sussiste dunque la colpa grave del ricorrente, il quale ha cliccato su un link contenuto in un SMS, apparentemente inviatogli dalla banca e ha poi seguito le istruzioni, consegnando ai truffatori le credenziali di accesso ai propri conti. Essi si sono posti così in condizione di operare con il Mobile Token e ricevere l'OTP, necessario per l'effettuazione dei bonifici. Come rilevato dal Collegio di Coordinamento (decisione n. 1820/13), in simili ipotesi, "*il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet*".

Decisiva, tuttavia, ai fini dell'integrale addebito all'intermediario dell'obbligo di restituzione delle somme fraudolentemente sottratte al ricorrente è una ulteriore circostanza che merge dagli atti. Il ricorrente afferma, infatti, che sui conti era posto un plafond di € 10.000,00 per i bonifici. Tale affermazione, che pure non trova supporto documentale, non viene in alcun modo contestata dall'intermediario e, pertanto, esse deve ritenersi accertata (art. 115 c.p.c.). Il limite è stato chiaramente superato da ciascuna delle due disposizioni.

In merito a tale ipotesi, ha osservato il Collegio di coordinamento (dec. n. 16237/18): "*il profilo del superamento del c.d. plafond (…) è del tutto assorbente di ogni altro rilievo attinente alla responsabilità nella custodia della carta e delle sue credenziali relative alla*

sua operatività online e ciò in quanto tale fatto (…) è dotato di efficienza causale dirimente. Infatti, è di palese evidenza, che il blocco per il superamento del plafond avrebbe evitato l'operazione contestata nella sua interezza (…). L'importo dell'operazione disposta fraudolentemente con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. plafond) per l'utilizzo dello strumento elettronico di pagamento deve essere quindi interamente restituita al cliente e ciò in quanto difetta del suo consenso risultando difforme alle limitazioni contrattuali di operatività dello stesso" (si vedano anche Collegio Palermo, decc.n. 3155/21; 11068/22).

Deve dunque affermarsi il diritto del ricorrente a ricevere il rimborso dell'intera somma illegittimamente prelevatagli, ammontante a € 43.767,84, oltre gli interessi legali come richiesti.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo di € 43.767,84, oltre interessi legali dalla data del reclamo.
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
MARIA ROSARIA MAUGERI