Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BUTA	Membro designato dalla Banca d'Italia
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) LIPANI	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GRAZIA BUTA

Seduta del 06/02/2023

FATTO

Parte ricorrente riferisce preliminarmente di essere cointestataria di un c/c acceso presso l'intermediario convenuto. In data 07/03/2022, afferma di aver ricevuto una telefonata dal numero verde dell'intermediario con la quale veniva invitata a installare sul proprio cellulare un'applicazione per utilizzare, tramite token, i servizi bancari. Nei giorni successivi, pervenivano sul cellulare della ricorrente degli sms nei quali si chiedeva di cliccare su un link per aumentare i criteri di sicurezza per le operazioni online della banca. Riferisce che durante queste operazioni non venivano mai chieste informazioni personali quali password, credenziali o codici. In data 17/03/2022, entrambe le cointestatarie del conto corrente ricevevano un sms da un numero riconducibile a quello dell'intermediario con cui venivano informate della disposizione di un bonifico di € 1.200,00.
Atteso che il conto in questione non era mai stato utilizzato dalle cointestatarie per bonifici o prelievi (trattandosi di conto dormiente per il pagamento delle tasse), entrambe le cointestatarie si allarmavano accorgendosi di altri tre prelievi per importi di: € 9.850,45, in data 07/03/2022; € 24.686,00 in data 08/03/2022; € 24.638,00 in data 09/03/2022, tutti a favore di un determinato destinatario.
Parte ricorrente contattava il servizio clienti dell'intermediario al medesimo numero telefonico, per disconoscere formalmente tutte le operazioni e bloccare il conto, ma ogni volta che iniziava a parlare con un operatore cadeva la linea. Pertanto, si recava presso la filiale dell'intermediario, dove riusciva a parlare con un'addetta allo sportello che procedeva a bloccare il conto per le operazioni online e che le comunicava che le prime tre operazioni

erano state contabilizzate, ma l'ultima operazioni di € 1.200,00 poteva ancora essere bloccata chiamando il numero verde.
Purtroppo, la ricorrente non riusciva a parlare con un operatore e così anche l'ultima operazione veniva contabilizzata. Entrambe le cointestatarie del conto corrente sporgevano formale denuncia querela.
Evidenzia che la truffa è stata commessa da un soggetto esperto e tecnicamente preparato che, chiamando dal numero verde ufficiale della convenuta e qualificandosi come dipendente della stessa, ha ingenerato un legittimo affidamento nella ricorrente la quale, credendo di installare un'applicazione necessaria per utilizzare l'app ufficiale dell'intermediario, è stata invece portata ad installare un'app chiamata "Anydesk" che ha permesso al truffatore di entrare nel cellulare di questa ed effettuare i bonifici. Difatti, ribadisce di non aver mai comunicato nessuna informazione sensibile al telefono o via sms.
Parte ricorrente afferma di aver ricevuto dal mittente, con denominazione dell'intermediario, degli sms in cui non veniva richiesto di comunicare alcun dato sensibile ma semplicemente di installare l'app al link riportato. Precisa che dal riscontro dell'intermediario si evince che questo fosse a conoscenza di tali pratiche relative all'utilizzo del numero ufficiale del suo servizio clienti da parte di potenziali truffatori.
Lamenta l'insufficienza del sistema di sicurezza predisposto dalla convenuta per tutelare il cliente dal momento che è previsto solo l'utilizzo di una OTP. Tale password, infatti, viene inviata sul cellulare stesso del cliente che se, come nel caso che ci occupa, risulta già compromesso e manomesso, non può fornire alcuna protezione.
Lamenta infine che l'intermediario non ha chiesto informazioni alle clienti, avendo visto delle operazioni così rilevanti e cicliche. Chiede pertanto il rimborso della somma complessiva di € 60.374,45.
Costituitosi, l'intermediario fa preliminarmente presente che parte ricorrente chiede il rimborso di € 60.374,45 relativi a n. 4 bonifici disposti online a valere sul conto corrente a questa cointestato, eseguiti da app dell'intermediario dal 7 al 17 marzo 2022, autorizzati con le credenziali di sicurezza della ricorrente. Al conto corrente in questione è collegato il servizio di home banking, che consente ai clienti di operare sui conti correnti personali a loro riferibili, utilizzando il telefono cellulare o internet; tale servizio si avvale di un sistema di autenticazione "forte". Soggiunge che le clienti hanno anche aderito al servizio di SMS alert collegato alle proprie utenze.
Precisa al riguardo che, nell'accesso all'home banking da app, per effettuare il login il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP; mentre per disporre le operazioni, è necessario inserire il PIN e il codice OTP. Il codice OTP viene generato dal mobile token integrato nell'app che il cliente ha attivato sul proprio device.
L'attivazione del mobile token è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP inviato al cliente via SMS al numero di cellulare collegato all'home banking, "indipendentemente dalla attivazione del servizio SMS alert".
Nel caso specifico, l'intermediario riferisce di aver inviato al ricorrente alle 13.37 del 07/03/2022 un SMS contenente il codice OTP per l'attivazione del mobile token. A questo punto, parte ricorrente avrebbe dovuto insospettirsi e rivolgersi al servizio clienti se non aveva effettuato la richiesta di attivazione del mobile token, soprattutto non avrebbe dovuto comunicare a nessuno il codice OTP contenuto nell'sms, come raccomandato nel testo del messaggio.
Soggiunge che il sistema di autenticazione a due fattori adottato dall'intermediario è riconosciuto come un sistema forte anche dall'orientamento diffuso dei Collegi ABF (richiama in proposito la decisione n. 5565/2019 del Collegio di Roma).

In presenza di un sistema in astratto valutabile come sicuro, come quello adottato dall'intermediario e in assenza di particolari anomalie di sistema, presume una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.
Al riguardo, evidenzia che al fine di prevenire possibili frodi in danno della clientela, la resistente da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nella pagina di accesso al portale, in cui avverte la clientela anche del fatto che nessun dipendente dell'intermediario chiederà mai le credenziali di sicurezza che sono strettamente personali e non devono essere comunicate a terzi.
Segnala che il tipo di operatività disconosciuta si rende possibile nei casi in cui il cliente abbocca a un tentativo di phishing rivelando le proprie credenziali.
Tanto premesso, rileva che nel caso di specie: il link ricevuto dalla ricorrente negli sms allegati non conteneva alcun riferimento all'intermediario, così come la nuova app che la ricorrente dichiara di aver attivato; l'app in questione a tratti spariva dal desktop del cellulare della ricorrente; si trattava di link non sicuro in quanto non contenente il protocollo di sicurezza https; il contenuto degli sms è alquanto generico e, a distanza di 18 minuti, la ricorrente riceveva n. 2 sms contenenti il medesimo link ma con motivazioni diverse; la telefonata si è ripetuta anche nei giorni 8 e 9 marzo ma ciò nonostante la ricorrente non ha avuto alcun dubbio né ha verificato se l'app dell'intermediario avesse continuato a funzionare (richiama a supporto la decisione n. 13855/22 del Collegio di Palermo).
Osserva come, dalla ricostruzione effettuata dalla ricorrente, risulti plusibile che per accedere al link riportato nell'sms fosse stato necessario inserire le credenziali di sicurezza dell'home banking, rivelandole così di fatto al terzo e che la ricorrente abbia anche inserito o comunicato su richiesta al suo interlocutore il codice OTP ricevuto via sms, necessario per attivare il mobile token. Ritiene quindi evidente che la ricorrente abbia attivato una nuova app, non riconducibile all'intermediario, attraverso la quale il terzo ha acquisito il controllo del suo device.
Al riguardo, ritiene che il comportamento tenuto dalla cliente integri gli estremi di una condotta gravemente colposa, in quanto questa ha abboccato a un messaggio seguito da una telefonata di phishing. Eccepisce di aver adottato un sistema di autenticazione forte "a due fattori" (statico e dinamico), come riconosciuto dai Collegi ABF (richiama, ex multis, la recente decisione n. 11254/2020 del Collegio di Milano la decisione n. 3782/20 del Collegio di Torino). Rileva altresì che l'importo delle operazioni non può essere considerato anomalo, in quanto la cliente avrebbe potuto modificare il plafond dispositivo dei bonifici, non potendo l'intermediario limitare al cliente l'utilizzo delle proprie disponibilità.
Inoltre, fa presente di aver inviato a entrambe le ricorrenti i relativi alert che risultano regolarmente consegnati; la resistente si è prontamente attivata con l'azione di recall verso l'intermediario del beneficiario a fronte della quale non ha ottenuto alcuna restituzione.
L'intermediario, pertanto, chiede all'Arbitro di respingere il ricorso nel merito in quanto infondato.
In sede di repliche la ricorrente ribadisce di non aver mai comunicato né le proprie credenziali né alcun codice personale né tantomeno il codice OTP diversamente da quanto affermato dall'intermediario. Il truffatore, infatti, ha installato una applicazione sul cellulare della ricorrente che gli ha permesso di operare da remoto e leggere i messaggi che pervenivano sull'utenza. Rammenta l'inadeguatezza del sistema di sicurezza, dal momento che la password è stata inviata sul cellulare stesso della cliente che se, come nel caso di specie, risulta già compromesso e manomesso, non può fornire alcuna protezione. Contesta che l'intermediario avrebbe dovuto rilevare i diversi indirizzi IP e l'importo anomalo rispetto alla normale operatività della ricorrente. Insiste per l'accoglimento del ricorso.

In sede di controrepliche, l'intermediario richiama la decisione n. 4219/22 del Collegio di Roma, che ha riconosciuto l'autenticazione forte nell'ambito del sistema di sicurezza descritto nelle controdeduzioni. Afferma che l'OTP inviato alla cliente era necessario per perfezionare l'attivazione del mobile token, a sua volta indispensabile per rendere operativa l'app dell'intermediario.
Rileva che anche nella fase successiva al disconoscimento delle operazioni, avvenuto da parte della ricorrente solo il 17/03/2022, l'intermediario ha posto in essere tutte le azioni possibili per tentare il recupero delle somme ma la frode - iniziata il giorno 7 marzo - era stata perpetrata durante ben 10 giorni precedenti al disconoscimento delle operazioni.
Come attestato dai LOG estratti dalle procedure informatiche dell'intermediario, ritiene di poter presumere che la ricorrente abbia consentito al frodatore di impossessarsi delle proprie credenziali di sicurezza.

DIRITTO

La controversia concerne una vicenda di utilizzo non autorizzato di uno strumento di pagamento, nella specie consistente in quattro operazioni di bonifico on line.
Il Collegio rileva innanzitutto che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, 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. Inoltre, le operazioni contestate sono state eseguite successivamente all'entrata in vigore delle nuove disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).
La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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". Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7." (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente". Ai sensi del successivo art. 12, co. 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta

alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve inoltre ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione. Infine, si deve rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema […]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella […] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014; nonché Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

Tale orientamento ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, in tema di onere probatorio a carico del debitore professionale, nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, "in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio […]; infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi

come parametro la figura dell'accorto banchiere" (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777; in senso conforme, cfr., più di recente, Cass., 12.4.2018, n. 9158).
Tanto premesso in termini generali, rileva il Collegio che, nel caso di specie, il ricorrente disconosce quattro operazioni di bonifico effettuate fra il 7 e il 9 marzo 2022 e, da ultimo, in data 17 marzo 2022, per un importo complessivo di € 60.374,45.
Sul piano della regolarità formale delle operazioni di pagamento, l'intermediario afferma, in via generale, che l'attivazione del mobile token è resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente tramite SMS al numero di cellulare certificato. Nel caso di specie eccepisce anzitutto che il 7/03/2022, alle ore 13:37, prima dell'esecuzione dei bonifici contestati, è avvenuta l'attivazione del Mobile Token tramite inserimento del PIN e utilizzando l'OTP trasmessa via sms, con "verifica a due fattori", utilizzando l'OTP generato da Mobile Token. Produce il log relativo alla suddetta operatività, con la relativa legenda esplicativa, da cui si evince l'inserimento del PIN e delle OTP. Produce altresì la schermata dell'sms inviato al ricorrente contenente il codice per attivare il mobile token; il numero di cellulare al quale è stato trasmesso il messaggio coincide con quello indicato dal ricorrente nella denuncia.
Quanto poi alle operazioni di bonifico, sulla base delle dichiarazioni dell'intermediario, per l'esecuzione delle stesse il sistema ha richiesto, necessariamente, l'utilizzo del PIN (fattore di conoscenza) e dell'OTP generato da mobile token (fattore di possesso), come pure si evince dai log prodotti dall'intermediario.
Ciò posto, sulla scorta delle evidenze documentali prodotte dall'intermediario resistente (estratto dei log con la relativa legenda, a supporto della corretta autenticazione; registrazione e contabilizzazione che può ritenersi riscontrata sulla scorta delle evidenze in atti) può sostenersi che la procedura seguita dall'intermediario sia conforme alla SCA (conf., ex multis, Collegio di Bari, nn. 32/2023, 21204/2021 e 14688/2022; Collegio di Milano, n. 5816/2022 e Collegio di Roma, n. 1178/2022). Il Collegio, pertanto, ritiene raggiunta la prova della corretta autenticazione dell'operazione.
Il soddisfacimento dell'onere probatorio gravante sull'intermediario resistente in ordine alla natura "forte" dell'autenticazione e all'assenza di anomalie consente di verificare la sussistenza o meno di profili di dolo o colpa grave nella condotta del ricorrente.
Sulla base di quanto prospettato e della documentazione agli atti, il Collegio osserva che nel caso di specie le operazioni non autorizzate sono avvenute tramite frode con sms spoofing.
Al riguardo, il ricorrente ha allegato copia dei messaggi civetta ricevuti da un mittente con denominazione dell'intermediario, all'interno della medesima chat in cui risulta ricevuto il messaggio relativo all'ultimo bonifico del 17/03/2022. Per contro, la resistente mette in luce che il link ricevuto dalla ricorrente negli sms allegati non conteneva alcun riferimento all'intermediario e che rimandava ad un sito contraddistinto da "http" anziché "https" (dove "s" sta per sicuro). Aggiunge poi che il contenuto degli sms è alquanto generico e, a distanza di 18 minuti, la ricorrente riceveva n. 2 sms contenenti il medesimo link ma con motivazioni diverse.
Ebbene, sulla base di quanto prospettato e della documentazione agli atti, è indubitabile che la truffa sia stata perpetrata anche tramite la condotta attiva del ricorrente, il quale – come dallo stesso ricostruito in atti - prima veniva contattato tramite telefonata e poi riceveva un sms con un link per installare sul telefono una nuova app per accedere ai servizi bancari.
È altrettanto vero, però, che la ricostruzione delle modalità della truffa subita dal ricorrente – come possibile dalla documentazione in atti – ne evidenzia i caratteri dell'insidiosità e della sofisticatezza.
Con riguardo alle operazioni contestate, il Collegio rileva altresì che il numero e l'importo delle suddette operazioni è decisamente anomalo in quanto difforme da quelle usualmente

poste in essere dalla ricorrente (per la valorizzazione di questo elemento, v. Collegio di Milano, n. 5346/2022 e Collegio di Roma, n. 595/2023).
Alla luce di quanto sopra, attesa anche la peculiarità del caso in esame legata all'anomalia di numero e importo delle operazioni contestate, il Collegio rileva quindi che possa ritenersi sussistente un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa e, dall'altro, alle criticità organizzative dell'intermediario, che giustifica l'accoglimento parziale della domanda di restituzione, nella misura dell'80% per cento.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 48.300,00.
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