Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

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

Relatore CARMELA ROBUSTELLA

Seduta del 19/12/2024

FATTO

Parte ricorrente, in qualità di rappresentante legale di una società in nome collettivo titolare di conto corrente presso la resistente, riferisce di essere stata contattata, tramite "clonazione telefonica", da un sedicente operatore dell'intermediario qualificatosi come dipendente dell'ufficio antifrode.
Afferma di aver constatato un accesso non autorizzato sulla propria home banking, nonché l'esecuzione di un bonifico istantaneo per € 19.900,00 a fronte di un massimale inferiore previsto per tale tipologia di operazioni.
Dichiara di aver denunciato l'accaduto alle autorità competenti e chiede la restituzione di quanto illegittimamente sottratto, anche in considerazione dell'inadeguatezza del sistema di sicurezza predisposto dalla resistente.
Costituitosi ritualmente, l'intermediario ricostruisce le modalità della frode, rappresentando che in data 19/07/2024 parte ricorrente veniva contattata telefonicamente da un numero non riferibile alla banca. Nel corso della telefonata un soggetto, qualificatosi come operatore antifrode, riusciva ad ottenere le credenziali di accesso al servizio di internet banking, come espressamente ammesso dal ricorrente in sede di denuncia.
Effettuato il login, afferma che veniva predisposto il bonifico urgente oggetto di ricorso, autorizzato dallo smartphone dello stesso cliente. Precisa, dunque, che nel corso della truffa in discorso non si verificava l'enrollment di un nuovo device.

In relazione all'operatività necessaria per eseguire un'operazione dispositiva, fa presente che è possibile accedere all'home banking tramite web browser utilizzando il token software installato sul dispositivo dell'utente (elemento di possesso) e inserendo le credenziali (UserID e Password) e il codice MPIN (elementi di conoscenza). Afferma che, dopo l'accesso, per disporre un bonifico occorre l'inserimento del MPIN (elemento di conoscenza) sull'app token software installata sul device (elemento di possesso). Precisa che sia la password sia il codice PIN vengono scelti dal cliente in fase di installazione del token software.
Segnala che, come evincibile dalla relazione trasmessa dal proprio outsourcer e dai log allegati, le operazioni disconosciute sono state autenticate, correttamente registrate e contabilizzate con un sistema a doppio fattore e senza alcuna anomalia.
Ritiene che la frode sia stata attuata mediante vishing e che i messaggi allegati dal ricorrente presentano chiari elementi di inattendibilità, con conseguente configurazione di colpa grave (cita a supporto Decisione ABF, n. 23344/2021).
Afferma che il bonifico in questione era di tipo urgente e non istantaneo, con previsione di un massimale giornaliero pari ad € 50.000,00.
Chiede, pertanto, il rigetto del ricorso.
Parte ricorrente, nelle repliche, afferma di non aver riscontrato, all'interno della propria home banking, il contratto relativo ai servizi di internet banking e, dunque, i limiti operativi dei bonifici urgenti.
Precisa che il documento di sintesi allegato alle controdeduzioni si riferisce ad un diverso rapporto, non pertinente con l'odierno ricorso.
Si duole della mancata adozione di un sistema di sicurezza ex post che consenta il blocco dei bonifici urgenti e dichiara di non aver mai autorizzato l'attivazione del "servizio di Bonifico Urgente", tipologia di operazione che, infatti, non aveva mai eseguito prima.
A tal proposito fa presente che, nello schema complessivo della truffa subita, era stato compiuto in maniera fraudolenta anche un bonifico ordinario che la banca riusciva a bloccare.
Nega la sussistenza di una sua colpa grave ed imputa l'accaduto alle criticità organizzative dell'intermediario (cita a supporto Corte di Cassazione, sentenza n. 3780/2024).
Insiste pertanto per l'accoglimento delle richieste avanzate in sede di ricorso.
La resistente, nelle controrepliche, eccepisce preliminarmente l'inammissibilità di domande ed eccezioni nuove, avanzate per la prima volta in sede di repliche.
Nel merito fa presente che non risulta allegata documentazione da cui evincere che parte ricorrente sarebbe stata vittima di caller id spoofing. Precisa, al riguardo, che la schermata versata in atti evidenzia esclusivamente il nome attribuito dal ricorrente all'interlocutore sconosciuto e non quello con cui questi si manifestava quando chiamava.
Dichiara che il rapporto di internet banking non è più operativo dal 22/07/2024 e che il documento di sintesi allegato alle controdeduzioni è relativo al rapporto oggetto di ricorso, con indicazione dell'indirizzo di spedizione cointestato tra il ricorrente ed il coniuge, al quale era collegato il rapporto di conto corrente principale.
Afferma che la possibilità di disporre bonifici urgenti è disciplinata nel contratto di conto corrente e che tale tipologia di operazioni "non costituisce un servizio a parte" e non è una caratteristica tipica dei rapporti di internet banking, ma solo una modalità che permette il trasferimento di denaro nella forma più rapida possibile. Precisa la differenza rispetto al servizio di bonifici istantanei, che possono essere inseriti solo tramite internet banking e che hanno limiti operativi, modalità e tempi di esecuzione diversi rispetto ai bonifici urgenti.
Insiste, pertanto, per il rigetto del ricorso.

DIRITTO

La controversia verte sulla responsabilità del prestatore di servizi di pagamento in caso di loro utilizzo non autorizzato, segnatamente quando il cliente, come nel caso di specie, abbia disconosciuto operazioni di home banking asseritamente eseguite, con mezzi fraudolenti, da terzi ignoti.

Il Collegio rileva, innanzi tutto, che l'operazione contestata è stata eseguita 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 sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Il comma 2 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 pi degli obblighi di cui all'articolo 7" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma, altresì, è 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, sí 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 sia 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 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. Da ultimo, cfr. Coll. Coord., decisione n. 22745/2019, 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). L'orientamento di questo Arbitro ha trovato ripetuto riscontro nella giurisprudenza della Corte di Cassazione, la quale ha avuto modo di chiarire che la disciplina speciale in materia di strumenti di pagamento, ha esplicitato un 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 ritenuto che non pu 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., 3.2.2017, n. 2950; in senso conforme, più di recente, Cass., 12.4.2018, n. 9158; Cass., 26 novembre 2020, n. 26916, anche per l'importante statuizione, secondo cui "al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento - prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente - la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo").

Fatte queste doverose premesse e tornando al caso di specie, il Collegio anzitutto rileva che nella denuncia, resa in data 22/07/2024, il ricorrente ricostruisce i fatti in modo analogo al ricorso. Afferma di essere stato "convinto a fornire le credenziali di accesso" durante la telefonata truffaldina del 19/07/2024. In particolare nella denuncia si riferisce che terzi ignoti, una volta acquisite le credenziali, hanno eseguito n. 2 bonifici rispettivamente di 14.900 euro su un conto corrente e 19.900 euro su altro conto corrente.
Il Collegio precisa che il bonifico di € 14.900,00 di cui si discorre in sede di denuncia è stato stornato dopo la segnalazione dell'accaduto e non è pertanto oggetto dell'odierna richiesta restitutoria.
L'operazione contestata consiste, quindi, in un bonifico disposto tramite home banking in data 19/07/2024 alle ore 16:25, di 19.900 euro.
L'intermediario ricostruisce l'operatività online in termini generali, affermando che per l'accesso tramite web browser è necessario l'uso congiunto di:

1) credenziali userid-password (elemento di conoscenza);
2) codice PIN (elemento di conoscenza) digitato su app Token Software installata sul device del cliente (elemento di possesso).

Rappresenta inoltre che per la disposizione di un bonifico è necessario l'uso congiunto (dopo l'accesso) di:

1) codice PIN (elemento di conoscenza) digitato su app Token Software installata sul device del cliente (elemento di possesso).

Quanto al caso di specie, anche alla luce delle affermazioni dello stesso ricorrente, l'intermediario sostiene che sia la fase di accesso, sia quella relativa ai bonifici, venivano autorizzate tramite il token software installato sul device del cliente il quale, dunque, ha verosimilmente autorizzato in prima persona le transazioni "mentre era in corso la telefonata con il truffatore, su indicazione di quest'ultimo". L'intermediario, al fine di provare la corretta autenticazione dell'operazione, produce i log corredati dalle relative didascalie, per ciascun passaggio dell'operatività contestata.
Nella schermata "evidenza 2", allegata in atti, sembra evincersi l'inserimento della password finalizzata all'accesso (elemento di conoscenza) dalla dicitura LOGIN UTENTE in corrispondenza della voce "CodiceFunzione" (si segnala anche la presenza del valore "0" in corrispondenza della voce "CodiceErrore").
Nella schermata "Evidenza 3", è presente il valore "_8" in corrispondenza della voce "Lunghezza password" che potrebbe confermare l'avvenuto inserimento di una password di 8 caratteri, in considerazione anche della presenza della dicitura "Operation Successful". Il Collegio, tuttavia, rileva che sempre nella schermata 3, in corrispondenza della voce "Serial", è presente un codice alfanumerico (FEF2079949) che potrebbe essere riconducibile all'utenza del ricorrente, per il quale, tuttavia, l'intermediario non fornisce chiarimenti in ordine al suo significato (non produce legenda esplicativa) e non precisa neppure le voci "dell'Evidenza 3" da cui ricavare "il corretto inserimento del criterio di Strong Customer Authentication – nel caso in oggetto del Token Software – per ultimare la sessione di login".
Anche in considerazione del fatto che l'intermediario ha affermato che non c'è stata alcuna attività di enrollment, è, pertanto, dirimente la valutazione dell'idoneità probatoria dei log sopra riportati, con particolare riferimento al fattore di possesso. Conseguentemente, in assenza di chiarimenti relativi al device (o all'app) concretamente utilizzato per l'esecuzione delle operazioni contestate, questo Collegio non può ritenere assolto l'onere relativo alla prova dell'autenticazione. Inoltre, l'intermediario, benché abbia affermato che, in via generale, sia la fase di accesso sia la fase di inserimento dei bonifici preveda il successivo invio di un alert informativo tramite e-mail, non produce documentazione attestante l'invio di tali alert. Il Collegio, in proposito, evidenzia che l'operazione oggetto di ricorso seguiva ad

un'altra tempestivamente stornata dall'intermediario. Considerata, dunque, la tempistica delle due operazioni, eseguite nell'arco temporale di circa sette minuti, è ragionevole presumere che la mancata attivazione del servizio di sms alert abbia determinato un effettivo *vulnus* per la sicurezza dell'utente, posto che l'attivazione di tale servizio avrebbe potuto verosimilmente scongiurare il pregiudizio patrimoniale risentito da quest'ultimo, consentendogli di evitare l'esecuzione del secondo bonifico.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 19.900,00.
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