COLLEGIO DI BARI

composto dai signori:

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

Relatore ESTERNI - SARA TOMMASI

Seduta del 20/11/2023

FATTO

La ricorrente, titolare di conto corrente acceso presso l'intermediario resistente, riferisce di aver ricevuto in data 30/03/2022 alle ore 13:26 un sms dal numero solitamente usato dall'intermediario per le proprie comunicazioni. Con tale sms la si informava di una "limitazione" della sua carta/conto per "mancata verifica della sicurezza web" e la si invitava a cliccare su un link.
Riferisce di aver cliccato su detto link e di essere stata così reindirizzata a un sito identico a quello dell'intermediario, in cui si chiedeva di inserire le credenziali (codice utente e PIN) per accedere all'home banking. Successivamente, precisa che appariva un messaggio "il cui senso complessivo era che la procedura non poteva essere completata senza un contatto telefonico da parte di un operatore della banca". Conseguentemente, fa presente di aver ricevuto un altro sms alle 14:05 che preannunciava la telefonata di un operatore dell'istituto.
Soggiunge di essere stata contattata telefonicamente alle 14:06 della medesima giornata dal numero verde dell'intermediario e che l'interlocutore le riferiva che era necessario procedere all'aggiornamento dei servizi di sicurezza web. Pertanto, veniva invitata a cliccare su un link nel frattempo ricevuto via sms (alle ore 14:13) sempre dal canale ufficiale di messaggistica dell'intermediario.
Rappresenta di aver seguito le istruzioni impartite dall'interlocutore telefonico e di aver dunque provveduto a disinstallare la app della banca e ad installarne un'altra ("[nome intermediario] sicura"). Riferisce di aver ricevuto ulteriori sms che confermavano quanto nel frattempo comunicato dal presunto operatore bancario.

Afferma di essere stata ricontattata il 31/03/2022 alle ore 13:05, come preannunciato il giorno prima, e che l'interlocutore la informava che per la risoluzione del problema informatico sarebbe stato necessario attendere 1-3 giorni lavorativi. Rappresenta di aver ricevuto ulteriori telefonate da parte del medesimo interlocutore sia in data 1/04/2022 sia il 4/04/2022.

Poiché "la reiterata inconcludenza delle operazioni e dei contatti sopra descritti appariva anomala", riferisce di essersi recata presso uno sportello dell'intermediario e di aver appreso, nella circostanza, che erano stati predisposti nei giorni precedenti quattro bonifici fraudolenti per un importo complessivo di € 109.380,00. Precisa che a seguito della procedura di recall uno dei quattro pagamenti, di € 24.998,00, è stato riaccreditato sul conto. Ritiene tuttavia di aver diritto al rimborso anche degli altri tre bonifici, per complessivi € 84.383,00, atteso che l'illecita sottrazione di denaro è stata possibile "grazie al fatto che gli strumenti tecnici utilizzati dai truffatori non hanno trovato ostacolo nel sistema di controllo e di protezione di cui si avvale [l'intermediario] per i servizi di pagamento online".

Evidenzia come per l'accesso all'home banking e per la successiva autorizzazione delle transazioni è stato sufficiente solo l'inserimento delle credenziali statiche (codice utente e PIN), "non sottoposte a procedure periodiche di rinnovo obbligato". Inoltre, sostiene di non aver ricevuto alcun sms alert a seguito dell'esecuzione delle operazioni in parola.

Rappresenta poi che l'importo complessivo delle operazioni fraudolente è del tutto incongruo rispetto alla sua normale operatività bancaria, per cui l'intermediario avrebbe dovuto rilevare l'evidente anomalia e impedire l'esecuzione delle transazioni.

Fa presente poi che tutti i canali utilizzati dai truffatori coincidevano con quelli ufficiali dell'intermediario e, dunque, ritiene di dover andare esente da addebiti di responsabilità.

Costituitosi, l'intermediario sostiene che – contrariamente a quanto affermato dalla ricorrente – il servizio di home banking prevede un sistema di autenticazione forte, in linea con la normativa vigente. In particolare, rappresenta che in fase di accesso all'home banking da app il sistema di autenticazione prevede, per effettuare il login e le operazioni di inquiry, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP, codice dinamico generato da Mobile Token. Per disporre le operazioni, invece, dopo avere effettuato la login come sopra e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP generato da Mobile Token.

Precisa che il MobileToken è una soluzione digitale studiata per garantire i più elevati standard di sicurezza dei pagamenti online, atteso che permette di generare automaticamente delle password valide per un solo utilizzo, OTP, direttamente sul proprio smartphone, protegge le credenziali di accesso all'area clienti e tutte le operazioni dispositive e di pagamento. Precisa inoltre che il cliente può attivare il Mobile Token contemporaneamente su due dispositivi (2 smartphone oppure 1 smartphone + 1 tablet) ed inoltre è libero di sostituire il proprio device se il numero di cellulare resta invariato.

Soggiunge che anche per l'attivazione del Mobile Token è necessaria l'autenticazione forte, attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via sms al cellulare collegato all'home banking. Nel caso di specie, evidenzia che la ricorrente il giorno 30/03/2022 alle ore 14:17:15, ha ricevuto sul suo cellulare un sms contenente il codice OTP necessario per l'attivazione del Mobile Token e che non avrebbe dovuto essere comunicato a nessuno, come raccomandato nel testo stesso del messaggio.

Afferma che è stato possibile eseguire le operazioni solo in quanto è stata la stesa cliente a rivelare le proprie credenziali di sicurezza dell'home banking dopo la ricezione di un sms di phishing, truffa ormai nota. Rappresenta che il canale di provenienza degli sms e della telefonata non avrebbe dovuto essere considerato affidabile. Evidenzia inoltre come il link

contenuto nel sms non sia in alcun modo riconducibile alla banca. Rileva come sia la stessa ricorrente ad aver affermato di aver assecondato incautamente le istruzioni ricevute dal finto operatore; inoltre, la frode è stata realizzata in più giornate e la ricorrente, nel frattempo, non ha mai controllato il proprio conto né ha interessato la banca per sincerarsi della genuinità dei contatti ricevuti.
Fa poi presente di aver inviato al cellulare della ricorrente le notifiche push e gli sms alert relativi alle operazioni contestate, che risultano regolarmente consegnati. Infine, rileva di essere riuscito ad effettuare il recall solo dell'ultima operazione eseguita dai truffatori il 4/04/2022, dato che la ricorrente ha comunicato la frode solo il 5/04/2022.
In sede di repliche, la ricorrente eccepisce la mancanza di procura ai firmatari degli atti depositati in nome e per conto dell'istituto bancario. Disconosce poi l'efficacia probatoria dei documenti allegati, "di cui non si rinvengono elementi identificativi, provenienza e data certa".
Ribadisce di non aver ricevuto alcun sms alert o notifica push in ordine alle operazioni oggetto di disconoscimento. Inoltre, afferma di non aver ricevuto alcuna comunicazione dalla banca circa l'avvenuta attivazione dell'app da parte del truffatore su un nuovo dispositivo.
Sostiene poi che gli "elementi di autenticazione" predisposti dalla banca "non erano tutti indipendenti tra loro, come risulta evidente dal fatto che, per l'attivazione dell'APP … e del Token Mobile su un altro smartphone … è stato sufficiente, per il truffatore, disporre soltanto del codice utente e del pin fraudolentemente carpiti all'inizio", tramite una frode sofisticata.
Con specifico riferimento all'attivazione del Mobile Token, evidenzia anzitutto che la sua contemporanea installazione su due dispositivi non è stata pattuita contrattualmente. In secondo luogo, fa presente che il suo numero di telefonia mobile era in uso solo sul suo smartphone, mentre i bonifici sono stati eseguiti da un diverso device. Evidenzia, ad ogni modo, che in base ai log allegati dall'intermediario vi è stato un intervallo temporale (tra le 14:17:38 e le 14:18:06) in cui l'app era attiva contemporaneamente su due smartphone diversi. Inoltre, fa presente che nelle istruzioni pubblicate sul sito dell'intermediario è previsto, per l'attivazione del Mobile Token, anche l'inserimento di un codice temporaneo inviato via mail, che tuttavia non è mai stato ricevuto nel caso di specie.
Evidenzia poi che se l'app viene attivata abusivamente da estranei su un altro dispositivo il cliente non ha più possibilità di sapere che c'è stato un accesso abusivo o di venire a conoscenza delle transazioni eseguite.
Reputa dunque che le operazioni di pagamento non sono state correttamente autenticate e, ad ogni modo, che l'intermediario debba essere considerato responsabile per quanto accaduto.
Quanto alle contestazioni sulla valenza probatoria dei log allegati alle controdeduzioni, l'intermediario in sede di controrepliche rileva che essi sono il risultato di una estrazione dalle procedure informatiche della banca, "trasformati in forma leggibile post operazione al fine di dimostrare l'autenticazione a doppio fattore (SCA)". Precisa che il documento log, corredato di legenda e non editabile, risponde a quanto richiesto dalla normativa in tema di prova di autenticazione forte ed esecuzione delle operazioni di pagamento ed è riconosciuto come valida prova dai Collegi ABF. Ciò vale anche per le ulteriori allegazioni, come quelle relative agli sms e alle notifiche push.
Riguardo alla attivazione del Mobile Token su due dispositivi, conferma che "può essere effettuata indipendentemente dall'eventuale diverso n. di telefono del secondo dispositivo, che peraltro può anche non esserci: ad esempio un Tablet non è necessariamente collegato ad un numero di telefono"; pertanto, la dichiarazione dell'utenza telefonica del cliente e la sua associazione al servizio di home banking "è finalizzata unicamente all'invio delle comunicazioni da parte della banca relativamente all'operatività online".

Insiste per il resto nell'evidenziare vari profili indicativi di colpa grave della condotta assunta dalla ricorrente.

DIRITTO

La controversia in esame concerne il disconoscimento di bonifici per complessivi € 84.382,00: uno di € 24.996,00 (+ € 1,00 per commissioni) eseguito il 30/03/2022; uno di € 29.498,00 (+ € 1,00 per commissioni) eseguito il 31/03/2022; uno di € 29.888,00 (+ € 1,00 per commissioni) eseguito l'1/04/2022.
Le operazioni contestate sono state eseguite 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 13/01/2018.
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".
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 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 50 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. Da ultimo, cfr. 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).

L'orientamento di questo Arbitro 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. 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), è 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").

Tanto premesso in termini generali, rileva il Collegio che, nella specie, oggetto di disconoscimento sono tre bonifici per complessivi € 84.382,00: uno di € 24.996,00 (+ € 1,00 per commissioni) eseguito il 30/03/2022; uno di € 29.498,00 (+ € 1,00 per commissioni) eseguito il 31/03/2022; uno di € 29.888,00 (+ € 1,00 per commissioni) eseguito l'1/04/2022.

Nello specifico, la ricorrente riceve in data 30/03/2022 alle 13:26 un messaggio civetta dal numero solitamente usato dall'intermediario per le proprie comunicazioni, come si evince dai precedenti sms genuini ricevuti dell'intermediario. Con tale sms la si informava di una "limitazione" della sua carta/conto per "mancata verifica della sicurezza web" e la si invitava a cliccare su un link. Riferisce di aver cliccato su detto link e di essere stata così reindirizzata a un sito identico a quello dell'intermediario, in cui si chiedeva di inserire le credenziali (codice utente e PIN) per accedere all'home banking. Fa presente di aver ricevuto un altro sms alle 14:05 che preannunciava la telefonata di un operatore dell'istituto e di essere stata contattata telefonicamente alle 14:06 della medesima giornata dal numero verde dell'intermediario e di aver seguito le istruzioni impartite dall'interlocutore telefonico e di aver dunque provveduto a disinstallare la app della banca e ad installarne un'altra. Riferisce di aver ricevuto ulteriori sms che confermavano quanto nel frattempo comunicato dal presunto operatore bancario.

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 rileva anzitutto che in data 30/03/2022, alle ore 14:15:22 vi è stato un tentativo di accesso propedeutico all'attivazione del Mobile Token, mediante inserimento di PIN da parte di un certo device (che risulta diverso da quello utilizzato in precedenza).

L'intermediario precisa poi che alle ore 14:17:33 dallo stesso indirizzo IP è stata effettuata l'attivazione del Mobile Token tramite l'inserimento del PIN (fattore di conoscenza) e della OTP trasmessa via sms (fattore di possesso).
L'intermediario produce inoltre la schermata del sms inviato alla ricorrente contenente il codice per attivare il Mobile Token; il numero di cellulare al quale è stato trasmesso il messaggio coincide con quello indicato dalla ricorrente nel modulo di ricorso.
Dal log prodotto dall'intermediario si evince che alle ore 14:26:11, è stato registrato un login con "verifica a 2 fattori" (come indicato dall'intermediario nelle controdeduzioni), mediante inserimento del codice OTP (***671) generato dal Mobile Token. Per l'esecuzione della prima operazione di bonifico alle ore 14:31:58 il sistema ha richiesto l'utilizzo del PIN (fattore di conoscenza) e del codice OTP (***183) generato da Mobile Token (fattore di possesso).
La stessa procedura di login e esecuzione dell'operazione di bonifico è stata seguita anche per le altre due operazioni, rispettivamente perfezionate alle ore 13:08:01 del 31/03/2022 (previo login alle 13:05:43) e alle ore 13:50:31 dell'1/04/2022 (previo login alle 13:45:52).
Ciò premesso, il Collegio rileva che tanto la preventiva configurazione del Mobile Token, quanto le operazioni contestate siano state autenticate mediante elementi che, in base agli standard tecnici fissati dall'EBA nell'Opinion del 21 giugno 2019, risultano riconducibili alle categorie della conoscenza (PIN per accedere all'home banking, nonché per generare le OTP) e del possesso e che dunque sia stata fornita la prova da parte dell'intermediario dell'autenticazione forte (cfr. Collegio di Bari, decisione 2663/23; Collegio di Bologna, decisione n. 23216/2)."
Alla luce delle richiamate disposizioni normative, peraltro, la prova della regolarità formale dell'operazione contestata non è sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento di pagamento, dovendo l'intermediario provare anche i fatti idonei a integrare il dolo o la colpa grave dell'utilizzatore. Questo aspetto risulta enfatizzato, a seguito della novella del 2017 (d.lgs. n. 218/2017), che ha introdotto nell'art. 10, co. 2, la disposizione sopra riportata, in tema di onere della prova del dolo o della colpa grave dell'utente. La prova in questione, evidentemente, non può coincidere con quella della mera regolarità formale delle operazioni, pena un'interpretazione abrogante della disposizione. Sul punto si è, da ultimo, pronunciato il Collegio di Coordinamento, nella menzionata decisione n. 22745 del 10/10/2019, nella quale è stato enunciato il principio secondo cui "la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente [....]Utili informazioni integrative potrebbero, ad esempio, riguardare l'assenza di tentativi falliti di digitazione del PIN, la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente, in assenza di deviazioni o intrusioni nel device, l'accertata assenza di malware, ecc.".
Nel caso di specie, il Collegio rileva che l'intermediario ha provveduto ad indicare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali può trarsi la prova, in via presuntiva, della colpa grave dell'utente (v. Collegio di Coordinamento, decisione n. 22745/2019), ai sensi degli artt. 7, comma 2, e 12, comma 4, del D.lgs. n. 11/2010, per non avere custodito con le dovute cautele i codici di accesso allo strumento di pagamento di cui è titolare. A parziale discolpa della ricorrente, non può essere priva di rilievo la sofisticata manipolazione perpetrata a suo danno, visto che ha prima ricevuto SMS confondibili con quelli provenienti dall'intermediario e poi ricevuto una telefonata fraudolenta apparentemente proveniente dall'intermediario, con ciò evidenziando l'agevole vulnerabilità

organizzativa dei canali di comunicazione adottati da quest'ultimo; vulnerabilità che viene ulteriormente testimoniata dalla crescente rilevazione di casi di truffe simili in danno della clientela (Collegio di Bari, decisione n. 9071/22: Collegio di Bari, decisione n. 9922/22; Collegio di Milano, decisione n. 3001/2021).
Per quanto innanzi, il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 42.191,00 liquidato in via equitativa.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 42.191,00.
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