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) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - PIERFRANCESCO BARTOLOMUCCI

Seduta del 09/09/2024

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 11/04/2024, una telefonata dal numero verde corrispondente a quello del servizio clienti dell'odierno resistente e da cui era già stato contattato precedentemente. Interloquiva con un soggetto che si qualificava come operatore dell'intermediario, il quale gli chiedeva di collegarsi sul sito dell'intermediario per effettuare "controlli su accessi abusivi". Il ricorrente, seguendo tali indicazioni, si collegava su un sito apparentemente analogo a quello della resistente, ove eseguiva il login; dopo l'accesso, il sedicente operatore confermava "di aver bloccato un accesso abusivo", ma il cliente si avvedeva che, in realtà, fosse stato disposto un bonifico istantaneo di euro 14.000,00.
Contestava che l'intermediario non avesse predisposto gli strumenti idonei ad evitare fenomeni di frode e a bloccare automaticamente operazioni anomale, in violazione delle norme di diligenza ex art 1176 cod. civ. Lamentava altresì che i truffatori fossero riusciti a perpetrare la frode utilizzando "un sito clone" e i canali di comunicazione ufficiali della resistente (nella specie, il numero verde). Chiedeva, pertanto, il rimborso dell'importo di euro 14.000,00.
Si costituiva ritualmente l'intermediario convenuto, il quale ricostruiva la vicenda rinviando alle dichiarazioni rese dal ricorrente in sede di denuncia precisando, anzitutto, che lo stesso non avesse fornito prova dell'asserita telefonata ricevuta il giorno della truffa alle ore 12:47 dal numero verde riferibile al resistente.

Soggiungeva che dall'analisi delle operazioni potesse evincersi che il ricorrente, seguendo le indicazioni telefoniche del sedicente operatore, avrebbe incautamente inserito le proprie credenziali accedendo ad un sito a sé non riconducibile, fornito il codice di sicurezza ricevuto via sms e inviato una copia del proprio documento di identità.
Tali informazioni avrebbero consentito l'esecuzione, tramite il servizio di internet banking, di tre bonifici, di cui due ordinari (rispettivamente di euro 20.000,00 e di euro 1.000,00), tempestivamente bloccati dal servizio clienti, e un ulteriore bonifico istantaneo di euro 14.000,00, immediatamente accreditato sul conto del beneficiario.
L'intermediario evidenziava altresì che, al momento della disposizione dei pagamenti, avesse inviato i relativi sms altert e, il giorno stesso, attivato la procedura di recall per il recupero delle somme in questione, la quale tutt'ora risultava sospesa.
Faceva presente che sul sito dell'intermediario sono presenti indicazioni volte a diffondere la "sicurezza on line" ed evitare fenomeni di frode. In particolare, viene raccomandato di non inserire mai user, password e numero di cellulare su siti internet o app non ufficiali, di non comunicare mai a presunti operatori bancari le proprie credenziali e di prestare attenzione alle telefonate o sms sospetti, anche se apparentemente provenienti dall'intermediario; viene infine precisato che l'intermediario non chiede mai dati personali o di accesso ai propri clienti.
In merito al sistema di internet banking, rappresentava che lo stesso è dotato di un sistema di autenticazione forte che prevede per il suo utilizzo l'inserimento di credenziali di accesso (codice utente e password) e di un codice pin temporaneo generato da un dispositivo software a ciò dedicato.
Sottolineava che dalle risultanze informatiche, potesse evincersi che il primo accesso al servizio di internet banking fosse avvenuto senza anomalie alle ore 12:56, a cui aveva fatto seguito un ulteriore accesso delle ore 13:45 e, qualche minuto dopo, l'esecuzione dei suddetti bonifici.
Rilevava altresì che sia il link su cui il ricorrente aveva ammesso di aver cliccato sia la pagina a cui lo stesso reindirizzava (in cui si richiedeva l'inserimento delle credenziali di accesso) non risultassero in alcun modo riconducibili a quelli dell'intermediario.
In conclusione, l'intermediario riteneva di aver predisposto ogni presidio utile a tutelare la sicurezza dei propri clienti e che, invece, la frode in esame fosse imputabile esclusivamente alla condotta negligente del ricorrente che aveva consentito a terzi sconosciuti di accedere al servizio di internet banking ed inserire il bonifico istantaneo in contestazione.
Chiedeva, pertanto, di respingere il ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale precisava di aver prodotto già in allegato al ricorso la documentazione comprovante la ricezione delle due telefonate truffaldine (alle ore 12:47 e alle 13:10), recanti come mittente il numero verde e la denominazione dell'intermediario (rispettivamente: "800****499" e "AGENZIA B*** SVILUPPO"). Allegava quindi una nuova videata delle chiamate in cui veniva riportata in chiaro la data delle telefonate (11/04).
Ribadiva altresì la responsabilità del resistente per non aver predisposto strumenti idonei ad evitare che soggetti terzi possano utilizzare canali di comunicazione ufficiali dell'intermediario per contattare i clienti e ingenerare negli stessi la convinzione di interloquire con reali operatori.
Per confermare l'insidiosità della truffa, di cui non si era subito avveduto, precisava che la chiamata al servizio clienti, da lui effettuata a seguito della seconda telefonata truffaldina, e nel corso della quale aveva appreso dell'esecuzione dei tre bonifici, fosse stata una circostanza del tutto fortuita, finalizzata alla richiesta di alcune informazioni.

Soggiungeva di non aver ricevuto alcun sms alert, né email e che dalla documentazione informatica allegata dal resistente non si evincesse l'invio degli stessi al numero di cellulare del ricorrente. Parimenti, affermava di non aver ricevuto, per i due bonifici ordinari, alcun sms contenente i codici otp necessari per autorizzare le operazioni.
Rappresentava altresì che il sito "civetta" su cui aveva eseguito l'accesso inserendo username e password, contenesse la denominazione dell'intermediario e reindirizzasse su una pagina avente schermata identica a quella reale. Reputava che tali circostanze, unitamente alla corrispondenza del numero verde da cui era stato contattato con quello ufficiale dell'intermediario, fossero in grado di indurre in errore i clienti.
Infine, evidenziava che l'intermediario avrebbe dovuto avvedersi dell'utilizzo insolito del conto corrente, posto che nell'arco di pochi minuti fossero stati disposti tre bonifici per un importo complessivo pari ad euro 35.000,00, da considerarsi anomali rispetto a quelli usualmente eseguiti dal ricorrente e che avrebbero dovuto allertarlo. Insisteva, quindi, per l'accoglimento del ricorso.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale ribadiva le proprie considerazioni in merito alla condotta negligente del ricorrente e alla collaborazione attiva di quest'ultimo ai fini della realizzazione della truffa.
Insisteva, quindi, per il rigetto del ricorso.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento on-line, successivamente disconosciuta.
La materia, come noto, è regolata dal d.lgs. n. 11/2010 come modificato dal d.lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- Payment Services Directive 2).
Tale disciplina - al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante – introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. strong customer authentication SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Orbene, risulta per tabulas che l'operazione contestata consiste in un bonifico istantaneo di importo pari ad euro 14.000,00 (oltre ad euro 5,60 di commissione non richieste dal ricorrente) disposto in data 11/04/2024 alle ore 13:47 addebitato al rapporto di conto corrente di titolarità del ricorrente.
Giova, altresì, rilevare che il giorno della truffa sono stati eseguiti anche due ulteriori bonifici ordinari: il primo, dell'importo di euro 20.000,00, è stato tempestivamente bloccato e stornato; il secondo, dell'importo di euro 1.000,00, non è andato a buon fine.
Con riferimento alle procedure di autenticazione e di esecuzione dei pagamenti, l'intermediario ha affermato che l'operazione è stata eseguita tramite il servizio Internet banking; il quale è dotato di un sistema di autenticazione forte che prevede, per il suo utilizzo, l'inserimento delle credenziali di accesso (codice utente e password) e di un codice PIN temporaneo, generato da un dispositivo software a ciò dedicato richiesto in fase di accesso all'Internet banking e/o di esecuzione dei pagamenti (token, App push notification o secure call). Sul punto, ha rinviato al "fascicolo norme contrattuali" richiamato anche nel contratto sottoscritto dal ricorrente, contenenti le disposizioni che regolano il servizio.
Parte resistente ha pure precisato che, dalla documentazione in atti e dalle dichiarazioni del ricorrente, emerge che l'operazione sia stata eseguita attraverso la collaborazione attiva di quest'ultimo, il quale "avrebbe incautamente inserito le proprie credenziali di accesso su un sito web non attendibile" e comunicato telefonicamente al sedicente operatore il "codice di sicurezza" inviato dall'intermediario sulla propria utenza via sms. Le parti costituite, tuttavia, nulla aggiungono in merito a tale messaggio né risulta prodotta in atti la relativa schermata.
Dal punto di vista documentale, parte resistente ha allegato una evidenza informatica precisando che il primo accesso al servizio di Internet banking sia avvenuto senza anomalie e con esatto inserimento di username e password alle ore 12:56:27 del 11/04/2024; che un ulteriore accesso andato a buon fine sia avvenuto alle ore 13:45:43; che il bonifico istantaneo di euro 14.000,00 (maggiorato di euro 5,60 di commissione) sia stato eseguito alle ore 13:47:15; che, pochi minuti dopo l'esecuzione del bonifico in contestazione, siano stati disposti due bonifici ordinari (di euro 1.000,00 ed euro 20.000,00) le cui somme sono state recuperate dalla banca.
Alla luce del quadro normativo sopra richiamato, e tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, il consolidato orientamento di questo Arbitro ha più volte ribadito che per valutare l'assolvimento dell'onere della prova della SCA possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione, oltre ad eventuali dichiarazioni confessorie del cliente, che assumono valore di prova legale ai sensi dell'art. 2730 cod. civ.
Orbene, nel caso di specie – ancorché dalle tracciature informatiche versate in atti emergano effettivamente le evidenze delle circostanze testé riferite – il Collegio deve pure rilevare che esse non siano in grado di fornire una prova certa riguardo l'inserimento del PIN temporaneo richiesto sia in fase di accesso che di esecuzione del pagamento; tale carenza sul piano probatorio non può essere colmata dalla descrizione del processo di autenticazione, tenuto conto dello stretto e rigoroso onere imposto dalla normativa di riferimento.
Deve quindi ritenersi che l'intermediario non abbia assolto all'onere probatorio sull'autenticazione dell'operazione di pagamento contestata dal cliente, di cui all'art. 10, comma 1 del D.lgs. 11/2010; conseguentemente, la domanda del ricorrente deve essere

integralmente accolta, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa allo stesso ascrivibili.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 14.000,00.
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