COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) CAMILLERI	Membro designato dalla Banca d'Italia
(BA) SEMERARO	Membro designato dalla Banca d'Italia
(BA) DI RIENZO	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FILIPPO BOTTALICO

Seduta del 15/12/2022

FATTO

Il ricorrente, contitolare assieme alle due aderenti volontarie al ricorso di due distinti rapporti di conto corrente presso l'intermediario resistente, riferisce di aver ricevuto sulla propria utenza telefonica, in data 31/03/2022 alle ore 16:30, un SMS apparentemente proveniente dall'intermediario, che lo informava di una limitazione del conto per una mancata verifica di sicurezza.
Riceveva, subito dopo, una chiamata dall'utenza n. ***60 (numero effettivo dell'intermediario), nel corso della quale un sedicente operatore lo invitava a rimuovere l'app della banca per installarne una nuova e gli inviava un link tramite SMS.
Dichiara di aver seguito le indicazioni fornite, senza tuttavia inserire alcun codice dispositivo; a quel punto, visualizzava "un'icona" sul proprio telefono cellulare.
Rappresenta che il sedicente operatore lo informava che, in considerazione della complessità della procedura, il completamento dell'installazione sarebbe proseguito il giorno successivo.
Afferma inoltre di aver ricevuto, nel corso della telefonata, due SMS con cui veniva informato dell'inserimento di due bonifici di € 25.560,00 e di € 22.320,63; veniva tuttavia rassicurato dall'interlocutore, il quale comunicava che si era verificato un errore e che avrebbe provveduto ad eliminare immediatamente le disposizioni di pagamento (circostanza avvalorata dalla ricezione di due ulteriori SMS relativi alla presunta revoca dei bonifici inseriti).

Il completamento della procedura veniva rinviato al successivo 4 aprile, a causa di un asserito blocco del server; in tale data, veniva contattato nuovamente dal medesimo operatore, il quale lo invitava a cliccare sull'icona della nuova applicazione e ad impostarla come predefinita.
Una volta completata l'operazione, riceveva un ulteriore apparente messaggio dell'intermediario che lo informava di dover attendere tre giorni lavorativi per poter accedere ai servizi dell'app.
Due giorni dopo, contattava l'intermediario per sollecitare l'invio delle credenziali di accesso alla nuova applicazione e, in tale sede, apprendeva che su uno dei due conti correnti erano state eseguite cinque operazioni di € 25.000,00 circa ciascuna e, nelle ore successive, veniva informato dalla figlia che era stata effettuata un'altra operazione di € 20.560,13 a valere sul secondo conto corrente.
Provvedeva dunque al disconoscimento delle operazioni, contestando all'intermediario la mancata predisposizione di misure volte a impedire l'accesso ai dati personali (tra cui il numero di cellulare utilizzato che, nel caso di specie era, tra l'altro, un'utenza intestata a terzi) e a segnalare tempestivamente la palese anomalia, per importo e arco temporale di esecuzione, delle operazioni contestate, di cui avrebbe dovuto disporre il blocco in conseguenza dell'attivazione dei presidi antiriciclaggio.
Evidenzia che i canali utilizzati per le comunicazioni con il sedicente operatore erano riconducibili all'intermediario, trattandosi dell'utenza e della chat utilizzate dalla banca per l'invio dei messaggi genuini; precisa che anche le schermate visualizzate dopo aver cliccato sul link erano prive di elementi di sospetto.
Rappresenta inoltre di non aver mai né rivelato, né inserito i propri codici dispositivi i quali, tra l'altro, non sono mai stati richiesti dall'interlocutore neanche dopo aver cliccato sul link ricevuto tramite SMS.
Ritiene che la frode di cui è stato vittima non possa essere qualificata come phishing classico, essendo presenti nel caso di specie elementi riconducibili allo spoofing e al pharming e che la stessa sia stata resa possibile dalla mancata adozione, da parte dell'intermediario, dei presidi di sicurezza a tutela della riservatezza dell'utente e dalla mancata attivazione di strumenti di monitoraggio delle transazioni dei conti on-line al fine di riscontrare eventuali comportamenti anomali, come specificamente indicato nel "Decalogo ABI per banche e clienti sui sistemi di protezione dal «phishing»".
A seguito del riscontro negativo ottenuto dall'intermediario alla richiesta di rimborso avanzata in sede di reclamo, si rivolge all'Arbitro, al quale chiede il rimborso della somma illecitamente sottratta, per un importo complessivo di € 145.045,68 (o, in subordine – "ma con riserva espressa di assumere, in tal caso, le ulteriori iniziative che si rendessero conseguentemente necessarie" – della "minor somma stimata come dovuta in restituzione per la denegata ipotesi in cui fosse nella fattispecie ritenuto sussistente concorso di colpa"), oltre alla rifusione delle spese legali, quantificate in € 2.880,00 (precisando che tale ultimo importo è stato ottenuto "abbattendo della percentuale massima consentita (ovverosia, ex art. 19 D.M. 55/2014, del 50%) i compensi indicati dalla tabella 25 bis (intitolata "procedura di mediazione e procedura di negoziazione assistita" ed allegata al D.M. 55 del 10 marzo 2014 (cfr. all. 33), da maggiorarsi del rimborso spese generali, spettante (ex art. 2, comma 2, D.M. 55/2014) in misura pari al 15%, e delle somme dovute come per Legge a titolo di C.P.A. ed I.V.A."), o nella diversa, maggiore o minore misura ritenuta equa, oltre accessori di legge.
Costituitosi, l'intermediario evidenzia preliminarmente che l'oggetto della controversia concerne la richiesta di rimborso della somma complessiva di € 145.045,68, addebitata sui conti correnti cointestati al ricorrente – abilitati al servizio di internet banking – a seguito

dell'esecuzione di sei operazioni di bonifico online disconosciute; precisa che, nel periodo in cui si sono verificati gli eventi contestati, era attivo il servizio SMS alert.
Rappresenta che, per effettuare il login e le operazioni di inquiry, è previsto l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) e del codice OTP; per disporre le operazioni, dopo avere effettuato il login, è prevista la conferma con codice PIN e OTP.
Specifica che il codice OTP viene generato in modo silente dal mobile token integrato nell'app dell'intermediario e attivato sullo strumento/device utilizzato dal cliente.
Soggiunge 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 via SMS al cellulare collegato all'home banking.
Ciò posto, rappresenta che, in data 31/03/2022, è stato inviato al dispositivo del ricorrente un SMS, oltre alla relativa notifica push, contenente il codice OTP necessario per l'attivazione del Mobile Token e l'avvertimento di non comunicare a nessuno – neanche al personale dell'intermediario – il codice ricevuto.
Asserisce che il ricorrente, a fronte di tale SMS, avrebbe dovuto insospettirsi ed interrompere la telefonata eventualmente in corso, chiamare il servizio clienti o rivolgersi al personale della sua agenzia di riferimento.
Eccepisce dunque che il mobile token è stato attivato in data 31/03/2022 alle ore 17:16, mediante l'inserimento del PIN e utilizzando l'OTP ricevuto tramite SMS; è stato poi eseguito l'accesso con verifica a 2 fattori, utilizzando l'OTP generato dal mobile token.
Rappresenta che i sei bonifici contestati sono stati autenticati con l'utilizzo del PIN e del codice OTP generato dal Mobile Token, come emerge dai log allegati.
Con specifico riferimento alla colpa grave, ritiene che le dichiarazioni rese in sede di denuncia abbiano natura confessoria, in quanto lo stesso ricorrente ha affermato di aver seguito incautamente le istruzioni ricevute dal sedicente operatore, di aver cliccato sul link inviato tramite SMS e di aver scaricato un'app diversa da quella ufficiale dell'intermediario, come risulta dalla documentazione allegata al ricorso.
Osserva altresì come il link in questione fosse palesemente inattendibile, non essendo presente il protocollo di sicurezza "https"; inoltre, in merito al canale di provenienza degli SMS e delle telefonate (riconducibili alla banca), rappresenta che è possibile in pochi passaggi modificare il mittente di un messaggio e l'identificativo del chiamante.
Quanto al servizio di SMS alert, osserva che l'utenza associata risulta intestata al ricorrente, come dimostrato dalla fattura allegata al ricorso; afferma di aver inviato, per ciascuna operazione, gli SMS relativi all'avvenuto inserimento dei bonifici.
Ritiene che l'importo delle operazioni non possa di per sé essere considerato un indice di anomalia, in assenza di una richiesta di modifica del plafond da parte del cliente.
Rappresenta infine di aver avviato le azioni di recupero dei fondi verso la banca dei beneficiari, ricevendo tuttavia un riscontro negativo ed eccepisce l'infondatezza della richiesta di rimborso delle spese legali.
Conclude, pertanto, per il rigetto del ricorso.
In sede di repliche, il ricorrente afferma di non aver ricevuto la notifica push contenente il codice OTP necessario per l'attivazione del mobile token; ritiene dunque che, nel caso di specie, possa essersi registrato uno "scambio della SIM" nell'ambito dello schema truffaldino del sim swap, per mezzo del quale i terzi hanno attivato il Mobile Token e, successivamente, hanno eseguito le operazioni contestate.
Ricostruisce la frode in esame come una sofisticata manipolazione perpetrata con le modalità dello smishing, del vishing, dello spoofing, della sim swap e del pharming e asserisce che la propria partecipazione causale alla frode si è limitata esclusivamente alla

disattivazione dell'app in uso sul proprio dispositivo, non avendo provveduto a comunicare o a digitare alcun codice.
Ritiene che l'intermediario non abbia assicurato misure di sicurezza adeguate per la tutela delle credenziali riservate.
Rappresenta di non aver ricevuto i messaggi di alert relativi all'inserimento degli ordini di bonifico e afferma che l'ordinaria operatività è consistita in bonifici per un importo massimo di € 1.389,43 ad intervalli mensili, con una movimentazione media mensile in uscita pari a € 9.824,32.
Evidenzia che la resistente non ha preso posizione in ordine alle contestazioni relative all'omessa rilevazione delle anomalie e alla mancata attivazione degli strumenti di monitoraggio delle transazioni dei conti on-line.
Infine, considera fondata la richiesta di rifusione delle spese legali, "quantomeno a titolo di risarcimento del danno", in considerazione della complessità della vicenda e del comportamento assunto dalla resistente nella vicenda.
Insiste pertanto per l'accoglimento integrale del ricorso.
In sede di controrepliche, l'intermediario ritiene che la frode in esame – contrariamente a quanto asserito dal ricorrente – non possa essere qualificata come SIM swap in quanto tale tipologia di truffa si realizza esclusivamente con la sostituzione della sim card del dispositivo dell'utente e non attraverso l'accesso ad un link; inoltre, il dispositivo del ricorrente avrebbe dovuto bloccarsi e smettere di funzionare, circostanza che non si è verificata nel caso di specie.
Afferma poi che, qualora volesse riconoscersi lo spoofing, tale modalità non escluderebbe comunque la responsabilità del cliente.
Osserva poi che il ricorrente avrebbe dovuto effettuare le opportune verifiche prima di cliccare sul link contenuto nel messaggio truffaldino e avrebbe dovuto insospettirsi nel momento in cui gli è stato richiesto di sostituire l'app ufficiale della banca con l'applicazione fake, non essendo tra l'altro presenti nell'estensione riferimenti all'intermediario.
Ribadisce di aver adottato, sia in fase di accesso che in fase di autorizzazione delle operazioni, un sistema di sicurezza conforme alla normativa di riferimento.
Relativamente al modello di device, afferma che il cliente può attivare il Mobile Token fino a due device diversi (2 smartphone o 1 smartphone + 1 tablet) e, inoltre, può sostituire il proprio cellulare,
cambiando modello, senza doverlo comunicare alla banca.
Ritiene di aver dimostrato l'invio e la consegna al cliente di tutti gli sms, incluso quello contenente il codice OTP indispensabile all'attivazione del mobile token.
Ritiene che non sia necessario che i meccanismi di monitoraggio operino in tempo reale, con conseguente insussistenza di un obbligo per gli intermediari di sottoporre a controllo ex ante tutte le operazioni disposte dal cliente.
Infine, quanto alla contestazione relativa alla movimentazione anomala dei conti corrente, rammenta che la banca non può impedire l'autonomia dispositiva della clientela, pena il venir meno al mandato conferitole con la sottoscrizione del contratto di conto corrente.

DIRITTO

Premesso che 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, le modalità della truffa della quale si protesta

vittima il ricorrente sono ricostruite, nel ricorso, in termini perfettamente sovrapponibile a quanto esposto nelle denunce in atti.
Oggetto di disconoscimento sono dunque sei bonifici online eseguiti tra il 31 marzo e il 4 aprile 2022, per un totale di € 145.045,68, come quantificato dal ricorrente.
Secondo quanto esposto dallo stesso ricorrente, a seguito della condotta fraudolenta perpetrata in suo danno sarebbe stato indotto alla disinstallazione dal suo device dell'app dell'intermediario tramite un'app fake; questo avrebbe consentito al truffatore la reinstallazione dell'app dell'intermediario su un proprio device, dal quale poi sarebbero state eseguite le operazioni contestate.
Pertanto, ancor prima di verificare le regolarità formale di queste, è necessario vagliare se la reinstallazione dell'app sia stata caratterizzata dalle cadenze della SCA.
Sul punto, 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 evidenzia anzitutto che, in data 31/03/2022, alle ore 17:16, è avvenuta l'attivazione del mobile token tramite l'inserimento del PIN (fattore di conoscenza) e della OTP trasmessa via SMS (fattore di possesso); produce il log relativo alla suddetta operatività, con la legenda esplicativa.
Inoltre, produce 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 riportato nella denuncia e nella fattura del gestore telefonico allegate al ricorso; senonché, il ricorrente nega di aver ricevuto il messaggio in questione.
Così effettuato l'enrollment dell'app (e quindi del mobile token) sul device del truffatore, sono state poi eseguite le operazioni contestate.
L'intermediario evidenzia che, in data 31/03/2022 alle ore 17:16, è stato registrato un login con "verifica a due fattori", mediante inserimento del codice OTP (***301) generato dal predetto mobile token.
Sulla base delle evidenze documentali prodotte dalla resistente, per l'esecuzione delle operazioni di bonifico il sistema ha richiesto l'utilizzo del PIN (fattore di conoscenza) e del codice OTP generato dal mobile token (fattore di possesso).
Si precisa che, nella documentazione in questione, emerge altresì l'inserimento di altre due operazioni di bonifico, poi rimaste ineseguite (cfr. stato "rifiutata" indicato nella colonna "Esito Operazione").
Si dovrebbe trattare delle operazioni per così dire "civetta", evidenziate dal truffatore come bonifici revocati negli sms inviati al ricorrente, a dimostrazione dell'esecuzione di semplici verifiche "tecniche".
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 delle operazioni che può ritenersi riscontrata sulla scorta delle evidenze in atti) può sostenersi che la procedura seguita dal medesimo intermediario – sin dalla prodromica fase dell'enrollment del device del truffatore – sia conforme alla SCA normativamente prevista.
Difatti, questo Collegio ha statuito che: "Con riguardo all'autenticazione delle operazioni l'intermediario ha dedotto che in caso di accesso all'home banking da sito web, per effettuare il login il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente e PIN) e codice OTP, quest'ultimo generato dal Mobile Token integrato nell'App e autorizzato dal cliente tramite notifica push che riceve sullo smartphone (o tablet), sulla quale dovrà cliccare e autorizzare inserendo il suo codice PIN o touchID o faceID. Per disporre le operazioni, occorre inserire l'operazione di pagamento e, sempre con il sistema della notifica push, confermarla; anche in questo caso, il cliente

riceve la notifica push sullo smartphone (o tablet) che dovrà cliccare e autorizzare inserendo il suo codice PIN o touchID o faceID, con conseguente generazione del codice OTP tramite Mobile Token integrato nell'App. Conferma che l'attivazione del mobile token è resa possibile esclusivamente 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, indipendentemente dall'attivazione del servizio SMS Alert" (Collegio di Bari, decisione n. 21204/21; conformi Collegio di Milano, decisione n. 5816/22; Collegio di Roma, decisione n. 1178/22; Collegio di Bologna, decisione n. 23216/21; Collegio di Milano, decisione n. 15074/21; Collegio di Napoli, decisione n. 14897/21; Collegio di Torino, decisione n. 3782/20).

Il soddisfacimento dell'onere probatorio gravante sull'intermediario resistente in ordine alla natura "forte" dell'autenticazione e all'assenza di anomalia consente – in conformità alla normativa vigente e secondo la giurisprudenza di consolidata – di analizzare la sussistenza o meno di profili di dolo o colpa grave nella condotta del ricorrente, analisi altrimenti preclusa in difetto del raggiungimento della suddetta prova.

La mancanza della prova di autenticazione, difatti, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente; la prova di autenticazione rappresenta, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente (sul punto, autorevolmente Collegio di Coordinamento, decisione n. 22745/19: "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").

Ebbene, è indubitabile che la truffa sia stata perpetrata anche tramite la condotta attiva e collaborativa del ricorrente, il quale – come dallo stesso ricostruito in atti – prima veniva contattato tramite un SMS civetta e poi accedeva alla richiesta telefonica del truffatore e cliccava sul link fraudolento giunto sul proprio device tramite SMS, così consentendo l'enrollment dell'app sul device del truffatore, dal quale poi venivano eseguite le operazioni contestate.

Peraltro intratteneva una seconda conversazione telefonica con il truffatore, nuovamente seguendo le indicazioni relative all'installazione dell'app malevola sul proprio device.

È altrettanto vero, però, che la ricostruzione delle modalità della truffa subita dal ricorrente – come possibile dalla documentazione in atti – ne evidenziano i caratteri dell'insidiosità e della sofisticatezza.

Non si può non evidenziare, difatti, che il primo SMS civetta veniva ricevuto dal ricorrente sulla chat utilizzata dall'intermediario resistente per l'invio, fino al momento della truffa, di SMS e comunicazioni genuine; tra l'altro, l'SMS civetta non conteneva errori grammaticali o altre anomalie (ad esempio, link nient'affatto riconducibili all'intermediario) che potessero evidenziarne la non genuinità (come stigmatizzato, ex multis, da Collegio di Bologna, decisione n. 9639/22; Collegio di Bologna, decisione n. 1697/22; Collegio di Bologna, decisione n. 9791/22; Collegio di Torino, decisione n. 969/22), anzi conteneva l'esatto riferimento, anche nel suo formato grafico, all'intermediario odierno resistente.

La telefonata fraudolenta veniva effettuata da un numero fisso analogo a quello utilizzato dall'intermediario, come risulta dagli screenshot in atti.

Sempre in atti, v'è copia della schermata apertasi sul device del ricorrente, dopo che costui aveva cliccato su link fraudolento, e in essa compare il riferimento ad un link (e un'app) apparentemente riconducibili all'intermediario resistente.

Riguardo ai sistemi di allerta, l'intermediario allega le tracciature informatiche attestanti l'invio e la consegna al cliente delle notifiche push e degli SMS relativi all'inserimento degli ordini di bonifico; senonché, v'è in atti prova dell'invio degli SMS con i quali venivano revocati due bonifici eseguiti durante le operazioni truffaldine, e di tale annullamento v'è corrispondenza anche nelle tracciature informatiche (sicché è condivisibile l'affermazione secondo la quale: "la ricezione sul cellulare del cliente anche di sms spoofed recanti messaggi di storno di bonifici non autorizzati costituisca ulteriore indice più che di una negligenza addebitabile all'utente piuttosto di criticità organizzativa dei servizi di pagamento offerti dall'intermediario": Collegio di Roma, decisione n. 9703/22).
Per tale motivo, verosimilmente il cliente veniva ingannato in ordine a quanto stava accadendo, anche a fronte delle rassicurazioni ottenute dal truffatore con la seconda telefonata.
Peraltro, il ricorrente nega di aver ricevuto i messaggi riportati nella schermata allegata dall'intermediario; al riguardo, non è noto se gli stessi siano effettivamente pervenuti sul dispositivo del cliente o se siano stati "dirottati" sul device del truffatore a seguito dell'installazione dell'app truffaldina, impostata dal ricorrente come "app SMS predefinita" su indicazione del sedicente operatore.
Non si deve dimenticare che, in alcuni casi vagliati dall'Arbitro, tali applicazioni hanno effettivamente consentito ai frodatori di gestire la messaggistica dell'utente, dirottandola sui propri dispositivi (cfr. Collegio di Torino, decisione n. 12136/22).
Se è pur vero che non può trovare accoglimento la doglianza del ricorrente in ordine all'omessa predisposizione di un sistema atto all'immediato e contestuale blocco delle operazioni contestate in quanto "sospette" (condivisibilmente, il Collegio di Roma, nella decisione n. 8520/21, ha statuito che: "il Regolamento n. 389/2018 (riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE - PSD2), in vigore dal 14 settembre 2019 prevede soltanto meccanismi di monitoraggio ex post, non essendo previsto un obbligo di monitoraggio delle operazioni in tempo reale (se non nei casi in cui l'intermediario voglia avvalersi della esenzione SCA), di talché tali indici di anomalia non possono essere valorizzati per desumerne una concorrente responsabilità della resistente"), è altrettanto vero che il complessivo funzionamento dei messaggi di allerta può essere valutato dall'Arbitro alla stregua delle circostanze di fatto del caso concreto (così Collegio di Coordinamento, decisione n. 24366/19).
Alla luce della normativa e della giurisprudenza richiamate, nonché in relazione alle modalità della vicenda come ricostruibile dalla documentazione in atti, appare dunque equo riconoscere una corresponsabilità dell'intermediario resistente (derivante dall'utilizzo da parte del truffatore di canali di comunicazione analoghi a quelli ufficiali, sintomatico di una sua criticità organizzativa) e del ricorrente (che ha comunque dato corso alle richieste fraudolente, consentendo l'esecuzione delle operazioni fraudolente in un arco temporale di diversi giorni), ripartendo il danno nella misura del 60% a carico del primo e del 40% a carico del secondo.
Tanto, in aderenza all'orientamento di questo Collegio in tema di c.d. sms spoofing come compendiato nella decisione n. 9071/22: "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. Ciò posto, il Collegio ritiene di aderire all'orientamento già espresso dal Collegio di Bari, il quale, con la decisione n. 284/22, ha avuto modo di affermare in caso analogo che: "Tuttavia, 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. Per le suesposte ragioni, ritiene il Collegio che, sussistendo un concorso di colpa, il ricorso sia meritevole di accoglimento parziale; e alla luce delle circostanze del caso reputa che le conseguenze dell'operazione fraudolenta debbano restare a carico dell'intermediario nella misura del 60%". Infatti nel caso di specie si riscontra una grave imprudenza del ricorrente che ha concorso nella produzione della frode perpetrata nei suoi confronti" (conformi, Collegio di Bari, decisione n. 9922/22); orientamento, peraltro, condiviso dagli altri Collegi territoriali (ex multis, Collegio di Roma, decisione n. 8723/22: "La frode riconducibile al ricorrente è riconducibile al cd. smishing in cui il messaggio reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini, effettivamente provenienti dall'intermediario. Secondo la più recente posizione condivisa dei Collegi territoriali, in questi casi non è generalmente ravvisabile la colpa grave del ricorrente, "a meno che non si rinvengano […] indici di inattendibilità o anomalia del messaggio; in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (Collegio di Roma, decisione n. 1652/2022)"; adde, Collegio di Roma, decisione n. 8719/22; Collegio di Milano, decisione n. 7410/22; Collegio di Torino, decisione n. 8978/22).

Il ricorrente chiede inoltre la rifusione delle spese legali, versando in atti una fattura emessa dall'Avvocato suo difensore, corredata dalla copia dell'assegno recante il suo pagamento; senonché, a fronte della parziale soccombenza, tale richiesta non può essere accolta.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 87.027,00.

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