Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

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

Relatore ESTERNI - MASSIMO DI RIENZO

Seduta del 08/07/2021

FATTO

Il ricorrente, titolare di un conto corrente acceso presso l'intermediario, riferisce che in data 28/09/2020 alle ore 16:25, mentre era al cellulare, la chiamata veniva improvvisamente interrotta per assenza di rete (essendo comparsa sul proprio smartphone la scritta "nessun servizio"). Poiché il problema persisteva a distanza di più di un'ora, si recava al centro di telefonia, ove scopriva che qualcuno alle 16:42 dello stesso giorno aveva chiesto e ottenuto la sostituzione della scheda sim a lui intestata; precisa di non essere riuscito a ottenere maggiori informazioni dal personale del centro, che adduceva ragioni di riservatezza. Afferma quindi di aver immediatamente proceduto alla sostituzione della propria scheda sim e di essersi poi recato presso le Autorità al fine di sporgere denuncia/querela.
Rappresenta di essere stato contattato telefonicamente il giorno successivo 29 settembre 2020, alle ore 19:00 circa, da un operatore dell'ufficio anti frodi dell'intermediario, il quale lo informava che il giorno precedente era stato effettuato "un movimento bancario" alle ore 16:50 circa, dell'importo di € 12.701,00; non avendo autorizzato tale operazione afferma di essersi recato la mattina del 30 settembre 2020 presso la propria filiale, dove prendeva atto dell'avvenuta frode. Afferma dunque di aver sporto una nuova denuncia e, in seguito, di essere stato rassicurato dalla banca che l'operazione era stata bloccata e sarebbe stata rimborsata dopo pochi giorni.
Dal momento che a distanza di venti giorni non perveniva alcun rimborso o altra comunicazione dalla banca, afferma di essersi nuovamente recato presso la propria filiale, dove gli veniva comunicata la difficoltà nel procedere al rimborso; rappresenta dunque di aver sporto reclamo all'intermediario, riscontrato da quest'ultimo affermando che l'operazione risultava regolarmente autenticata, correttamente registrata e contabilizzata

mediante l'utilizzo delle credenziali corrette ed inserimento del codice OTP, nonché contestando al cliente una negligente custodia dei codici di sicurezza.
Il ricorrente sostiene piuttosto di essere stato vittima di sim swap e afferma che l'intermediario non si è assicurato che le credenziali per accedere al servizio di internet banking non fossero note a soggetti diversi dall'utente; sostiene inoltre che l'intermediario stesso aveva riscontrato l'anomalia dell'operazione oggetto di causa, tanto che, dopo il suo compimento, si era attivato l'ufficio antifrodi.
Sostiene che se, dunque, la transazione in discorso presentava profili di anomalia, l'intermediario avrebbe dovuto bloccarla, cosa che nel caso di specie non ha provveduto a fare.
Evidenzia che in sede di riscontro al reclamo l'intermediario ha sostenuto che alle ore 16:49 del 28 settembre 2020 risulterebbe consegnato sull'utenza intestata al ricorrente il messaggio di attivazione del Mobile Token, con cui veniva invitato a non comunicare a nessuno il codice riservato ivi riportato; peraltro, rappresenta che la data e l'orario del messaggio coincidono con quelle dell'operazione disconosciuta, ed egli afferma di essere rientrato in possesso della propria utenza telefonica soltanto alcune ore dopo l'avvenuta frode. Sostiene dunque che il codice OTP sia stato ricevuto da chi ha fraudolentemente carpito la sua identità telefonica con la nuova sim.
In riferimento poi all'affermazione della banca – contenuta sempre nel riscontro al reclamo – secondo cui sulla sua utenza telefonica sarebbe stato consegnato un messaggio in data 24 settembre 2020 analogo a quello ricevuto il 28 settembre, precisa di non avere risposto ad alcun tipo di sms "civetta" e di avere sempre custodito diligentemente le credenziali di accesso al conto.
Chiede pertanto all'Arbitro di "disporre a carico dell'intermediario la restituzione dell'importo di € 12.701,00 … disponendo altresì a carico dell'intermediario il rimborso delle spese e competenze della procedura".
Costituitosi, l'intermediario fa presente, innanzi tutto, che il ricorrente è titolare di conto corrente al quale è collegato il servizio di home banking e che egli ha altresì aderito al servizio sms alert.
Con riferimento al sistema di sicurezza adottato, precisa in generale che per effettuare il login all'home banking da app il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP generato da Mobile Token; per disporre le operazioni, invece, dopo avere effettuato il login le operazioni devono essere confermate mediante l'inserimento del PIN + codice OTP generato da Mobile Token.
Per effettuare invece il login all'home banking da sito web il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente + PIN codice statico noto solo al cliente) e codice OTP; precisa che la OTP viene generata dal Mobile Token integrato nell'app della banca che il cliente deve avere attivato sul proprio smartphone o tablet, e detto codice deve essere autorizzato dal cliente tramite la 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, invece, una volta effettuato il login si può inserire l'operazione di pagamento e, sempre con il sistema della notifica push, la si può confermare; 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, a cui poi segue la generazione del codice OTP da Mobile Token integrato nell'app.
Precisa inoltre che il cliente può attivare il Mobile Token su due dispositivi diversi (es: due smartphone, uno smartphone e un tablet), mentre non è possibile attivare sullo stesso device più di un Mobile Token.

Con specifico riferimento all'operazione fraudolenta oggetto di ricorso, rappresenta di aver inviato al cellulare del ricorrente "in prossimità dell'operazione disconosciuta" quattro comunicazioni riguardanti l'attivazione del Mobile Token, e in particolare un sms e una notifica push in data 24 settembre 2020 alle ore 16:42:53, nonché un sms ed una notifica push in data 28 settembre 2020 alle ore 16:49:21; precisa che tutte le comunicazioni di cui sopra risultano regolarmente consegnate al cliente e a fronte delle stesse il ricorrente non ha assunto alcuna iniziativa.
Ritiene plausibile ritenere che il cliente abbia omesso di dichiarare i fatti precedenti al 28 settembre (giorno della frode), "presumibilmente accaduti il giorno 24 settembre", che hanno consentito a terzi sconosciuti di venire a conoscenza delle credenziali di sicurezza dell'home banking direttamente dal ricorrente; afferma poi che il ricorrente, a fronte dello sms e della notifica push del 24 settembre 2020, avrebbe dovuto attivarsi urgentemente chiedendo informazioni all'intermediario (non essendo stato lui ad operare, come dichiarato), evitando ogni danno a suo carico.
Conclude dunque che la frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai presunti frodatori, delle credenziali di accesso all'home banking, senza le quali non sarebbero stati in grado di accedere alla app, scaricare il Mobile Token e disporre operazioni, infatti la sola conoscenza del numero telefonico del ricorrente e l'eventuale accesso alla relativa sim ad opera di malfattori non è sufficiente per consentire di scaricare l'app della banca e disporre le operazioni; per scaricare l'app, infatti, è necessario conoscere le credenziali di sicurezza dell'home banking (n. cliente + PIN), quindi attivare il Mobile Token mediante l'inserimento del codice OTP ricevuto via SMS. I malfattori dovevano necessariamente essere venuti a conoscenza delle citate credenziali (n. cliente + PIN) direttamente dal ricorrente, in circostanze che il ricorrente omette di descrivere.
Sostiene che la reticenza del ricorrente nella descrizione dei fatti che possono aver portato alla frode a suo danno debba essere valutata negativamente, alla stregua dell'orientamento consolidato dei Collegi ABF.
Soggiunge che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, poiché l'operazione risulta correttamente autenticata, registrata e contabilizzata, come evincibile dai log che afferma di produrre, nonché dei quali riporta una descrizione. Precisa che il codice OTP necessario per il perfezionamento dell'operazione, come sopra descritto, non è stato inviato tramite sms (come accade per l'OTP necessario all'attivazione del mobile token), ma viene generato dal Mobile token stesso, attivato in precedenza.
Ritiene dunque che il cliente sia rimasto vittima di phishing e, con riferimento alla dichiarazioni di questi circa il malfunzionamento della linea telefonica, rappresenta che trattasi di dichiarazioni non documentate; sostiene comunque che "proprio sulla base delle stesse è plausibile ritenere che l'SMS e la notifica PUSH del 24.09.2020 siano stati regolarmente ricevuti dal ricorrente"; precisa inoltre che "le notifiche push, anche quella del 28 settembre, indipendentemente dalla disponibilità della linea telefonica, potevano essere visualizzate anche dal device del ricorrente se solo fosse collegato ad una rete wi-fi".
Sostiene dunque che la colpa grave del ricorrente consista nell'omessa custodia delle proprie credenziali di sicurezza (che ha consentito a terzi non autorizzati di scaricare l'app della banca, attivare il mobile Token e disporre operazioni) nonché nella dimostrazione che già in data 24 settembre, con la ricezione dello sms alert contenente il codice OTP necessario per attivare il mobile token il ricorrente avrebbe potuto/dovuto attivarsi e non lo ha fatto, tenuto conto che il bonifico di cui si chiede il rimborso è stato inserito ben quattro giorni dopo.

Rappresenta di essersi attivato per tentare il recupero dei fondi presso il beneficiario non appena venuto a conoscenza del disconoscimento del bonifico fraudolento, ma che "purtroppo … non ci sono stati ritorni".
Fa poi presente di aver contattato il cliente in seguito alla rilevazione di "compulsivi ulteriori tentativi di inserimento di operazioni dispositive" (bloccate dalla banca) avvenuti in data 29 settembre 2020.
Evidenzia che al fine di prevenire possibili frodi in danno alla clientela da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nonché avendo promosso un'azione di mailing indirizzata a tutta la clientela il 4 agosto 2020.
Sostiene inoltre che il sistema di autenticazione "a due fattori" come quello adottato è riconosciuto come un sistema "forte" anche dall'orientamento diffuso dei Collegi ABF, e in presenza di un siffatto sistema nonché in assenza di particolari anomalie si deve presumere che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.
Contesta infine la richiesta di rifusione delle spese legali eventualmente sostenute dal ricorrente.
Conclude affermando di dover andare esente da ogni responsabilità, precisando che le modalità di esecuzione dell'asserita frode sono comunque estranee alla banca "e le conseguenze negative sul ricorrente sono tutte ascrivibili e ricollegabili alla negligenza dello store telefonico, come riconosciuto espressamente dallo stesso ricorrente; tanto che l'AGCOM, tenuto conto del fenomeno del sim swapping fraud nel novembre 2020 ha avviato un procedimento e una consultazione pubblica al fine di introdurre meccanismi per prevenire e contrastare eventuali tentativi di truffa a danno degli utenti finali di telefonia mobile". Precisa che "il sim swapping non è ascrivibile alla Banca ma avviene sempre grazie alla negligenza o peggio alla connivenza degli addetti agli store telefonici, che superficialmente accordano il cambio di SIM a terze persone o non identificandole in modo adeguato, accontentandosi di documentazione parziale; detta circostanza è del tutto estranea alla Banca". Ad ogni modo, sostiene il mancato assolvimento dell'onere della prova incombente sul ricorrente in ordine ai fatti costituitivi dell'asserita frode.
Chiede pertanto che il ricorso sia respinto.
In sede di repliche, il ricorrente fa presente che, nonostante i tentativi di controparte di addossare ogni responsabilità sul cliente, dalla documentazione in atti non emergono elementi atti a dimostrare che le operazioni contestate siano scaturite da un fenomeno di phishing, ritenendo piuttosto che, per come esposto e documentato, lo stesso sia stato vittima della frode nota come "sim swap fraud"; afferma di non avere mai ricevuto alcun messaggio in data 28 settembre 2020 alle ore 16:49:21 proprio in ragione del tipo di frode subita; evidenzia che i messaggi del 24 settembre e del 28 settembre 2020 non rappresentano in ogni caso messaggi atti a indurre il cliente a fornire a terzi le proprie credenziali; sottolinea inoltre che l'operazione di bonifico disconosciuta risulta essere stata effettuata in data e ora "2020-09-28 16:53:28.063" dal dispositivo "iPhone di C*** (iPhone 6s)" che con tutta evidenza è un dispositivo assolutamente estraneo al ricorrente, a conferma del fatto che i frodatori, attraverso la sostituzione della scheda sim, sono riusciti ad appropriarsi dei suoi dati di accesso bancari e a disporre l'operazione in contestazione, sostenendo pertanto che il sistema di sicurezza predisposto dall'intermediario sia inadeguato; ritiene infine di aver fornito una precisa e puntuale contestualizzazione dei fatti e dei dettagli dai quali si evince la estraneità dello stesso all'operazione contestata.
L'intermediario, a sua volta, ha replicato, affermando, con riferimento alla mancata ricezione, da parte del cliente, dell'sms del 28 settembre 2020 alle ore 16:49:21, di potere solo verificare che il servizio sms non subisca dei malfunzionamenti che impediscano la

consegna al numero di cellulare del cliente collegato all'home banking e, sul punto, sostiene che gli sms risultano regolarmente consegnati come dimostrato dalle evidenze allegate; evidenzia che il cliente ha indirettamente ammesso di avere ricevuto il messaggio del 24 settembre 2020, avente lo stesso contenuto di quello del 28 settembre; precisa che gli sms sopra menzionati, contrariamente a quanto affermato dal ricorrente, confermavano al cliente che un terzo non autorizzato stava operando dalla app della banca sul suo home banking ed avrebbero dovuto allertarlo, inducendolo a chiedere informazioni all'istituto; con riferimento, poi, all'utilizzo di un device che il ricorrente riconosce come non suo, precisa che il cliente può attivare sino a due Mobile Token su altrettanti dispositivi diversi e la banca non è tenuta a conoscere il modello di cellulare utilizzato dal ricorrente, il quale può liberamente sostituirlo senza dover informare la banca; ribadisce nuovamente che la sola sostituzione della sim card ad opera di malfattori non è sufficiente per consentire di accedere all'app e disporre operazioni se non si conoscono le credenziali di sicurezza, pertanto, riaffermando che i malfattori dovevano necessariamente essere venuti a conoscenza del numero di telefono del cliente e delle sue credenziali di sicurezza (n. cliente + PIN) in circostanze che il ricorrente omette di descrivere.

DIRITTO

La questione oggetto del ricorso attiene all'uso non autorizzato di uno strumento di pagamento ed è stata posta in essere 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).
Sebbene il citato decreto n. 218/2017 risulti entrato in vigore il 13 gennaio 2018, tuttavia, a tenore di quanto previsto dall'art. 5, comma 6, dello stesso decreto "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366", ed inoltre "fino alla data di applicazione delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366, con riferimento alle materie disciplinate dalle medesime norme tecniche di regolamentazione continuano a trovare applicazione le disposizioni emanate dalla Banca d'Italia, ai sensi di norme abrogate o sostituite per effetto del presente decreto in quanto compatibili con le disposizioni dello stesso" (art. 5, comma 8).
Tali norme tecniche sono state adottate con il Regolamento Delegato (Ue) 2018/389 della Commissione del 27 novembre 2017, entrato in vigore il 14 settembre 2019.
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. […] 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" (Collegio di Coordinamento, decisione n. 3947/2014, ma v. anche le precedenti decisioni nn. 991/2014 e 3498/2012, nonché, più di recente, la decisione n. 22745/2019). L'orientamento di questo Arbitro ha trovato riscontro nella sentenza della Corte di Cassazione, n. 2950/2017, la quale ha ritenuto che la disciplina speciale, in tema di strumenti di pagamento, espliciti il principio generale, in materia 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" (cfr. anche Cass., n. 13777/2007 e, da ultimo, Cass., n. 9158/2018).
Questo implica che, ai fini della odierna decisione, resta fermo che la disciplina applicabile 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 dando dimostrazione che le operazioni contestate sono state correttamente eseguite e non sono frutto di malfunzionamenti delle procedure esecutive e fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7, 10, co. 2 e 12, D.Lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011 ed inoltre che i riferimenti all'esigenza di una 'autenticazione forte' del cliente da parte dei prestatori di servizi di pagamento presenti nelle norme riformate del D.Lgs. n. 11/2010 (artt. 10-bis e 12), costituivano diritto vigente al momento dei fatti qui in rilievo.
In ragione di ciò, considerato altresì che la richiamata normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute (anche) laddove quest'ultimo non abbia predisposto un "sistema di autenticazione forte" e che detto sistema deve trovare applicazione, ai sensi di quanto disposto dall'art. 10-bis, D.Lgs. n. 11/2010, anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi, va altresì tenuto presente che l'art. 12, comma 2-bis, D.Lgs. n. 11/2010, stabilisce che "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"; diversamente, qualora il prestatore di servizi di pagamento abbia adottato un sistema di autenticazione forte del cliente, si ricade nelle fattispecie regolate dai commi terzo e quarto dello stesso art. 12 D.Lgs. n. 11/2010, che prevedono a quali condizioni ed in che misura possa ammettersi e sussistere una responsabilità del pagatore.
Quanto accaduto al ricorrente, secondo quanto affermato dall'intermediario, sarebbe da ricondursi, in una sua fase iniziale, ad un fenomeno di phishing, giacché in data 24 settembre 2020 (dunque prima del lamentato malfunzionamento dell'utenza telefonica) alle ore 16:42 il ricorrente avrebbe ricevuto un sms e una notifica push contenenti codici per attivare il c.d. mobile token (strumento utile a generare le OTP) su un nuovo device; a tale riguardo, afferma l'intermediario che, poiché "l'attivazione del Mobile Token è possibile solo se si è a conoscenza delle credenziali di sicurezza dell'home banking ed in particolare dell'OTP specifico inviato via sms" "presumibilmente", in tale data il ricorrente avrebbe consentito a terzi sconosciuti di venire a conoscenza delle credenziali di sicurezza dell'home banking.
Tuttavia, rileva il Collegio che, a supporto di tali affermazioni, l'intermediario allega alcune schermate, che sarebbero relative alle notifiche ricevute dal cliente via sms e push in data 24 settembre 2020, ma non produce alcuna evidenza relativa a tale giornata su eventuali

accessi all'home banking o sull'attivazione del Mobile token su un nuovo device; né l'assolvimento di tale onere probatorio – incombente sull'intermediario – può ritenersi essere stato sostituito da un'affermazione incidentale contenuta nelle repliche del ricorrente, da cui sembrerebbe però soltanto potersi desumere che in effetti un messaggio in tale data (24 settembre) a quest'ultimo sarebbe pervenuto.
Sulla base invece delle affermazioni del ricorrente, riportate anche nella denunzia alle autorità, sembrerebbe dimostrato che quest'ultimo sia stato vittima di una truffa più sofisticata mediante la tecnica denominata "SIM-swap fraud", grazie alla quale terzi soggetti trasferiscono l'utenza telefonica del titolare di carta su una nuova SIM, ricevendo così le password dinamiche OTP inviate a tale numero.
Tanto invero già risulterebbe sufficiente ad una decisione nel merito del ricorso considerando che, secondo le posizioni condivise dai Collegi, nei casi di sim swap fraud le richieste del cliente risultano meritevoli di accoglimento integrale, in quanto la sostituzione della sim card deve essere equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10 del D.lgs. 11/2010.
Volendo esaminare le circostanze ulteriori del caso di specie, dalle evidenze prodotte in atti si evince che l'operazione oggetto di ricorso consiste in un bonifico di € 12.701,00 (inclusivo della commissione pari ad un euro) a valere sul conto corrente del ricorrente, disposto in data 28/09/2020 tramite home banking e autorizzato tramite app e l'intermediario ha precisato che l'operazione è stata autorizzata alle ore 16:53.
Al fine di comprovare la corretta autenticazione dell'operazione contestata, l'intermediario ha descritto il processo di autenticazione e per dimostrarne la correttezza e l'assenza di anomalie, ha esplicato analiticamente nelle proprie controdeduzioni come dalle registrazioni elettroniche effettuate in occasione dell'operatività contestata, si evinca che: il 28 settembre 2020 alle ore 09:48:55, è stato effettuato un login mediante inserimento di PIN con il device "iPhone di c*** (iPhone 6s)" nonché inserendo l'OTP (99**7119) generata dal Mobile Token (per vero, dunque, prima del malfunzionamento dell'utenza telefonica lamentato dal ricorrente); alle ore 15:12:20, è stato registrato un tentativo di accesso mediante inserimento di impronta digitale con il device "W***** (iPhone SE 2nd Gen)"; alle ore 16:03:14 stato effettuato un login mediante inserimento di PIN con il device "iPhone di c*** (iPhone 6s)" nonché inserendo l'OTP (79**3005) generata dal Mobile Token; alle ore 16:48:11, è stato effettuato un login mediante inserimento di PIN con il device "iPhone di c*** (iPhone 6s)" nonché inserendo l'OTP (94**5985) generata dal Mobile Token; alle ore 16:48:45, è stato registrato un tentativo di accesso mediante inserimento di PIN con il device "iPhone (iPhone 7)"; alle ore 16:50:00, è stato attivato il Mobile Token (con nickname w*****0) mediante inserimento di PIN e utilizzando l'OTP (83**9578) ricevuto via sms, "con verifica a 2 fattori, utilizzando l'OTP (77**5702) generato dal Mobile Token"; alle ore 16:51:20, è stata autorizzata l'operazione di login al sito della banca in particolare con PIN e OTP (88**4004) generato da Mobile Token, con il dispositivo "iPhone di c*** (iPhone 6s)"; alle ore 16:53:28, è stato effettuato un login mediante inserimento di PIN con il device "iPhone di c*** (iPhone 6s)" inserendo l'OTP (63**4772) generato dal Mobile Token; alle ore 16:53:48, è stata autorizzata l'operazione di bonifico SEPA, in particolare con PIN e OTP (36**2650) generato da Mobile Token, con il dispositivo "iPhone di c*** (iPhone 6s)".
Venendo ad essere evidenziati così dallo stesso intermediario taluni elementi che confermerebbero la sussistenza di anomalie nel completamento dell'operazione fraudolenta (accessi o tentativi di accessi plurimi da device diversi e sembrerebbero esserne stati utilizzati almeno tre**,** anche se il sistema consente l'attivazione sino a due Mobile Token su altrettanti dispositivi) che avrebbero dovuto comportare una reazione maggiormente 'cautelativa' da parte dello stesso intermediario, come in effetti avvenuto per gli asseriti (secondo quanto riferito ma non documentato dall'intermediario) ulteriori tentativi di frode

tentati il giorno successivo, e che l'hanno determinato ad un intervento più incisivo ed a contattare personalmente il proprio cliente, anche in merito all'operazione (oramai già) compiuta il giorno precedente.
Per queste ragioni, ritiene il Collegio che, nella vicenda in esame, resti dunque preponderante ed assorbente quanto evidenziato circa la (non) esaustiva dimostrazione di una corretta autenticazione dell'operazione contestata e dell'assenza di anomalie, come anche emergano riscontri nel segno dell'inadeguatezza del sistema predisposto dall'intermediario per garantire la sicurezza delle operazioni effettuate on line dai propri clienti, giacché come già ritenuto da questo Collegio, decisione n. 13952/20 pur "essendo incontrovertibile che la fraudolenta sostituzione della SIM è circostanza riferibile, innanzi tutto, all'operatore telefonico …, non di meno, la circostanza che l'intermediario si avvalga di una modalità di autenticazione, che affida, quanto meno in parte, a terzi soggetti la procedura che conduce all'esecuzione delle operazioni di pagamento, appare sintomatica di una vulnerabilità organizzativa dell'intermediario, riconducibile al rischio tipico dell'attività d'impresa e quindi da fare ricadere sull'intermediario medesimo".

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 12.701,00.
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
BRUNO DE CAROLIS