Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) COEN	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 30/03/2023

FATTO

La parte ricorrente espone quanto segue:
- il ricorrente è titolare di un c/c acceso presso la convenuta al quale risulta collegata la carta di pagamento n.***6521;
- in data 18.05.2022, alle ore 16:00 circa, a seguito di un controllo del citato conto rilevava che gli era stata sottratta da ignoti la somma complessiva di euro 86.400,00, tramite una serie di bonifici non autorizzati;
- le operazioni disconosciute venivano eseguite tra il 14 e il 16 maggio 2022;
- una volta avvedutosi dell'ammanco, il ricorrente contattava immediatamente il servizio clienti;
- riferisce di non aver mai ricevuto alcun messaggio di alert.

Esperita infruttuosamente la fase di reclamo, presenta l'odierno ricorso chiedendo la restituzione dell'importo fraudolentemente sottrattogli.

Costituitosi l'intermediario ricostruisce, preliminarmente, la dinamica della vicenda come segue:
- durante la chiamata intercorsa con il servizio clienti il ricorrente riferiva all'operatore di aver ricevuto, in data imprecisata, una serie di telefonate da un'utenza fissa, con cui veniva informato di un blocco temporaneo del proprio strumento di pagamento per un periodo non definito a causa di un'asserita "assicurazione assistenza";
- aggiungeva, inoltre, di aver ricevuto vari SMS contenenti link e di aver comunicato i propri dati sensibili ai frodatori. Questi ultimi gli avrebbero rappresentato che l'accesso al conto era interdetto per dei presunti "aggiornamenti";

- il 20.05.2022, il ricorrente trasmetteva copia del verbale di denuncia;
- successivamente la banca contattava il cliente al fine di ottenere ulteriori dettagli in relazione alla dinamica del fatto e, contestualmente, chiedeva la trasmissione di una copia degli *screenshot* dei messaggi ricevuti dai frodatori o dei numeri dai quali tali soggetti lo avrebbero contattato;
- il ricorrente, per tramite del proprio avvocato, presentava reclamo al fine di ottenere il rimborso e allegava un file PDF contenente gli SMS ricevuti;
- su ulteriore sollecitazione della banca, il ricorrente trasmetteva la medesima documentazione già inoltrata e, diversamente da quanto riferito al servizio clienti, sosteneva di non aver ricevuto nessuna chiamata sulla propria utenza, ma unicamente dei messaggi;
- in data 13.10.2022, la resistente riscontrava negativamente il reclamo attesa la violazione da parte del cliente delle regole di diligenza nella custodia delle proprie credenziali;
- in particolare, rilevava che la truffa era stata realizzata solo grazie alla colpevole collaborazione del cliente verosimilmente rimasto vittima di *phishing* a seguito della ricezione di alcuni SMS "civetta" e di successivi contatti telefonici da parte di uno o più frodatori;
- presumibilmente, dunque, il ricorrente fornendo i propri dati e credenziali aveva permesso a terzi di associare l'app ad un diverso device, tramite il quale venivano effettuate in autonomia le 12 transazioni in esame. La banca evidenziava, altresì, che le operazioni disconosciute erano state eseguite attraverso un sistema SCA.

Tanto premesso, l'intermediario eccepisce quanto segue:

- il procuratore non descrive, neppure sommariamente, le modalità della frode subìta dal suo assistito e anche quest'ultimo, in sede di denuncia, si limita ad affermare di non aver autorizzato le operazioni delle quali si sarebbe avveduto solo in data 18.05.2022;
- in ogni caso, la ricostruzione dei fatti, così come prospettata, non risulta coincidente con le dichiarazioni rese al servizio clienti né con le risultanze probatorie in possesso della banca (cfr. all. 1 contenente la trascrizione della conversazione telefonica intercorsa tra il ricorrente e il Servizio Clienti);
- richiama l'orientamento dell'arbitro secondo cui, laddove sia fornita prova della corretta autenticazione dell'operazione disconosciuta, la scarsa contestualizzazione dei fatti costituisce "un elemento da cui il Collegio può trarre il proprio convincimento circa la colpa grave del ricorrente medesimo";
- in ogni caso, la frode sembrerebbe riconducibile alla fattispecie dello *smishing/vishing* attraverso il quale il ricorrente ha fornito al frodatore le credenziali di accesso al conto e i codici di sicurezza dinamici necessari ad associare l'applicazione della banca ad un diverso dispositivo mobile tramite il quale venivano poste in essere (tra il 14 e il 16 maggio) le 12 operazioni disconosciute;
- l'app, infatti, veniva installata dal frodatore sul proprio device attraverso l'immissione del codice PIN di conferma creato dal ricorrente in occasione dell'apertura del c/c, di sua esclusiva conoscenza e modificato solo il 18.05.2022;
- alla luce delle informazioni rese e delle risultanze informatiche, è indubbio che le operazioni siano state rese possibili dal comportamento particolarmente incauto del cliente che condivideva con il frodatore, le proprie credenziali unitamente ai codici OTP;
- la banca ha adottato sistemi informatici che rispettano i più alti standard di sicurezza, predisponendo un sistema di autenticazione forte sia per il servizio di home banking tramite web-app sia per l'autorizzazione delle operazioni dispositive;
- invero, alle 13:39 (UTC+2) del 14 maggio 2022, vale a dire poco prima che la prima delle dodici operazioni contestate venisse eseguita, un device con sistema operativo Android

(diverso dal dispositivo IOS associato al conto del ricorrente e normalmente utilizzato da questi per accedere ai servizi bancari) effettuava l'accesso al conto del cliente utilizzando i dati di login (e-mail e password) normalmente in uso e precedentemente impostati dallo stesso e un codice OTP inviato al dispositivo mobile IOS associato al conto del ricorrente, sempre in possesso del medesimo;

- in pari data, alle ore 13:45 (UTC+2), il dispositivo mobile IOS normalmente in uso al ricorrente veniva dissociato; poco dopo veniva immediatamente associato al conto il dispositivo mobile Android del frodatore;
- il cliente veniva immediatamente reso edotto delle operazioni di dissociazione e successiva riassociazione per mezzo di 4 e-mail inviate all'indirizzo di posta elettronica da questi associato al proprio conto nonché tramite 6 SMS inviati alla sua utenza telefonica registrata (cfr. all. n. 6, pag. 1); il ricorrente avrebbe quindi potuto contattare la Banca attraverso i canali di comunicazione ufficiali al fine di sventare il perfezionamento della frode;
- rileva, inoltre, che allorché un cliente esegue l'accesso al conto da un dispositivo non associato, gli viene chiesto di confermare una notifica push sul proprio dispositivo associato o, in alternativa, può chiedere la ricezione di un codice via SMS sul numero di telefono registrato al proprio conto per confermare l'accesso al medesimo;
- questa procedura di autenticazione a due fattori, garantisce che soltanto il titolare del conto possa accedervi e possa dissociare o associare un determinato device;
- in relazione agli SMS pervenuti al ricorrente, rileva che:
  - in questi non compare il numero telefonico, ma unicamente la denominazione dell'intermediario;
  - i link allegati non sono riconducibili alla banca;
  - risultano formulati in termini assolutamente generici (vedasi lo scopo dei presunti "aggiornamenti") e caratterizzati dalla presenza di errori grammaticali e di sintassi (illogica alternanza della seconda e della terza persona singolare);
  - non risultano in coda ad una chat genuina;
  - inoltre, i messaggi sono datati 13.05.2022, mentre il ricorrente ha sempre collocato la frode il giorno successivo;
- in ragione delle circostanze sopra richiamate, rileva come sia ravvisabile la colpa grave del ricorrente, stanti anche i molteplici indici di inattendibilità e di anomalia presenti nei messaggi "civetta" summenzionati;
- riferisce di aver da tempo intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela in merito al fenomeno del *phishing* e alle sue possibili declinazioni oltre a mettere a disposizione, sul proprio sito internet, importanti informazioni relative alle misure di tutela che il cliente è tenuto ad adottare nell'utilizzo degli strumenti di pagamento;
- evidenzia, infine, la colpa del ricorrente derivante dall'omessa tempestiva segnalazione dell'uso non autorizzato dello strumento di pagamento in violazione dell'obbligo di cui all'art. 7, co. 1, lett. b) del D.Lgs. n. 11/2010 e delle condizioni generali di contratto;
- tutto ciò premesso, l'intermediario produce copia delle tracciature informatiche attestanti la regolarità formale delle operazioni disconosciute;
- rileva che il sistema di autenticazione, nel pieno rispetto dei requisiti previsti dal d.lgs. 11/2010 e dalle norme tecniche di cui al Regolamento 2018/389, è fondato su una tecnologia multifattoriale tanto nella preventiva fase di accesso all'internet banking, quanto nel successivo compimento delle operazioni dispositive;
- in termini generali, sia i bonifici che i trasferimenti istantanei, possono essere predisposti dal cliente dall'app dopo avervi fatto accesso, attraverso le seguenti modalità che assicurano l'applicazione di due diversi fattori di autenticazione:

- credenziali personali (indirizzo e-mail di registrazione e password) o, in alternativa, dall'ID biometrico (riconoscimento facciale o impronta digitale) (rispettivamente elementi di conoscenza e inerenza);
- utilizzo dell'app installata sul dispositivo associato in via esclusiva al conto del cliente (elemento di possesso);

- una volta predisposto un ordine di bonifico o di trasferimento, questo dev'essere necessariamente autorizzato all'interno della app;
- a tal fine, al cliente viene presentata una schermata contenente i dettagli del bonifico - incluso il nome del beneficiario, la causale di riferimento e l'ammontare - e, a conferma della propria identità, viene richiesto al cliente di inserire il codice PIN, da lui stesso creato al momento di prima associazione del device personale (elemento di conoscenza);
- infine, al cliente viene presentata una seconda schermata riepilogativa dell'operazione di bonifico in cui viene richiesto di confermare o annullare l'operazione di bonifico tramite notifica push dal dispositivo associato (elemento di possesso);
- nel caso di specie le operazioni venivano autorizzate inserendo il Pin di conferma;
- la resistente non riscontrava alcun'anomalia nell'esecuzione delle operazioni di bonifico e non risulta responsabile in quanto l'obbligo che grava sull'intermediario "è solo quello di eseguire gli ordini di pagamento impartiti (e quindi appositamente autorizzati) dall'utilizzatore dello strumento di pagamento (…)" (Coll. Coord., dec. n. 1259/2014);
- anche le operazioni eseguite tramite MoneyB***, (sistema di trasferimento istantaneo di denaro tra utenti della resistente) sono state disposte direttamente dal frodatore – il quale dopo aver eseguito l'*enrollment* dell'app associata al conto sul proprio dispositivo e in possesso del codice Pin – li predisponeva e autorizzava in piena autonomia;
- analogamente alle operazioni di bonifico, anche in questo caso è stata richiesta una SCA;
- invero, al fine di autenticare una singola operazione di pagamento istantaneo MoneyB***, il cliente che voglia effettuarla deve selezionare un contatto dalla sua lista utenti, inserire l'importo del pagamento e una causale e, infine, immettere il PIN di conferma da lui stesso creato al momento della prima associazione del device personale (elemento di conoscenza). A questo punto, al cliente viene presentata una seconda schermata riepilogativa del pagamento in cui viene richiesto di confermare o annullare l'operazione MoneyB*** tramite una notifica push dal dispositivo associato (elemento di possesso);
- anche in questo caso, trattandosi di pagamenti disposti sullo stesso istituto, gli importi venivano immediatamente trasferiti e prelevati dal beneficiario;
- alla luce di quanto esposto, l'intermediario esclude qualsiasi responsabilità per l'accaduto;
- conclude domandando il rigetto del ricorso.

Il ricorrente replica alle controdeduzioni chiarendo che:

- è rimasto vittima di *phishing* perpetrato tramite ricezione di un messaggio esca sul proprio telefono cellulare;
- la frode è stata, dunque, realizzata solo grazie al trafugamento di dati sensibili detenuti dalla banca. Invero, i frodatori non avrebbero potuto sottrarre le somme se non fossero stati a conoscenza: del numero della carta, del numero di cellulare e delle generalità del ricorrente;
- l'intermediario, peraltro, non era dotato di un adeguato sistema di monitoraggio su eventuali anomalie nella movimentazione bancaria;
- invero, successivamente al cambio di device associato al conto corrente, venivano disposte in rapida successione ben 10 operazioni (di cui 5 bonifici di euro 2.000,00 e

altrettanti pagamenti, per un importo complessivo di euro 15.000,00) senza che ciò inducesse la banca a procedere ad una immediata verifica e conseguente sospensione delle attività dispositive;
- tale circostanza permetteva il compimento di ulteriori 2 operazioni, di cui l'ultima pari ad euro 70.000,00;
- la banca ha l'onere non solo di provare la corretta autenticazione, registrazione e contabilizzazione delle operazioni, impostogli dal d.lgs. 11/2010, ma anche di appontare idonee misure di monitoraggio della movimentazione dei clienti rispetto all'usuale operatività del conto;
- nega, inoltre, di aver effettuato volontariamente la dissociazione del proprio dispositivo come asserito da controparte.

Il ricorrente, dunque, rinnova la richiesta originariamente formulata domandando, in subordine, quantomeno il rimborso delle operazioni disposte in data 16.05.2022 (pari a complessivi euro 71.000,00) attesa la mancata attivazione dei citati sistemi di monitoraggio.

L'intermediario, in sede di controrepliche, contesta quanto dedotto dal ricorrente eccependo che:
- l'accesso del malfattore è stato possibile esclusivamente grazie al contributo prestato dal ricorrente non essendosi verificato, nel caso di specie, alcun "data breach";
- il ricorrente -tra l'altro- in sede di interlocuzione con il servizio clienti, ha sostanzialmente ammesso di aver dato seguito alle istruzioni contenute nei messaggi e a quelle impartitegli telefonicamente;
- la credulità del ricorrente appare quindi non scusabile, in quanto le modalità con cui la truffa è stata perpetrata rientrano tra quelle più diffuse, che qualunque cliente dotato di normale avvedutezza e prudenza doveva essere in grado di individuare (cfr. *ex multis* Collegio di Roma, decisione n. 8048/17);
- esclude una propria responsabilità in ordine al mancato blocco delle operazioni in contesa, peraltro disposte ben due giorni prima dalla denuncia sporta dal ricorrente;
- pur essendosi immediatamente adoperata al fine di stornare le operazioni disconosciute, la banca non poteva revocarle in virtù del fatto che, trattandosi di bonifici istantanei verso banche terze e di cinque trasferimenti istantanei di denaro disposti sullo stesso istituto, gli importi in oggetto erano stati immediatamente trasferiti e, nel caso specifico, già prelevati dal beneficiario;
- sottolinea come il ricorrente abbia sporto denuncia tardivamente, ossia ben cinque giorni dopo la consumazione della frode, nonostante fosse stato informato correttamente – tramite mail e SMS –delle modifiche intervenute sul conto;
- se il ricorrente avesse tenuto conto di tali comunicazioni avrebbe potuto allertarsi tempestivamente e impedire le operazioni in esame;
- contrariamente a quanto affermato, alla luce di un monitoraggio ex post, le operazioni contestate non si discostavano dalla normale operatività del conto, considerato che il ricorrente era solito effettuare transazioni anche di notevole entità verosimilmente riferibili alla sua attività lavorativa;
- ribadisce quanto già affermato in merito alla conformità alla SCA del sistema di autenticazione delle operazioni.

Alla luce di quanto osservato rinnova la richiesta di rigetto del ricorso.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite il 14 e il 16 maggio 2022. Risultano, pertanto, effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tale operazione è altresì successiva alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.
Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "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". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.
2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento 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. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".
3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".
Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- Nel caso di specie, il ricorrente, intestatario di un conto corrente acceso presso la resistente, riferisce di essere rimasto vittima di una frode perpetrata ai suoi danni da soggetti terzi, per l'importo complessivo di euro 86.400,00.

Si tratta, nello specifico, di n. 7 bonifici e n. 5 operazioni di MoneyB***, (trasferimenti istantanei di denaro tra utenti della resistente) dell'importo di euro 1.000,00 cadauno.

Nella denuncia alle forze dell'ordine, come nel ricorso, il ricorrente non ricostruisce le modalità della truffa subìta né allega circostanze utili a ricondurre il fatto ad una determinata fattispecie, limitandosi ad affermare di essere venuto a conoscenza degli addebiti fraudolenti solo a seguito di un controllo del proprio contro corrente in data 18.05.2022.

Le operazioni disconosciute venivano poste in essere tra il 14 e il 16 maggio 2022.

In sede di controdeduzioni, l'intermediario ipotizza che il cliente sia rimasto vittima di una frode riconducibile alla fattispecie dello *smishing/vishing*.

Solo in sede di repliche il ricorrente ammette di aver ricevuto un messaggio esca sul proprio telefono cellulare, senza fornire ulteriori dettagli e negando la ricezione di ipotetiche telefonate da parte di sedicenti operatori della banca.

Dalla schermata contenente gli sms si può rilevare quanto segue:

- in data 13 maggio 2022 il ricorrente riceve un messaggio esca;
- il messaggio risulta provenire da un Id riconducibile all'intermediario ed è preceduto da altri messaggi risalenti nel tempo (il primo dei quali apparentemente truffaldino);
- reca un link che contiene un riferimento alla denominazione della banca;
- l'sms è seguito, all'interno della medesima chat, da un ulteriore messaggio del 14 maggio 2022 -anche questo verosimilmente truffaldino- con il quale il ricorrente veniva invitato a non utilizzare il conto, a causa di non meglio identificate procedure di aggiornamento in corso;
- questo secondo messaggio reca errori grammaticali (per es. 'Egreggio') e di sintassi (alternanza della seconda e della terza persona singolare);
- inoltre, riporta un numero telefonico da contattare al fine di ottenere informazioni.

L'intermediario d'altro canto evidenzia le contraddizioni presenti nelle affermazioni del ricorrente e del di lui procuratore.

A tal proposito, riporta la trascrizione della conversazione intervenuta tra il ricorrente e il servizio clienti in data 18.05.2022 (giorno in cui l'istante si avvedeva dell'ammanco).

In tale sede, il ricorrente ammetteva di aver ricevuto sia messaggi che telefonate a cui rispondeva fornendo i dati richiesti.

5.- L'intermediario ha riferito di adottare un sistema di autenticazione multifattoriale sia per l'accesso all'internet banking sia per l'autorizzazione delle singole operazioni dispositive.

Queste ultime, in particolare, venivano disposte dal frodatore tramite App della banca previamente installata e associata su un device diverso da quello del ricorrente.
Dalle tracciature informatiche si evince che alle ore 13:39 (UTC+2) del 14 maggio 2022, poco prima che le operazioni di pagamento oggetto di disconoscimento venissero iniziate, il frodatore effettuava l'accesso al conto del ricorrente dalla App utilizzando:
- i dati di login - e-mail e password - normalmente in uso e precedentemente impostati dallo stesso ricorrente;
- un codice OTP monouso a 6 cifre inviato al dispositivo mobile IOS associato al conto del ricorrente e probabilmente comunicato dal ricorrente allo stesso.

A supporto di quanto dichiarato allega evidenza correlata da apposita legenda. Evidenzia, in particolare, la voce MFA_OTP alla colonna "Process", riga 5 dall'alto, che indica il secondo fattore di autenticazione tramite codice OTP.
L'intermediario allega evidenze dell'avvenuto invio degli SMS contenenti gli OTP autorizzativi di accesso al conto, precisando che gli stessi risultano inviati e verificati (v. campo result=confirmed) dal cliente come da codice User_Id allo stesso associato.
Dalle evidenze di cui sopra, risulta quindi che l'accesso al conto è stato correttamente autenticato con inserimento:
- fattore di conoscenza: digitazione delle credenziali del cliente (email e password);
- fattore di possesso: il secondo fattore di autenticazione (il codice OTP).

Nel caso di specie, il frodatore ha disposto le operazioni direttamente all'interno dell'app installata sul proprio dispositivo previamente associato al conto corrente del ricorrente.
In pari data, alle ore 13:45 (UTC+2), il dispositivo mobile IOS normalmente in uso al ricorrente veniva da questi dissociato, per essere poco dopo immediatamente associato al dispositivo mobile Android del frodatore. Allega, in proposito, evidenza informatica riguardante lo storico di associazione/dissociazione del device collegato al c/c.
L'intermediario rileva che il ricorrente veniva debitamente informato in merito alle attività di associazione e dissociazione dei dispositivi, innanzitutto, tramite 4 email inviate all'indirizzo indicato in sede di apertura conto e mai oggetto di variazione.
Le operazioni disconosciute sono: 7 bonifici; 5 ordini di pagamento istantaneo effettuati tramite M*B* dell'importo di euro 1.000,00 cadauno; questo servizio è un sistema di trasferimento istantaneo di denaro tra utenti dell'intermediario che consente al cliente di effettuare un'operazione selezionando un contatto dalla sua lista utenti.
Relativamente alle modalità di autorizzazione di tali operazioni l'intermediario osserva che, predisposto l'ordine sia di M*B* che di bonifico, l'autorizzazione dell'operazione avviene attraverso:
- l'inserimento di un codice PIN (fattore di conoscenza);
- la conferma dell'operazione tramite notifica push ricevuta sul device associato (fattore di possesso).

Osserva l'intermediario che il codice PIN viene creato unicamente dal cliente medesimo nel momento in cui questi effettua - per la prima volta - l'associazione del dispositivo personale al proprio conto corrente e quindi non consiste in un codice generato dalla banca.
Dalle tracciature informatiche in possesso della resistente, risulta che il suddetto PIN di conferma sia stato creato dal ricorrente in fase di apertura del conto corrente il giorno 6.11.2020 e da questi mai modificato fino al giorno 18.05.2022, data posteriore al verificarsi della frode.
Produce evidenze relative alle operazioni eseguite dal frodatore precisando che sono state autorizzate e regolarmente contabilizzate con un sistema SCA compliant.
Quanto alla modalità autorizzativa dell'operazione riferisce che alla colonna "RESULT" compare la dicitura "*Transaction Successfully Certified*, a significare, come esplicitato nel

glossario ivi riportato, che l'operazione è stata autorizzata applicando la SCA - "*Transaction SCA Approved*".
Dalle evidenze prodotte dall'intermediario risulta quindi che le operazioni sono state correttamente autenticate in seguito all'accesso alla App installata sul device del frodatore e associato al conto del cliente e autorizzate tramite inserimento del PIN e notifica push.
Questo Collegio ha ritenuto *compliant* alla SCA una modalità autorizzativa simile, predisposta dal medesimo intermediario (Coll. Roma, dec. n.6036/22).
6.- Il ricorrente contesta la mancata ricezione dei messaggi di alert relativi alle operazioni oggetto di disconoscimento.
In sede di controdeduzioni l'intermediario non fornisce evidenze in merito all'invio/ricezione dei messaggi.
Riferisce che al cliente -al momento dell'autorizzazione dell'operazione- viene presentata una seconda schermata riepilogativa in cui viene richiesto di confermare o annullare l'operazione tramite notifica *push* dal dispositivo associato.
Produce evidenza delle citate notifiche che, tuttavia, pervenivano sul nuovo device abbinato, ovvero quello del frodatore.
In termini generali occorre osservare che, ai sensi dell'art. 8 del d. lgs. n. 11 del 2010, il prestatore dei servizi di pagamento è tenuto ad "assicurare che siano sempre disponibili strumenti adeguati affinché l'utilizzatore dei servizi di pagamento possa eseguire la comunicazione di cui all'art. 7, comma 1, lett. b)".
L'orientamento del Collegio è costante nel ritenere che la mancata attivazione o il mancato funzionamento di un sistema di alert costituisca una disfunzione organizzativa imputabile all'intermediario con conseguente responsabilità, eventualmente in concorso con il comportamento gravemente negligente del cliente, per le operazioni non autorizzate.
In particolare, data la natura di misura di sicurezza del sistema di sms alert, gli intermediari non dovrebbero limitarsi a proporlo al cliente ma dovrebbero adottarlo in modo generalizzato (Coll. Roma, dec. 12441/2019).
7.- Secondo la più recente posizione condivisa da tutti i Collegi territoriali, nelle fattispecie di *spoofing* 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".
8.- Pertanto, alla luce delle risultanze istruttorie, il Collegio ritiene che sussistano profili di colpa grave del cliente - consistente nell'avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa posta in essere dall'intermediario - e che essi siano tali da contribuire alla causazione dell'evento dannoso; tuttavia, ritiene altresì che la loro efficienza causale non sia esclusiva. Il caso di specie si discosta, infatti, dallo *smishing* perpetrato attraverso modalità tipiche e ampiamente note, dove la colpa grave del cliente è causa sufficiente dell'evento dannoso, in quanto capace di deviare la catena causale che collega il comportamento illecito del frodatore e il concretarsi della frode, assorbendo del tutto, così, il nesso di causalità.
Infatti, il truffatore ha adottato un sistema tecnicamente più sofisticato, tale da concretare un'ipotesi di malfunzionamento del servizio di pagamento o altro inconveniente connesso al servizio di disposizione di ordine di pagamento, pur inteso in senso ampio, destinato a ricadere nella sfera del rischio di impresa dell'intermediario. Non è dubbio, infatti, che le operazioni siano un effetto di tale malfunzionamento, sul quale si innesta la colpa grave del cliente. Quest'ultima, però, a parere del Collegio, non è adeguata ad assorbire

completamente il nesso di causalità, ma concorre con esso (Coll. Milano, dec. n. 2892/2021). In tal senso, incide altresì la mancata attivazione del servizio di sms alert.
9.- Alla luce di quanto sopra esposto il Collegio valuta il concorso paritario tra le parti e liquida in via equitativa in favore del ricorrente a titolo risarcitorio l'importo di € 45.000,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 45.000,00, determinata in via equitativa.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA