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) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

ESTERNI - MARCO MARINARO

Seduta del 15/02/2023

FATTO

La parte ricorrente espone quanto segue:
- in data 10.08.2022, riceveva un sms sul proprio telefono con il quale veniva informato che l'applicazione della banca odierna resistente sarebbe stata bloccata;
- l'sms in questione non riportava alcuna motivazione in ordine al blocco dell'app ma solo un link ipertestuale;
- dopo pochi minuti, riceveva una telefonata dove una voce maschile si qualificava come "Dario del servizio clienti della banca ***" e lo informava di alcuni movimenti sospetti sul proprio conto corrente;
- dopo aver aperto l'applicazione, notava che erano state disposte delle operazioni non autorizzate che comunque la banca aveva provveduto a bloccare;
- successivamente, riceveva un'altra telefonata sempre dallo stesso numero e sempre dallo stesso operatore che lo informava circa il fatto che anche su altro conto corrente acceso presso altro intermediario, parimenti intestato al ricorrente, erano presenti dei movimenti sospetti; lo stesso sedicente operatore della resistente consigliava di trasferire i fondi da detto ultimo conto corrente sul conto acceso presso la resistente, fino a quando non sarebbe stata risolta "la problematica";
- riferisce: "*al termine della chiamata, cioè quando chiedevo quanto tempo passasse prima dello storno, l'operatore mi diceva che sarei stato ricontattato da un suo collega a mezzanotte poiché avevo quasi raggiunto il limite massimo dei bonifici effettuabili*":
- successivamente, accedendo all'app della banca, il ricorrente si avvedeva che vi erano altri movimenti non autorizzati e capiva di essere stato truffato;
- contattava quindi la resistente per renderla edotta della truffa e provvedeva immediatamente a contestare le transazioni che erano state effettuate verso quattro distinti beneficiari;

- dopo qualche giorno, contattava la banca tramite chat e gli veniva riferito che la sua contestazione non era stata accettata; gli veniva consigliato “di mandare anche la denuncia”;
- il 9 settembre inviava la denuncia ma non veniva ricontattato;
- dopo altri 20 giorni, contattava la banca tramite app e gli veniva riferito che la richiesta non era stata accolta perché era stata utilizzata la carta con chip originale; il ricorrente faceva presente che la carta era in suo possesso e che “i movimenti venivano effettuati in altre località”.

L’intermediario resiste al ricorso ed eccepisce quanto segue:

- precisa che il ricorrente ha disconosciuto otto transazioni di importo complessivo pari a euro 15.956,01:
  - n. 2 operazioni di addebito su carta di debito fisica n. 8891 effettuate sull’e-wallet Android Pay rispettivamente dell’importo di 1.000,00 EUR e di 215,00 EUR;
  - n. 1 operazione di addebito su carta di debito fisica n. 8891 effettuata sull’e-wallet Android Pay dell’importo di 3.750,00 EUR;
  - n. 1 operazione di addebito su carta di debito n. 6407 dell’importo di 1.021,48 EUR;
  - n. 1 operazione di addebito su carta di debito n. 6407 dell’importo di 3.977,53;
  - n. 1 operazione di addebito su carta di debito n. 2084 dell’importo di 999,00 EUR;
  - n. 1 operazione di addebito su carta di debito n. 2084 dell’importo di 3.613,00 EUR;
  - n. 1 operazione di addebito su carta di debito n. 2010 dell’importo di 1.380,00 EUR;
- avviava la procedura di chargeback tramite apposita funzione in app;
- il giorno 29 agosto 2022, a seguito dell’analisi del caso, l’ufficio preposto rigettava la richiesta di storno avanzata dal cliente. In particolare, per quanto riguarda le operazioni controverse effettuate con carta fisica veniva riscontrato che queste erano state autorizzate dal cliente tramite sistema multifattoriale e per mezzo del protocollo di sicurezza c.d. 3D Secure dalla App installata sul dispositivo mobile personale associato al proprio conto corrente, mentre il rimborso relativo alle operazioni effettuate tramite e-wallet Android Pay veniva rigettato perché era stato riscontrato l’utilizzo del chip della carta presso un sistema POS;
- ritiene, preliminarmente, che il ricorso sia inammissibile in quanto il ricorrente non ha presentato reclamo all’intermediario, che costituisce condizione insanabile di procedibilità del ricorso (Coll. Coord., decisione n. 5304/2013 e n. 6666/2014); rileva che il ricorrente ha dichiarato di aver presentato reclamo il giorno 10.08.2022, mentre in tale data ha avanzato al Servizio Clienti una mera richiesta di storno delle operazioni di pagamento fraudolente, che non può essere qualificata come reclamo;
- eccepisce, inoltre, che, anche laddove la richiesta di storno fosse qualificata come reclamo, in ogni caso tra la presentazione di quest’ultima e la proposizione del ricorso non sarebbero intercorsi i 60 giorni;
- precisa che, dopo aver ricevuto in tal senso istruzioni dal frodatore, sedicente operatore della resistente, il ricorrente provvedeva a trasferire i propri fondi dal conto corrente acceso presso altro intermediario a quello sul quale sono state addebitate le operazioni contestate mediante nr. 3 operazioni di bonifico, per l’importo complessivo di 14.942,99 EUR; precisa che il frodatore, non ha specificato come potesse essere in grado di conoscere quanto stava asseritamente avvenendo su un conto corrente aperto presso un altro istituto di credito ma ha spiegato di poter offrire la propria assistenza solo sul conto corrente della banca odierna resistente;
- rileva inoltre che, tra la seconda e la terza operazione di bonifico, il ricorrente provvedeva ad aumentare il plafond giornaliero della carta 8891 da 2.500,00 ad € 5.000,00;

- successivamente, un'operazione di pagamento per euro 2.036,00 in favore di un sito internet non veniva autorizzata dal ricorrente e, pertanto, risulta "canceled" nell'allegato n. 1, pagina 1, paragrafo n. 3;
- in seguito, il frodatore eseguiva n. 2 operazioni di addebito su carta di debito "fisica" n. 8891 intestata al ricorrente tramite e-wallet Android Pay rispettivamente dell'importo di 1.000,00 EUR e di 215,00 EUR;
- tra la prima e la seconda transazione di cui sopra, il ricorrente aveva provveduto ad innalzare anche il limite giornaliero della carta virtuale n. 6407 dall'importo di 2.500,00 EUR a 5.000,00 EUR;
- successivamente, il frodatore effettuava n. 2 operazioni di pagamento, rispettivamente tramite e-wallet Android Pay con carta virtuale n. 6407, dell'importo di 900,00 EUR e con carta fisica n. 8891 per l'importo di 3.850,00 EUR, in favore di due distinti esercenti, ma entrambe le operazioni venivano bloccate dalla banca per sospetta frode;
- successivamente, il truffatore disponeva altre due operazioni di pagamento, addebitate su due carte di debito (n. 8891 e n. 6407) ed effettuate tramite e-wallet Android Pay, dell'importo di € 500,00 ed € 3.750,00; l'operazione di euro 500,00 non andava a buon fine perché i sistemi informatici della banca avevano rilevato elementi di sospetta frode;
- in seguito, il ricorrente disponeva un quarto bonifico dal proprio conto corrente acceso presso altro intermediario a quello della resistente dell'importo di 2.065,00 EUR;
- successivamente, il frodatore eseguiva n. 4 operazioni di addebito su carte di debito virtuali:
  - n. 2 operazioni di addebito sulla carta di debito n. 6407, rispettivamente dell'importo di 1.021,48 EUR e di 3.977,53 EUR;
  - n. 2 operazioni di addebito sulla carta di debito n. 2084, rispettivamente dell'importo di 999,00 EUR e di 3.613,00 EUR;
- inoltre, il frodatore disponeva un ulteriore tentativo di pagamento con la carta digitale n. 2010 dell'importo di 980,00 EUR a favore della medesima piattaforma online; il pagamento non andava a buon fine poiché la relativa richiesta di autorizzazione veniva disattesa dal cliente stesso in quanto non confermata entro il termine previsto di cinque minuti (cfr. Status EXPIRED nei log allegati);
- il ricorrente disponeva poi un quinto bonifico dal proprio conto corrente acceso presso altro intermediario a quello della resistente dell'importo di 1.380,00 EUR;
- infine, il ricorrente eseguiva n. 1 operazione di addebito su carta di debito n. 2010 dell'importo di 1.380,00 EUR a favore di piattaforma online;
- rileva: "prima di concludere la telefonata, il ricorrente domandava al sedicente operatore quando sarebbe avvenuto lo storno delle suddette operazioni. Il frodatore rassicurava il ricorrente comunicandogli che sarebbe stato ricontattato da un altro operatore a mezzanotte poiché il ricorrente avrebbe superato, a detta del frodatore, i limiti massimi giornalieri del conto (…) per la disposizione di bonifici";
- precisa che, in occasione dell'analisi del ricorso, l'intermediario ha ritenuto di rimborsare esclusivamente le operazioni effettuate tramite e-wallet per l'importo complessivo di 4.965,00 €, erogato sul conto corrente del ricorrente in data 02 novembre 2022 (Allegato n. 2);
- le operazioni per cui non ritiene che possa essere accolta la domanda del ricorrente, ancora oggetto di contesa, sono dunque cinque, effettuate con tre distinte carte di debito in favore della medesima piattaforma online:
  - n. 2 operazioni di addebito su carta di debito n. 6407 rispettivamente dell'importo di 1.021,48 EUR e di 3.977,53 EUR (Allegato n. 1, pagina n. 3-4, paragrafi n. 9-10; Allegato n. 3 pagine 1 e 2; 7 e 8);

- n. 2 operazioni di addebito su carta di debito n. 2084 rispettivamente dell'importo di 999,00 EUR e di 3.613,00 EUR (Allegato n. 1, pagina n. 4, paragrafo n. 11; Allegato n. 3 pagine 9 e 10; 5 e 6);
- n. 1 operazione di addebito su carta di debito n. 2010 dell'importo di 1.380,00 EUR (si rimanda all'Allegato n. 1 pagina n. 3, paragrafo n. 8; Allegato n. 3, pagine 3 e 4);

- rileva che la frode subita dalla ricorrente rientra nella tipologia del c.d. smishing e del c.d. vishing, considerati per costante giurisprudenza dell'Arbitro modalità non particolarmente sofisticate e ampiamente note di frode, rientranti nella più estesa categoria del phishing;
- evidenzia che "in riferimento al generale fenomeno del phishing e alle sue possibili declinazioni, da tempo [la banca] ha intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela in merito"; riassume alcune iniziative a pagina 10 delle controdeduzioni;
- ritiene che le modalità con le quali si è perpetrata la frode dimostrino la sussistenza di un comportamento incauto e una grave negligenza del ricorrente; evidenzia che il cliente non fornisce prova della dedotta circostanza relativa alla ricezione di un sms proveniente da una "catena genuina" della banca;
- eccepisce, inoltre, che il cliente ha ricevuto una telefonata da un'utenza mobile privata in alcun modo riferibile alla banca e "il frodatore invitava il ricorrente a trasferire dei fondi dal proprio conto corrente [presso intermediario terzo] a quello [presso l'intermediario odierno resistente]; osserva che "il ricorrente non avrebbe assolutamente dovuto dare seguito a questa richiesta soprattutto alla luce dei movimenti sospetti asseritamente riscontrati, poco prima, a valere sul proprio conto (…)";
- rileva che il ricorrente non ha provveduto a disporre il blocco delle carte ma, anzi, ha ordinato altre due carte virtuali, le menzionate carte n. 2084 e 2010, favorendo il perpetrarsi della frode;
- osserva che il ricorrente, avendo verificato che dopo aver disposto n. 3 operazioni di bonifico dal proprio conto corrente acceso su altro intermediario a quello della resistente, erano state effettuate 3 operazioni fraudolente, avrebbe dovuto percepire che si trovava dinanzi ad un tentativo di truffa e non avrebbe dovuto, in quel momento e per nessun motivo, trasferire ulteriori fondi; rileva che, ciononostante, disponeva una quarta operazione di bonifico incrementando i fondi sul conto corrente oggetto di truffa;
- evidenzia che in fase di denuncia il ricorrente dichiarava di essersi avveduto della frode soltanto al termine della telefonata con il sedicente operatore; osserva che tale asserzione risulta inverosimile in quanto il ricorrente medesimo accettava le transazioni effettuate con la propria carta confermandole attraverso le notifiche push inviate correttamente dalla banca all'utenza mobile telefonica registrata al proprio conto corrente;
- aggiunge che alla luce della ritenuta natura sospetta del primo sms ricevuto, non avrebbe dovuto assecondare le richieste del frodatore e avrebbe dovuto contattare egli stesso la banca chiedendo informazioni a riguardo;
- ritiene, in ogni caso, sussistente un concorso di colpa del danneggiato ex art. 1227 c.c., che avrebbe in ogni caso aggravato le conseguenze dell'evento dannoso, in particolare seguendo tutte le istruzioni impartite dal frodatore, incrementando la provvista del conto corrente acceso presso l'intermediario tramite bonifici a valere su c/c acceso presso alta banca, ordinando nuove carte di debito virtuali, innalzando i limiti di pagamento delle carte in uso e accettando debitamente le transazioni effettuate con le proprie carte associate al conto corrente, confermandole attraverso le notifiche push inviate correttamente dalla banca all'utenza mobile telefonica registrata dal ricorrente;
- in tema di autenticazione delle operazioni disconosciute e non rimborsate, precisa che è stata chiesta autorizzazione da parte del ricorrente attraverso applicazione

dell'autenticazione forte a mezzo dell'app e nel corso della telefonata con il frodatore; in particolare, riporta le modalità di autenticazione e produce copia delle tracciature informatiche "che dimostrano la regolarità formale" dell'operazione;

- osserva: "per la disposizione di un'operazione di pagamento online attraverso carta di debito per la quale viene richiesta l'autenticazione forte (SCA) da parte dell'esercente, [la banca] applica il processo di sicurezza 3D Secure e una richiesta di autenticazione viene trasmessa da parte dell'esercente a quest'ultima (Allegato n. 4, Sez. 1). Sulla base dei dettagli relativi all'operazione per cui è trasmessa la richiesta, i sistemi informatici della banca effettuano l'analisi degli elementi di rischio dell'operazione di pagamento per determinare:
  - l'esecuzione dell'operazione senza applicazione dell'autenticazione forte alla luce dell'applicabilità di una delle esenzioni previste dagli artt. 11-18 del Regolamento delegato (UE) 2018/389 (Accepted);
  - il rifiuto di esecuzione dell'operazione alla luce della presenza di fattori di rischio alti (es. esercente in blacklist, soggetto fraudolento, ecc.) (Rejected);
  - l'applicabilità dei requisiti di autenticazione forte ai sensi dell'art. 10-bis D.Lgs. 11/2010 (Challenged).

  In relazione ad una transazione soggetta ad autenticazione forte da parte del cliente (Challenged), si premette che i sistemi informatici di [banca] attivano il flusso di certificazione in virtù del quale si chiede conferma dell'operazione al cliente esclusivamente attraverso l'App (…) installata sul dispositivo mobile associato al conto corrente (…)";
- con riguardo al processo di associazione in via esclusiva dell'app installata su un determinato dispositivo al conto corrente del cliente, precisa che la banca invia un sms contenente un codice OTP di quattro cifre all'utenza mobile utilizzata ai fini della registrazione del proprio account personale; il codice OTP deve essere immesso nell'app dal cliente e, in tal modo, l'app viene univocamente associata ad un unico dispositivo mobile, "secondo una soluzione tecnologica qualificabile come elemento nella categoria del possesso ai sensi di quanto previsto al para. 25 dell'Opinion EBA-Op-2018-04 in materia di Strong Customer Authentication (…)";
- precisa che, al fine dell'autenticazione delle singole operazioni di pagamento, la banca trasmette al cliente una specifica notifica push tramite l'app installata sul dispositivo associato al conto corrente e, attraverso la notifica push, il cliente viene indirizzato all'apertura della schermata iniziale dell'app; il cliente è quindi tenuto a effettuare il log in nell'app "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) - elementi, rispettivamente, nella categoria della conoscenza e inerenza; e
  - utilizzo dell'App (…) installata sul dispositivo associato in via esclusiva al conto del cliente - elemento nella categoria del possesso (Allegato n. 4, Sez. 3)";
- in seguito all'accesso all'area riservata dell'app sul dispositivo associato, al cliente viene presentata una schermata contenente i dettagli di ciascuna transazione (incluso il nome dell'esercente e l'ammontare) e la richiesta di dare autorizzazione o meno all'operazione, da validare entro un tempo massimo di 5 minuti; precisa che la validazione da parte del cliente con la conferma dell'operazione determina l'autenticazione attraverso un elemento rientrante nella categoria del possesso ai sensi di quanto previsto al paragrafo 26 dell'Opinion EBA di giugno 2019, "*in quanto dà luogo a una verifica nel back end - attraverso la private key conservata all'interno del dispositivo del cliente e un sistema di private key linking - che l'autenticazione dell'operazione avviene dall'App (…) installata*

sul dispositivo associato al conto e che causa il rigetto dell'operazione laddove tale circostanza non sia soddisfatta (Allegato n. 4, Sez. 2)";

- conclude sull'autenticazione: "*la soluzione implementata da parte della banca permette così di soddisfare i requisiti di autenticazione forte dell'operazione previsti dall'art. 10-bis D.Lgs. 11/2010 attraverso l'autenticazione della disposizione dell'operazione di pagamento per mezzo di un fattore nella categoria del possesso e all'interno di una sessione già avviata da parte del cliente a seguito dell'autenticazione con due diversi fattori nella categoria del possesso e, rispettivamente, della conoscenza o dell'inerenza. secondo una modalità in linea con quanto espressamente previsto al para. 40 dell'Opinion EBA-Op-2019-06. L'elemento di autenticazione richiesto al momento della disposizione di operazione di pagamento genera altresì un codice di autenticazione univoco associato specificatamente a quella transazione e alle sue caratteristiche, vale a dire importo e beneficiario, volto a soddisfare i requisiti di dynamic linking ai sensi dell'art. 5 del Regolamento delegato (UE) 2018/389*";
- fornisce una nota esplicativa dei log relativi all'operazione contestata;
- evidenzia che dalla documentazione allegata si rileva come data di ultima associazione del dispositivo mobile al conto corrente della ricorrente il 20.08.2021, data coincidente con quella di apertura del rapporto di conto corrente; rileva: "*ciò anche a riprova del fatto che le operazioni di pagamento in questa sede contestate non potevano che verificarsi previa debita autorizzazione del ricorrente medesimo tramite l'App (…) installata sul proprio e personale dispositivo mobile associato al conto corrente*";
- evidenzia che dalle tracciature informatiche emerge che la ricorrente ha effettuato, il 10.08.2022, tra le ore 17:15:26 e le ore 18:11:14 (arco temporale coincidente con l'orario in cui si è consumata la vicenda) l'accesso al proprio conto online tramite l'app installata sul device associato al proprio conto.

Con le repliche il ricorrente precisa quanto segue:

- le operazioni disconosciute non sono state autorizzate tramite l'invio di OTP o sistema di autenticazione forte, come affermato ma non dimostrato dall'intermediario;
- non è stata eccepita l'inaffidabilità del primo sms ricevuto ma anzi la "combinazione" tra sms e telefonata lo ha indotto a ritenere che i contatti ricevuti provenissero dall'intermediario;
- sostiene che la credibilità delle richieste del truffatore è avvalorata dal fatto che il primo sms ricevuto si sia inserito in coda a quelli genuini provenienti dall'intermediario, nonché dalla circostanza che le prime operazioni non autorizzate, menzionate anche dal truffatore nella telefonata descritta, risultavano visibili dall'app ed effettivamente bloccate in quanto non autorizzate;
- inoltre, è stato indotto a credere che la telefonata provenisse effettivamente dall'intermediario in quanto l'interlocutore era a conoscenza del fatto che il ricorrente fosse titolare di altro conto corrente presso altro intermediario, in ciò avvalorando la tesi secondo cui i sistemi informatici della resistente sarebbero stati violati ipotizzando la collaborazione di un dipendente della banca stessa;
- ritiene che la decisione dell'intermediario di rimborsare alcune delle operazioni contestate, effettuate con carta fisica nonostante la stessa sia sempre rimasta in possesso del ricorrente, confermi la violazione dei suoi sistemi informatici, ed inoltre ribadisce di non aver ricevuto mai alcun codice OTP.

La parte ricorrente, confermata la restituzione dell'importo di € 4.965,00, chiede la restituzione della restante somma di euro 10.991,01.

Nelle controrepliche l'intermediario precisa quanto segue:

- ribadisce l'eccezione di inammissibilità del ricorso per mancanza del preventivo reclamo nonché la parziale cessazione della materia del contendere con riferimento alle operazioni rimborsate;
- eccepisce la difformità di quanto dichiarato dal ricorrente in ordine alla ritenuta affidabilità del primo sms ricevuto, avendo questi dichiarato di aver nutrito dubbi sulla genuinità del sms in sede di denuncia;
- contesta la ricostruzione avversaria secondo cui l'accesso ai dati del ricorrente quali nominativo e numero di telefono sarebbe avvenuto grazie alla collaborazione di un dipendente della banca, ritenendo che il furto dei dati avrebbe potuto essere perpetrato in numerosissime circostanze di utilizzo dello strumento di pagamento, cui la banca era certamente estranea;
- specifica che prima delle operazioni disconosciute, il frodatore ha effettuato l'accesso al conto corrente del ricorrente in due momenti distinti, realizzatisi per effetto della imprescindibile collaborazione del ricorrente;
- il primo accesso al conto corrente, disposto da PC, è stato autorizzato tramite invio di codice OTP all'utenza mobile del ricorrente, nello specifico deduce che "Tale codice OTP dev'essere stato verosimilmente e necessariamente condiviso dal ricorrente con il frodatore nel corso della telefonata o deve averlo inserito nella pagina web a cui il ricorrente è stato reindirizzato tramite il link contenuto nell'sms fraudolento";
- il secondo accesso al conto corrente sarebbe stato effettuato dall'app mobile installata sul telefono del frodatore, accesso questo autorizzato inserendo le credenziali del ricorrente e da questi confermato tramite notifica inviata sul proprio device;
- eccepisce di non aver mai affermato che le operazioni in commento sono state autorizzate tramite l'invio di codici OTP, ribadendo che per il sistema di autenticazione adottato, nel caso venga rilevato un elevato livello di rischio per una data transazione, viene inviata al cliente una notifica push contenente il riepilogo dei dettagli dell'operazione;
- per mezzo di tale notifica push, la banca chiede quindi al cliente di autorizzare la transazione entro il termine massimo di 5 minuti all'interno dell'App installata sul dispositivo mobile associato al conto corrente;
- l'applicazione del sistema multifattoriale consiste proprio nel fatto che, per poter procedere all'autorizzazione o meno dell'operazione, il cliente deve prima accedere al proprio conto tramite l'App installata sul proprio device personale e univocamente associato al conto (accesso che avviene con doppio fattore) per poi confermare o meno, all'interno della propria App, la richiesta di addebito in cui sono indicati i dettagli riepilogativi della singola operazione (beneficiario e importo);
- ritiene pertanto confermata la correttezza del proprio operato, considerato che in ragione della rilevata rischiosità delle operazioni, era stato richiesto al ricorrente di autorizzarle per mezzo del descritto sistema multifattoriale;
- eccepisce che il rimborso delle operazioni contestate effettuate con carte "fisiche" non è stato disposto per avere la banca riscontrato che dette carte erano rimaste in possesso del ricorrente, ma l'accezione "fisica" delle carte in commento significa semplicemente che la carta per mezzo della quale queste operazioni erano state effettuate era quella previamente associata al portafoglio digitale in questione, avente natura fisica;
- il rimborso delle operazioni è stato disposto in ragione della mera natura telematica delle stesse, con ciò non ammettendo tuttavia alcuna responsabilità in relazione alla frode subita dal ricorrente;
- al contrario, ritiene corretto il proprio operato in ragione di quanto accertato in merito all'autenticazione delle operazioni disconosciute, che ritiene imputabili al ricorrente.

Pertanto, l'intermediario chiede che venga dichiarata la parziale cessazione della materia del contendere e contestualmente il rigetto del ricorso con riguardo alle residue pretese.

DIRITTO

1.- L'intermediario ha eccepito preliminarmente l'improcedibilità del ricorso ai sensi della Sez. VI, par. 1 e 2 delle Disposizioni ABF, per mancata preventiva presentazione del reclamo.

In particolare, l'intermediario sostiene che la comunicazione inviata in data 10.08.2022 al Servizio Clienti costituisca una mera richiesta di storno delle operazioni contestate e non sia qualificabile come reclamo in quanto:

(i) il reclamo, pur in assenza di requisiti formali, deve contenere una vera e propria contestazione di un comportamento dell'intermediario, seppure omissivo;

(ii) il disconoscimento delle operazioni contestate doveva essere indirizzato all'Ufficio Reclami.

La parte ricorrente ha prodotto la risposta dell'intermediario alla richiesta di rimborso avanzata. Al riguardo si deve rilevare che non è in atti la prima richiesta di rimborso/segnalazione di frode inoltrata dal ricorrente e, inoltre, che dal tenore delle risposte, si può ritenere formalizzata una contestazione delle operazioni fraudolente, con richiesta di rimborso.

Peraltro, ai sensi delle disposizioni ABF il reclamo non richiede particolari requisiti formali ed è un "atto con cui un cliente chiaramente identificabile contesta in forma scritta (es., lettera, fax, e-mail) all'intermediario un suo comportamento anche omissivo", per cui la risposta di diniego di rimborso del 29.08.2022 appare sintomatica dell'avvenuta interlocuzione finalizzata ad una risoluzione inter partes della controversia.

Peraltro, questo Collegio di recente e proprio nei confronti dell'intermediario odierno resistente ha avuto modo di ritenere soddisfatta la condizione di procedibilità anche nel caso di mera richiesta di rimborso (Coll. Roma, dec. n. 1037/2023; v. anche, Coll. Roma, dec. n. 14775/2022).

L'eccezione deve quindi ritenersi priva di pregio e deve rimanere disattesa.

2.- L'intermediario ha altresì eccepito che, "*anche nella denegata ipotesi in cui si dovesse ritenere che il ricorrente abbia presentato reclamo prima di proporre il ricorso, non sarebbe comunque integrata la condizione di procedibilità*" per il mancato decorso del termine dilatorio di 60 giorni fra il reclamo e il ricorso.

Sul punto si osserva che le Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari dispongono: «Il cliente rimasto insoddisfatto o il cui reclamo non abbia avuto esito nel termine di 60 giorni dalla sua ricezione da parte dell'intermediario, o nei più brevi termini eventualmente previsti da specifiche disposizioni di legge o dalle disposizioni emanate dalla banca d'Italia in attuazione del Titolo VI del TUB, può presentare ricorso all'Arbitro bancario Finanziario» (Sez. VI, § 1).

Pertanto, nel caso di specie – trattandosi di un ricorso in tema di servizi di pagamento – trova applicazione il più breve termine di 15 giorni, previsto dalle disposizioni di trasparenza della banca d'Italia (Disposizioni di trasparenza delle operazioni e dei servizi bancari e finanziari, Sez. XI, § 3, nota 1) ai fini della risposta dell'intermediario.

In ogni caso, la questione sollevata dall'Intermediario non è fondata posto che il ricorso è stato proposto in data 29.9.2022, ovverosia a seguito del riscontro negativo alla contestazione del cliente (cfr. comunicazione del 29.8.2022).

Si richiama a riguardo il seguente principio di diritto fissato dal Collegio di Coordinamento con decisione n. 15400/2021: "*La presentazione del ricorso prima dello scadere del termine di 60 giorni dalla presentazione del reclamo comporta l'inammissibilità del ricorso*

stesso che tuttavia può essere riproposto previo nuovo reclamo. Resta salva l'ipotesi di ricorso presentato prima della scadenza del predetto termine, ma in data successiva alla replica dell'intermediario che abbia espresso la volontà di non accogliere il reclamo".

3.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 10 agosto 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.

4.- 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".

5.- 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)*".

6.- Le operazioni contestate sono state eseguite in data 10.08.2022 e consistono in cinque disposizioni di pagamento online per un totale di euro 10.991,01: n. 2 operazioni di addebito su carta di debito n. 6407 rispettivamente dell'importo di 1.021,48 EUR e di 3.977,53 EUR; n. 2 operazioni di addebito su carta di debito n. 2084 rispettivamente dell'importo di 999,00 EUR e di 3.613,00 EUR; n. 1 operazione di addebito su carta di debito n. 2010 dell'importo di 1.380,00 EUR.

In sede di denuncia, il ricorrente riferisce di aver ricevuto un sms apparentemente proveniente dall'intermediario resistente.

In sede di repliche, ha prodotto la schermata di una chat, dalla quale non è evincibile l'ID mittente del messaggio. Da tale evidenza si evince, nondimeno, che il messaggio esca:

- è inserito in una chat preesistente, in quanto preceduto da un messaggio presumibilmente genuino contenente un link riconducibile alla ragione sociale dell'Intermediario;
- non presenta evidenti errori grammaticali;
- contiene l'indicazione che l'app "sta per essere bloccata" e l'invito a cliccare su un link (anch'esso contenente riferimenti all'Intermediario) per evitare il blocco;
- è seguito da messaggi genuini che contengono i codici per l'*onboarding* delle carte dell'Intermediario su Google Pay.

Il ricorrente ha dichiarato di non aver cliccato sul link ricevuto.

Dopo pochi minuti, riceveva la telefonata da un'utenza mobile e l'interlocutore, qualificatosi come operatore del servizio clienti della resistente, lo informava di alcuni "movimenti sospetti" sul conto corrente, precisando che si era provveduto a bloccare tali movimenti. Il ricorrente controllava tramite app e notava la presenza di "un paio di movimenti", mai autorizzati, che la banca "aveva appunto bloccato".

A circa 30 minuti di distanza dalla prima telefonata, riceveva ulteriore chiamata dal medesimo sedicente operatore che chiedeva nuova conferma del disconoscimento dei movimenti e riferiva "che ne stavano avvenendo altri e addirittura" da un altro conto del ricorrente, intrattenuto presso banca terza.

L'interlocutore riferiva di poter bloccare solo i movimenti anomali sul conto della banca odierna resistente e quindi consigliava all'odierno ricorrente di trasferire il denaro dal suo conto intrattenuto presso intermediario terzo al conto intrattenuto presso l'intermediario odierno resistente. Tale trasferimento avrebbe consentito al sedicente operatore di procedere a uno storno.

Fidandosi di quanto gli era stato riferito, durante la telefonata effettuava volontariamente cinque bonifici da un proprio conto presso intermediario terzo al conto intrattenuto presso l'intermediario resistente, per un totale di euro 14.942,99.

Al termine della chiamata l'interlocutore gli riferiva che sarebbe "stato ricontattato da un suo collega a mezzanotte" in quanto aveva "quasi raggiunto il limite massimo dei bonifici effettuabili".

7.- L'intermediario ha precisato che le operazioni contestate sono state autorizzate, previa notifica push per ciascuna transazione, attraverso l'inserimento delle credenziali personali

(fattore di conoscenza) ovvero, in alternativa, dell'ID biometrico (fattore di inerenza), all'interno dell'app installata sul dispositivo della ricorrente e univocamente associata al suo conto (fattore di possesso).
L'intermediario produce diversi log relativi alle operazioni contestate e riporta una nota esplicativa. Dalla nota esplicativa emerge che l'indicazione "CHALLENGE" della colonna "risk_model_decision" è indicativa del fatto che l'algoritmo predittivo ha determinato che le transazioni dovevano essere soggette ad autenticazione forte. La dicitura "CONFIRMED" nella colonna "status" indica che le operazioni di pagamento sono state autenticate.
L'Intermediario descrive il sistema di autorizzazione per le disposizioni di pagamento sui siti di e-commerce tramite carta di debito: la richiesta di autenticazione del pagamento viene trasmessa dall'esercente all'intermediario; l'intermediario valuta, sulla base degli elementi di rischio dell'operazione stessa, se rifiutare (Rejected) ovvero dare seguito alla transazione, la cui esecuzione può avvenire senza autenticazione forte (Accepted) oppure applicando la SCA (Challenged).
L'intermediario ha altresì precisato che, per le operazioni soggette ad autenticazione forte da parte del cliente (Chellenged), si chiede conferma della transazione al cliente esclusivamente attraverso l'App installata sul dispositivo mobile associato al conto corrente.
L'intermediario produce evidenza delle notifiche "in app" inviate per autorizzare l'operazione e riporta anche i log relativi all'accesso all'app. In particolare, per il primo accesso che viene in rilievo nel caso di specie è presente la dicitura "MFA_OSC" che, secondo la legenda esplicativa fornita, corrisponde a un'autenticazione multifattoriale in cui il secondo fattore proviene da un device certificato e la richiesta di autenticazione proviene dal medesimo dispositivo "accoppiato" (in questo caso dallo stesso device sul quale è configurata l'app).
Questo Collegio ha ritenuto compliant alla SCA una modalità autorizzativa simile, predisposta da altro intermediario (Coll. Roma, dec. n. 19734/2021).
9.- 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*".
Pertanto, alla luce delle risultanze istruttorie, il Collegio ritiene che sussistano profili di colpa grave del cliente - consistente nell'avere dato seguito alle istruzioni telefoniche del frodatore e nonostante l'anomala richiesta che lo ha condotto a creare la provvista sul conto mediante la disposizione di ben cinque bonifici dal altro conto intrattenuto presso un altro 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.
Nel caso in esame, invece, 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; Coll. Roma, dec. n. 1625/2022).

6.- Alla luce di quanto sopra esposto il Collegio valuta il concorso in misura sostanzialmente paritaria tra le parti e liquida in via equitativa in favore del ricorrente a titolo risarcitorio l'importo di € 5.500,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 5.500,00, 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