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) CATERINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ANDREA TUCCI

Seduta del 09/09/2021

FATTO

Il ricorrente, titolare di una carta di credito (***835) e di una carta bancomat (***907) emesse dall'intermediario resistente, riferisce di aver ricevuto, in data 08/12/2020, alcuni SMS, che lo avvertivano di operazioni non autorizzate eseguite durante la notte con la propria carta di credito.
Da un controllo dell'estratto conto, si avvedeva dell'esecuzione di pagamenti fraudolenti anche tramite la carta bancomat. Provvedeva quindi a bloccare entrambe le carte e "l'accesso all'home banking".
Nella denuncia allegata, cui rinvia, espone che le operazioni disconosciute sono nove, per la carta di credito n. ***835, di cui due effettuate in data 07/12/2020, rispettivamente per € 200,00 ed € 69,00, e sette in data 08/12/2020 (cinque pagamenti di € 200,00, uno di € 100,00 e uno di € 249,00). Quanto alla carta bancomat n. ***907, disconosce tre pagamenti di € 966,00 (uno eseguito il 07/12/2020 e due il 08/12/2020), nonché un pagamento di € 2.575,00, eseguito in data 08/12/2020.
Precisa di non aver mai ceduto le carte a terzi e di non aver mai rivelato i "codici segreti".
Aggiunge che l'intermediario provvedeva, in un primo momento, a riaccreditare gli importi delle operazioni disconosciute, per poi riaddebitarli, in violazione delle disposizioni legislative in materia, che escludono il diritto al rimborso per il cliente soltanto nel caso di dolo o colpa grave, la cui prova è a carico dell'intermediario.
Tanto premesso, il ricorrente chiede di "riaccreditare i pagamenti fraudolenti, meglio specificati nella querela allegata".

L'intermediario, nelle controdeduzioni, precisa che il ricorrente ha disconosciuto presso la filiale, in data 16/12/2020, le operazioni fraudolente di cui alla carta n. ***907, che sono state prima accreditate e poi riaddebitate, in data 11/01/2021, per l'importo di € 3.541,00. Aggiunge che, in data 25/01/2021, il cliente formulava reclamo, contestando "genericamente" siffatto riaddebito.
Tanto premesso, l'intermediario eccepisce, preliminarmente, la genericità del ricorso e del precedente reclamo, atteso che il ricorrente domanda il riaccredito di somme tramite un mero rinvio alla querela allegata, senza specificare per quali operazioni e per quali importi viene chiesta la retrocessione.
Ritiene, pertanto, che – alla luce dell'indeterminatezza del petitum – l'oggetto del ricorso debba essere individuato per relationem. Al riguardo, evidenzia come il ricorrente abbia prodotto - quale prova della preventiva proposizione di un reclamo rigettato dall'intermediario - la lettera dell'11/01/2021, "con la quale la Banca ha comunicato di non aver accolto il disconoscimento relativo alle operazioni compiute con la carta n. ***907, per l'importo complessivo di 3.541 €".
L'intermediario ritiene, pertanto, che – sebbene in denuncia venga fatto riferimento anche ad altre operazioni – la pretesa di cui al ricorso debba essere circoscritta alle operazioni oggetto della pratica di disconoscimento relativa alla carta n. ***907, ossia due operazioni di € 966,00 e di € 2.575,00.
Nel merito, l'intermediario precisa che il ricorrente è titolare di un conto corrente abilitato al servizio di internet banking. Per accedere al servizio, è richiesto l'inserimento simultaneo di password statiche e dinamiche: il codice titolare, il PIN e il codice OTP. Una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario il codice dinamico OTP.
Precisa che l'OTP può essere generato tramite App ovvero tramite sms. Afferma inoltre che, in caso di utilizzo dell'App, l'OTP è generato a seguito della selezione della notifica ricevuta sullo smartphone o sul tablet su cui è stata attivata l'App e della digitazione del PIN, sullo smartphone o sul tablet oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale.
Inoltre, "per aumentare ulteriormente il livello di sicurezza di alcune disposizioni di pagamento, oltre alla consueta autenticazione e conferma con codice dinamico, è richiesto al cliente di rispondere alle domande di sicurezza precedentemente censite dal medesimo. Per i clienti che non hanno censito le domande di sicurezza ed in altri specifici casi, verrà richiesto l'inserimento di un secondo codice inviato via sms".
L'intermediario allega una certificazione che attesta come tale sistema sia in grado di "offrire massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici".
Relativamente alle operazioni eseguite con la carta n. ***907, l'intermediario afferma che sono state effettuate dopo essere state autenticate, correttamente registrate e contabilizzate e non hanno subito "le conseguenze del malfunzionamento delle procedure necessarie per la [loro] esecuzione o di altri inconvenienti". A tal fine, produce l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta, riportando i log estratti dai propri archivi informatici.
Al riguardo, specifica che l'operatività disconosciuta è stata eseguita da app installata su un dispositivo identificato dalla chiave "***77f", mentre il cliente si connette solitamente da smartphone con codice "***9E8".
In particolare, alle 19.02 del 07/12/2020 veniva eseguito un login da app, validato con PIN, e l'enrollment dell'app sul nuovo dispositivo, confermato con il codice OTS inoltrato via SMS al numero certificato del cliente. Veniva, quindi, inoltrata al cliente una notifica push, in cui si evidenziava "l'accesso all'app da un nuovo dispositivo".

Alle 19.05 veniva modificato il PIN e di tale operazione il ricorrente veniva avvisato con SMS al numero di telefono certificato e riceveva notifica push.
In seguito, veniva eseguito un pagamento di € 966,00 con carta n. ***907, confermato con OTP virtuale.
Dopo un login da app alle 12.55 del 08/12/2020, confermato con OTP virtuale, veniva eseguito alle 13.16, sempre con la carta n. ***907, un pagamento di € 2.575,00, anch'esso confermato con OTP virtuale.
Quanto alla condotta tenuta dal ricorrente, l'intermediario eccepisce che quest'ultimo, nei propri scritti difensivi e nella denuncia, non ha fornito elementi utili alla ricostruzione dell'accaduto, limitandosi a disconoscere le operazioni in argomento, senza fornire ulteriori elementi. Osserva che tale condotta è stata censurata dal Collegio di Milano nelle decisioni nn. 12763/20 e 19237/20.
Il cliente, inoltre, non avrebbe lamentato anomalie nel funzionamento del telefono, guasti o sospensioni del servizio e, pertanto, le operazioni fraudolente sarebbero state rese possibili solo grazie alla sua condotta gravemente colposa, avendo il cliente ricevuto le credenziali senza le quali non sarebbe stato possibile installare l'applicazione su un diverso telefono e compiere le operazioni poi disconosciute.
Richiamando il d.lgs. n. 11/2010, afferma che la colpa grave del ricorrente si evince da una serie di circostanze. In particolare, evidenzia come dalle stesse dichiarazioni del cliente emerga che questi ha ricevuto i messaggi della banca attestanti l'operatività in corso, senza tuttavia attivarsi per bloccare la prosecuzione della truffa, prima che le operazioni potessero essere effettuate.
Richiama alcune decisioni ABF (Collegio di Milano, n. 7131/2017, Collegio di Bologna, n. 11284/2019 e n. 7258/2020), secondo cui l'adozione di un sistema di autenticazione "a due fattori", quale quello utilizzato nel caso di specie, induce a ritenere, da un lato, che la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del d. lgs. n. 11/2010 e, dall'altro lato, che il cliente si sia reso gravemente inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online.
L'intermediario chiede, pertanto, di dichiarare "inaccoglibile", in quanto immotivata e infondata, la richiesta restitutoria oggetto del ricorso e in subordine, ove il Collegio ravvisi profili di responsabilità nell'accaduto in capo all'intermediario, chiede di definire la ripartizione tra le parti del danno in esame, in misura proporzionale alle rispettive responsabilità, ai sensi dell'art. 1227, 1° e 2° comma, c.c.
In sede di repliche, il ricorrente sottolinea l'assenza di profili di indeterminatezza nel ricorso, ritenendo che tale atto possa contenere anche solo un richiamo al contenuto degli atti propedeutici.
Al riguardo, rappresenta di aver "regolarmente" riportato per relationem l'elenco degli addebiti anomali di cui alla denuncia del 10/12/2020, versata in atti. Ritiene, pertanto, che l'oggetto del contendere non possa essere limitato soltanto alle due operazioni richiamate nelle controdeduzioni, a nulla rilevando l'allegazione della nota trasmessa dall'intermediario l'11/01/2021.
Quanto al merito, evidenzia profili di colpa grave nella condotta della banca, avendo questa proceduto a riaddebitare le somme di cui agli utilizzi fraudolenti, precedentemente accreditate, senza alcuna autorizzazione del correntista e, soprattutto, senza avere prima ottenuto un qualsivoglia riconoscimento della legittimità del proprio operato.
Ritiene, peraltro, che tale condotta non possa essere giustificata dalla clausola del modulo di disconoscimento, nella parte in cui riconosce alla banca il diritto alla restituzione dell'importo rimborsato, ove sia successivamente dimostrata la regolare autorizzazione delle operazioni. Tale clausola, infatti, limita la responsabilità risarcitoria della banca, in

violazione del disposto dell'art. 1229 c.c., e risulta pertanto "nulla e/o inopponibile al reclamante che neppure la ha accettata espressamente per iscritto".
Il ricorrente disconosce ex art. 2712 c.c. "tutte le risultanze dei detti "fogli push" e "fogli s.m.s.", contestandone la conformità agli originali ex art. 2719 c.c. Richiama, sul punto, l'orientamento della giurisprudenza di legittimità secondo cui "lo short message service (SMS) contiene la rappresentazione di atti, fatti o dati giuridicamente rilevanti ed è riconducibile nell'ambito dell'art. 2712 c.c., con la conseguenza che forma piena prova dei fatti e delle cose rappresentate se colui contro il quale viene prodotto non ne contesti la conformità ai fatti o alle cose medesime" (Cassazione civile, sez. II, 21/02/2019, n. 5141).
Esclude, peraltro, la genericità di tale disconoscimento, atteso che l'onere prova della ricezione delle comunicazioni in contestazione grava sul mittente, in ragione del pacifico assoggettamento della fattispecie al regime degli atti recettizi (cita, sul punto, la sentenza n. 20167/14 della Cassazione).
Ad ogni buon conto, eccepisce che l'intermediario non ha fornito alcuna prova della riconducibilità al ricorrente del device n. "***9E8", su cui sarebbero stati trasmessi i messaggi di alert.
Evidenzia, peraltro, come la banca – pur avendo accertato che l'operatività fraudolenta proveniva da un dispositivo non riconducibile al ricorrente tramite un browser inusuale – abbia omesso di bloccare le operazioni, non controllando che l'OTP fosse inserito dal cliente e limitandosi a inviare comunicazioni la cui ricezione da parte del cliente doveva essere ritenuta incerta.
Insiste, pertanto, per l'accoglimento del ricorso.
L'intermediario, in sede di controrepliche, osserva, in primo luogo che il cliente - anche in sede di repliche - si è limitato a richiamare la denuncia, senza tuttavia precisare per quali operazioni ed importi agisce e senza dimostrarne l'addebito e l'avvenuto disconoscimento.
Ribadisce, pertanto, che la pretesa del ricorrente dev'essere limitata alle due operazioni di € 966,00 e 2.755,00 eseguite con la carta n. ***907, oggetto della comunicazione della banca del 11/01/2021, allegata al ricorso.
Quanto alle altre due operazioni di € 966,00, riportate in sede di denuncia per la medesima carta, fa presente che le stesse non sono state addebitate sul conto del cliente e non hanno, peraltro, formato oggetto di disconoscimento.
Con riferimento alle operazioni eseguite con l'altra carta (n. ***835), rileva, in primo luogo, che due di queste (rispettivamente di € 200,00 e di € 249,00) erano state recuperate e stornate già alla data del reclamo.
Quanto alle altre, ritiene che la domanda del ricorrente sia viziata da improcedibilità, mancando un pregresso reclamo rigettato dall'intermediario, nonché da carenza di interesse ad agire, in quanto al momento del ricorso erano ancora in corso verifiche e gli importi disconosciuti erano stati riaccreditati salvo buon fine.
Con riferimento alla formulazione della clausola del modulo di disconoscimento, rammenta che tali pattuizioni sono state sottoscritte in applicazione della norma primaria di recepimento della PSD2.
Nel merito, rileva la conformità delle tracciature prodotte in sede di controdeduzioni con quanto risultante a sistema. Aggiunge che dai file allegati emerge "inconfutabilmente" la riconducibilità al ricorrente del device identificato con il codice "***9E8", associato a precedenti accessi e operazioni non contestate.
L'intermediario, inoltre, ritiene contrario a correttezza e buona fede processuale il tentativo del ricorrente di disconoscere la ricezione dei numerosi messaggi di alert inviati dalla banca tramite SMS e push. In particolare, quanto agli SMS, fa presente che lo stesso ricorrente ha dichiarato in denuncia di aver ricevuto i messaggi che lo informavano delle operazioni poi contestate. Con riferimento alle notifiche push, evidenzia che il regolare

recapito delle stesse sul dispositivo del cliente è evincibile dell'assenza di codici di errore nella colonna H del foglio "push".
Ad ogni buon conto, richiama l'orientamento dei Collegi secondo cui non si può "ritenere che la negazione di avere ricevuto le comunicazioni dell'intermediario, pure documentate da quest'ultimo, comporti automaticamente una conclusione di assenza di responsabilità del cliente che abbia disconosciuto un'operazione online". Cita, sul punto, la decisione n. 10751/20 del Collegio di Bologna.
Insiste, pertanto, per il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio attiene all'uso non autorizzato di uno strumento di pagamento.
Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018.
Mette conto precisare, inoltre, che le operazioni contestate sono state eseguite successivamente all'entrata in vigore delle nuove disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, 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 (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).
La disciplina richiamata 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 fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d. lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7." (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".
Ai sensi del successivo art. 12, co. 2 bis, "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". Per "autenticazione forte" si

intende (art. 1, co. q bis) “una 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”.
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. Laddove una simile responsabilità non possa essere dimostrata dall’intermediario prestatore del servizio, pertanto, l’utilizzatore non sarà tenuto a sopportare le conseguenze dell’uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall’intermediario, di una franchigia non superiore a 150 euro). 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” (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014. Da ultimo, cfr. Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l’insufficienza della prova della regolarità formale dell’operazione contestata, ai fini dell’assolvimento dell’onere della prova gravante sull’intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).
L’orientamento di questo Arbitro ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, in tema 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” (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777. In senso conforme, cfr., più di recente, Cass., 12.4.2018, n. 9158; Cass., 26 novembre 2020, n. 26916, anche per l’importante statuizione, secondo cui “al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento - prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente - la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo”).
Procedendo all’esame del ricorso, mette conto esaminare l’eccezione dell’intermediario circa la genericità del ricorso e del precedente reclamo, ritenendo insufficiente il rinvio alla

denuncia in essi contenuto, senza alcuna specificazione delle operazioni contestate e degli importi richiesti in restituzione.
Al riguardo, l'orientamento di questo Arbitro è nel senso che "il ricorrente è tenuto a formulare una domanda che sia articolata nel petitum (il provvedimento o il bene della vita richiesto) e nella causa petendi (la situazione giuridica giustificatrice della domanda) e a produrre la documentazione dimostrativa". L'Arbitro, peraltro, ha "il potere – dovere di interpretare la domanda, nel senso di enucleare tutte le possibili implicazioni che vi sono contenute. Tale attività si rivela tanto più opportuna in una procedura che non prevede l'assistenza professionale (anche se nella pratica si sta ormai diffondendo la tendenza dei clienti ad avvalersi dell'opera di un professionista). Ma si tratta di un potere – dovere che non può esorbitare dai limiti dell'interpretazione (cioè della decrittazione della volontà del ricorrente) per estendersi ad una interpretazione "integrativa" o "additiva", nel senso di esaminare situazioni di fatto non ricavabili dal tenore della domanda" (Collegio di Coordinamento, decisione n. 10929/16). A tal fine, l'oggetto della domanda può essere desunto dal complesso della documentazione in atti, dovendo trovare applicazione il principio enunciato dalla Corte di Cassazione, con riferimento agli atti introduttivi del giudizio, secondo cui "la valutazione deve essere fatta caso per caso "dovendosi tener conto, a tal fine, del contenuto complessivo dell'atto di citazione, dei documenti ad esso allegati, nonché, in relazione allo scopo del requisito di consentire alla controparte di apprestare adeguate e puntuali difese, della natura dell'oggetto e delle relazioni in cui, con esso, si trovi la controparte" (in questi termini: Coll. Bari, dec. n. 17995/20, citando Cass., n. 1681/15).
Nel caso di specie, lo stesso intermediario resistente riconosce che il petitum del ricorso possa essere individuato per relationem. Ritiene, tuttavia, che per ricostruire il petitum si debba far riferimento, non alla denuncia, ma alla lettera dell'11/01/2021, allegata al ricorso, con la quale la banca ha comunicato di non aver accolto il disconoscimento relativo alle due operazioni di € 966,00 del 07/12/2020 e di € 2.575,00 del 08/12/2020, entrambe eseguite con la carta n. ***907. Svolge, pertanto, le proprie controdeduzioni solo con riferimento a tali due operazioni.
Al riguardo, ritiene il Collegio che l'eccezione dell'intermediario non possa essere accolta, alla luce della documentazione prodotta dalle parti, che consente al Collegio di circoscrivere l'oggetto della domanda e le ragioni poste a suo fondamento dal ricorrente.
Soltanto in sede di controrepliche, l'intermediario eccepisce – limitatamente alle operazioni riferibili alla carta n. ***835 – che "la domanda del ricorrente risulta comunque viziata da improcedibilità, mancando nel caso di specie il pregresso reclamo rigettato dall'intermediario".
Al riguardo, si osserva che, ai sensi delle Disposizioni ABF, Sez. VI, par. 1, per la presentazione del ricorso non è necessario che il reclamo sia stato "rigettato" dall'intermediario, essendo a tal fine sufficiente che il reclamo non abbia avuto esito nel termine di 60 giorni dalla presentazione ovvero nel termine più breve previsto da specifiche disposizioni di legge o dalle disposizioni emanate dalla Banca d'Italia in attuazione del Titolo VI del TUB". Nel caso di servizi di pagamento, le Disposizioni di Trasparenza prevedono che "i tempi massimi di risposta non sono superiori a 15 giornate lavorative dalla ricezione del reclamo".
Nel caso di specie, tra la data in cui l'intermediario resistente afferma di aver ricevuto il reclamo (25/01/2021) e la data del ricorso (16/02/2021) sono intercorsi 16 giorni lavorativi (sabato esclusi). Si rileva, altresì, che lo stesso intermediario ha allegato alle controrepliche il modulo di disconoscimento relativo alla carta n. ***835, datato 11/12/2020, al quale deve riconoscersi natura di reclamo (cfr., ex multis, Collegio di Bari, decisione n. 4817/21 e Collegio di Roma, decisione n. 9476/18).

Per le suesposte ragioni, l'eccezione dell'intermediario non merita accoglimento.
Sempre in sede di controrepliche, l'intermediario sostiene che "la domanda del ricorrente risulta comunque viziata […] da carenza di interesse ad agire, avendo la banca operato all'atto del disconoscimento il temporaneo riaccredito delle somme disconosciute".
Al riguardo, risulta incontestato tra le parti che almeno sette delle nove operazioni fraudolente eseguite con la carta di credito n. ***835, dopo l'iniziale accredito, sono state riaddebitate. Il che comporta senz'altro la sussistenza di un interesse concreto e attuale del ricorrente, dovendosi, poi, esaminare del merito l'eventuale insussistenza del diritto al rimborso di specifiche operazioni.
Da ultimo, si osserva che non merita accoglimento l'eccezione del ricorrente in merito al successivo riaddebito di operazioni precedentemente stornate, trattandosi di procedura conforme al regolamento pattizio convenuto dalle parti, in conformità con la disciplina di rango primario applicabile (all'art. 11, co. 3, d.lgs. n. 11/10).
Procedendo all'esame del merito del ricorso, si osserva, innanzi tutto, che il ricorrente non ha fornito elementi utili per ricostruire le modalità di svolgimento dell'asserita truffa, limitandosi a dichiarare "di non aver mai ceduto a terzi le carte in questione né tantomeno i codici segreti" e di essersi accorto "la mattina del giorno 08 dicembre" di alcuni SMS ricevuti sul suo numero di cellulare che lo avvertivano di alcuni pagamenti eseguiti con la carta di credito.
L'intermediario, d'altronde, ha prodotto documentazione utile a ricostruire la procedura di autorizzazione delle operazioni contestate – in particolare, il log delle operazioni – soltanto in relazione ai due pagamenti eseguiti con la carta n. ***907, rispettivamente per € 966,00 in data 07/12/2020 e per € 2.575,00 in data 08/12/2020.
In relazione a siffatte operazioni, l'intermediario afferma che le operazioni sono state correttamente autorizzate, senza anomalie, con un sistema di autenticazione forte a due fattori.
Al riguardo, l'intermediario precisa che, dalla documentazione in atti, risulta che:

- l'accesso all'home banking avviene con l'inserimento di codice titolare e PIN (credenziali statiche) e di una password dinamica OTP;
- le operazioni dispositive richiedono un codice OTP, che può essere generato tramite app ovvero tramite sms. In caso di utilizzo dell'app, l'OTP è generato a seguito della selezione della notifica ricevuta sullo smartphone o sul tablet su cui è stata attivata l'app e della digitazione su tale smartphone o tablet del PIN oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale.

L'intermediario ha allegato alle controdeduzioni un file excel di "tracciature informatiche" relative all'autenticazione, registrazione e contabilizzazione delle due operazioni in questione.
Trattasi di un file composto da sei fogli, così denominati:

1) "legenda";
2) "anagrafica" (sui dati anagrafici del cliente reperiti nell'archivio del servizio internet banking);
3) "accessi" (sull'elenco degli accessi al servizio effettuati dall'utenza del cliente);
4) "tracciatura" (sulla tracciatura informatica dell'operazione disconosciuta);
5) "sms" (sull'elenco dei messaggi sms inviati al numero telefonico mobile del cliente);
6) "push" (sull'elenco delle push notification inviate all'APP mobile del cliente).

In sede di repliche, parte ricorrente disconosce ex art. 2712 c.c. "tutte le risultanze dei detti "fogli push" e "fogli s.m.s.", contestandone peraltro la conformità agli originali ex art. 2719 c.c. Nega, in particolare, di aver ricevuto gli SMS e le push indicate nei fogli.
Al riguardo, in linea con il proprio orientamento, il Collegio ritiene che le sopra riportate tracciature possano costituire strumento di prova – anche in considerazione dei limiti del potere istruttorio dell'Arbitro -, ove contenenti, come nell'ipotesi in esame una descrizione analitica degli eventi (cfr. Coll. Bari, decisione n. 12971/21; decisione n. 4053/2020)
L'intermediario ha inoltre depositato in atti una schermata, dalla quale risulterebbe che le due operazioni sono state eseguite su commercio elettronico sicuro con autenticazione del titolare tramite OTP e che non è stata rilevata alcuna anomalia.
Tanto premesso, osserva il Collegio che il sistema di sicurezza adottato dall'intermediario risulta costituito dall'impiego di un doppio fattore di autenticazione e soddisfa i requisiti della autenticazione forte dell'utente, come evidenziata nella normativa su richiamata, potendosi quindi ritenere fornita dimostrazione che tutte le operazioni sono state correttamente eseguite e non sono frutto di malfunzionamenti delle procedure esecutive" (cfr., in relazione a fattispecie analoga, Collegio di Bari, decisione n. 15869/21).
Per le suesposte ragioni, ritiene il Collegio che l'intermediario abbia fornito la prova della regolarità formale delle operazioni contestate.
Alla luce delle richiamate disposizioni normative, peraltro, la prova della regolarità formale di un'operazione contestata non è sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento di pagamento, dovendo l'intermediario provare anche i fatti idonei a integrare il dolo o la colpa grave dell'utilizzatore.
Questo aspetto risulta enfatizzato, a seguito della novella del 2017 (d.lgs. n. 218/2017), che ha introdotto nell'art. 10, co. 2, la disposizione sopra riportata, in tema di onere della prova del dolo o della colpa grave dell'utente. La prova in questione, evidentemente, non può coincidere con quella della mera regolarità formale delle operazioni, pena un'interpretazione abrogante della disposizione. Sul punto si è, da ultimo, pronunciato il Collegio di Coordinamento, nella menzionata decisione n. 22745 del 10/10/2019, nella quale è stato enunciato il principio secondo cui "la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente [….]Utili informazioni integrative potrebbero, ad esempio, riguardare l'assenza di tentativi falliti di digitazione del PIN, la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente, in assenza di deviazioni o intrusioni nel device, l'accertata assenza di malware, ecc..".
Nel caso di specie, il ricorrente si è limitato al mero disconoscimento delle operazioni, in tal modo non consentendo una valutazione della propria condotta, se non in termini indiziari. Sul punto, ritiene il Collegio di dover dare continuità al proprio orientamento, secondo cui, in presenza di mero disconoscimento delle operazioni regolarmente autenticate, è possibile desumere la colpa grave del ricorrente, "valorizzando, da un lato, la prova dell'invio via SMS del codice OTP da parte dell'intermediario e, dall'altro, la mancata allegazione di un malfunzionamento dell'utenza telefonica da parte del ricorrente o di una contestazione da parte sua della ricostruzione in fatto operata dall'intermediario (cfr. fra le altre, Collegio di Bari, decisione n. 17718/20; Collegio di Bari, decisioni nn. 10067/2020, 525/2020 e 8894/2020).

Vero è, peraltro, che anche la condotta dell'intermediario non può dirsi immune di censure, sotto il profilo dell'efficiente organizzazione del servizio.
Al riguardo, dalla documentazione prodotta dall'intermediario, risulta che, in concomitanza con le operazioni in esame, risultano elementi di anomalia, quali tentativi di accessi, poi bloccati, e variazione dei massimali di utilizzo della carta. Si tratta di circostanze sospette, che il sistema antifrode dell'intermediario ha rilevato, senza, tuttavia, adottare efficaci contromisure, anche rispetto alla successiva operatività.
In secondo luogo, dalla documentazione in atti non si rinviene l'invio di messaggi di alert con riferimento alle singole operazioni. Il che costituisce una violazione dei doveri di protezione dell'utente gravante sull'intermediario (cfr. Collegio di Coordinamento decisione n. 24366/2019, per il rilievo secondo cui "fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto").
Alla luce di quanto sin qui osservato, ritiene il Collegio che, in relazione alla prima delle due operazioni in esame, sia configurabile un concorso di colpa del ricorrente e dell'intermediario, nella misura del 50%, che giustifica una corrispondente riduzione del rimborso dovuto. Le conseguenze pregiudizievoli della seconda operazione, per contro, devono restare a carico dell'intermediario, poiché l'adozione di un efficiente sistema di sms alert avrebbe potuto evitare il compimento dell'operazione fraudolenta.
In relazione alle restanti operazioni l'intermediario non ha fornito al Collegio elementi per accertare la corretta autenticazione e la regolarità estrinseca. La domanda di rimborso del ricorrente, pertanto, merita, sul punto, accoglimento, anche in relazione alle operazioni per le quali l'intermediario afferma di avere effettuato il riaccredito, poiché la circostanza è stata dedotta soltanto in sede di controrepliche, non consentendo al ricorrente di replicare, anche alla luce di un eventuale successivo riaddebito, come pure accaduto per altre operazioni contestate.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 6.608,00.
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