Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

## COLLEGIO DI ROMA

composto dai signori:

| | |
|---|---|
| (RM) GRECO | Presidente |
| (RM) PATTI | Membro designato dalla Banca d'Italia |
| (RM) ACCETTELLA | Membro designato dalla Banca d'Italia |
| (RM) CAPPIELLO | Membro di designazione rappresentativa degli intermediari |
| (RM) CHERTI | Membro di designazione rappresentativa dei clienti |

Relatore FRANCESCO ACCETTELLA

Seduta del 08/06/2021

## FATTO

1. L'odierno ricorrente afferma di avere subito il furto della propria identità digitale, a seguito del quale ignoti malfattori hanno posto in essere – tramite una "sim swap fraud" – una serie di operazioni dispositive a valere sul suo conto corrente, realizzate nel periodo compreso tra il 17 e il 25 agosto 2020. A tal riguardo il ricorrente premette di aver richiesto, in data 12/08/2020, il rilascio di una nuova scheda SIM abbinata al numero telefonico *******114 presso un centro di assistenza del proprio gestore telefonico. Riferisce di aver consegnato al personale addetto copia del proprio documento di identità e del proprio codice fiscale. Afferma inoltre di aver richiesto, il giorno successivo, l'attivazione del *mobile token* dell'intermediario convenuto e di aver ricevuto conferma di attivazione tramite sms, pervenutogli quello stesso giorno, alle ore 12:51. Sostiene di essere quindi partito per la Croazia e di essersi avveduto, in data 17/08/2020, di non poter più effettuare operazioni dispositive tramite la propria carta di credito e di non poter più impiegare il proprio telefono cellulare, che risultava non avere linea. Aggiunge di essersi recato al ritorno, in data 26/08/2020, presso un centro assistenza del proprio gestore telefonico per ottenere la riattivazione della sim e di avere appreso in quell'occasione che, il 17/08/2020 alle ore 11:32, la scheda a lui intestata era stata disattivata a seguito di una denuncia di furto. Apprendeva altresì che su richiesta di terzi ignoti, in pari data, era stata effettuata l'attivazione di nuova sim con abbinato il medesimo numero telefonico. Il

ricorrente afferma poi di aver ricevuto, una volta ottenuta la riattivazione della propria sim, una chiamata dal servizio clienti dell'intermediario convenuto, il quale lo informava che il suo conto corrente era stato bloccato a seguito di operazioni sospette. Si avvedeva quindi che, nelle more del blocco, erano state effettuate operazioni dispositive tramite la sua carta di credito *******9332, per un importo complessivo di euro 418,90, presso varie località della Sardegna. Rileva che ad esse si aggiungeva un bonifico di euro 14.400,50. Il ricorrente precisa altresì che, dal controllo della movimentazione bancaria, risultava effettuato, in data 25/08/2020, a conto praticamente azzerato, anche un bonifico in suo favore di euro 26.000, seguito in pari data da altri due bonifici in uscita, di importo pari rispettivamente a euro 14.900 ed euro 11.000,50, che provvedeva a disconoscere. Con comunicazione del 2/09/2020, l'intermediario sosteneva tuttavia che le operazioni in contestazione erano state autorizzate all'interno di un sistema di autenticazione forte e senza anomalie. Rilevava inoltre che le operazioni in questione fossero imputabili a negligenza del ricorrente nella custodia delle credenziali. L'intermediario precisava di aver recuperato l'importo (parziale) di euro 4.230.00, che veniva riaccreditato al ricorrente in data 01/09/2020, ma negava ogni ulteriore rimborso. Con successiva missiva il ricorrente contestava le ragioni dell'intermediario, evidenziando che l'oggetto della contestazione "non era inerente alla procedura di doppia autenticazione utilizzata ma, a priori, riguardava proprio il rilascio delle credenziali di accesso". Il ricorrente afferma di aver richiesto, con pec dell'11/11/2020, spiegazioni al gestore telefonico in ordine alle modalità di conservazione dei suoi dati personali e delle copie dei suoi documenti di identità (consegnati in sede di richiesta di attivazione della sim), senza ricevere riscontro. Ribadisce quindi di esser stato vittima di un episodio di *sim swap fraud* e sostiene che l'operazione di modifica dell'utenza telefonica sulla quale sarebbero pervenute le OTP, utilizzate nel caso di specie, abbia avuto rilievo determinante nella realizzazione dell'operazione fraudolenta. Sottolinea in particolare che "l'operazione di modifica dell'utenza telefonica sulla quale ricevere la OTP o la semplice possibilità di venire a conoscenza del numero di telefono, può rischiare di svuotare la password dinamica della propria funzione protettiva di verificare la genuinità dell'operazione, e dunque costituisce di per sé un'operazione o una situazione anomala" e che "a nulla pertanto valgono le considerazioni di controparte relative al richiamo dell'sms del 17/8/2020, h. 11.43, visto che tale utenza telefonica era stata generata, a seguito del Sim Swap Frauding, pochi minuti prima […] ed era in possesso del soggetto che ha frodato il Sig. C.". Obietta inoltre che l'intermediario non ha adempiuto all'onere di provare la colpa grave del ricorrente.
Parte ricorrente chiede pertanto il rimborso delle somme sottratte, al netto di quanto già recuperato dalla banca, per un importo complessivo quantificato in euro 10.629,40, oltre alla rifusione delle spese di assistenza professionale.
2. L'intermediario resistente, con le proprie controdeduzioni, afferma che il ricorrente è titolare di un conto corrente abilitato al servizio di *home banking* e che quest'ultimo consente l'accesso al servizio di *inquiry* e la realizzazione di operazioni dispositive, mediante un sistema di autenticazione forte. L'intermediario sostiene in particolare che, ai fini dell'accesso alla *home banking* da *App*, sono necessari i seguenti passaggi: i) "per effettuare il login e le operazioni di inquiry, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (One Time Password), generato da Mobile Token"; ii)"per disporre le operazioni, dopo avere effettuato la login come sopra e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP (One Time Password), generato da Mobile Token". Afferma inoltre che l'attivazione del *Mobile Token* è avvenuta tramite la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via sms al numero di cellulare collegato all'*home banking*. Parte resistente sostiene che, nel

caso di specie, il ricorrente ha attivato il *mobile token* sul dispositivo in suo possesso il 13/08/2020.L'intermediario richiama inoltre le campagne informative intraprese per sensibilizzare la clientela circa i rischi di frode legati all'operatività *online* e sottolinea la "bontà" ed intrinseca sicurezza dei sistemi di autenticazione forte. Sostiene che "la frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai presunti frodatori, delle credenziali di accesso all'home banking" e ipotizza "che i presunti malfattori siano entrati in possesso del codice Pin e codice cliente, […] necessari per accedere all'home banking, a causa di un'incauta conservazione degli stessi". Contesta al ricorrente di aver atteso nove giorni prima di verificare i motivi del mancato funzionamento della propria carta di credito e del proprio cellulare, il che integrerebbe una negligenza inescusabile. Rileva che "è lo stesso ricorrente che nell'ambito della dettagliata descrizione del tipo di frode subita, conferma che la sostituzione della SIM è preceduta dalla sottrazione di vari dati, tra cui i dati di accesso (credenziali di sicurezza) ai servizi di home banking". Quanto alla dinamica delle operazioni in contestazione, la banca, nel confermare quanto già dedotto dal ricorrente, afferma che: "in data 17.08.20, dopo avere scaricato l'app … inserendo le credenziali di sicurezza dell'home banking (utilizzando ID cliente + PIN noto solo al ricorrente) già in suo possesso, perché apprese dal ricorrente, il presunto frodatore ha attivato il mobile token inserendo il codice OTP che aveva ricevuto via SMS il 17/8/2020 alle ore 11:43 […] sul proprio device ed ha potuto disporre operazioni". Afferma quindi l'estraneità della banca alla vicenda in esame, nella quale la frode realizzata in danno del ricorrente è imputabile "alla negligenza o peggio alla connivenza degli addetti agli store telefonici". Contesta altresì la "genericità" della ricostruzione dei fatti fornita dal ricorrente, il quale avrebbe omesso di dichiarare "come si sono svolti i fatti antecedenti alla scoperta della mancanza di linea sul telefono e quindi della asserita frode, in quanto necessariamente deve essere intervenuto un momento in cui ha rivelato a terzi almeno il ID Utente ed il PIN (noti solo alla ricorrente) per poter scaricare in autonomia APP, MT dopo lo SIM Swapping". L'intermediario precisa che le operazioni contestate sono state correttamente autenticate, registrate e contabilizzate, senza anomalie. Richiama inoltre i contenuti dei *log* allegati, in base ai quali il cliente: "ha attivato il Mobile Token (nickname 242290) in data 2020-08-17 11:44:47.383 mediante inserimento di Pin e utilizzando l'OTP (07221532) ricevuto via SMS; ha inserito il Bonifico in data e ora 2020-08-17 11:49:50.486 di euro 14.400,00 verso il beneficiario ***** con Iban **********457 (causale pagamento fattura), firmata con Strong Customer Authentication, in particolare con PIN e OTP (47202743) generato da Mobile Token con id operazione 23244230".Con riferimento alle operazioni effettuate con carta di pagamento, la banca sostiene che le stesse sono state realizzate previa "digitalizzazione delle carte di credito e di debito intestate al ricorrente utilizzando l'App **** che il frodatore ha attivato sul proprio device, come risulta dal dettaglio degli SMS". Produce i *log* relativi a dette operazioni, dai quali – a suo dire – emerge quanto segue:"- nella prima schermata di ciascuna operazione sono riportati i dettagli del pagamento: numero carta, importo, data, ora, rifermenti del fornitore;- nella seconda schermata di ciascuna operazione è riportato il codice PosEntryMode: 07, che identifica le operazioni eseguite tramite POS in modalità Contactless, cioè effettuate ponendo la carta digitalizzata a contatto con il Pos;- nella terza schermata di ciascuna operazione, è riportato il codice wallet id 127, che identifica le operazioni eseguite con carta digitalizzata su wallet *****". Parte resistente afferma, ad ogni modo, che anche queste operazioni "risultano correttamente autenticate, registrate ed eseguite senza che sia emerso alcun malfunzionamento o compromissione dei sistemi della Banca". L'intermediario precisa, inoltre, di aver invitato il ricorrente a rivolgersi alla propria compagnia assicurativa, con la quale aveva sottoscritto una polizza legata alla carta, per

verificare la possibilità di attivare la copertura. Conferma infine di aver riaccreditato al ricorrente l'importo di euro 4.230,00 in relazione al bonifico in contestazione.
Parte resistente chiede pertanto il rigetto del ricorso avversario, ivi inclusa la eventuale domanda di rifusione delle spese legali.
3. Nelle successive repliche parte ricorrente rileva che l'intermediario sostiene che l'utente avrebbe rivelato a terzi le proprie credenziali di accesso all'*home banking* o abboccato a un tentativo di *phishing*, sulla base di mere supposizioni, quando l'art. 10, comma 2, d.lgs. n. 11/2010, impone alla banca l'onere di provare la colpa grave del ricorrente. Quanto al presunto ritardo nel disconoscimento delle operazioni, il ricorrente afferma di non essere stato in grado di attivarsi prima del rientro in patria. Sottolinea come in casi del genere il ricorrente non si trova immediatamente nella possibilità di associare il malfunzionamento della sim a un evento fraudolento. In ogni caso, sostiene che, trovandosi all'estero senza telefono, in assenza di filiali dell'intermediario e di un centro di assistenza del proprio operatore telefonico, non poteva che attendere il rientro in Italia per adottare qualsivoglia iniziativa. Precisa che nessuna negligenza gli può essere addebitata per i fatti posti in essere da personale riferibile al gestore telefonico. Evidenzia che nel caso di specie non si discute dell'autenticazione e contabilizzazione delle singole operazioni dispositive, ma di come un terzo abbia potuto attivare, all'insaputa del ricorrente, una nuova sim ponendo in essere, sei minuti dopo, le operazioni fraudolente. Rileva ancora che i *log* prodotti dall'intermediario, lungi dal provare una colpa grave del ricorrente, rivelerebbero piuttosto l'utilizzo del portale di *home banking* del ricorrente senza alcun controllo da parte della banca. A tal riguardo, il ricorrente sottolinea come i *log* evidenzino 20 tentativi di accesso in 8 giorni e che, il 21/08/2020, il *mobile token* sarebbe stato attivato per 4 volte, utilizzando un telefono diverso da quello impiegato per gli accessi precedenti. Contesta che, a fronte degli utilizzi anomali, l'intermediario non ha comunicato nulla al cliente, quando avrebbe potuto utilizzare il canale email o il numero fisso per farlo. Aggiunge di essere stato avvertito solo il 26/08/2020, una volta riattivata la propria sim. A detta del ricorrente, la condotta dell'intermediario, che gli ha rimborsato il minor importo di euro 4.230,00, è in contraddizione con la tesi di una presunta colpa grave dell'utente. Quanto alle operazioni con carta, parte ricorrente afferma che le stesse sono avvenute con modalità *contactless* e richiama le considerazioni già svolte con riferimento all'operazione di bonifico. Con riferimento alla domanda di rimborso delle spese di assistenza professionale, il ricorrente sostiene che l'assistenza tecnica si è resa necessaria a causa del comportamento ostile e ostruzionistico dell'intermediario, il quale in sede di reclamo preventivo ha omesso di produrre qualsivoglia documento inerente alle operazioni in contestazione.
Parte ricorrente insiste pertanto per l'accoglimento del ricorso.
4. Con le proprie controrepliche, la banca afferma che, se il ricorrente si fosse realmente trovato nella situazione descritta (all'estero senza accesso ai fondi e senza telefono), difficilmente avrebbe potuto continuare la vacanza. Ipotizza che egli avrebbe potuto reperire un telefono per comunicare con la famiglia o con la banca, anche dall'estero. Afferma che la mera sostituzione della *sim card* non consente di accedere automaticamente all'*home banking*, senza conoscerne le credenziali di accesso. Rileva, in altre parole, che non sarebbe possibile generare la OTP necessaria all'attivazione della *app* senza conoscere id cliente e codice PIN. Ribadisce che non è emersa alcuna anomalia nel funzionamento del sistema di autenticazione dell'intermediario e che i tentativi di accesso evidenziati nei *log* e le corrispettive richieste di autenticazione, mediante inserimento del doppio fattore di autenticazione, non rivelano nulla di anomalo. Quanto all'utilizzo di un dispositivo differente rispetto a quello precedentemente impiegato, l'intermediario precisa che il sistema consente l'attivazione della *app* su due distinti

dispositivi. In merito al parziale rimborso riconosciuto al ricorrente, sostiene infine che non si tratta di una "elargizione liberale" della banca, ma della somma che l'intermediario è riuscito a recuperare direttamente dal conto del malfattore.
Per quanto sopra, e per le ragioni altresì esposte nelle controdeduzioni, l'intermediario resistente chiede il rigetto del ricorso avversario.

**DIRITTO**

1. La presente controversia ha ad oggetto il disconoscimento di n. 11 operazioni di pagamento a mezzo carta digitalizzata e di un bonifico *online*, a valere sul conto corrente del ricorrente.
Le operazioni, di ammontare complessivo pari a euro 10.589,40, sono avvenute tra il 17/08/2020 e il 20/08/2020 e, dunque, risultano essere state effettuate nel vigore della Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta *PSD* 2 - *Payment Services Directive* 2), recepita con il d.lgs. n. 218 del 2017 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.
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*, commi1, 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.
2. La nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un cd. "sistema di autenticazione forte". Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis* del predetto d. lgs. n. 11/2010, 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".
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.
3. Qualora il prestatore di servizi di pagamento abbia adottato un sistema di autenticazione forte del cliente, si ricade nelle fattispecie regolate dai commi terzo e quarto dell'art. 12 d.lgs. n. 11/2010. In base al primo, "salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Mentre, ai sensi del secondo, "qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3". A sua volta, l'art. 7 del decreto prevede gli obblighi che l'utente dei servizi di pagamento deve osservare in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate. In particolare, il comma primo, lett. a) impone a costui di "utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso", mentre il comma secondo dispone che, ai fini del corretto utilizzo dello strumento di pagamento, "l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate". Il Provvedimento della Banca d'Italia del 5/07/2011 di *Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)* ribadisce e precisa le suddette previsioni normative.
Va altresì richiamatala previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs. n. 218/2017], in relazione alla *prova di autenticazione ed esecuzione delle operazioni di pagamento*: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già 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 comma secondo della medesima norma precisa che: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente 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. 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".
4. Nel caso di specie, il ricorrente sostiene che le operazioni dispositive contestate nel ricorso sono state realizzate a seguito di un episodio di *sim swap fraud*. Al riguardo, allega di aver richiesto, in data 12/08/2020, presso un centro di telefonia sito in Roma, il rilascio di una nuova *sim card* abbinata al proprio numero telefonico, consegnando a tal fine al personale competente copia dei propri documenti di identità. Riferisce altresì di aver attivato, il giorno seguente, la *token app* dell'intermediario e di essere quindi partito, in

data 15/08/2020, per la Croazia. Allega, a supporto di tale affermazione, i titoli di viaggio e le ricevute di prenotazione di soggiorni in Croazia a lui intestati, relativi al periodo 15-25/08/2020. Afferma, infine, che, a partire dal 17/08/2020 il suo telefono cellulare non ha avuto più linea e non gli è stato più consentito di effettuare operazioni di pagamento con la carta. Produce sul punto una serie di ricevute (in lingua straniera), che riferisce essere inerenti a pagamenti e tentativi di prelievo non andati a buon fine, effettuati in Croazia in quei giorni. In base a quanto trascritto nei verbali di denuncia allegati, il ricorrente avrebbe anche tentato di accedere all'*app* bancaria, senza riuscirvi, in quanto il sistema non avrebbe riconosciuto le credenziali inserite. Infine, il ricorrente sostiene di avere appreso, solo al momento del rientro in Italia, che, in data 17/08/2020, la sua sim era stata disattivata a seguito di denuncia di furto e che, su richiesta di terzi, ne era stata attivata una nuova. Allega al riguardo il tabulato rilasciato presso il centro di assistenza riferibile al gestore telefonico.
Dalle affermazioni del ricorrente emerge peraltro che l'ultimo utilizzo della carta, a lui riconducibile, è avvenuto in Croazia (a Zadar) il 16/08/2020 e dalle allegazioni della banca si evince che le successive operazioni effettuate con lo stesso strumento di pagamento (e disconosciute dal ricorrente) sono state realizzate in Sardegna.
5. Alla luce delle affermazioni di parte ricorrente e della documentazione prodotta agli atti, il Collegio ritiene verosimile l'avvenuta sostituzione della sim del cliente e, dunque, la riconducibilità della frode da questi subita alla fattispecie della *sim swap fraud.*
Al riguardo, è orientamento condiviso dai Collegi territoriali dell'ABF quello secondo cui una "*la sostituzione della sim card va (…) equiparata alla mancanza di autenticazione dell'operazione di pagamento*", ai sensi dell'art. 10 del d.lgs. n. 11/2010. In particolare, diversamente da altre fattispecie – come quella nota con l'espressione *man in the browser* – in cui la valutazione della vicenda rientra nell'ambito dell'art. 12 d.lgs. n. 11/2010 e riguarda i profili di colpa dell'utente, nei casi di *sim swap fraud* l'operazione di pagamento non può ritenersi "regolarmente autenticata" e la fattispecie va dunque affrontata alla luce della previsione di cui all'art. 10 del menzionato decreto.
La *sim swap fraud* si caratterizza per essere una fattispecie nella quale, dopo il furto di identità e la captazione dei dati di accesso relativi al servizio di *home banking*, la sim del cliente viene duplicata o sostituita dai malfattori, in maniera tale da deviare su una diversa utenza telefonica i messaggi provenienti dalla banca contenenti i codici autorizzativi delle operazioni *online*. Tale particolare modalità di sottrazione dell'identità (telefonica) del cliente è destinata ad esautorare la funzionalità protettiva del sistema di autenticazione multifattoriale, pur in astratto predisposto dall'intermediario, essendo l'utenza telefonica – modificata dai malfattori – il naturale canale di ricezione dei codici OTP. In particolare, viene meno il requisito dell'indipendenza dei fattori di autenticazione, in quanto "*la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità dell'altra, quando, al contrario, la piena operatività del sistema di autenticazione multifattore si fonda sull'indipendenza tra le singole misure di sicurezza*" (cfr., tra gli altri, Collegio di Roma, decisione n. 11777/2019; Collegio di Milano, decisione n. 1066/2019).
In conseguenza della sostituzione della sim dell'utenza telefonica associata al servizio di *home banking*, si deve ritenere che manchi l'autenticazione delle operazioni di pagamento, ai sensi e per gli effetti dell'art. 10 d.lgs. n. 11/2010, e che parte ricorrente abbia diritto al rimborso integrale della somma sottratta all'esito delle operazioni fraudolente.
6. A rafforzare tale conclusione appare altresì significativa la circostanza per cui, sulla base della documentazione versata in atti, nella giornata del 20/08/2020 sono state effettuate nove operazioni di pagamento con la medesima carta di pagamento.
Tale circostanza vale quale elemento sintomatico di un rischio di frode in base alle previsioni del d.m. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto

2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento". In particolare, ai sensi dell'art. 8, comma 1, lett. b), n. 1) del decreto, si configura un rischio di frode con riguardo alle carte di pagamento quando si verificano "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento". In un caso del genere, è necessaria una valutazione circa i presidî adottati dall'intermediario, come per esempio l'esistenza di un sistema di monitoraggio.
Gli stessi *Orientamenti finali sulla sicurezza dei pagamenti via internet* – adottati il 19 dicembre 2014 dall'Autorità Bancaria Europea e recepiti in Italia, nel maggio 2016, con il 16° aggiornamento alla Circolare n. 285/2013, nella parte prima.IV.4.24 – raccomandano l'adozione di sistemi di monitoraggio delle operazioni in grado di rilevare modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente. Più in dettaglio, al punto 10 si afferma che: "I meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti dovrebbero essere attivati prima dell'autorizzazione finale del prestatore di servizi di pagamento; le operazioni sospette o ad alto rischio dovrebbero essere oggetto di una specifica analisi e procedura di valutazione". E al punto 10.1 si precisa che: "I prestatori di servizi di pagamento dovrebbero utilizzare sistemi di rilevamento e prevenzione delle frodi per individuare operazioni sospette prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici. Tali sistemi dovrebbero essere basati, per esempio, su regole parametrizzate (come le "Black-list" dei dati relativi alle carte compromesse o rubate) e monitorare i modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente".
Orbene, è orientamento costante di questo Arbitro (cfr. Collegio di Roma, decisioni n. 1785/2018, n. 3932/2017, n. 4712/2017 e n. 11027/2017) quello secondo cui l'intermediario diligente *ex* art 1176 c.c. è gravato dell'obbligo di predisporre un sistema di monitoraggio della carta di pagamento (ai fini del possibile blocco della stessa) in relazione ad operazioni anomale per frequenza e tipologia, idonee a configurare un rischio di frode oggettivo, imminente e rilevabile attraverso l'analisi delle informazioni riguardanti le transazioni "sospette".
Nel caso di specie, considerata l'anomalia nell'utilizzo della carta di pagamento, l'adozione da parte dell'intermediario di un apposito meccanismo di monitoraggio delle operazioni (per esempio, con un sistema automatico di blocco) avrebbe potuto prevenire il traffico di una parte dei pagamenti fraudolenti, riducendo le conseguenze negative per il cliente.
7. Nel ricorso introduttivo parte ricorrente chiede il rimborso di "tutte le spese sostenute per la presente procedura". Tuttavia, non produce alcuna documentazione al riguardo, né tantomeno una parcella che attesti le spese sostenute.
Una simile pretesa non può pertanto essere accolta.
8. Ai sensi delle *Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*, gli importi indicati nel dispositivo della presente decisione sono arrotondati all'unità di euro (per eccesso se la prima cifra dopo la virgola è uguale o superiore a 5; per difetto, se la prima cifra dopo la virgola è inferiore a 5).

**PER QUESTI MOTIVI**

**Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 10.589,00. Respinge nel resto.**
**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
FERNANDO GRECO