Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SCIUTO	Presidente
(RM) PROTO	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del21/09/2020

Esame del ricorso n. 0285450/2020 del 28/02/2020

proposto da Savelli Pierluigi

nei confronti di 3442 - WIDIBA

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SCIUTO	Presidente
(RM) PROTO	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del 21/09/2020

FATTO

1. L'odierno ricorrente premette di utilizzare il conto *on line*, detenuto presso l'intermediario convenuto, esclusivamente per investimenti di breve termine e di eseguire le operazioni sempre presso i locali della banca, con l'assistenza del proprio consulente e usufruendo del suo computer. Sostiene di aver ricevuto, in data 4 maggio 2019, due SMS per confermare, attraverso un *link* ipertestuale, l'esecuzione di un bonifico di euro 20.000 a valere sul suddetto conto. Afferma di non aver dato seguito a tali messaggi, ritenendoli frutto di comunicazioni illecite. Rileva però che, da tale data, si sono susseguite diverse attività non autorizzate sul proprio conto, in relazione alle quali non ha mai ricevuto alcuna comunicazione da parte della banca. In particolare, il ricorrente segnala le seguenti movimentazioni: in data 8 maggio 2019, sono stati liquidati anticipatamente alcuni depositi vincolati a lui intestati, rispettivamente di euro 50.000 e di euro 40.000, al fine di alimentare la provvista sul conto in vista del bonifico fraudolento; in data 9 maggio 2019, è stato aperto un deposito vincolato a suo favore, per euro 30.000, e contestualmente è stato predisposto un bonifico di euro 60.000 a beneficio del Sig. Mxxx Pxxx; il ricorrente

sostiene di essersi recato, nel medesimo giorno – dopo essersi avveduto che il proprio cellulare non era funzionante –, presso un centro assistenza e di aver appreso che la sua SIM non risultava più attiva, provvedendo dunque alla sostituzione della stessa; in data 13 maggio 2019, è stata eseguita una ricarica telefonica di euro 60 su una diversa utenza telefonica; in data 14 maggio 2019, è stato liquidato anticipatamente il deposito vincolato aperto il 9 maggio 2019; il ricorrente afferma di aver riscontrato sulla SIM, nel medesimo giorno, lo stesso problema rilevato pochi giorni prima e di essersi recato presso il centro assistenza, provvedendo a una nuova sostituzione della scheda; in data 15 maggio 2019, la banca lo contatta via filo per chiedergli conferma dell'esecuzione di un bonifico di euro 32.000 a beneficio del Sig. Sxxx Axxx; al riguardo, il ricorrente afferma di aver negato la genuinità di questa nuova operazione e di aver chiesto il blocco del conto, nonché di aver comunicato l'accaduto al proprio consulente e sporto querela presso la P.G. Così ricostruita la vicenda, il ricorrente prospetta di essere stato vittima di una duplice ipotesi di *Sim Swap Fraud*, verosimilmente consumatasi, nella prima occasione, in un periodo precedente all'8 maggio e, nella seconda occasione, in un periodo compreso tra il 10 maggio e il 13 maggio. Ha dunque reclamato la restituzione dell'importo di euro 60.000 oggetto del bonifico fraudolento del 9 maggio 2019, lamentando la mancata predisposizione, da parte della banca, di idonei presidi di sicurezza volti all'intercettazione e alla neutralizzazione di possibili transazioni fraudolente. Rileva che il *vulnus* al sistema di autenticazione multifattoriale emerge direttamente dal *log* informatico inoltrato dalla banca, in sede di riscontro al reclamo. Da tale evidenza ricava che risultano censite le attività anomale, senza che l'intermediario – oltre all'invio degli SMS, peraltro mai ricevuti dal ricorrente a causa della clonazione della SIM – abbia eseguito ulteriori attività di verifica della genuinità delle operazioni o abbia previsto il blocco preventivo di quelle sospette. Aggiunge che, con riguardo al bonifico contestato, la banca ha dichiarato di aver contattato via filo il cliente – continuando dunque a utilizzare un canale di comunicazione ormai compromesso – per sottoporgli delle domande, relative ai propri dati personali, a scopo di verifica della correttezza del pagamento inoltrato. Ritiene che il soggetto che ha risposto abbia potuto fornire tutti i dati richiesti, agevolmente reperibili sul portale del conto e anche sul suo sito internet personale. Con il presente ricorso il ricorrente chiede il rimborso dell'importo di euro 60.000,00, relativo al predetto bonifico disconosciuto, oltre agli interessi e alla rifusione delle spese di assistenza professionale pari a euro 800,00.

2. Parte resistente, con le proprie controdeduzioni, afferma che la liquidazione anticipata dei depositi vincolati e il bonifico disconosciuto sono stati preceduti dall'avviso di "accesso insolito", inoltrato al cliente su tre canali distinti (sms, *push-up* su App e mail). Con riguardo ai depositi vincolati, la banca sostiene di aver inviato anche il documento di sintesi via PEC. Rileva che, successivamente, il bonifico disconosciuto è stato perfezionato inserendo correttamente il codice OTP inoltrato via SMS. Con riguardo a tali comunicazioni, l'intermediario allega gli estratti dei *log* informatici con le coordinate

temporali e l'esito di tutte le notifiche delle varie transazioni eseguite nella vicenda. Ciò premesso, la banca ritiene gravemente negligente la condotta del ricorrente che, già il 4 maggio 2019, era rimasto vittima di un primo tentativo di bonifico fraudolento (di euro 20.000) ma che, in quell'occasione, aveva deciso di non allertare la banca circa la ricezione dei due SMS contenenti un *link* ipertestuale di conferma. Osserva al riguardo che la segnalazione tempestiva da parte del cliente avrebbe consentito alla banca di intervenire prontamente per evitare successive transazioni fraudolente. Con riguardo all'operazione contestata, la banca precisa che la stessa è stata preceduta dal corretto inserimento delle credenziali di accesso al conto e del codice OTP inviato via SMS. Aggiunge che, poiché la transazione si discostava dalla consolidata operatività del cliente, l'ufficio antifrode ha deciso di sospenderne l'esecuzione e di attivare l'ulteriore presidio di controllo, via filo, della genuinità di alcuni dati non visibili sul portale del conto (ad es., il numero del documento d'identità). Da quanto sopra parte resistente ricava, a fronte dell'adozione di molteplici presidi di sicurezza, la sussistenza di una condotta gravemente negligente in capo al ricorrente cui sono stati carpiti, nel caso di specie, sia le credenziali per accedere al conto, sia alcuni dati personali utilizzati durante l'ulteriore contatto telefonico con la banca. Infine, la banca resistente evidenzia di essersi immediatamente attivata, una volta scoperta la frode, per richiamare il bonifico, contattando la banca del beneficiario ed ottenendo dalla stessa il vincolo cautelativo dell'importo residuo sul conto di quest'ultimo, pari a euro 15.500, come da mail allegata. Ritiene che, anche laddove sia accertata la sua responsabilità nella vicenda in esame, il pregiudizio sofferto dal ricorrente sarebbe pari a euro 44.500. Parte resistente chiede pertanto il rigetto del ricorso.

3. In sede di repliche, il ricorrente, oltre a reiterare le argomentazioni formulate negli scritti precedenti, censura la condotta dell'intermediario che, nella vicenda in esame, non ha mai contattato il proprio consulente, circostanza che avrebbe evitato l'operazione contestata, considerato che il cliente operava esclusivamente con l'assistenza del primo. Osserva poi che, in occasione del blocco del conto, la banca ha richiesto al ricorrente l'invio di una registrazione video durante la quale egli, inquadrato in viso, ha fornito le proprie generalità. Ne ricava che un simile presidio di sicurezza, se fosse stato utilizzato anche con riguardo alla transazione fraudolenta, ne avrebbe impedito l'esecuzione. Ancora, il ricorrente ribadisce che i propri dati personali – a differenza di quanto sostenuto dalla banca – risultano agevolmente reperibili sul portale del conto e allega alcuni *screenshot* della propria area personale. Ritiene che tale possibilità abbia neutralizzato il sistema di autenticazione multifattoriale, minando l'indipendenza dei due fattori predisposti, e abbia agevolato i terzi ignoti nella clonazione della scheda SIM. Per quanto attiene, infine, alle varie comunicazioni inoltrate dalla banca, il ricorrente precisa che: a) l'intermediario non ha fornito la prova dell'invio e della ricezione delle mail, se non con un estratto di *log* informatici di cui si contesta tuttavia la genuinità probatoria, essendo privi di una firma elettronica o di una marca temporale; b) le notifiche *push* non sono mai state ricevute dal

cliente perché questi non ha installato l'App di IHB, peraltro non obbligatoria; c) gli SMS, anche laddove inviati e ricevuti, sono stati captati dai terzi ignoti. In conclusione, il ricorrente insiste per l'accoglimento del ricorso, chiedendo inoltre lo sblocco del conto e la restituzione delle somme su di esso attualmente depositate, pari a euro 32.000,00, nonché il pagamento degli interessi e la rifusione delle spese di assistenza professionale per euro 2.990,00.

4. Nelle proprie controrepliche, la banca ribadisce quanto già sostenuto nelle controdeduzioni, precisando di essere tenuta a informare soltanto il cliente, e non i propri consulenti, della rilevazione di anomalie relative al conto.

DIRITTO

1. La presente controversia verte su una frode *on line*, subita dall'odierno ricorrente in relazione al servizio di *home banking* messo a sua disposizione dall'intermediario convenuto.

In via pregiudiziale, va segnalato che il ricorrente chiede lo sblocco e la restituzione delle somme giacenti sul proprio conto corrente, pari ad euro 32.000,00, solo in sede di repliche alle controdeduzioni dell'intermediario resistente.

Una simile domanda non può essere presa in considerazione, dal momento che è orientamento consolidato dell'Arbitro quello di ritenere inammissibili le domande nuove proposte in sede di repliche, dovendo queste ultime essere volte unicamente "*a ribadire e puntualizzare le rispettive posizioni delle parti*", in modo da non precludere il contraddittorio (così, *ex multis*, Collegio di Roma, decisioni n. 1995/2020 e n. 14088/2019).

2. In relazione alla domanda di rimborso della somma sottratta, va rilevato che il bonifico *on line* disconosciuto dal ricorrente, di ammontare pari a euro 60.000,00, è avvenuto in data 09/05/2019 e, dunque, risulta essere stato effettuato 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*, 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.

3. Ferma la suddetta precisazione in merito all'entrata in vigore delle disposizioni, in parte non ancora applicabili al momento dell'esecuzione delle operazioni qui contestate, 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.

4. 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 richiamata la 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".

5. Nel caso di specie, l'intermediario resistente ha fornito apposite evidenze circa l'autenticazione, la registrazione e la contabilizzazione dell'operazione contestata sia in fase di accesso sia in fase di esecuzione del bonifico, allegando un apposito *log* informatico. Da quest'ultimo si ricava che, in relazione alla fase di accesso, l'intermediario ha inviato tre notifiche di avviso di "accesso insolito" con le seguenti modalità: sms, *push notification* ed e-mail. Con riguardo alla fase di perfezionamento del bonifico contestato, dal log si evince che l'operazione di pagamento è stata preceduta dal corretto inserimento delle credenziali di accesso al conto e del codice OTP inviato via sms. Infine, in merito alla

verifica dei dati personali del ricorrente, la banca resistente afferma che il bonifico disconosciuto è stato intercettato dall'ufficio antifrode perché il suo importo si discostava dalla consolidata operatività del cliente e che il predetto ufficio ha attivato l'ulteriore presidio di controllo, via filo, della genuinità di alcuni dati personali del cliente (per esempio, il numero del documento di identità). Su quest'ultimo punto, l'intermediario allega una schermata dalla quale risulta l'avvenuto contatto del numero telefonico del titolare del conto, al fine della verifica di autenticità dell'operazione.

L'operazione di pagamento contestata è stata dunque effettuata mediante l'utilizzo di un sistema di protezione a due fattori che, per costante orientamento di questo Arbitro e di questo Collegio (cfr. Collegio di Roma, decisioni n. 3245/2019, n. 24759/2018, n. 16900/2018, n. 474/2018 e n. 6606/2016; v. pure Collegio di Milano, decisioni n. 3865/2019 e n. 3892/2019), si ritiene assicuri al cliente il massimo grado di protezione che l'intermediario può garantire con l'attuale stato della tecnologia. In particolare, esso preclude a terzi di utilizzare gli strumenti di pagamento del cliente se non conoscendo le sue credenziali. Dalla documentazione in atti, può ritenersi dunque che l'intermediario resistente abbia dato dimostrazione della vigenza, per le transazioni *on line* e, in particolare, per quella oggetto di contestazione, di un sistema di sicurezza a due fattori e dell'accessibilità dello stesso solo al cliente, con la conseguenza di ritenersi assolto l'onere della prova richiesta dall'art. 10 d.lgs. n. 11/2010 in merito all'autenticazione e alla corretta registrazione delle operazioni contestate.

6. In relazione alla condotta del ricorrente, nella veste di utente del servizio di pagamento, va rilevato che il Collegio di Coordinamento, con la recente decisione n. 22745/2019, ha enunciato il seguente principio di diritto: "*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*". Ha, tuttavia, precisato anche che, "*nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio possa comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso*".

Circa le modalità con le quali possono avvenire operazioni di pagamento fraudolente, il Collegio di Coordinamento, nella predetta decisione, ha rilevato che, "*nella casistica dei ricorsi esaminati dall'Arbitro, si rinvengono svariate ipotesi di intrusioni sofisticate, come, ad esempio, modifiche della linea telefonica associata agli strumenti di pagamento o installazione di App dell'intermediario su un device diverso da quello del ricorrente,*

escludendo in tal modo il cliente dalla fase conclusiva di autorizzazione dell'operazione fraudolenta (ad es., cfr. le decisioni Coll. Bari nn. 7225/19, 14530/18, 14190/17, Coll. Roma n. 10125/18, Coll. Bologna n. 4564/18). (…)".

7. A queste ipotesi di frodi sofisticate sembra riconducibile anche quella di cui è stato vittima il ricorrente nel caso in esame. Dalle affermazioni rese dallo stesso ricorrente e dalla documentazione versata agli atti la truffa sembra essersi realizzata mediante una frode particolarmente articolata, nota come *SIM swap fraud.* Il ricorrente lamenta, in particolare, il mancato funzionamento della propria *SIM card* in ben due occasioni, una delle quali risulta precedente all'effettuazione dell'operazione fraudolenta di bonifico. Gli inconvenienti di linea telefonica gli hanno imposto, in entrambi i casi, di sostituire la carta *SIM* con una nuova.

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 conto *home banking*, la *SIM* del cliente della banca 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 *on line*.

In simili casi, è orientamento consolidato di questo Collegio quello di ritenere che tale particolare modalità di sottrazione dell'identità (telefonica) del cliente esautori 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).

Nel caso che ci occupa, peraltro, il ricorrente contesta la visibilità, sul portale relativo al proprio conto corrente, dei dati personali che la banca afferma essere stati forniti durante il contatto telefonico. In effetti, sebbene parte resistente sostenga che tali dati – in particolare gli estremi del documento d'identità – non fossero immediatamente ricavabili dall'area personale, il ricorrente evidenzia come le domande poste dall'ufficio antifrode riguardassero informazioni agevolmente estraibili da tale area. Al riguardo, allega alcune schermate della procedura *on line* richiesta dalla banca per l'attivazione di una carta di debito, dalle quali si evince che, se un soggetto avesse accesso all'area personale del cliente e richiedesse il rilascio di una carta, il sistema predisporrebbe automaticamente il relativo contratto rendendo visibili tutti i dati personali del correntista, tra cui il numero di cellulare e gli estremi del documento d'identità.

A giudizio di questo Collegio, nella vicenda in esame l'intermediario non ha dunque fornito la prova della frode, del dolo o della colpa grave dell'utente, richiesta dall'art. 10, comma

2, d.lgs. n. 11/2010, né vi sono elementi tali da far presumere una colpa grave dell'utente sia in relazione alla captazione dell'*OTP* necessaria per l'effettuazione dell'operazione fraudolenta, sia per quanto concerne l'inosservanza del proprio obbligo di proteggere e mantenere segrete le credenziali di accesso al conto *on line* (in tal senso, con riguardo a una fattispecie analoga a quella ora in esame, cfr. Collegio di Roma, decisione n. 2431/2020).

8. Alla luce dei suddetti elementi di fatto e tenuto conto delle previsioni richiamate del d.lgs. n. 11 del 2010, si deve ritenere che la responsabilità dell'operazione fraudolenta oggetto di contestazione gravi sull'intermediario e che parte ricorrente abbia diritto ad ottenere il rimborso dell'importo ad essa corrispondente, al netto della franchigia di cui all'art. 12, comma 3, d.lgs. 11/2010.

Resta ferma la possibilità, per l'intermediario resistente, che ha dato corso alla procedura di richiamo del bonifico fraudolento nei confronti della banca del beneficiario, di recuperare da quest'ultima la somma di euro 15.500,00, assoggettata a vincolo cautelativo.

9. In relazione alla domanda di rifusione delle spese di assistenza professionale, quantificate in sede di ricorso in euro 800,00, va rilevato che la domanda era presente anche nel reclamo e risulta supportata da tre fatture, prodotte dal procuratore del ricorrente, per una somma complessiva di euro 2.990,00.

La domanda va dunque accolta e liquidata, in via equitativa, nell'importo di euro 500,00.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 59.950,00, con interessi legali dalla richiesta al saldo, nonché l'importo di euro 500,00 per spese di assistenza professionale.

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
MAURIZIO SCIUTO