Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) SCIUTO	Membro designato dalla Banca d'Italia
(RM) SIRGIOVANNI	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SCIUTO MAURIZIO

Seduta del 21/06/2021

FATTO

1. Espone il ricorrente di essere titolare di un rapporto di conto corrente cointestato con la moglie, nonché titolare di una carta di debito rilasciata dalla banca convenuta. In data 4.9.2019, al ritorno dalle vacanze, si accorgeva di avere il conto in rosso: esaminato l'estratto conto, si avvedeva infatti di cinque operazioni fraudolente di importo complessivamente pari ad € 11.609,98 (un prelievo di € 4.990,00 in data 1.8.2019; due pagamenti *online* con carta, per € 869,00 e, rispettivamente, € 1.099,00 in data 16.8.2019; due bonifici *online*, per € 3.124,99 in data 28.08.2019 e, rispettivamente, € 1.526,99 in data 2.9.2019). Chiedeva allora il blocco della carta, sporgendo denuncia e disconoscendo le operazioni presso l'intermediario.
   Nel verbale di denuncia il ricorrente ha precisato di esser solito accedere alla *home banking* tramite *app*, inserendo codici personali e il codice *otp* generato da *token* fisico e di non aver mai comunicato le credenziali a terzi; riferisce di non aver utilizzato la carta, né effettuato operazioni tramite *home banking*, né ricevuto *sms* di notifica sul proprio cellulare, dopo il 1.8.2019. A seguito di successivi accertamenti, sarebbe emerso che in data 1.8.2019 il numero di cellulare abbinato alla carta sarebbe stato sostituito, come numero abilitato ai fini del servizio di *home banking,* con altro numero non riconducibile al ricorrente, e che i limiti di prelievo giornaliero sarebbero stati elevati da € 250,00 a € 5.000,00.

Nella stessa giornata, inoltre, la stessa utenza abilitata sul dispositivo di parte ricorrente risultava disattivata, il che non era stato richiesto al gestore telefonico dell'utenza stessa; nella stessa giornata, quindi, parte ricorrente contattava il gestore e riattivava l'utenza.

Ciò nonostante, la banca negava ogni responsabilità e non concedeva alcun rimborso.

Tanto premesso, il ricorrente invoca la responsabilità contrattuale della banca per non aver adottato tutte le cautele del caso, sostenendo che la sottrazione dei codici del correntista rientra nel rischio di impresa dell'intermediario sul quale grava l'onere di dimostrare la condotta colposa del danneggiato. Afferma inoltre che nella fase di preventivo reclamo, la banca riteneva che le operazioni fraudolente fossero state ordinate da *smartphone* di marca A****I, accedendo al sito di home banking tramite *app* e mediante l'autenticazione forte, che prevede l'inserimento del numero cliente, il Pin ed il codice Otp dinamico; il ricorrente sostiene tuttavia di non aver mai posseduto uno *smartphone* di quella marca e di non aver mai attivato il *token* virtuale. In definitiva, la sottrazione delle credenziali del ricorrente sarebbe imputabile al solo intermediario.

Tanto premesso, il ricorrente chiede il rimborso della somma indebitamente sottrattagli per effetto delle cinque operazioni disconosciute, al netto dell'eventuale franchigia di legge.

2. Nelle sue controdeduzioni, l'intermediario afferma che il ricorrente è titolare di conto un corrente abilitato ai servizi di *home banking* al quale si accede, sia per le funzioni di *inquiry* che dispositive, mediante un sistema di autenticazione "forte": inserimento delle credenziali di accesso (numero cliente + PIN), per effettuare il login; PIN + One Time Password /OTP per disporre le operazioni. Aggiunge che nel periodo ante 14.9.2019, prima cioè dell'entrata in vigore delle nuove norme introdotte dalla PSD2, l'Otp poteva essere generato anche da *token* fisico.

   Tanto precisato, la banca contesta la negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento, affermando che il ricorrente sarebbe rimasto vittima di un episodio di "*sim swapping*", come sarebbe desumibile dai contenuti del verbale di denuncia. Sottolinea come la carta *sim* disattivata fosse intestata alla figlia del ricorrente e che tale "promiscuità" non consentirebbe di stabilire se l'utenza telefonica fosse in uso completo al ricorrente oppure se il dispositivo in questione venisse dallo stesso utilizzato solo per le transazioni e/o le consultazioni sul sito. Contesta altresì la condotta del ricorrente che, a seguito della disattivazione della *sim*, non ha ritenuto di approfondire l'evento; circostanza questa che avrebbe potuto impedire le operazioni in contestazione.

   Quanto alle conseguenze dell'episodio di *swapping*, la banca afferma che i frodatori, una volta appropriatisi dell'utenza telefonica, sarebbero stati in grado di installare la *app* telefonica e il mobile *token* su dispositivo in loro possesso; dispositivo presso il quale sono stati recapitati gli *sms alert* relativi alle operazioni fraudolente. Nel caso di specie "*il Mobile Token è stato attivato in data 1.8.2020 alle ore 12:16:40, proprio nella giornata in cui il ricorrente dichiara che il suo cellulare, numero *******005 era stato disattivato, infatti l'sms con il "codice riservato" risulta inviato ad altro cellulare numero *******329*".

   La banca precisa tuttavia che la conoscenza delle sole credenziali statiche (numero cliente e PIN) non sarebbe sufficiente ad accedere al *mobile token*, perché in ogni caso sarebbe necessario attivare il servizio *mobile token* con il numero (OTP) inviato dalla banca al telefono del cliente. Rileva a tale riguardo che se l'ipotetico frodatore cambiasse il numero di telefono in anagrafe, il cliente riceverebbe un SMS al vecchio numero, una e-mail, un messaggio nella *message box* e una notifica *push*; tuttavia, nel caso in esame "ciò non è avvenuto, verosimilmente perché le credenziali sono state

carpite al ricorrente, probabilmente tramite un *phishing* telefonico o via e-mail, in epoca antecedente alla frode stessa".

Quanto alle singole operazioni in contestazione, l'intermediario precisa che:

(i) la prima operazione, di prelievo, è stata eseguita in modalità *cardless*, ovvero tramite l'inserimento delle credenziali di sicurezza previste per l'accesso all'home banking (numero cliente e codice segreto PIN) e, all'atto della conferma dell'operazione, del codice OTP "dinamico" (valido solamente per una singola operazione dispositiva) in analogia a quanto previsto per l'esecuzione di operazioni sui canali diretti" (all. 4);

(ii) le due successive operazioni di pagamento sono state invece poste in essere *on line* tramite carta di debito con PAN n. ********9672;

(iii) quanto alle due successive operazioni di bonifico online l'intermediario richiama invece i contenuti dei Log (all. 7 e 8) per affermare che: il 28.8.2019 alle ore 13:31 è stato effettuato Login mediante inserimento di pin, con verifica a 2 fattori, utilizzando l'OTP generato dal Mobile Token; alle ore 13.34 è stato quindi inserito un bonifico di € 3.124.99 validato con PIN e OTP generato da Mobile Token; con le stesse modalità, in data 28.08.2019, alle ore 13:39 e il 29.08.2019 alle ore 20:01 sono stati inseriti due bonifici di importo pari a € 1.938,00, bloccati dall'intermediario. Infine il 2.9.2019 alle ore 9:21 è stato effettuato nuovo login mediante inserimento di pin e verifica a 2 fattori, utilizzando l'OTP generato dal Mobile Token; alle ore 9.23 è stato inserito un bonifico di € 1.526,99 verso il beneficiario ***** spa […], validato con PIN e OTP generato da Mobile Token.

In definitiva, la banca contesta al ricorrente di aver fornito una ricostruzione dei fatti lacunosa e chiede il rigetto del ricorso avversario, considerato che:

(i) le operazioni in contestazione sarebbero state correttamente autenticate, registrate e contabilizzate attraverso un sistema di autenticazione "forte";

(ii) la banca avrebbe predisposto e messo a disposizione del cliente tutti i dispositivi utili a prevenire il verificarsi di eventi fraudolenti;

(iii) il presunto frodatore sarebbe venuto a conoscenza delle credenziali di accesso alla app a causa di grave negligenza del cliente nella custodia delle stesse;

(iv) la presunta frode sarebbe avvenuta per fatti in ogni caso estranei alla banca.

3. Il ricorrente ha depositato repliche nelle quali ribadisce di non aver comunicato a nessuno le credenziali personali, gravando sulla banca l'onere di provare la colpa grave dell'utilizzatore; precisa che la scheda sim disattivata era intestata alla figlia del ricorrente ma in uso esclusivo di quest'ultimo; d'altra parte egli non aveva ragione di collegare la disattivazione dell'utenza a una truffa bancaria, tanto più che utilizzava ancora il *token fisico*.

   Contesta pertanto la ricostruzione dei fatti fornita dall'intermediario, sostenendo sia più probabile che il truffatore (hacker o dipendente infedele di BNL) si sia prima impossessato delle credenziali (forse approfittando di una falla del sistema), per poi visionare dati anagrafici e numero di cellulare all'interno dell'anagrafica dell'*home banking*, e non il contrario come invece sostenuto dalla banca; questa ammetterebbe peraltro che al ricorrente non è stato trasmesso alcun *alert* relativo alla variazione dell'utenza telefonica.

   Quanto ai due bonifici da € 1.938,00 il ricorrente sostiene che gli stessi non vennero bloccati dalla banca, ma semplicemente non andarono a buon fine in quanto il conto era

stato già svuotato. In ogni caso, censura la condotta della banca che ha consentito l'esecuzione del successivo bonifico di € 1.526,99.
Evidenzia in via generale come l'intermediario riconosca che le operazioni sono state poste in essere nell'ambito di una *sim swap fraud,* ma non spiega perché la variazione di utenza telefonica non sia stata notificata al ricorrente tramite i canali indicati dalla stessa banca nelle controdeduzioni.

4. Nelle controrepliche parte resistente afferma che se è vero che il numero di telefono del ricorrente è stato acquisito fraudolentemente dai malfattori, è vero anche che le credenziali per poter procedere alla digitalizzazione delle carte, sono state fornite dal ricorrente stesso poiché il numero cliente (ID) e il PIN per accedere all'*home banking*, una volta ottenuta la *sim*, sono a conoscenza del solo intestatario degli strumenti di sicurezza. Quanto alla mancata ricezione delle notifiche relative alla variazione dell'utenza telefonica, essa non sarebbe ascrivibile alla banca, ma "alla negligenza del ricorrente che, caduto colpevolmente nelle richieste del presunto frodatore, ha permesso la asserita frode, rivelando forse inconsapevolmente le credenziali d'accesso del suo home banking antecedentemente alla frode". Sottolinea inoltre che tutti gli *sms alert*, a cominciare da quelli relativi all'attivazione del *token*, sono stati inviati a un numero diverso da quello dichiarato a suo tempo dal ricorrente, e che la sostituzione della *sim* è imputabile a negligenza degli operatori dello *store* telefonico. Quanto al presunto trafugamento dei dati a cura di presunti *hacker*, invocato dal ricorrente, quest'ultimo non fornirebbe alcuna prova.

DIRITTO

5. La questione sottoposta al Collegio concerne la richiesta di rimborso dell'importo di cinque operazioni che, come è pacifico fra le parti, non vennero autorizzate dal ricorrente bensì effettuate da terzi, riusciti momentaneamente a disattivare la SIM del ricorrente sulla cui utenza, in quel frangente, venne inviato l'OTP dispositivo necessario a completare le operazioni, secondo le normali procedure di autenticazione predisposte dall'intermediario.
6. La vicenda descrive quindi il compimento, a danno del ricorrente, una frode nota come "*Sim swap fraud*", diffusasi in tempi relativamente recenti, al fine di vanificare i presidi di sicurezza basati su autenticazione con OTP inviato tramite SMS. Merita rammentare, a tale riguardo, che con comunicato stampa diffuso dalla Polizia di Stato il 2.7.2018 la truffa perpetrata ai danni dei clienti delle banche sia stata così descritta:
"*La SIM SWAP è una avanzata tipologia di frode informatica articolata in vari passaggi. Una volta individuata la vittima si procede alla acquisizione dei suoi dati e delle credenziali di home banking tramite tecniche di hacking ovvero di ingegneria sociale e, successivamente, utilizzando documenti falsificati ad hoc, si sostituisce la Sim card della vittima e, attraverso lo stesso numero telefonico, si ottengono dalla banca le credenziali per operare sul conto corrente on-line. Nel caso specifico, carpiti i dati anagrafici e il numero di telefono della vittima, nonché i dati dei conti correnti e le relative credenziali di accesso, gli indagati, utilizzando un falso documento di identità intestato alla vittima, si recavano presso un dealer al fine di chiedere la sostituzione della SIM in uso alla persona offesa. La scheda SIM del titolare veniva allora disabilitata in quanto sostituita da quella attivata fraudolentemente. La vittima rilevava il mancato funzionamento della sua SIM ma, generalmente, non associava immediatamente l'evento ad una frode in corso. Sostituita la SIM, gli autori del reato penetravano nel sistema informatico dell'istituto di credito presso cui la vittima aveva acceso il conto corrente, riuscendo il più delle volte a reimpostare le credenziali di accesso attraverso*

una telefonata all'assistenza clienti, presentandosi come il titolare del conto e rispondendo alle varie domande di sicurezza. Una volta effettuato l'accesso, gli indagati erano abilitati ad operare sul conto corrente on-line della vittima, disponendo bonifici e/o ricariche di carte prepagate in favore di altri conti correnti e/o carte prepagate nella loro disponibilità, in quanto appositamente accesi da complici e prestanome, così ostacolando l'identificazione della provenienza delittuosa delle somme e l'individuazione degli effettivi beneficiari dei proventi del reato attraverso il tracciamento dei flussi finanziari generati dall'operazione dispositiva indebita. La serrata successione temporale delle varie sequenze attraverso le quali si snoda la frode informatica in esame non consentiva alla vittima di attivare tempestivamente i dispositivi di sicurezza; la vittima acquisiva dunque consapevolezza del prelievo indebito solo al momento della lettura dell'estratto del conto corrente (…)".

7. In diritto, quindi, la vicenda qui considerata si inquadra nella casistica del furto di strumenti di pagamento e di identità elettronica e va pertanto valutata alla luce delle vigenti disposizioni normative in materia di servizi di pagamento, con particolare riguardo agli artt. 7, 10 e 12 del d.lgs. n. 11 del 27.1.2010 (come modificato dal d. lgs. n. 218 del 15.12.2017, di recepimento della direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno); vi risulta altresì applicabile il Regolamento delegato (UE) della Commissione 2018/389, che stabilisce i requisiti dell'autenticazione forte ai sensi della PSD 2 e i criteri interpretativi forniti dall'EBA in merito ai più stringenti requisiti dell'autenticazione forte richiesti dal citato Regolamento, e segnatamente il parere dell'EBA del 21 giugno 2019.
8. Tali disposizioni delineano un quadro normativo dal quale promana, in sintesi, la seguente regola di giudizio: l'intermediario che non intenda farsi carico delle perdite sofferte dal cliente per operazioni che non siano state effettivamente autorizzate, ha l'onere: *(i)* di provare innanzitutto di aver adottato un sistema di "autenticazione forte" per l'utilizzo degli strumenti di pagamento da parte del cliente nonché, nel caso specifico, che le operazioni siano state correttamente autenticate, registrate e contabilizzate; *(ii)* e poi, fornita questa preliminare prova, di provare altresì, se non il dolo, almeno la colpa grave del cliente nell'aver reso possibile il compimento delle operazioni non autorizzate.
9. A tale riguardo, se la prima delle due prove può ritenersi essere stata fornita dall'intermediario resistente, che ha provato come l'operazione venne regolarmente autorizzata nel rispetto di un sistema che secondo gli *standard* valevoli *illo tempore* poteva ritenersi di autenticazione forte (sistema a duplice fattore tramite inserimento dei dati della carta di credito e di un codice OTP di conferma generato automaticamente tramite *mobile token*), altrettanto non può dirsi per la seconda.
10. Emerge infatti incontestata, dalle stesse difese dell'intermediario (che vorrebbe ascrivere l'esclusiva responsabilità al gestore dell'utenza telefonica della ricorrente, ma non a questi), la mancanza d'ogni colpa del ricorrente, che subì la disattivazione della sua utenza telefonica, verosimilmente appropriata dai terzi malfattori, proprio nello stesso giorno nel quale questi ultimi - avvalendosi della temporanea disponibilità di tale utenza - riuscivano ad abbinare al servizio di *home banking* una nuova utenza sulla quale ricevere ogni nuova notifica da parte della banca (salvo eventualmente la prima, ricevuta sull'utenza originaria momentaneamente nella disponibilità dei terzi) così riuscendo altresì ad attivare il mobile *token* (con conseguente *alert* ricevuto sulla nuova utenza abilitata).
11. Da questo punto di vista, anche se l'operazione complessivamente deve aver richiesto la disponibilità da parte dei terzi di alcuni dati – nome, numero dell'utenza telefonica, forse un documento) e credenziali statiche del ricorrente - non emerge tuttavia la prova

di una colpa grave del ricorrente, che invece rappresenterebbe la necessaria condizione normativa che l'intermediario potrebbe invocare per esonerarsi dall'obbligo di rimborso della ricorrente.

12. Da questo punto di vista, anzi, può dirsi che l'operazione contestata non è direttamente collegabile ad una sua condotta, come è a dirsi semmai per le fattispecie di furto, o smarrimento o appropriazione indebita dello strumento di pagamento, come previste dall'art. 12, comma 3, d. lgs. 11/2010, ai fini di un'eventuale franchigia a carico del ricorrente (dunque inapplicabile nel caso di specie).

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 11.609,98.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA