Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) STELLA	Membro designato dalla Banca d'Italia
(MI) BARILLA'	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNI AFFERNI

Seduta del 06/07/2021

Esame del ricorso n. 0247240 del 16/02/2021

proposto da

nei confronti di -

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) STELLA	Membro designato dalla Banca d'Italia
(MI) BARILLA'	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNI AFFERNI

Seduta del 06/07/2021

FATTO

Nel ricorso parte ricorrente afferma quanto segue:
- è contitolare con il marito, il Sig. B., di un conto corrente acceso presso una filiale dell'intermediario e che tale conto veniva utilizzato per prelievi e pagamenti bancomat, nonché bonifici di modesto importo. La cliente riferisce inoltre di aver attivato sul proprio smartphone l'applicazione O-Key Smart e che, nell'utilizzo della suddetta App, non ha mai effettuato dei prelievi cardless né effettuato bonifici istantanei;
- afferma che i limiti operativi erano impostati in € 300,00 giornalieri ed € 600,00 mensili;
- in data 14/05/2020, alle ore 11.30, riceveva un sms apparentemente proveniente dall'intermediario, inserito tra gli altri precedenti messaggi dell'Istituto di credito, che le segnalava un "alert" sul suo conto, chiedendole di compilare un form tramite il link allegato;
- aprendo il link suddetto le appariva sul proprio smartphone la normale schermata di accesso all'home banking di Intesa San Paolo che richiedeva i codici di accesso. La cliente digitava poi i codici e subito le compariva un'altra schermata con la richiesta di ulteriori informazioni, quali il numero di telefono;
- poco dopo, veniva contattata, attraverso un numero verde riconducibile all'Istituto di Credito (********03) e una persona qualificatasi come addetto della Banca la convinceva a fornirgli i codici che le sarebbero stati inviati. Prima di terminare la chiamata, l'operatore

rassicurava l'odierna istante comunicandole che avrebbe chiamato anche il giorno seguente per verificare se l'operazione di blocco fosse andata a buon fine;
- il giorno successivo, alle ore 17.30 circa, infatti, la cliente veniva nuovamente ricontattata dal medesimo operatore, il quale, sostenendo che probabilmente lo smartphone avesse preso un virus, dichiarava che l'operazione di blocco non era andata a buon fine e che si rendeva, pertanto, necessario che la stessa comunicasse ancora una volta i codici che le sarebbero arrivati via sms per stornare le operazioni fraudolente in atto. La cliente però comunicò solo un codice;
- terminata la comunicazione, l'odierna istante, non riuscendo ad entrare nell'applicazione home banking - che pensava fosse stata sbloccata al termine dell'operazione - contattava il numero verde della Banca per una verifica di quanto le era stato riferito, ma l'operatore non poté fornirle alcuna informazione perché l'account risultava bloccato;
- solo il lunedì mattina, pertanto, l'odierna ricorrente, recatasi in filiale, poté accorgersi dell'accaduto e quindi dell'addebito dei seguenti movimenti: (i) data 14/05/20 prelievo cardless presso abi 3069 – ATM 7640 di € 1.000,00; (ii) data 14/05/20 prelievo cardless presso abi 3069 – ATM 7640 di € 1.000,00; (iii) data 14/05/20 prelievo cardless presso abi 3069 – ATM 7640 di € 1.000,00; (iv) data 15/05/20 bonifico istantaneo n. 0120051516844805 a favore di S***o F***o di € 1.499,00 - causale: acquisto orologio; (v) data 15/05/20 bonifico istantaneo n. 0120051516850249 a favore di E***a di € 1.499,00 - causale: pagamento polizza; (vi) data 15/05/20 prelievo cardless presso abi 3069 – ATM 5581 di € 2.000,00;
- la cliente immediatamente disconosceva i suelencati movimenti e sporgeva formale querela contro ignoti presso le pubbliche autorità;
- in data 04/06/20 l'intermediario riaccreditava le operazioni disconosciute per poi, in data 11/09/20, riaddebitare con valuta 14/05/20 e 15/05/20 i suddetti importi, riferendo di ritenersi totalmente estranea all'accaduto. In data 09/11/20 sporgeva formale reclamo, il quale però sortiva esito negativo;
- ha provveduto a segnalare (e disconoscere) tempestivamente le operazioni contestate e ad effettuare la denuncia all'autorità competente, e ritiene che, non essendo alla stessa imputabile alcuna colpa per l'occorso, opera a tutti gli effetti il Dlgs. n. 11/2010, come integrato dal D.lgs. n. 218/2017 di attuazione della Direttiva 2015/2366/EU (PSD II);
- risulta evidente che sia stata tratta in inganno dalle modalità particolarmente insidiose che hanno caratterizzato la vicenda, dovendo quindi riconoscersi la responsabilità dell'intermediario che non ha adottato la necessaria diligenza professionale, presupposto indefettibile dell'"accorto banchiere";
- ritiene inoltre che le operazioni, che presentavano obiettivamente indici di anomalia agevolmente identificabili, avrebbero dovuto far attivare la Banca con un ulteriore blocco (cautelativo) dell'operatività del conto stesso. Tra l'altro segnala come, anche come evidente dagli estratti conto depositati, la cliente ha sempre utilizzato la propria carta di pagamento solo per importi modesti e mai in modalità cardless, e così anche per i bonifici e mai in modalità istantanea;
- nel caso in esame inoltre risultano dei prelievi cardless di importi anomali e superiori ai limiti giornalieri e dei bonifici istantanei appena al di sotto dei limiti, tutti ravvicinati in un arco temporale ristretto. Il superamento dei limiti giornalieri, almeno per quanto riguarda i prelievi cardless ATM, avrebbe dovuto indurre la banca ad intervenire per bloccare l'operazione;
- infine, non è da sottovalutare il fatto che la Banca non abbia attivato o, comunque, consigliato di attivare all'odierna istante il sistema di sms "alert", cosicché la stessa avrebbe potuto nell'immediatezza rendersi conto dei prelievi non autorizzati e truffaldini;

In conclusione parte ricorrente, visto l'esito negativo del reclamo, chiede il rimborso degli addebiti contestati pari a € 7.998,00, oltre interessi legali e spese di procedura.
Nelle controdeduzioni, l'intermediario ha eccepito quanto segue:
- nelle modalità del servizio di internet banking non risulterebbero anomalie, le operazioni sarebbero state impartite con il corretto inserimento di tutte le credenziali possedute dalla cliente;
- afferma come la colpa grave della cliente, come si evincerebbe dalla ricostruzione operata dalla ricorrente nell'esposizione dei fatti, sia sufficiente a dimostrare che l'esecuzione delle operazioni non possa essere imputabile alla banca ma esclusivamente alla cliente che avrebbe fornito all'interlocutore, spacciatosi per il numero verde dell'intermediario, i proprio codici personali che avrebbero consentito al truffatore di procedere all'enrollment dal dispositivo e a predisporre la truffa poi attuata;
- ulteriormente segnala come non si tratterebbe di una truffa particolarmente sofisticata e ribadisce che dalla documentazione prodotta vi sarebbe la conferma che le operazioni fraudolente sarebbero state rese possibili solo grazie alla condotta gravemente colposa della ricorrente, la quale avrebbe inserito ripetutamente le proprie credenziali personali;
- ribadisce la correttezza del sistema a due fattori ed inoltre sottolinea come la banca abbia allertato il cliente inoltrando al medesimo messaggi con i quali si informava la cliente dell'inserimento dell'operazione; tali messaggi, sebbene inviati ad un numero di telefono certificato, sarebbero stati del tutto ignorati con la conseguenza che la banca non ha avuto alcun dubbio circa la legittimità dei pagamenti. Nei messaggi inviati inoltre il cliente veniva avvisato di non fornire ad alcuno il codice contenuto.
In conclusione l'intermediario chiede il rigetto del ricorso e, nelle denegata ipotesi che si ravvisino dei suoi profili di responsabilità, la ripartizione tra le parti del danno in esame ai sensi dell'art. 1227 c.c.
Nelle repliche la ricorrente afferma di riportarsi alle conclusioni e a quanto già eccepito e dedotto in sede di ricorso. Intende però replicare alle controdeduzioni della convenuta.
Riguardo all'informativa in merito alla prevenzione delle truffe la ricorrente fa presente che i fatti sono accaduti a maggio 2020 ed in tale data non risulterebbero campagne informative sul sito internet dell'intermediario. Riguardo alle modalità con cui si è svolta la truffa la ricorrente ritiene non assolto dall'intermediario l'onere di dimostrare la colpa grave della cliente. La truffa infatti appare come "sofisticata", essendo avvenuta con la metodologia dell'SMS SPOOFING e ravvisandosi, secondo la stessa, la possibilità del SIM SWAP FRAUD.
La chiamata proveniente dal sedicente operatore, che l'intermediario ribadisce come non esibita, è stata richiamata in sede di denuncia e soprattutto è stata repertata dai pubblici ufficiali contestualmente alla denuncia.
Ritiene sussistente la responsabilità della Banca per mancato rispetto dei limiti operativi e ritiene non sufficiente quanto esposto dalla Banca in sede di controdeduzioni, dovendo depositare essa stessa i diversi limiti operativi impostati nel periodo in questione.
L'intermediario controreplica che:
- in merito alla prevenzione delle truffe afferma che la Banca è da tempo impegnata in campagne informative anche sul tema delle frodi realizzate con diverse tecniche;
- riguardo la colpa grave della ricorrente richiama quanto esposto in sede di controdeduzioni, richiamando la condotta particolarmente incauta della cliente;
- afferma che la truffa non sia riconducibile allo schema della sim swap fraud in quanto in tal caso il telefono cellulare avrebbe smesso di funzionare e non avrebbe permesso nemmeno la ricezione dei messaggi;
- relativamente ai limiti operativi, si richiama al contratto allegato con importi limite pattuiti in euro 30.000 giornalieri e in euro 60.000 mensili;

- afferma in ultimo come ritenga corrette e adeguate le determinazioni precedentemente assunte in sede di controdeduzioni confermando le conclusioni già espresse.

DIRITTO

La questione in oggetto riguarda 6 operazioni disconosciute dalla cliente. Trattasi di quattro prelievi cardless e due bonifici istantanei effettuati in data 14/5/2020 e in data 15/5/2020 per un importo complessivo di € 7.998,00.
Si osserva innanzitutto che le operazioni contestate sono state effettuate in vigenza del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D. Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
Sulla base della normativa sopra indicata, in primo luogo è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore (cfr. art. 10, comma 2 del decreto legislativo n. 11/2010, secondo cui *"l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento .... non è di per sé necessariamente sufficiente a dimostrare che (...) questi [il cliente] 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"*). In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo e alla frode, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. Si fa presente che - sulla materia in esame - si è recentemente pronunciato il Collegio di Coordinamento (Decisione n. 22745/19 del 10.10.2019), ove viene enunciato il seguente principio interpretativo: *"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".*
Sotto il primo profilo, l'intermediario fornisce la prova dell'autenticazione, della corretta registrazione e contabilizzazione delle operazioni disconosciute. L'intermediario nelle controdeduzioni illustra le modalità di funzionamento del servizio internet banking che risulta prevedere un'autenticazione forte (ossia a doppio fattore di cui uno dinamico). Inoltre, produce le evidenze delle tracciature dei log con la relativa spiegazione.
Parte ricorrente afferma che l'intermediario non avrebbe attivato il sistema di SMS alert. L'intermediario in sede di controdeduzioni riferisce di aver allertato la cliente inviando alla stessa n. 9 SMS/Push con i quali è stata informata dell'inserimento delle operazioni. Riferisce che nonostante i messaggi fossero inviati ad un numero di cellulre certificato e al device della cliente – sono stati del tutto ignorati. Si osserva in proposito che dalla documentazione in atti risulta che gli alert sono stati inviati e ricevuti.
Si deve poi esaminare quanto sostenuto dalla cliente in tema di plafond di spesa. Secondo parte ricorrente i limiti operativi non sarebbero stati rispettati e allega uno screenshot, che però è privo, tra l'altro, di firma. L'intermediario nelle controdeduzioni allega copia del contratto dove sono riportati i limiti operativi. I limiti indicati sono riferiti alle operazioni di pagamento effettuate tramite il servizio a distanza e sono di € 30.000,00 al giorno ed €

60.000,00 al mese. I limiti operativi quindi sono stati rispettati (anche se si deve censurare il comportamento della banca che prevede di defalut limiti giornalieri e mensili così alti).
Sotto il profilo della colpa di parte ricorrente, si osserva inoltre quanto segue.
Dalla ricostruzione dei fatti sopra esposta, parrebbe possibile che la cliente sia stato vittima di phishing, realizzato sia mediante vishing/ID caller che mediante smishing/spoofing.
In sede di repliche la ricorrente riferisce come sia possibile che la truffa subita corrisponda alla modalità del SIM SWAP FRAUD. Si precisa che non risultano né in denuncia né in sede di ricorso o negli allegati elementi a sostegno di un possibile scambio di SIM.
Per quanto riguarda il possibile spoofing, si osserva quanto segue. In sede di denuncia e di ricorso la ricorrente riferisce di aver ricevuto un sms che riteneva provenire dall'intermediario.
Dall'evidenza in atti sembra che il messaggio si sia accodato nella chat utilizzata dall'intermediario, infatti il successivo messaggio è riconducibile ad uno dei messaggi inviati dalla banca contenente l'Okey smart.
Successivamente la cliente veniva contatta da un numero di telefono riconducibile al numero verde dell'intermediario, durante la quale, un interlocutore, presentatosi come operatore della banca, chiedeva di seguire le indicazioni via via impartite per procedere all'operazione di storno. Non risulta fornita evidenza della chiamata, ma in sede di denuncia parte ricorrente dichiara di essere stata contattata dal numero verde *******03 (che è riconducibile all'intermediario).
Parte ricorrente, se pur in buona fede, ha seguito le istruzioni del truffatore, laddove l'utilizzo di una media diligenza avrebbe evitato il perpetrarsi della condotta delittuosa. Infatti, molti dei tentativi di truffa posti in essere in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza (c.d. *phishing* che, se tradizionalmente prende le forme di una mail civetta, può tuttavia presentarsi, come nel caso di specie, anche mediante l'invio di sms - c.d. *smishing* - o l'effettuazione di chiamate vocali – c.d. *vishing*).
La diffusione del fenomeno è tale che i Collegi ABF ritengono che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa. Si veda, fra le tantissime la decisone del Collegio di Roma n. 13780/2019, nonché le decisioni di questo Collegio nn. 682/2020 e 2391/20.
Sennonché, dalle risultanze istruttorie, la fattispecie in oggetto va ricondotta al cd "spoofing". Sul punto si richiama, fra le tante, la decisione n.8087/20 di questo Collegio, che riconosce il concorso di responsabilità delle parti in quanto, da un lato, non ravvisava elementi sufficienti tali da far dubitare circa la genuinità del messaggio, e, dall'altro lato, ravvisava comunque una condotta imprudente del Cliente successivamente alla ricezione dello stesso. Nella citata decisone si legge: *[...] La fattispecie andrebbe ricondotta ad un caso di c.d. "SMS spoofing", che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che esso appaia provenire da un soggetto differente - in questo caso, dall'intermediario -, rimpiazzando il numero originario con un testo alfanumerico (ossia quello utilizzato dall'intermediario per i propri messaggi genuini). In tal modo, il truffatore può inviare SMS-civetta che sembrano provenienti da numeri o contatti legittimi. In proposito il Collegio considera quanto affermato dal Collegio di Coordinamento nella già citata decisione n. 22745/19 [...]. Ritiene il Collegio che, nel valutare le implicazioni dell'impiego delle più recenti ed insidiosetecniche informatiche truffaldine occorra*

*nondimeno considerare in prima istanza il contenuto del messaggio che – vuoi via email, vuoi via SMS – la vittima del raggiro riceve; e, successivamente, gli eventuali estremi di colpa nella condotta successiva alla ricezione. Il ricorrente ha ricevuto un SMS che veniva raffigurato come proveniente dall'effettivo intermediario: detta circostanza è sicuramente dirimente ai fini di una diminuzione della responsabilità in capo al ricorrente medesimo, che non aveva elementi per poter distinguere la genuina provenienza del messaggio. La concatenazione delle circostanze è tale da consentire al Collegio di affermare che l'intermediario non abbia predisposto tutti i presidi di sicurezza necessari a impedire che il ricorrente fosse ingannato. D'altro canto, si può al contempo affermare che il ricorrente non abbia tenuto un comportamento improntato alla massima prudenza, là dove egli ha con ogni probabilità inviato il codice OTP ricevuto sul proprio cellulare: i sistemi di controllo dell'intermediario hanno infatti correttamente recepito e verificato l'esatta corrispondenza tra il codice che l'ignoto malfattore ha digitato nella pagina di pagamento del sito 2G*** ed il codice inviato sul cellulare del cliente, circostanza che ha reso possibile il buon esito della transazione. L'insieme delle circostanze così esposte e considerate consente di affermare in capo ad entrambe le parti una responsabilità per i fatti oggetto di controversia. Al ricorrente dovrà quindi essere riconosciuto un accoglimento parziale della sua pretesa".*
Questo Collegio ritiene che nel caso di specie si possa ravvisare un concorso di colpa nella misura dei 2/3 e, conseguentemente, l'intermediario dovrà rimborsare le operazioni disconosciute per 2/3.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda con buona valuta alla parte ricorrente la somma di € 5.332,00.
Il Collegio dispone inoltre, ai sensi della normativa vigente, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA