Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) COTTERLI	Membro designato dalla Banca d'Italia
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) MUNARI	Membro di designazione rappresentativa degli intermediari
(TO) DE FRANCESCO	Membro di designazione rappresentativa dei clienti

Relatore - FABRIZIO DE FRANCESCO

Seduta del 19/05/2021

FATTO

La parte ricorrente ha rappresentato:

- di essere titolare, unitamente ad altro soggetto aderente al ricorso, di un conto corrente presso l'intermediario resistente, cui risulta collegato il servizio di *internet banking* accessibile tramite *App* collegata alla sua SIM telefonica;
- che in data 03/08/2020, accortasi dell'assenza di linea sul proprio cellulare, contattava immediatamente l'operatore telefonico dal quale apprendeva che la sua SIM risultava disattivata per furto/smarrimento, verosimilmente a causa di un errore tecnico;
- di aver pertanto richiesto l'immediato ripristino dell'operatività della sua SIM, poi riattivata il 07/08/2020;
- che in data 05/08/2020 un operatore del nucleo antifrode dell'intermediario la contattava telefonicamente per comunicare l'inserimento di un'operazione di bonifico di € 4.995,00 da *home banking* ritenuta sospetta ed in effetti dalla stessa mai disposta;
- che, in quell'occasione, apprendeva altresì che nelle giornate del 03/08/2020 e del 04/08/2020 erano stati effettuati, sempre da *home banking*, due bonifici istantanei rispettivamente dell'importo di € 7.930,00 ed € 7.980,00, anch'essi mai autorizzati;
- che dunque disconosceva tutti i menzionati bonifici, riuscendo però a bloccare soltanto il terzo, ossia quello di € 4.995,00;

- di aver presentato denuncia alla Pubblica Autorità e reclamo all'intermediario, ricevendo tuttavia da quest'ultimo un riscontro negativo;
- che non è chiaro come terzi malfattori siano riusciti a entrare in possesso delle sue credenziali di accesso all'*home banking*, posto che né lei né l'aderente al ricorso le hanno mai comunicate ad alcuno e le hanno sempre custodite con cura;
- che è quindi evidente che le perdite dalla stessa subite siano imputabili unicamente all'intermediario, il quale non ha fornito un sistema di autenticazione e presidi di protezione idonei a garantire il livello di sicurezza richiesti dalla disciplina di settore;
- che infatti l'intermediario avrebbe dovuto attivarsi tempestivamente nel predisporre sistemi di allerta dei clienti in caso di accessi anomali (il sistema di *alert* a mezzo email veniva attivato soltanto successivamente alle vicende di cui è controversia);
- che invece nemmeno il sistema di *SMS alert* è risultato funzionante nei giorni del 3 e 4 agosto 2020, posto che in tali date nessun SMS risulta essere stato inviato dall'intermediario;
- che, nonostante l'evidente anomalia delle operazioni controverse (bonifici "immediati" di importo elevato, eseguiti in favore dello stesso soggetto in due giorni consecutivi e da un *device* diverso da quello solitamente utilizzato), l'intermediario si è attivato soltanto in occasione del terzo bonifico (disposto il 05/08/2020 e il cui importo è stato poi recuperato);
- che le operazioni disconosciute non sono state correttamente autorizzate, registrate e contabilizzate e che, in ogni caso, l'intermediario resistente non ha in alcun modo assolto l'onere di provare il dolo o la colpa grave dei clienti, sullo stesso incombente in base al D.lgs. 11/2010 ed al consolidato orientamento dell'ABF;
- che è inconferente la circostanza – indicata dall'intermediario nel riscontro al reclamo – per cui già in data 27/07/2020 la stessa avrebbe ricevuto tre *SMS alert* al proprio cellulare, contenenti l'avviso dell'attivazione di un *mobile token*: tale accesso infatti è verosimilmente attribuibile alla stessa cliente, la quale eccezionalmente in quella data utilizzava il servizio di *home banking* dal pc aziendale;
- che il servizio di *home banking*, bloccato in via cautelativa, non è ancora stato riattivato, causando alla stessa enormi disagi, e che il servizio di *SMS alert* continua a non essere funzionante;
- che l'intermediario non le ha fornito tutte le informazioni e la documentazione reiteratamente richieste.

La ricorrente pertanto, esperita inutilmente la fase del reclamo, chiede al Collego il riaccredito sul conto corrente della somma di € 15.910,00 pari all'ammontare dei bonifici illegittimamente eseguiti in data 03.08.2020 e 04.08.2020, o di altra veriore somma accertanda nel corso del presente procedimento, oltre al rimborso delle spese sostenute per la presente procedura.

Nelle proprie controdeduzioni l'intermediario – per quanto qui rileva – ha invece rappresentato quanto segue:

- le operazioni oggetto di controversia sono due bonifici di importo complessivo pari ad € 15.810,00, disposti tramite *App* installata su telefono cellulare;
- l'importo delle menzionate operazioni veniva addebitato sul conto corrente cointestato alla ricorrente e all'aderente al ricorso, abilitato al servizio di *home banking* e al quale è collegato il servizio di *SMS alert* via cellulare;
- il servizio di *internet banking* collegato al conto corrente della ricorrente prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte", in linea con la normativa europea PSD2, che prevede per 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*), codice dinamico generato da *Mobile Token* e, per disporre le operazioni, dopo avere effettuato il *login*, la conferma con inserimento del PIN + codice OTP, anch'esso generato da *Mobile Token*;

- il codice OTP è una *password* temporizzata, valida per un solo utilizzo, che viene generata in modo silente dal *Mobile Token* integrato nell'*App* che il cliente ha attivato sullo strumento che sta utilizzando;
- l'attivazione del *Mobile Token* è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'*home banking*, indipendentemente dalla attivazione del servizio *SMS Alert*;
- le operazioni oggetto di controversia risultano disposte dall'utenza e con le credenziali riferite all'odierna ricorrente, a nulla rilevando il tipo di dispositivo dal quale le stesse sono state eseguite;
- è infatti verosimile che i presunti malfattori siano entrati in possesso del codice Pin e del codice cliente negligentemente custoditi dalla ricorrente e necessari per accedere all'*home banking* e per carpire il codice OTP (comunicato via SMS solo al cliente, al numero di telefono cellulare associato all'*home banking*), indispensabile per attivare il *Mobile Token* ed inserire le operazioni dispositive;
- questo tipo di operatività si rende infatti possibile soltanto quando sia stato il cliente stesso a rivelare a terzi in qualche modo le proprie credenziali di accesso all'*home banking*;
- la banca ha dato ampio risalto sui propri canali a questo tipo di frodi, pubblicando specifici avvisi;
- la frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai presunti criminali, delle credenziali di accesso all'*home banking*, senza le quali non sarebbero stati in grado di accedere all'*App*, scaricare il *mobile token* e disporre operazioni;
- la ricorrente non ha ricostruito in modo completo la vicenda, limitandosi a riferire in sede di denuncia del malfunzionamento della propria SIM, circostanza che certamente non può essere addebitata alla banca;
- con tutta probabilità, nel caso di specie, è stata realizzata ai danni della cliente la truffa nota come "*sim swap fraud*", resa spesso possibile dalla negligenza o peggio connivenza degli addetti agli *store* telefonici;
- il frodatore che si appropria del numero di cellulare di un cliente deve conoscere: (i) il numero di cellulare associato al nominativo del cliente, carpito precedentemente mediante *phishing*; (ii) i dati anagrafici del cliente per chiedere la sostituzione della SIM; (iii) il numero cliente ed il PIN per accedere all'*home banking* del cliente una volta ottenuta la SIM;
- la cliente in data 27/07/2020 ha ricevuto 3 SMS al proprio numero di telefono certificato che la avvisavano dell'attivazione del *mobile token* e tuttavia la stessa non ha assunto nessuna iniziativa;
- le operazioni controverse sono state correttamente autenticate con un sistema di autenticazione a due fattori (PIN + OTP generato da *Mobile Token*) sia per l'accesso sia per le operazioni dispositive, come documentato dai LOG versati in atti ed i propri sistemi interni non hanno rilevato alcun malfunzionamento;
- l'intermediario riusciva comunque a intercettare come operazione sospetta e a stornare la transazione di € 4.995,00 disposta in data 05/08/2020 e ciò dimostra che, se la cliente avesse controllato il proprio saldo e le proprie operazioni tramite *home banking* ed avesse informato tempestivamente la banca circa le operazioni asseritamente fraudolente, molto probabilmente non avrebbe subito alcun danno;

- è infondata la contestazione per cui la banca avrebbe dovuto ritenere anomali accessi all'*home banking* da dispositivi diversi da quello della ricorrente posto che gli stessi erano avvenuti con l'inserimento corretto delle credenziali;
- constano numerosi precedenti, anche del Collegio di Torino, in base ai quali, in presenza di un sistema di autenticazione forte, si deve presumere che vi sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.

L'intermediario ha pertanto richiesto il rigetto del ricorso in quanto infondato.
Entrambe le parti hanno fatto pervenire memorie di replica e controreplica, insistendo nelle proprie difese e richieste. In particolare l'intermediario ha confermato che le operazioni fraudolente oggetto di ricorso sono riconducibili ad un'ipotesi di *sim swap fraud*.

DIRITTO

Il presente caso riguarda due operazioni bancarie *online*, disconosciute dal cliente, consistenti in particolare in un primo bonifico istantaneo dell'importo di € 7.930,00, effettuato il 03/08/2020, ed in un secondo bonifico istantaneo di € 7.880,00, eseguito il 04/08/2020. Dai fatti narrati da entrambe le parti, emerge inoltre che dapprima le credenziali di accesso al conto corrente *online* di parte ricorrente, e poi quelle di autenticazione delle operazioni illecite disconosciute, sono state carpite da ignoti malfattori mediante il sistema noto come "*sim swap fraud*". Secondo tale schema delittuoso l'utilizzo fraudolento di strumenti elettronici di pagamento è associato al furto di identità telefonica il quale consente di fatto un aggiramento del sistema di autenticazione a doppio fattore, laddove questo sia attuato mediante invio della cd. "*one time password*" (OTP) tramite SMS: in questi casi, infatti, il codice OTP viene ricevuto da chi ha fraudolentemente carpito l'identità telefonica, ottenendo una nuova SIM, attiva e funzionante sino a quando l'effettivo titolare non se ne accorge e non procede al blocco della stessa. Concretamente il mancato funzionamento dell'utenza telefonica, l'avvenuta attivazione di una SIM da parte di un altro soggetto e l'esecuzione di un'operazione tramite utilizzo fraudolento dello strumento di pagamento sono eventi di non immediata associazione da parte dell'utente e fra i quali può intercorrere un lasso di tempo sufficiente affinché il malfattore riesca a compiere la propria azione criminale.
Così sinteticamente ricostruito l'oggetto del contendere, dal punto di vista normativo le operazioni contestate vanno ricondotte nell'alveo del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13 gennaio 2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (cd. PSD2). Ricordiamo in particolare che l'art. 10 del D.lgs. 27 gennaio 2010, n. 11, così prevede: "1. *Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.* 1-bis. *Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, questi ha l'onere di provare che, nell'ambito delle proprie competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato.* 2. *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 se' necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, ne' 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. E' 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".

Sulle modalità applicative delle norme appena citate e sul riparto degli oneri di allegazione e prova in questa materia, il Collegio di Coordinamento ha espresso il seguente, consolidato 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*" (Coll. Coordinamento, decisione n. 22745 del 10 ottobre 2019).

Nel caso di specie, alla luce di tali condivisibili principi, l'intermediario non risulta aver fornito prova della colpa grave del ricorrente. La *sim swap fraud* costituisce infatti una truffa particolarmente insidiosa, tale da escludere di per sé – salvi casi particolari che qui non ricorrono – qualsiasi ipotesi di colpa grave del cliente.

Quanto appena osservato è conforme agli orientamenti più recenti dei collegi ABF, i quali hanno più volte rilevato, in generale, l'insidiosità del meccanismo di aggressione mediante *sim swap fraud*. Sul punto può richiamarsi quanto osservato dalla decisione n. 14909/2017 di questo Collegio di Torino: "*Nel caso di specie, il dolo o la colpa grave della parte ricorrente non emergono con sufficiente evidenza, dato che il malfunzionamento della propria utenza telefonica cellulare e il rischio di una truffa sui sistemi di pagamento sono eventi di non immediata associazione e che quindi la richiesta di blocco poteva esigersi non a partire dalla data dall'interruzione del collegamento telefonico ma semmai a partire dalla data dalla ricezione della e-mail che evidenziava la variazione del saldo del conto corrente (…) Quanto poi alla custodia dei codici che consentono l'operazione di pagamento, nel caso di specie non occorreva, secondo quanto descritto dalla parte ricorrente e dagli intermediari, l'utilizzo di un PIN personale né dei dati per l'autenticazione su di un Portale Titolari, non trattandosi di operazioni di home banking per un bonifico on line (come invece nei casi decisi da Collegio di Roma, pronuncia n. 1181/2017, Collegio di Milano, pronuncia n. 2430/2015, Collegio di Napoli, pronuncia n. 8292/2014; Collegio di Napoli, pronuncia n. 7731/2014, dove, oltre agli OTP, i frodatori avrebbero dovuto carpire anche le credenziali di accesso al portale dell'home banking), ma bisognava necessariamente conoscere i dati della carta di credito e delle one time password (OTP) di volta in volte trasmesse tramite SMS per perfezionare gli acquisti on line. Ma nemmeno qui il dolo o la colpa grave della parte ricorrente emergono con sufficiente evidenza, dato che i codici OTP, necessari per il perfezionamento dell'operazione, sono stati verosimilmente carpiti attraverso il già ricordato furto di identità telefonica mentre i dati della carta di credito, per i quali non si è ricostruito come potessero essere conosciuti da persone diverse dal titolare, possono essere stati parimenti carpiti o all'atto stesso della trasmissione della carta via posta, come suggerito dalla parte ricorrente, o con altre modalità. E nel dubbio deve farsi applicazione dell'art. 10, comma 2, D.Lgs. n. 11 del 2010*". In senso conforme questo stesso Collegio di Torino ha confermato più di recente che: "*Benché siano stati versati in atti dall'intermediario i log informatici dai quali si desume che l'accesso all'home banking, l'autorizzazione del bonifico e la creazione delle carte virtuali siano state autorizzate con sistema di autenticazione forte a doppio fattore*

(codice utente e pin e codice OTP/OTS), va osservato che tale prova non risulta sufficiente per escludere la responsabilità ex art. 12, comma 2-bis dell'intermediario, quando, come nel caso di specie, si sia verificata una c.d. SIM swap fraud. Il ricorrente ha allegato, infatti, che si è verificata una frode informatica di questo genere. Ciò risulta documentato, per un verso, dall'SMS ricevuto dal ricorrente, nel quale la compagnia telefonica afferma la cessazione dell'operatività della SIM; per l'altro, dal fatto che pochi minuti dopo la ricezione di tale SMS avviene l'enrollment dell'App sul device del malfattore (come risulta dal log versato in atti dalla parte resistente). Ciò consente in un breve intervallo di tempo al malfattore di effettuare le operazioni di pagamento oggetto del ricorso, senza che la notifica push ricevuta dal ricorrente al momento dell'enrollment dell'App abbia consentito al ricorrente di intervenire tempestivamente. Come anticipato, in caso di SIM swap fraud, l'orientamento condiviso dei Collegi equipara la sostituzione fraudolenta della SIM alla mancanza di autenticazione dell'operazione ai sensi dell'art. 10 d.lgs. n. 11/2010, giacché il prestatore del servizio di pagamento è tenuto a sopportare integralmente il rischio di impresa conseguente all'affidamento a terzi (i.e. le compagnie telefoniche) di elementi necessari alla autenticazione delle operazioni di pagamento. Pertanto, in assenza della dimostrazione della corretta autenticazione forte, il rischio di operazioni di pagamento disconosciute da quest'ultimo deve essere integralmente sopportato dal prestatore del servizio di pagamento" (Collegio di Torino, decisione n. 5827/2021). E così il Collegio di Milano (decisione n. 2885/2021): "*Il non funzionamento dell'utenza telefonica, l'avvenuta attivazione di una SIM da parte di un altro soggetto e l'esecuzione di un'operazione tramite utilizzo fraudolento dello strumento di pagamento sono eventi di non immediata associazione da parte dell'utente al fine di percepire la truffa in atto, e fra i quali può intercorrere un lasso di tempo sufficiente affinché il malfattore riesca a compiere la propria azione criminale. In proposito, secondo l'orientamento recentemente condiviso dai Collegi, la sostituzione della sim card va equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10 bis del D.lgs. n. 11/2010, sull'autenticazione c.d. forte; in ogni caso, per le modalità di attuazione, la c.d. "SIM swap fraud" costituisce una manovra fraudolenta nell'ambito della quale non si può ravvisare la colpa grave del cliente*" (vedi anche Collegio di Milano, decisioni nn. 7440/2019 e 25551/2019).

Né paiono sufficienti a superare quanto appena detto tanto le modalità di autenticazione attraverso il sistema di *mobile token* adottato dall'intermediario, il quale in caso di *sim swap fraud* viene completamente aggirato, quanto i presunti messaggi del 27/07/2020 di attivazione del predetto *mobile token*, i quali si rivelano inidonei a consentire al cliente di comprendere quanto stia succedendo, soprattutto ove inviati – come nel caso di specie – tramite il medesimo sistema potenzialmente compromesso dall'intrusione in corso.

Ed è appena il caso di rilevare, infine, come non colga nel segno la difesa dell'intermediario, volta a sostenere che la frode mediante utilizzo indebito della SIM telefonica esulerebbe dal proprio ambito di responsabilità, coinvolgendo semmai quella dell'operatore telefonico o dei sui addetti. Una simile opzione ermeneutica collide infatti palesemente con la *ratio* della citata direttiva (UE) 2015/2366 (cd. PSD2), recepita in Italia col D.lgs. 27 gennaio 2010, n. 11 (e s.m.i.), la quale – in un'ottica di riparto complessivo – pone evidentemente in capo all'intermediario il rischio per fattori esterni, connessi all'operatore telefonico, anche in considerazione del rischio di impresa collegato all'affidamento a terzi delle procedure di autenticazione delle operazioni di pagamento. Resta ovviamente salva, secondo gli ordinari principi civilistici, la possibilità dell'intermediario di rivalersi su detto soggetto terzo – nel caso di specie sull'operatore telefonico – nel caso ritenga di poterne dimostrare profili dolosi o colposi che abbiano contribuito a dar corso all'illecito.

Pertanto, alla luce di tutto quanto sopra, parte ricorrente ha diritto alla restituzione dell'importo delle due operazioni disconosciute, e così per l'importo di € 15.810,00.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 15.810,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA