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 ESTERNI - FABRIZIO DE FRANCESCO

Seduta del 28/07/2021

FATTO

La parte ricorrente ha affermato di essere titolare, insieme alla madre, di un conto corrente accesso presso l'intermediario convenuto, individuato dal n. xxx654; ha precisato inoltre che la madre/cointestataria è a sua volta titolare anche del conto corrente n. xxx677, sul quale il ricorrente è delegato ad operare; infine ha allegato di essere titolare di tre carte di pagamento, individuate dai nn. xxx6511, xxx0834 e xxx4216.
Nell'ambito di tali rapporti, parte ricorrente ha più nel dettaglio rappresentato:

- di essere stato contattato telefonicamente in data 20/05/2020 dall'intermediario resistente, il quale lo informava che sui predetti conti correnti erano state eseguite operazioni sospette (bonifici e prelievi *cardless*), tra il 19/05/2020 e il 20/05/2020, per un ammontare complessivo di € 23.800,00 sul conto n. xxx654 e di € 5.500,00 sul conto n. xxx677;
- di essersi recato in filiale il 21/05/2020 e di aver ricevuto le stampe delle contabili degli addebiti, dalle quali risultavano una serie di operazioni da lui mai eseguite né autorizzate;
- di aver appreso che in data 19/05/2020 ignoti avevano tentato di effettuare due ulteriori bonifici, di cui uno di € 4.900,00, alle ore 16:04, e uno di € 2.500,00, alle ore 16.31, ma che entrambi erano stati bloccati in quanto operazioni sospette;
- di aver segnalato alla filiale come sospetto anche il bonifico di € 5.500,00 ma che questo veniva comunque eseguito dalla banca;

- di aver appreso dal resistente che gli autori delle operazioni fraudolente suindicate avevano generato anche due carte virtuali attraverso le quali non erano riusciti ad operare in quanto queste venivano bloccate dal servizio antifrode;
- di aver ricevuto comunicazione che "*come risulta dalle citate comunicazioni l'ufficio antifrode della Banca ha accertato "il cambio device (certificazione di un nuovo dispositivo mobile)" e l'incertezza "sull'identità dell'interlocutore", ammettendo di non aver "proceduto al contatto telefonico con il cliente"*";
- che il 21/05/2020 la banca ha riaccreditato le somme indebitamente prelevate, salvo poi procedere al riaddebito dei medesimi importi in data 14/09/2020, determinando così uno scoperto di conto;
- che "*le operazioni non autorizzate sono state eseguite a seguito di una truffa perpetrata ai danni del Ricorrente mediante furto della sua identità telefonica (cd. "Sim Fraud Swap") e delle sue credenziali bancarie, mai comunicate a terzi dal ricorrente*"; che "*dal primo pomeriggio del 19 maggio 2020 alla prima mattina del 20 maggio 2020, [il ricorrente] si era infatti improvvisamente trovato privo della propria linea telefonica*";
- di aver contattato il proprio operatore telefonico il quale inizialmente gli riferiva che il disservizio poteva essere dovuto a problemi "connessi ai ponti telefonici", ma che successivamente, effettuati ulteriori controlli, veniva informato che la sua linea telefonica era stata trasferita il giorno precedente su un'altra SIM card;
- che il furto dell'identità telefonica "*è occorso nella provincia di Caserta, dove sono state eseguite le operazioni di prelievo cardless sopradescritte*" e che "*l'operatore provvedeva successivamente a riattivare la linea, come si è detto nella prima mattina del 20 maggio 2020, fornendo al cliente una nuova SIM card*";
- che l'ammontare delle operazioni oggetto di contestazione è superiore al *plafond* giornaliero previsto per i prelievi (€ 500,00) e per i bonifici (€ 5.000,00);
- che gli ultimi due prelievi, effettuati il 20/05/2020 alle ore 00:04 e 00:05, sono stati eseguiti dopo il blocco dei bonifici avvenuti da parte dello stesso intermediario il 19/05/2020, alle ore 16:04 e 16:05;
- che nonostante la propria irreperibilità a causa dei problemi di linea, la cointestataria del presente ricorso era raggiungibile telefonicamente sul proprio numero di cellulare alla stessa intestato ed in possesso della filiale, nonché sul numero fisso, ma che l'intermediario resistente non ha provveduto ad allertarla in alcun modo di quanto stava avvenendo;
- infine, che parte resistente ha comunicato solo in data 23/09/2020 l'avvenuto storno dei precedenti riaccrediti effettuato in data 14/09/2020.

La parte ricorrente, pertanto, dopo aver vanamente esperito la fase del reclamo, chiede all'ABF il rimborso della somma fraudolentemente sottratta di € 29.300,00, oltre "*al risarcimento dei danni subiti, corrispondenti agli interessi negativi addebitati nell'ambito dei rapporti di conto corrente e al mancato rendimento del capitale non goduto e al risarcimento del danno non patrimoniale per i disagi subiti*".

Con le proprie controdeduzioni l'intermediario resistente ha per contro affermato ed eccepito quanto segue:

- i ricorrenti sono contitolari del conto corrente n. xxx654 mentre la madre/cointestataria è titolare anche del rapporto n. xxx677;
- con addebito su tali rapporti, nelle date del 19 e 20 maggio 2020 sono state disposte diverse operazioni per complessivi € 29.300,00;
- a seguito del disconoscimento delle operazioni fraudolente, la banca provvedeva a riaccreditare in favore dei clienti le somme oggetto di disconoscimento, salvo poi procedere in data 14/09/2020 allo storno delle operazioni e al riaddebito della somma;

- con lettera del 18/01/2021 la banca si dichiarava disponibile a risolvere bonariamente la vicenda riconoscendo in favore dei clienti la somma € 14.650,00, pari al 50% del danno lamentato;
- per accedere ai servizi di pagamento *online* è richiesto l'inserimento simultaneo di *password* statiche e dinamiche, identificabili nel codice titolare (codice statico), nel codice PIN (statico) e nel codice *O-Key* (OTP dinamico);
- una volta collegati al servizio *online*, per autorizzare le operazioni è necessario il codice OTP dinamico;
- il codice dinamico può essere generato via *app* (per i clienti *O-Key smart*) ovvero tramite sms (per i clienti *O-Key SMS*);
- in caso di *smartphone* o *tablet* con "*connessione dati assente o momentaneamente non funzionante*", il codice dinamico viene inviato tramite sms al numero di cellulare certificato;
- il sistema di sicurezza ed autenticazione di cui si avvale è conforme alla regolazione vigente in materia, posto che per aumentare il livello di sicurezza di alcune operazioni viene richiesto al cliente anche l'inserimento di un secondo codice inviato tramite sms;
- per aumentare ulteriormente il livello di sicurezza di alcune disposizioni di pagamento, è richiesto al cliente di rispondere alle domande di sicurezza o, qualora non le abbia censite, l'inserimento di un ulteriore codice inviato vis SMS;
- tale sistema di sicurezza ha ottenuto la certificazione ISO/IEC 27 001 ed è conforme ai requisiti del Regolamento europeo 2018/389;
- vengono periodicamente poste in essere campagne informative a favore della clientela al fine di sensibilizzarla in merito al rischio di frode;
- le operazioni contestate sono state regolarmente autenticate, registrate e contabilizzate (come emerge dalle tracciature informatiche prodotte in atti);
- in occasione delle operazioni non è stata riscontrata alcuna anomalia tecnica e le disposizioni sono state tutte impartite con corretto inserimento delle credenziali possedute dal cliente;
- essendo l'intermediario estraneo al contratto concluso tra il cliente e la compagnia telefonica, anche in caso di *"Sim Swap, è evidente che non può essere addebitata alla Banca alcuna responsabilità per la condotta del gestore telefonico nel caso in cui lo stesso consegni un duplicato della SIM a terzi senza il consenso del proprio cliente*";
- tra il primo accesso *all'internet banking* (h. 14:20 del 19/05/2020) e l'ultima operazione disconosciuta (h. 00:05 del 20/05/2020) sono trascorse 10 ore e tale lasso di tempo avrebbe dovuto indurre il ricorrente ad attivarsi, bloccando cautelativamente il conto;
- il sistema di autenticazione impiegato nel caso di specie è "a due fattori", sicché non è plausibile che le operazioni siano state poste in essere da un soggetto che non era a conoscenza delle *password* necessarie e in possesso dei relativi dispositivi.

L'intermediario resistente chiede pertanto il rigetto del ricorso, ovvero – nel caso in cui il Collegio ritenga di poter ravvisare profili di responsabilità a suo carico – di definire proporzionalmente la misura del danno ai sensi dell'art. 1227 c.c.
Le parti hanno fatto pervenire memorie di replica e controreplica, insistendo per le proprie difese e richieste e contestando le avverse argomentazioni.

DIRITTO

Il presente caso riguarda sette operazioni disconosciute, consistenti in cinque prelievi *cardless* eseguiti il 19/05/2020 ed il 20/05/2020, di cui quattro prelievi di € 1.000,00 ed uno di € 800,00, e di due bonifici, rispettivamente di € 19.000,00 ed € 5.500,00, risalenti sempre al 19/05/2020. Dai fatti narrati da entrambe le parti e dalla documentazione

prodotta dal ricorrente, emerge inoltre che le credenziali di accesso ai conti correnti *online* – attraverso le quali sono state compiute le operazioni illecite – sono state carpite da ignoti malfattori con 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 o del conto *online* 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, che può risultare anche gravemente dannosa: ciò è particolarmente evidente nel caso di specie, in cui grazie alla disponibilità dell'utenza telefonica violata i truffatori sono riusciti a compiere le operazioni illecite in un arco di circa dieci ore (la prima è delle ore 14:38 del 19/05/2020 e l'ultima delle ore 00:05 del 20/05/2020).

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; ancor più recente la decisione n. 16437/2021). 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).

Pertanto, alla luce di tutto quanto sopra, parte ricorrente ha diritto alla restituzione dell'intero importo delle operazioni disconosciute, pari ad € 29.300,00 (in particolare, come richiesto in atti, € 23.800,00 in favore dei entrambi i ricorrenti ed € 5.500,00 in favore dell'intestataria del conto corrente n. xxx677).

Non può invece essere accolta, allo stato degli atti, la richiesta di "*risarcimento dei danni subiti, corrispondenti agli interessi negativi addebitati nell'ambito dei rapporti di conto corrente e al mancato rendimento del capitale non goduto e al risarcimento del danno non patrimoniale per i disagi subiti*" in quanto sfornita di adeguate allegazioni e prove a supporto. Allo stesso modo non può essere accolta la richiesta di rimborso della perizia di parte prodotta dal ricorrente, non sussistendo i presupposti indicati a tal fine dal Collegio di Coordinamento.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 29.300,00.

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