Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRAZIADEI	Membro designato dalla Banca d'Italia
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) DALMOTTO	Membro di designazione rappresentativa degli intermediari
(TO) CATTALANO	Membro di designazione rappresentativa dei clienti

Relatore MICHELE GRAZIADEI

Seduta del 07/04/2020

FATTO

Il ricorrente ha affermato di essere titolare della carta bancomat n. ***269 e di aver riscontrato in data 30/07/2019 che il proprio telefono era disabilitato; contattata la compagnia telefonica, apprendeva che ignoti avevano richiesto al fornitore di servizi telefonici la disabilitazione della Sim, adducendo il furto del telefonino, e il rilascio di una nuova Sim con un nuovo numero; i predetti avevano poi registrato questo numero sul portale della resistente per le operazioni *on line*; di aver conseguentemente subito la sottrazione di € 4.992,00, secondo il noto sistema di frode denominato della “SIM SWAP”; parte resistente non ha spontaneamente rimborsato le operazioni contestate.

L’intermediario, nelle controdeduzioni, ha rappresentato quanto segue: parte ricorrente è titolare di conto corrente abilitato allo svolgimento di operazioni tramite *internet banking*; l’operatività del predetto servizio – al fine di *Inquiry* e di operazioni dispositive - prevede l’utilizzo della c.d. autenticazione *forte*, vale a dire, l’inserimento delle credenziali di accesso (num. cliente + PIN) e del codice OTP generato (nel vigore della pre-vigente disciplina PSD, fino al 14/09/2019) da dispositivo *token* fisico o mobile (quest’ultimo attivato tramite credenziali e OTP inviato via sms al cliente); per l’attivazione del predetto servizio *mobile token* è pertanto necessario possedere anche le credenziali del titolare.

Pertanto, il contratto e i messaggi informativi periodicamente diffusi dalla resistente invitano gli utenti alla massima accuratezza nella custodia delle credenziali; il sistema di sicurezza adoperato è riconosciuto quale affidabile dalla giurisprudenza dell'ABF. L'operazione disconosciuta è eseguita tramite canale ATM, con il servizio "*prelievo extra*" messo a disposizione dei clienti con comunicazione di modifica unilaterale del 2/04/2019; il servizio consente prelievi da ATM sino a 4.990,00 settimanali, secondo due canali: inserimento della carta, digitazione PIN e del codice di 8 caratteri trasmesso via SMS; senza inserimento carta, digitando le credenziali di accesso all'*home banking* oltre al codice OTP generato tramite *token* fisico o *mobile*. L'operazione è stata correttamente eseguita in assenza di malfunzionamenti dei sistemi e risulta autenticata in modalità *cardless* con inserimento credenziali, come sopra descritto; i codici necessari all'attivazione del *mobile token* e il codice OTP sono stati inviati al numero di parte ricorrente indicato per il servizio di SMS alert. Come asserito da parte ricorrente, l'utenza telefonica era disattiva e la frode si è potuta perpetrare "*a causa di eventi estranei alla banca*"; riguardo la condotta di parte ricorrente, appare particolarmente scarna la descrizione da questa fornita in atti: tale condotta in sé risulta censurabile alla luce di precedenti ABF. Nondimeno, la circostanza che sia necessario l'inserimento delle credenziali di parte ricorrente per l'esecuzione dell'operazione descritta denota una necessaria collaborazione del ricorrente al verificarsi dell'episodio: collaborazione data nella forma della gravemente colposa negligenza nella custodia delle credenziali.

La parte ricorrente chiede il rimborso di € 4.992,00 fraudolentemente sottratte.

L'intermediario resistente chiede il rigetto del ricorso.

DIRITTO

Le operazioni contestate sono disciplinate dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
L'operazione oggetto di contestazione consiste in un prelievo ATM di € 4.990,00 (oltre commissioni) eseguito da terzi malfattori in modalità *cardless* in data 30/07/2019. Parte resistente specifica che trattasi di operazione eseguita secondo le modalità del servizio extra prelievo su circuito ATM, ma senza inserimento della carta, mediante digitazione delle credenziali di accesso all'*home banking* (codice cliente e PIN) e mediante digitazione del codice OTP generato tramite *token* (nel caso di specie: *mobile token*), inviato dalla banca tramite sms. Per dare dimostrazione della autenticazione delle operazioni contestate, l'intermediario ha prodotto evidenza della tracciatura informatica. Parte resistente ha inoltre fornito evidenza degli SMS inviati alla parte ricorrente, tale evidenza è però compatibile con il tipo di meccanismo frodatorio del tipo SIM SWAP FRAUD. Si rileva in particolare che nella giornata del 30/07/2019 - precedente l'operazione di pagamento contestata - risultano n. 5 messaggi (al n. tel. xxx1004) con cui è stata richiesta l'attivazione del *mobile token* (messaggio consegnato al service provider); risulta la comunicazione dell'avvenuta modifica sul servizio SMS alert (consegnato al service provider); risulta inviato al nuovo numero (tel. xxx447) comunicazione di avvenuta modifica servizio SMS alert (consegnato al cliente) e di attivazione del *mobile token*; nella giornata

del 31/07/2019, risulta inoltre comunicata al cliente sull'utenza telefonica precedente la modifica (n. XXX1004) la notifica di modifica della configurazione del servizio SMS alert.
Ricostruito in questi termini quanto è accaduto, è onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/10). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute (no franchigia). Tuttavia, tale prova, che è data nella specie, non è comunque di per sé sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento. In tema di riparto dell'onere probatorio, deve essere richiamata la recente decisione n. 22745/2019 del Collegio di Coordinamento secondo cui: "*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*". Nel caso di specie, la prova della colpa grave del cliente non è raggiunta, in quanto la frode si è consumata con modalità tali che consentono di escludere che il cliente si sia reso responsabile di un comportamento gravemente negligente. Giova richiamare in proposito quanto ha statuito in relazione a fattispecie analoga il Collegio di Roma, decisione n. 14550/2019:

> "*Sotto altro aspetto, questo Collegio ritiene che il sistema di autenticazione forte delle operazioni predisposto dall'intermediario non sia idoneo ad arginare tentativi fraudolenti di accesso al sistema di home banking del cliente. Preliminarmente, è opportuno segnalare come si intenda per autenticazione forte, quel sistema di autenticazione basato sull'uso di due o più elementi indipendenti, in quanto la violazione di uno non deve compromettere l'affidabilità degli altri. Nel caso di specie, appare evidente come il sistema di autenticazione approntato dall'intermediario si sia rivelato inadeguato, atteso che è possibile desumere dalla documentazione in atti che agli autori della truffa sia stato sufficiente avere accesso abusivo alla casella e-mail del ricorrente per poi, conseguenzialmente, senza ulteriori ostacoli, accedere al conto home banking, venire a conoscenza del numero di utenza telefonica al quale venivano inviati i codici alfanumerici e procedere all'operazione di Sim swap, in modo da garantirsi la ricezione di questi ultimi, disabbinando il token dal vecchio al nuovo dispositivo.*
> *Sul punto, è orientamento dell'ABF ritenere che l'esistenza di una relazione funzionale tra le singole misure di sicurezza consente di eludere la doppia autenticazione e rende tale sistema non più forte, bensì debole, in quanto la violazione di una misura di sicurezza è in grado di compromettere anche l'affidabilità dell'altra, quando, al contrario, la piena operatività del sistema di autenticazione multifattore deve fondarsi sull'indipendenza tra le singole misure di sicurezza (ABF, Collegio di Milano n. 10666 del 16.01.2019) (…)".*

Il Collegio di Torino ritiene di condividere questi rilievi, del tutto pertinenti anche rispetto al caso di specie, ove risulta come il sistema di sicurezza adottato dall'intermediario, a causa dello scambio della Sim del cliente, non sia più da considerare un sistema di autenticazione forte, non essendo più presidiato da uno dei due fattori che dovrebbe intervenire nell'autenticazione delle operazioni. Pertanto, è da restituire al cliente la somma che gli fu indebitamente sottratta, pari a Euro 4.992,00.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.992,00.
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