Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) BONGINI	Membro designato dalla Banca d'Italia
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) FERRETTI	Membro di designazione rappresentativa degli intermediari
(MI) TINA	Membro di designazione rappresentativa dei clienti

Relatore BONGINI PAOLA AGNESE

Seduta del 20/03/2018

Esame del ricorso n. 1074955 del 06/09/2016

proposto da

nei confronti di 3069 - INTESA SANPAOLO S.P.A.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) BONGINI	Membro designato dalla Banca d'Italia
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) FERRETTI	Membro di designazione rappresentativa degli intermediari
(MI) TINA	Membro di designazione rappresentativa dei clienti

Relatore BONGINI PAOLA AGNESE

Seduta del 20/03/2018

FATTO

La cliente riferisce di essere titolare di un conto corrente con servizio di internet banking; di essere stata contattata dalla banca resistente il giorno 8/08/2016 per informarla di 3 ricariche "internet" effettuate a carico del suo conto, a pochi minuti l'una dall'altra, per un totale di € 6.500,00. La cliente ha disconosciuto tali operazioni. Riferisce altresì di essere stata informata dal direttore della filiale che vi fossero stati ben 8 tentativi di operazioni fraudolente con "inserimenti plurimi di password" e che il beneficiario delle operazioni andate a buon fine fosse un cliente della banca stessa, e che nella stessa giornata erano avvenuti altri episodi simili. Afferma di aver sempre custodito con diligenza i codici e la chiavetta necessari per operare on line sul conto corrente.
La cliente chiede quindi il rimborso delle somme fraudolentemente distratte dal suo conto, per € 6.500,00, oltre interessi e spese.

In sede di controdeduzioni, l'intermediario:

- sostiene che non risultano manomissioni del sistema della banca all'epoca dei fatti in ricorso, e che la cliente è stata vittima di phishing, reso possibile da suoi comportamenti che integrano violazioni contrattuali; ciò sarebbe confermato dal fatto che le operazioni truffaldine sono state disposte da un indirizzo IP mai usato in precedenza dalla cliente;

- afferma che il login è avvenuto regolarmente con le credenziali della cliente ed è stato confermato con il suo codice OTP, e che le operazioni di ricarica di carta prepagata delle 21.01 e delle 21.02 (per € 3.000,00 ciascuna) sono state confermate dalla cliente inserendo sul sito fasullo il codice OTP generato dalla apposita chiavetta;
- riferisce che tre ulteriori tentativi di ricarica a beneficio della medesima carta, susseguitisi fra le 21.03 e le 21.04, non sono andati a buon fine per incapienza della "carta di addebito", mentre alle 21.04 è andato a buon fine un ulteriore tentativo per il minore importo di € 500,00;
- afferma che il sistema di sicurezza predisposto per l'utilizzo del canale home banking è un sistema a più fattori, per cui l'utilizzo fraudolento non può che essere ricondotto a un difetto di custodia dei dispositivi.

L'intermediario chiede:

- in via principale il rigetto del ricorso perché infondato;
- in via subordinata, la ripartizione fra le parti del danno anche ex art. 1227 c.c., in misura proporzionale alle effettive responsabilità.

DIRITTO

Il Collegio dopo aver accertato che le operazioni oggetto di contestazione sono successive all'entrata in vigore del d. lgs. n. 11/2010 di recepimento della PSD (Direttiva 2007/64/CE) e considerato il proprio costante orientamento relativamente alla materia dei furti e smarrimenti di strumenti elettronici di pagamento, rileva che, in base a tale indirizzo interpretativo, è applicabile al caso di specie l'art. 12 del citato decreto. In particolare, l'articolo 12, al comma terzo, prevede una franchigia di € 150,00 entro la quale l'utilizzatore può essere tenuto a sopportare la perdita prima della comunicazione di furto/smarrimento dello strumento di pagamento, fa salva l'ipotesi «in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento». L'art. 7, co. 2, dello stesso decreto legislativo prescrive poi che «l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo.
Questa valutazione deve essere compiuta alla luce delle circostanze di fatto che, di volta in volta, caratterizzano il caso di specie,
Nel caso in esame, il Collegio ritiene che l'intermediario resistente non abbia fornito la prova, nemmeno a livello presuntivo, della riconducibilità delle operazioni contestate ad una condotta del ricorrente nella quale sia ravvisabile quella "straordinaria e inescusabile imprudenza o negligenza" richiamata dalla giurisprudenza quale elemento costitutivo della colpa grave. L'effettuazione delle operazioni, da parte di soggetto diverso dal titolare del conto corrente, con l'utilizzo delle credenziali di accesso e dispositive corrette, non concreta per ciò solo un'omessa diligente custodia dello strumento di pagamento da parte del cliente, posto il chiaro dettato dell'art. 10, comma secondo, del D. Lgs. n. 11/2010 cit ("*in ogni caso, l'apparentemente corretta autenticazione non è di per sé necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca*").
Di fatto, l'assunto dell'intermediario secondo cui il correntista sarebbe rimasto vittima di *phishing* – assunzione che, comunque, non trova preciso riscontro nella narrativa del ricorrente – è rimasto a livello di ipotesi indimostrata.

Né l'intermediario ha spiegato le ragioni per le quali ben 8 disposizioni di ricarica di una medesima carta prepagata, effettuate una di seguito all'altra, non siano state intercettate come sospette anche in considerazione del fatto tali disposizioni sono state disposte da un indirizzo IP mai usato in precedenza dalla ricorrente.
Da quanto sopra, in conclusione, consegue l' applicazione dell'art. 12, comma terzo, D.Lgs. n. 11/2010 cit., nella parte in cui configura in via ordinaria una responsabilità fondata su un rigido criterio oggettivo e limitata alla franchigia, che espone l'utilizzatore a sopportare il danno conseguente all'utilizzo fraudolento di uno strumento di pagamento smarrito o sottratto avvenuto prima della comunicazione all'intermediario, per un importo di € 150,00, rimanendo il residuo importo delle operazioni fraudolentemente eseguite (€ 6.350,00) a carico del prestatore del servizio.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 6.350,00, oltre agli interessi legali dal reclamo al saldo.
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
FLAVIO LAPERTOSA