Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore MAURILIO D'ANGELO

Seduta del 12/03/2025

FATTO

La parte ricorrente, nella denuncia, ha affermato che il 12.08.2024 riceveva, sul proprio cellulare, un messaggio da parte della propria banca che le comunicava l'avvenuto pagamento di € 125,70, operazione effettuata all'estero. Ha quindi riferito di aver provveduto a segnalare la cosa all'intermediario e di essersi accorta, il giorno seguente, che erano stati effettuati altri pagamenti a propria insaputa, rispettivamente di € 125,70, € 126,18, e € 126,18.
La parte ricorrente domanda il rimborso della somma sottratta, pari a € 503,76.
L'intermediario ha eccepito che il ricorso è carente dei requisiti minimi di specificità, essendosi la parte ricorrente limitata a riferire di non aver mai autorizzato tali pagamenti e che tali carenze non consentono di ricostruire la dinamica dei fatti. Ha quindi precisato che, in ogni caso, le operazioni sono state eseguite tramite autenticazione forte.
L'intermediario resistente chiede che l'Onorevole Collegio oggi adito Voglia rigettare le domande del Ricorrente e, in via subordinata, nel merito, nella denegata ipotesi in cui dovesse essere accolta la domanda di controparte, in applicazione dell'art. 1227 c.c., graduare la responsabilità in ragione delle responsabilità imputabili al ricorrente.

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. In particolare, risulta applicabile il co. 3-ter dell'art.2, che estende l'applicazione delle disposizioni del titolo II (Diritti ed obblighi delle parti), a: "i servizi di pagamento in tutte le valute laddove soltanto uno dei prestatori di servizi di pagamento sia insediato nell'Unione europea, per le parti dell'operazione di pagamento ivi effettuate.
Nel merito si chiarisce che i pagamenti disconosciuti sono complessivamente 4, eseguiti tramite G***** P***fuori dall'UE in data 12.08.2024, per un totale di € 503,76
L'intermediario ha riferito che le operazioni contestate sono state autenticate tramite G***** Wallet, previa tokenizzazione della carta.
In generale sul proprio sistema di autenticazione l'intermediario ha riferito che *"L'utente deve scaricare l'applicazione ed effettuare un primo accesso per la registrazione, durante il quale viene indicato un indirizzo e-mail – che viene certificato mediante un codice OTP inviato sulla stessa e-mail – e una password. Al primo accesso all'applicazione l'utente è inoltre tenuto a procedere alla certificazione del dispositivo stesso, sempre tramite invio di un codice OTP al numero di telefono indicato in sede di conclusione del contratto (ove il Cliente ha dichiarato «di essere l'unico utilizzatore del numero di Cellulare sopra indicato» - cfr. pag. 17 sub doc. 1). Una volta autenticato il dispositivo, l'Utente potrà eseguire l'autenticazione solo da quello e accedere alla propria area personale mediante l'autenticazione forte a due fattori e, solo a quel punto, operare sul proprio conto.*
In ordine alla prova, nella riunione del 29.01.2025, il Collegio di Torino ha disposto che *"parte resistente fornisca piena prova circa l'autenticazione a doppio fattore per l'esecuzione delle operazioni di pagamento oggetto di controversia, nonché per la fase di tokenizzazione della carta di pagamento che ha preceduto l'operatività fraudolenta con digital wallet, allegando idonea documentazione a supporto"* e *"parte ricorrente fornisca chiarimenti in ordine alle circostanze della frode perpetrata a suo danno, allegando, se disponibile, documentazione a supporto",* fissando per tale adempimento il termine di 30 giorni dalla ricezione della comunicazione.
Orbene, l'intermediario, con nota del 28.02.2025, rispetto alla prova di autenticazione della tokenizzazione della carta di pagamento ha chiarito che i termini e le condizioni per la tokenizzazione della carta (doc. 4) prevedono la registrazione della carta su wallet tramite i seguenti passaggi:

- inserimento all'interno dell'App G**** P dei "*dati della propria Carta (Numero Carta/scadenza/CVC) e [de]i suoi dati personali (nome, cognome, indirizzo di residenza)";*
- utilizzo del codice OTP: se il Cliente riceve l'OTP e lo inserisce correttamente, la configurazione della Carta si concluderà con successo: verrà creato il Token associato alla Carta e il Cliente riceverà una comunicazione o tramite una notifica push in app sul device certificato o tramite SMS, che conferma l'avvenuta registrazione della Carta su G***** P**. Da questo momento il Cliente potrà procedere con pagamenti tramite G***** P**;

Nel caso di specie il ricorrente ha ricevuto il codice OTP via sms; il messaggio, come già indicato nelle controdeduzioni, chiariva come l'OTP servisse proprio per attivare G*** Pay.
Va rilevato che, nel caso di operazioni di pagamento disposte tramite *Digital Wallet* (ad es. Google Pay o Apple Pay) occorre verificare che l'intermediario fornisca la prova dell'autenticazione forte sia per la fase di c.d. "*tokenizzazione*" della carta nel wallet (registrazione e digitalizzazione della carta) – cfr. art. 10-*bis*, comma 1 del d.lgs. 11/2010 -

sia per la fase di pagamento vera e propria (anche se l'autenticazione è demandata ad un soggetto terzo).
Per quanto riguarda la prima fase, sono possibili due modalità di *tokenizzazione* della carta o direttamente dal *wallet*, catturando i dati della carta dalla fotocamera o inserendoli con input manuale (come avvenuto nel caso di specie) oppure dall'App di Mobile Banking: in questo caso la carta risulta già registrata e l'utente può aggiungere la carta al wallet.
Quanto alla seconda fase, l'autenticazione del pagamento avviene direttamente nel Mobile Wallet presente sullo smartphone, ove gli elementi necessari per la SCA sono il possesso dello smartphone con App e Token a bordo e uno a scelta tra un elemento di inerenza ed un elemento di conoscenza.
In caso di operazioni presso un esercente fisico, al momento del pagamento la combinazione di questi due fattori genera il codice univoco di autenticazione (cfr. RTS, art. 4) che viene inviato al POS. Le transazioni sono pertanto proposte al POS dal *wallet* come "già autenticate" e perciò il POS non chiede il PIN
Nel caso di specie, parte resistente non ha prodotto evidenze sulla prova della SCA per la tokenizzazione della carta. In ogni caso, poi, per la tokenizzazione risultano, per stessa dichiarazione dell'intermediario, essere stati utilizzati i seguenti fattori:

1. elemento di possesso: OTP inviato tramite Sms;
2. dati della carta e altri dati personali del cliente (elemento inidoneo a costituire fattore di autenticazione – cfr. l'Opinion dell'EBA "*on the elements of strong customer authentication under PSD2*" del 21 giugno 2019, citata nella decisione del Collegio di coordinamento n. 21285/2021).

In tale contesto si deduce, quindi, che il sistema di autenticazione per l'effettuazione delle operazioni di pagamento on-line è a un fattore.
Sul punto occorre rammentare che l'EBA, in merito alle carte di pagamento, ha precisato, nella sua Opinion del 21/06/2019, che le credenziali della carta non possono costituire né un elemento di conoscenza né un elemento di possesso.
Ne consegue che, nel caso in esame, l'intermediario non prova l'esistenza di un sistema di autenticazione forte per l'esecuzione delle operazioni.
Sotto tale profilo, in aderenza alla disciplina dell'art. 10 del d.lgs. 11/2010 che prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare l'autenticazione (che rappresenta un antecedente logico rispetto alla prova della colpa grave e/o del dolo dell'utente) nonché – per l'appunto – il comportamento gravemente colposo (o fraudolento e/o doloso) dell'utilizzatore, il ricorso deve essere accolto, in considerazione del fatto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 504,00.
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