COLLEGIO DI TORINO

composto dai signori:

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

Relatore LUCA CATTALANO

Seduta del 15/11/2024

FATTO

Parte ricorrente, dopo aver inutilmente esperito reclamo in data 09.04.2024, riferiva le proprie ragioni di controversia che si possono così riepilogare:

- di essere stata vittima di *phishing* a seguito del quale le venivano sottratto l'importo di € 1.070,00;
- che, in particolare, i malfattori camuffavano il numero di telefono, facendole vedere che i messaggi e la chiamata provenivano dalla banca stessa.

Spiegava conclusioni chiedendo il rimborso della somma di € 1.070,00.
Nel costituirsi con controdeduzioni l'intermediario resistente deduceva le proprie ragioni che possono così brevemente essere riassunte:

- che le operazioni di € 1.000,00 e di € 70,00 disconosciute dalla ricorrente erano state correttamente autorizzate mediante l'utilizzo delle credenziali statiche e dinamiche in possesso della ricorrente medesima con autenticazione forte a due fattori, in assenza di anomalie;
- che la descrizione di quanto occorso rendeva inoltre evidente come la ricorrente avesse violato con colpa grave l'art. 7 del D.Lgs. 11/2010;

- che, infatti, la ricorrente aveva fornito le proprie credenziali personalizzate nonostante la banca mettesse a disposizione dei clienti numerosi contenuti, in costante aggiornamento, sulla sicurezza informatica e nonostante la stessa avesse ricevuto un'apposita email volta ad informare i clienti in merito alla truffa dello *spoofing*;
- che, in particolare, per assicurare ai propri clienti di avere la certezza di essere in contatto telefonicamente con la Banca, simultaneamente all'avvio della telefonata, la banca inviava sempre al destinatario della stessa un avviso di conferma mediante il canale "i miei messaggi" accessibile esclusivamente nell'App;
- che pertanto in assenza di tale notifica, il cliente poteva avere la certezza che si trattava di una frode;
- che inoltre il testo degli SMS contenti le OTP conteneva la specifica indicazione di non condividere i tali dati con alcuna persona;
- che la Banca, nel medesimo giorno della frode, aveva inviato alla ricorrente varie segnalazioni via *push* nell'App: dell'accesso all'area riservata della ricorrente mediante un nuovo dispositivo, dell'inizio del processo per l'attivazione del Riconoscimento Biometrico, della conferma dei pagamenti con Carta.

Concludeva chiedendo il rigetto del ricorso.

Il Collegio, nella riunione del 25.09.2024, ha disposto che "*parte resistente fornisca piena prova del sistema di autenticazione a doppio fattore per l'esecuzione delle due operazioni di pagamento contestate, integrando la documentazione già in atti con idonea legenda esplicativa al fine di rendere al Collegio intellegibile la medesima*".

DIRITTO

Il presente ricorso riguarda due transazioni *e-commerce* di € 1.000,00 e di € 70,00, effettuate con la carta di debito.

Tali operazioni risultano dalla denuncia e dalle evidenze prodotte dalla banca resistente.

Il Collegio richiama ai fini della decisione la normativa di attuazione della c.d. PSD2 – che ha novellato tra l'altro le norme del T.U.B. e del decreto legislativo n.11/2010 - ed ha introdotto, a carico dei prestatori di servizi di pagamento, l'obbligo di adottare requisiti tecnici e commerciali uniformi, anche allo scopo di garantire una maggior sicurezza, efficienza e competitività dei pagamenti elettronici, a vantaggio di esercenti e consumatori.

L'art. 8 comma 1 lett. a) del decreto legislativo n.11/2010 come integrato dal d.lgs. 218/2017 dispone che il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7: ovvero utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso ed inoltre comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza, comunque adottando tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.

Di seguito l'art. 10 della medesima disposizione prescrive che, qualora l'utilizzatore del servizio di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita, incombe in capo al prestatore del servizio di pagamento l'onere di provare che l'operazione disconosciuta 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.
Il comma secondo della suddetta disposizione aggiunge, tra l'altro, che in caso di operazione disconosciuta l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento (ad esempio un dispositivo personalizzato cd. chiavetta o token, ecc.) non è di per sé solo necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dal cliente, né che questi abbia agito in modo fraudolento o che non abbia adempiuto con dolo o colpa grave ad uno o più degli obblighi di cui all'art. 7.
Infine, l'art. 9 del D.lgs. n. 11/2010 e smi dispone che l'utilizzatore, venuto a conoscenza di un'operazione di pagamento non autorizzata o eseguita in modo inesatto, ne ottiene la rettifica solo se comunica senza indugio tale circostanza al proprio prestatore di servizi di pagamento secondo i termini e le modalità previste nel contratto quadro o nel contratto relativo a singole operazioni di pagamento. La comunicazione in ogni caso deve essere effettuata entro 13 mesi dalla data di addebito, nel caso del pagatore, o di accredito, nel caso del beneficiario.
Ne consegue che qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio; e nel contempo quest'ultimo è obbligato a rifondere con sostanziale immediatezza il cliente in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode e salva la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata.
Pertanto, con riferimento all'utilizzazione di servizi e strumenti con funzioni di pagamento elettronici deve sempre essere operata la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio, in ragione del fatto che la diligenza posta a carico dell'intermediario ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere, essendo in ogni caso tenuta a fornire la prova della riconducibilità dell'operazione al cliente.
Corollario di tale impostazione giuridica è che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, va esclusa solo se ricorre –integralmente o in ragione parziale - una situazione di colpa grave dell'utente (cfr. *ex multis* Collegio di Milano, decisione 8262/2020).
Parte resistente ha fornito, anche a seguito della integrazione istruttoria, ampia documentazione atta a comprovare l'articolata procedura di autenticazione di tutte le fasi delle operazioni in contestazione.
In particolare parte resistente ha allegato i log interni della Banca relativi all'esecuzione dei pagamenti con carta oggetto di contestazione, corredati da una legenda esplicativa delle sigle e dei dati riportati nei log medesimi e nelle controdeduzioni.
Sempre parte resistente ha precisato che le ulteriori informazioni presenti negli allegati documentali di cui non era stata fornita esplicazione nella legenda costituivano meri dati tecnici inerenti all'esecuzione delle operazioni di pagamento con carta e non attenevano alla relativa autorizzazione.
Posto quanto appena richiamato, il Collegio, nonostante l'integrazione istruttoria, non riesce a ricavare l'impiego dei singoli fattori concretamente impiegati per l'autenticazione forte e descritti dall'intermediario nelle proprie controdeduzioni (biometria, quale elemento di inerenza, e Token e CVV dinamico quali elementi di possesso).

Anche il riferimento al protocollo *M*** Securecode* non è risolutivo in tal senso, dal momento che al pari del protocollo 3DSecure esso rappresenta esclusivamente un protocollo di trasmissione dati che non è di per sé in grado di indicare l'impiego dell'autenticazione forte.
In sintesi risulta impossibile individuare con certezza i fattori di autenticazione indicati dall'intermediario per l'autenticazione dell'operazione in parola.
Il Collegio, quindi, nel pronunciarsi a favore della parte ricorrente richiama le argomentazioni espresse con la propria decisione n. 5255/2024, secondo cui *"Il Collegio ha richiesto al PSP un'integrazione documentale per chiarire il contenuto delle evidenze già fornite relativamente alla esecuzione dei due pagamenti di e-commerce.*
Neppure a seguito delle precisazioni fornite dall'intermediario risulta chiaro se le notifiche push richiamate nelle controdeduzioni dallo stesso intermediario e documentate si riferiscano ad un fattore di autenticazione (push dispositive in app), mancando il testo del messaggio, oppure a push di alert di avvenuta transazione, posto che sembra che siano state inviate ulteriori push con testo "Acquisto con carta autorizzato".
Per altro, l'intermediario nulla ha riferito in merito ai fattori di autenticazione impiegati per la modifica dei massimali preordinata a consentire l'esecuzione di tali operazioni. Per le operazioni di pagamento con carta assume, dunque, natura dirimente la mancata prova della SCA, sicché esse andranno interamente rimborsate al ricorrente (…)"
Come è noto, infatti, deve senz'altro affermarsi la responsabilità dell'intermediario resistente in ordine al danno lamentato dalla parte ricorrente, conformemente al prevalente orientamento ABF secondo il quale, in caso di operazioni bancarie effettuate a mezzo di strumenti elettronici, la non corretta operatività del servizio bancario mediante collegamento telematico, ivi compresa la possibilità di una abusiva utilizzazione delle credenziali di accesso da parte di terzi, rientra nel rischio d'impresa della banca intermediaria. Su quest'ultima grava pertanto una responsabilità di tipo oggettivo, dalla quale la banca va esente solo provando che le operazioni contestate dal cliente sono attribuibili a dolo o colpa grave di quest'ultimo e comunque abbia provato quale intermediario di essersi comunque dotato di un procedimento pluri-fattoriale di autenticazione delle operazioni di pagamento secondo i parametri-base della c.d. PSD2 e dell'EBA, costituendo essa un *prius* logico rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.
La domanda della parte ricorrente merita pertanto accoglimento, atteso che la predisposizione da parte dell'intermediario di un sistema di autenticazione forte per l'operatività su conto on line di per sé rappresenta, come dedotto, il minimo della cautela pretesa dal legislatore per evitare che il prestatore di servizi di pagamento risponda in ogni caso (quindi anche nell'ipotesi di colpa grave del pagatore) di qualsiasi operazione non autorizzata, salva la frode ai sensi dell'art. 12.2-*bis* del d.lgs. 11/2010.
Era, al sommar di tutto, onere di parte resistente dover provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento sulla base di un principio di buona fede nell'esecuzione del contratto. In assenza di tale prova è corretta la decisione di imputare all'intermediario il rischio professionale della possibilità che terzi accedano ai profili dei clienti con condotte fraudolente, senza che sia necessario vagliare la condotta tenuta da parte ricorrente nell'occorsa truffa subita.
Il Collegio riconosce, quindi, a parte ricorrente l'integrale rimborso della somma pretesa pari ad € 1.070,00.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.070,00.
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