COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) GRIPPO

Seduta del 18/04/2023

FATTO

Parte ricorrente afferma che: è titolare di un conto corrente presso l'intermediario resistente; in data 5/04/22 ha ricevuto un SMS apparentemente proveniente dall'intermediario con il quale le veniva comunicato il blocco della carta; poco dopo ha ricevuto una telefonata apparentemente proveniente dall'intermediario, durante la quale il sedicente operatore le spiegava che avrebbe dovuto scaricare un'applicazione tramite il link inviato via SMS; si è avveduta di essere stata vittima di una truffa quando, insospettita dalla chiamata ricevuta il giorno precedente e dopo aver scaricato nuovamente la vecchia applicazione, in data 6/04/22 accedeva al proprio conto corrente e scopriva che il giorno prima era stato disposto un bonifico di € 18.469,23 a favore di un soggetto terzo sconosciuto; ha immediatamente contattato il servizio clienti dell'intermediario, senza tuttavia riuscire a bloccare il bonifico; ha presentato denuncia presso le Autorità competenti per il disconoscimento dell'operazione; ha inviato formale reclamo all'intermediario contestando i tempi di esecuzione delle operazioni e la mancata revoca del bonifico, nonché la mancata ricezione di SMS alert; è stata vittima incolpevole di spoofing, da ritenersi truffa sofisticata.

Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma di € 18.470,23.
L'intermediario, con le controdeduzioni, precisa che: la ricorrente è stata vittima di phishing; le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risulta che sono avvenute con il corretto inserimento delle credenziali; le operazioni sono state validate correttamente con un sistema di autenticazione a due fattori, uno statico (PIN – fattore di conoscenza) e uno dinamico (OTP – fattore di possesso); gli SMS alert e le notifiche push risultano regolarmente consegnati; sussiste la colpa grave del cliente in quanto ha seguito le istruzioni impartite dal sedicente operatore, cancellando l'applicazione della banca e installandone un'altra non ufficiale, nella quale ha immesso le proprie credenziali, venendo dunque meno al dovere di diligenza richiesto per la custodia di tali dati; sussiste la colpa grave del cliente anche perché i link contenuti negli SMS non erano in alcun modo riconducibili all'intermediario e presentavano inoltre il protocollo "http" invece di "https"; infine non ha potuto bloccare il bonifico in quanto l'operazione è stata disconosciuta il giorno successivo, dunque fuori dal termine utile.
L'intermediario chiede, pertanto, di rigettare il ricorso perché infondato.
Parte ricorrente, in sede di repliche, afferma che: l'intermediario non ha adempiuto l'onere della prova in quanto l'estratto dei log prodotto non permette di ricostruire l'intera sequenza delle operazioni; come affermato anche dall'intermediario, se il cliente può attivare il Mobile Token contemporaneamente su due dispositivi (2 smartphone oppure 1 smartphone e 1 tablet) ed è libero di sostituire il proprio device senza dover comunicare il nuovo modello alla banca se il numero di cellulare resta invariato, è evidente che tale regola sia stata violata dal momento che il truffatore ha attivato il Mobile Token sul suo device, ma con un numero di cellulare diverso.
L'intermediario, in sede di controrepliche, precisa che: i log nel formato esibito, non editabile e corredato di legenda, rispondono a quanto richiesto dalla normativa in tema di prova di autenticazione forte ed esecuzione delle operazioni di pagamento e sono riconosciuti dall'orientamento diffuso dell'ABF; l'attivazione del Mobile Token sul nuovo device è avvenuto correttamente seguendo i quattro passaggi richiesti (1. Scarica app *** dallo Store; 2. Inserisci numero cliente e PIN; 3. Scegli un Nickname; 4. Conferma mediante inserimento del codice OTP inviato per SMS); sussiste la colpa grave della ricorrente per aver cliccato su link non riconducibili all'intermediario e per aver addirittura cancellato l'applicazione ufficiale seguendo acriticamente le istruzioni impartite dal sedicente operatore, consentendo in questo modo al terzo di assumere il controllo del suo strumento di pagamento e/o delle sue credenziali di sicurezza.

DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
L'operazione contestata da parte ricorrente rientra nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi

personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici dispositivi). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
In tal senso sono chiare le indicazioni delle Direttiva 2015/2366/UE, laddove, al considerando n. 95, si afferma che: "*La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico. Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, adottando tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre al massimo il rischio di frode*".
La normativa mostra un chiaro *favor*e probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo ovvero che questi abbia agito in modo fraudolento, con dolo o colpa grave.
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
Nel caso di specie, sotto il primo profilo, l'intermediario ha prodotto una completa documentazione relativa alla registrazione, contabilizzazione e autenticazione delle operazioni disconosciute, assolvendo in questo modo il proprio onere probatorio di autenticazione ed esecuzione. Sul punto si precisa che non risulta meritevole di accoglimento l'eccezione del ricorrente circa l'inutilizzabilità dell'allegato riportanti i log delle operazioni.
Si tratta, quindi, di verificare se ricorra o meno una violazione degli obblighi di cui all'art. 7 D.Lgs. n. 11/2010 imputabile ad un comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore.
I vari Collegi ABF hanno chiarito, in conformità alle decisioni assunte dalla giurisprudenza di legittimità, che la colpa grave consiste in un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti: non dunque ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che appaia abnorme ed inescusabile.
Nel caso di specie, il Collegio rileva che la fattispecie va ricondotta ad un caso di c.d. "*SMS spoofing*", che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che esso appaia provenire da un soggetto differente - in questo caso, dall'intermediario -, rimpiazzando il numero originario con un testo alfanumerico (ossia quello utilizzato dall'intermediario per i propri messaggi genuini). In tal modo, il truffatore può inviare SMS-civetta che sembrano provenienti da numeri o contatti legittimi. Ritiene il Collegio che, nel valutare le implicazioni dell'impiego delle più recenti ed insidiose tecniche informatiche truffaldine occorra nondimeno considerare in prima istanza il contenuto del messaggio che – vuoi via email, vuoi via SMS – la vittima del raggiro riceve; e, successivamente, gli eventuali estremi di colpa nella condotta successiva alla ricezione.

Il ricorrente ha ricevuto un SMS che veniva raffigurato come proveniente dall'effettivo intermediario: detta circostanza è sicuramente dirimente ai fini di una diminuzione della responsabilità in capo al ricorrente medesimo, che non aveva elementi per poter distinguere la genuina provenienza del messaggio. La schermata prodotta dal ricorrente, infatti, contiene, oltre ai messaggi truffaldini, anche messaggi genuini, quale quello di certificazione del numero di telefono ("*Ti confermiamo di aver certificato il tuo numero. Per info:* ****"), nonché un messaggio precedente alla data del 5/04/22.
La concatenazione delle circostanze è tale da consentire al Collegio di affermare che l'intermediario non abbia predisposto tutti i presidi di sicurezza necessari a impedire che il ricorrente fosse ingannato. D'altro canto, si può al contempo affermare che il ricorrente non abbia tenuto un comportamento improntato alla massima prudenza, là dove egli ha inviato i vari codici ricevuti sul proprio cellulare.
Sul tema, peraltro, il Collegio di Coordinamento (decisione n. 22745/19) ha affermato che la nuova disposizione sull'onere probatorio di cui al comma 2 dell'art.10 va a potenziare la tutela dell'utente il quale, nell'utilizzo degli strumenti di pagamento, può restare vittima di attività fraudolente che, allo stato delle conoscenze tecnologiche, possono prevalere sui presidi di sicurezza approntati dal PSP, senza che al comportamento dell'utilizzatore possa riconoscersi alcuna efficienza causale (o quanto meno non determinante) nella produzione del fatto illecito. Va in proposito sottolineato come lo sviluppo tecnologico abbia reso sempre più sofisticate e aggressive le attività fraudolente volte a interferire con il corretto utilizzo degli strumenti di pagamento. In particolare, appare significativa la segnalazione da parte degli stessi organismi gestori dei servizi di pagamento di possibili intrusioni truffaldine tramite Messaggi SMS "spoofed", attraverso i quali gli aggressori utilizzano dei software per modificare l'ID del mittente del messaggio in modo che appaia con il nome del PSP. In sostanza, il messaggio truffaldino verrebbe visualizzato negli smartphone insieme a precedenti messaggi legittimi provenienti effettivamente dal PSP (come nel caso di specie), aumentando la probabilità che il messaggio stesso venga considerato genuino.
Ciò posto, nell'opera di valorizzazione delle singole e specifiche circostanze relative alla fattispecie in esame, il Collegio ritiene che nel caso di specie sia configurabile un concorso di colpa tra le parti e, quindi, dispone a favore di parte ricorrente il rimborso della somma di € 9.235,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 9.235,00.
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
FLAVIO LAPERTOSA