Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) GRIPPO

Seduta del 22/11/2022

Esame del ricorso n. 1066583 del 08/07/2022

proposto da

nei confronti di 7601 -

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) GRIPPO

Seduta del 22/11/2022

FATTO

Parte ricorrente afferma che: alle ore 13.26 del 23/02/2022 riceveva un SMS che sembrava provenire dall'intermediario in quanto collocato nella chat genuina; con l'SMS gli veniva comunicato che doveva essere eseguito un aggiornamento per evitare un blocco del sistema e veniva quindi contattato telefonicamente da un soggetto che si qualificava come operatore dell'intermediario e che conosceva anche la password di accesso all'home banking; solo successivamente si avvedeva di essere stato vittima di una truffa, in quanto veniva contattato dal servizio antifrode che lo avvisava di numerose operazioni dal suo conto e con la sua carta, operazioni mai autorizzate.
Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma di € 12.247,95.
L'intermediario, con le controdeduzioni, precisa che: il ricorrente è stato vittima di phishing; tutte le operazioni, infatti, sono state correttamente contabilizzate, registrate e autenticate e sono avvenute con il corretto inserimento delle credenziali personali; non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici; nel caso di specie sussiste la colpa grave del ricorrente.
L'intermediario chiede, pertanto, di rigettare il ricorso perché infondato ovvero in via subordinata di applicare la franchigia prevista per legge.
Parte ricorrente, in sede di repliche, afferma che: non è contestato che l'SMS civetta era collocato nella chat genuina; le falle nei sistemi dell'intermediario hanno consentito di

eseguire la truffa; non ha mai fornito i propri dati a terzi soggetti; le operazioni eseguite dal truffatore non sono operazioni bancarie; non è chiaro come possano essere state eseguite operazioni tramite POS senza la carta; le operazioni erano per lo più successive al contatto dell'ufficio antifrode e pertanto revocabili.

DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
Le operazioni contestate da parte ricorrente (n. 15 operazioni eseguite con due diverse carte di pagamento nei giorni 23 e 24 febbraio 2022, per un importo complessivo di € 12.247,95) rientrano 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).
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*".
Su tale presupposto l'art. 10-bis del d.lgs. n. 11 del 2010 prevede che "*1. [...] i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quanto l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare il rischio di frode nei pagamenti o altri abusi. 2. Nel caso dell'avvio di un'operazione di pagamento elettronico di cui al par. 1, lett. b), per le operazioni di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico. 3. [...] i prestatori di servizi di pagamento predispongono misure di sicurezza adeguate per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento*".
In altri termini, la disciplina in parola, al fine di fornire una tutela effettiva all'utente, richiede che per le operazioni di pagamento elettronico il prestatore di servizi di pagamento applichi sistemi di autenticazione forte del cliente, tanto da prevede, all'art. 12, co. 2-bis, d.lgs. n. 11 del 2010, che "*salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente*", con ciò escludendo quindi l'applicazione della franchigia di € 50,00 applicabile "negli altri casi", ai sensi del comma 3 dello stesso articolo.
Risulta pertanto agevole rilevare che in tale contesto una importanza centrale assume la nozione di "autenticazione forte del cliente", individuata dall'art. 1, lett. q-bis), d.lgs. n. 11 del 2010, il quale, nel definire la stessa ne individua gli specifici requisiti, prevendendo che sia tale "*un'autenticazione basata sull'uso di due o più elementi, classificati nella categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".

Ciò premesso, 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 PIN). 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.
La normativa mostra un chiaro *favor* 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 oppure che questi abbia agito in modo fraudolento ovvero 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 non ha prodotto una completa documentazione relativa alla registrazione, contabilizzazione e autenticazione delle operazioni disconosciute, non assolvendo in questo modo il proprio onere probatorio di autenticazione ed esecuzione.
In particolare, l'intermediario afferma che sono stati richiesti l'inserimento della password (elemento di conoscenza) e l'inserimento di un codice OTP via SMS (elemento di possesso); sulla base della legenda prodotta, si osserva che è in effetti presente il codice "02", ma il dettaglio dei log presenta il diverso codice "03" in corrispondenza di *authentication type* ed in ogni caso non è agli atti copia degli SMS inviati.
Il Collegio ricorda che è onere dell'intermediario provare, in modo rigoroso, che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/2010). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute (cfr. Collegio di Milano, decisione n. 1588 del 17 febbraio 2017).
Questo stesso Collegio recentemente ha stabilito che: "*seppure il sistema di autenticazione predisposto dall'intermediario sia astrattamente conforme ai requisiti della SCA, ciò non lo esime dal fornire la prova che le operazioni disconosciute siano stata effettivamente ed in concreto autenticate con un sistema a due fattori*" (Collegio di Milano, decisione n. 2932 del 17/2/2022).
Pertanto, posto che secondo il consolidato orientamento di questo Arbitro spetta all'intermediario resistente offrire preliminarmente la prova della corretta autenticazione delle operazioni disconosciute di cui il cliente chiede il rimborso, in mancanza di allegazione della documentazione comprovante la specifica e corretta autenticazione delle operazioni contestate queste devono essere considerate non autorizzate con conseguente integrale rimborso dell'importo delle stesse alla parte ricorrente; nel caso di specie, peraltro, non può trovare applicazione la franchigia di cui all'art. 12, co. 3, d.lgs. n. 11 del

2010, in quanto trattasi di utilizzi fraudolenti on line. (cfr. Collegio di Coordinamento, decisione n. 24366/2019).
Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma di € 12.248,00.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 12.248,00.
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