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) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CETRA

Seduta del 25/05/2023

FATTO

Con ricorso del 28 gennaio 2023, parte ricorrente riferiva che, in data 8.11.2022, la sua sim smetteva di funzionare, sicché contattava l'assistenza dell'operatore telefonico, che apriva una richiesta di intervento. Il ricorrente aggiungeva che, due giorni dopo (il 10.11.2022), sua moglie, cointestataria del conto corrente, accedeva tramite app al servizio di *home banking* e si accorgeva che lo 8.11.2022 erano stati disposti due bonifici istantanei fraudolenti per complessivi € 10.180,00. Il ricorrente, il giorno seguente (lo 11.11.2022), sporgeva denuncia e disconosceva le due operazioni truffaldine. Integrava, poi, la denuncia con quanto riusciva ad apprendere dall'assistenza dell'operatore telefonico, il quale lo informava che il giorno in cui la sim smetteva di funzionare era stata effettuata una sostituzione della stessa, tramite esibizione di una denuncia di furto a suo nome, a sua insaputa. Il che comportava l'attivazione della sim in possesso del truffatore e la disattivazione della sua precedente. Il ricorrente negava di aver mai fornito a terzi codici di accesso o password ed affermava che la sostituzione fraudolenta della sua sim con modalità sim swap fraud aveva permesso ai truffatori di impossessarsi del suo numero di telefono certificato e di perpetrare la truffa ai suoi danni, vanificando uno degli elementi su cui si basa l'autenticazione forte ossia l'elemento del possesso. Parte ricorrente, esperito infruttuosamente il reclamo, si rivolgeva all'Arbitro per domandare il rimborso dell'importo dei bonifici disconosciuti, pari ad euro 10.180,00.

L'intermediario, nelle proprie controdeduzioni, eccepiva preliminarmente il difetto di legittimazione passiva: la domanda di rimborso della somma indebitamente sottratta al ricorrente era, infatti, da intendersi come rivolta alla compagnia telefonica, la quale aveva contribuito in maniera determinante al verificarsi della truffa, non avendo protetto adeguatamente i dati del cliente. Nel merito, affermava la colpa grave del cliente per aver presumibilmente comunicato le credenziali di accesso all'app dell'intermediario nonché alla piattaforma di trading online D***: tutte le operazioni contestate risultavano, infatti, correttamente autenticate, registrate e contabilizzate, in assenza di alcun malfunzionamento delle procedure necessarie per la loro esecuzione. Affermava che la frode sarebbe stata resa possibile non solo tramite la duplicazione della SIM, bensì anche dalla conoscenza delle suddette credenziali, reperite tramite una diversa e separata azione. Addebitava, inoltre, al ricorrente di non aver tenuto conto di tre comunicazioni avvenute lo stesso giorno della frode - sia via e-mail sia via sms - da parte dell'intermediario, con le quali veniva avvisato, rispettivamente, del reset del PIN dispositivo e dell'avvenuta esecuzione dei due bonifici. Rappresentava di avere tentato, ma inutilmente, il richiamo dei due bonifici in data 11.11.2022 (alle ore 15:57). Concludeva per il rigetto del ricorso ovvero, in subordine, per la ripartizione tra le parti del danno in misura proporzionale alle effettive rispettive responsabilità.
Il ricorrente, con le repliche, insisteva per la legittimazione passiva dell'intermediario. Negava di aver mai comunicato a terzi codici di accesso o password di alcun tipo, precisando di non avere potuto ricevere le comunicazioni dell'intermediario perché la sua mail era stata violata con l'inserimento di filtri tramite i quali il truffatore, a sua insaputa, bloccava, rifiutava e reindirizzava in uscita e in entrata qualsiasi tipo di comunicazione intrapresa con la piattaforma di trading online. Confermava le richieste avanzate nel ricorso. L'intermediario, con le controrepliche, o eccepiva un comportamento gravemente imprudente e negligente del cliente, per aver contribuito alla divulgazione di ben tre credenziali (della mail, dell'home banking e della piattaforma di trading online). Precisava che il sistema non avesse impedito lo "sgancio token" poiché la certificazione era avvenuta nel pieno rispetto del sistema di autenticazione forte. Sosteneva, infine, che la contemporanea elusione di due distinti fattori di autenticazione, aveva permesso la realizzazione della frode. Insisteva nelle richieste delle controdeduzioni.

DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte a seguito di due bonifici istantanei dell'importo complessivo di euro 10.180,00. Le operazioni contestate sono state compiute in data 8.11.2022, rispettivamente, alle ore 13:31 e alle ore 16:46: rientrano, dunque, nell'ambito di applicazione della disciplina del d. lgs. 27.1.2010, n. 11 di recepimento della Direttiva 2007/64/CE sui servizi di pagamento, come modificata dal d. lgs. 15 dicembre 2017, n. 218 di recepimento della Direttiva 2015/2366/UE.

Da quanto in atti, risulta pacifico che le operazioni fraudolente siano avvenute con la tecnica della sim swap fraud, sicché l'intermediario ha eccepito il proprio difetto di legittimazione passiva sostenendo che alla realizzazione della truffa abbia contribuito in modo determinante la compagnia telefonica, venendo meno al suo obbligo di garantire la protezione dei dati del cliente e, nello specifico, di identificare i clienti anche per la mera sostituzione delle sim. Ritiene, dunque, che sia ad essa unicamente imputabile l'avvenuta appropriazione indebita dell'utenza telefonica del cliente da parte di terzi, che nel caso concreto avrebbe reso possibile il perpetrarsi della truffa.

L'eccezione preliminare, pur in linea con alcune recenti pronunce di merito (Tribunale di Milano, 31.10.2022; Tribunale di Monza, 6.7.2022), non coglie pienamente nel segno. Per pacifico orientamento di questo Arbitro, a prescindere dalla tipologia di truffa, allorché il cliente disconosca una o più operazioni fraudolente, la normativa vigente fa gravare sull'intermediario l'obbligo di dimostrare la regolare autenticazione delle operazioni contestate e di fornire la prova del dolo ovvero della colpa grave del cliente stesso. Inoltre, pur essendo la sostituzione della sim riferibile ad un soggetto terzo (la compagnia telefonica), rientra nel rischio tipo dell'attività d'impresa dell'intermediario e, dunque, è ad esso imputabile l'avvalersi di una modalità di autenticazione (sms; otp) che affida in parte a terzi la procedura che conduce all'esecuzione delle operazioni di pagamento.

Il Collegio, passando al merito, ricorda che, ai sensi del d.lgs. 11/2010, la corretta esecuzione di un'operazione di pagamento è subordinata al consenso del pagatore (art. 5 d. lgs. 11/2010), prestato nella forma e secondo la procedura contrattualmente prevista. Qualora l'utente neghi di aver autorizzato l'operazione o sostenga che questa non sia stata correttamente eseguita, lo stesso può ottenerne il rimborso dell'importo (art. 11 d. lgs. 11/2010), a meno che il prestatore dei servizi di pagamento non riesca a provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10 d. lgs. 11/2010). Il prestatore dei servizi, peraltro, assolto con successo questo primo onere, necessario ma di per sé insufficiente a dimostrare che l'operazione sia stata autorizzata dal titolare, deve ancora provare, al fine dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento, fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010, trattandosi primariamente di obblighi di custodia del dispositivo e delle chiavi di accesso al servizio. La valutazione della condotta dell'utilizzatore, ai fini dell'eventuale giudizio di colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.

Il Collegio ricorda, inoltre, che la suddetta autenticazione si deve realizzare in forma di autenticazione forte (c.d. strong customer authentication in acronimo SCA), secondo quanto stabilito dagli artt. 97 e 98 della PDS2, dall'art 10-*bis* del d. lgs. 10/2011 e nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dallo stesso EBA. E questo sia nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni: l'autenticazione, in tutti questi casi, richiede almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso; gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Il Collegio, venendo allo specifico caso oggetto di decisione, rileva che l'intermediario afferma che i truffatori hanno configurato un nuovo dispositivo, cosa che normalmente avviene con l'utilizzo di credenziali statiche (username e password) nonché con l'inserimento dell'OTP ricevuto via sms al telefono certificato. L'intermediario ha documentato l'invio del codice OTP tramite sms ma non l'inserimento della password, che rappresenta l'elemento di conoscenza; quindi, non ha documentato in dettaglio e non ha offerto una precisa evidenza del secondo fattore di autenticazione richiesto, ossia il fattore di conoscenza, in aggiunta all'OTP. Quanto poi, all'accesso all'area personale e alle disposizioni dei due bonifici, l'intermediario documenta l'invio della notifica push a numero riconducibile al ricorrente, verosimilmente in uso dei truffatori a seguito di sim swap fraud,

ma non dà evidenza dell'impiego degli altri fattori di autenticazione dichiarati, considerato anche che le tracciature allegate e riferite all'operatività contestata sono prive di legenda.

Il Collegio, da tutto questo, ritiene che non si possa considerare raggiunta la prova della corretta autenticazione richiesta all'intermediario, rendendo, allora, irrilevante qualunque valutazione in merito alla condotta tenuta dalla ricorrente. L'intermediario, pertanto, deve sopportare tutto il peso economico delle operazioni disconosciute.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 10.180,00.
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