



COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) GENOVESE	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore ANDREA GENOVESE

Seduta del 09/12/2025

FATTO

Insoddisfatta dell'interlocuzione con l'intermediario nella fase del reclamo, con ricorso n. 1842254 del 24.09.2025, la parte ricorrente si rivolge all'Arbitro al quale chiede di disporre il rimborso della somma di Euro 2.000,00, corrispondente all'importo di n. 8 operazioni di pagamento online fraudolentemente eseguite. A sostegno delle pretese, deduce che: (i) in data 24.06.2025 riceveva un SMS apparentemente proveniente dall'intermediario, con il quale le veniva segnalato il blocco della carta; (ii) cliccava su un link e, su indicazione di un sedicente operatore, forniva i propri dati personali; (iii) resasi conto della truffa, bloccava la carta e sporgeva denuncia; (iv) veniva a conoscenza che erano stati eseguiti n. 8 operazioni di pagamento, per un totale di Euro 2.000,00, su un sito internet; (v) l'intermediario non ha apprestati presidi di sicurezza efficienti per la propria carta di pagamento né ha fornito adeguata assistenza.

Costituitosi, l'intermediario chiede all'Arbitro di rigettare il ricorso perché infondato, sul rilievo che: a) si tratta di un tipico caso di *phishing*; b) le operazioni sconosciute sono avvenute nel pieno rispetto delle procedure previste contrattualmente e normativamente, correttamente autenticate, registrate e contabilizzate, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi; c) i

truffatori aggiravano il processo di *enrollment* in SCA attraverso la necessaria partecipazione del cliente, dal quale carpiavano i dati personali ed i codici di sicurezza; d) non consta un generale obbligo di monitoraggio *ex ante* delle operazioni disconosciute in capo al PSP; e) le operazioni disconosciute, tenuto conto della modalità con cui sono state autorizzate, potevano essere eseguite soltanto dal titolare dello strumento di pagamento, ossia il ricorrente, che è in possesso del *device* su cui è inviata la notifica in APP per l'inserimento del codice di sicurezza "P***", o, in ultima istanza, da un terzo a cui potrebbero essere stati forniti - anche inconsapevolmente nell'ambito di uno schema fraudolento di *phishing* tradizionale - i codici di sicurezza e la password dinamica necessari per l'abilitazione di tale procedura di autenticazione; f) il blocco della carta è avvenuto alle ore 8:42 del giorno 25.06.2025, successivamente alle operazioni contestate. Pertanto, il ricorrente non ha adempiuto ai propri doveri di tempestiva segnalazione all'intermediario; g) nella data in cui si sono verificate le operazioni contestate, la carta del ricorrente è stata associata su un nuovo dispositivo. Tale operazione è stata possibile a seguito dell'inserimento del codice OTP ricevuto sul suo numero di telefono certificato; h) ha messo a disposizione dell'utente il servizio SMS *alert* e ha inviato una notifica in App; i) ha realizzato campagne informative sulle truffe di tale specie; l) nel caso di specie, è provata la colpa grave del ricorrente.

In sede di repliche, la parte ricorrente deduce che: (i) l'intermediario, in sede di controdeduzioni, non fornisce prove effettive sul fatto che le operazioni contestate siano state dalla stessa autorizzate o che la propria condotta sia gravemente colpevole; (ii) il riferimento ai log informatici e alle procedure SCA non dimostra che sia stata lei stessa – e non il frodatore – a operare; (iii) l'intermediario ammette, in sede di controdeduzioni, che *"la carta del ricorrente è stata associata su un nuovo dispositivo"*, confermando che le autorizzazioni non provenivano dal proprio *device* ma da uno diverso. Ciò implica che il frodatore abbia potuto attivare il codice di sicurezza P*** su un altro dispositivo utilizzando codici OTP ricevuti sul proprio telefono, dinamica che l'intermediario avrebbe dovuto impedire; (iv) che l'inesistenza dell'obbligo di monitoraggio *ex ante*, sostenuta da parte dell'intermediario, non è giuridicamente fondata in quanto ex art. 8 D.lgs. 11/2010, i prestatori di servizi di pagamento devono adottare misure di sicurezza adeguate e proporzionate al rischio. Nel caso di specie, trattandosi di n. 8 operazioni consecutive online, l'intermediario avrebbe dovuto constatarne l'anomalia; (v) è stata vittima di un'operazione di *social engineering*.

La parte resistente, con le controrepliche, in risposta a quanto dedotto dal ricorrente, ha richiamato integralmente le controdeduzioni precedentemente presentate ed ha ulteriormente rilevato la mancanza di evidenze probatorie in merito all'asserita *mala gestio* a proprio carico.

DIRITTO

Si osserva che le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27.01.2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive

2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

In particolare, la presente controversia ha per oggetto la richiesta di rimborso di n. 8 operazioni di pagamento online, effettuate in data 24.06.2025 con la carta di pagamento intestata al ricorrente, dell'importo complessivo di Euro 8.000,00, così sintetizzate:

DATA	ORA	TIPOLOGIA	IMPORTO (€)
24.06.2025	19:13	Pagamento e-commerce	250,00
24.06.2025	19:14	Pagamento e-commerce	250,00
24.06.2025	19:15	Pagamento e-commerce	250,00
24.06.2025	19:16	Pagamento e-commerce	250,00
24.06.2025	19:17	Pagamento e-commerce	250,00
24.06.2025	19:18	Pagamento e-commerce	250,00
24.06.2025	20:12	Pagamento e-commerce	250,00
24.06.2025	20:20	Pagamento e-commerce	250,00

Da quanto risulta dalla documentazione versata in atti dalla parte resistente, la carta di pagamento veniva bloccata in data 25.06.2025 alle ore 8:42, dunque dopo l'esecuzione delle operazioni di pagamento di disconosciute.

Per quanto riguarda l'autenticazione delle operazioni, la parte resistente ha versato in atti documentazione informatica dalla quale si evince che sia l'*enrollment* della carta su un altro *device* sia le operazioni di pagamento *online* sono stati correttamente autenticati, eseguiti e contabilizzati attraverso in modalità multifattoriale (SCA). In particolare, l'*enrollment* della carta sull'altro dispositivo mobile è avvenuto pochi minuti prima dell'esecuzione delle operazioni contestate mediante la digitazione del codice OTP (fattore di conoscenza) inviato via SMS sul numero di telefono certificato del ricorrente (fattore di possesso), previo accesso nell'App dell'intermediario con l'utilizzo delle credenziali personali della parte ricorrente stessa (nome utente e password).

In seguito, dopo aver inserito i dati della carta e la propria password sul sito dell'esercente commerciale, l'esecuzione delle operazioni di pagamento online è stata autorizzata tramite inserimento

del codice di sicurezza “P***” attivato al momento dell'*enrollment* (fattore di conoscenza) al ricevimento della notifica *push* nell'APP installata sul *device* (fattore di possesso).

Per quanto osservato, è possibile affermare che l'intermediario ha assolto al proprio onere di dimostrare che le operazioni contestate sono state correttamente autenticate, eseguite e contabilizzate, ex art. 10, comma 1, D.lgs. 11/2010.

È ora opportuno scrutinare la condotta serbata dalle parti in occasione dei fatti che conducevano al compimento delle operazioni contestate perché - come sancito dal Collegio di Coordinamento, con la decisione n. 22745/19 - *“la previsione di cui all'art. 10, comma 2, del d. lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente”*.

Sul punto, questo Arbitro osserva che il ricorrente è stato vittima di una truffa originata da un episodio di *phishing* attuato attraverso telefonate e messaggi fraudolenti ricevuti sulla propria utenza telefonica. Parte ricorrente, nel ricorso e in sede di denuncia, riferisce che, in data 24.06.2025, riceveva una chiamata da uno sconosciuto che riferiva di essere un operatore dell'intermediario, il quale le riferiva che la carta di pagamento era stata bloccata. La invitava, quindi, a comunicargli i codici che riceveva via SMS. Poco dopo veniva contattata dal malfattore, attraverso una diversa utenza telefonica, che le inoltrava via whatsapp un link per procedere al cambio delle credenziali. Il link la indirizzava su una pagina clone rispetto a quella dell'intermediario, ed eseguiva l'accesso inserendo nome utente e password. Riceveva immediatamente un altro SMS con un codice OTP, che comunicava al truffatore. Poco dopo si accorgeva di essere stato truffato allorché veniva informato con un messaggio SMS, proveniente da un'utenza diversa da quelle dalle quali era stato precedentemente contattato, che era stato eseguito un pagamento di Euro 250,00. Il giorno seguente si recava presso la sede dell'intermediario e veniva a conoscenza che erano stati effettuati n. 8 pagamenti e-commerce da Euro 250,00 ciascuno. A dimostrazione della truffa, parte ricorrente ha allegato gli screenshot dei messaggi SMS e whatsapp e delle chiamate.

Ciò posto, il Collegio rileva che le utenze telefoniche da cui provenivano le telefonate e gli SMS truffaldini non sono riconducibili all'intermediario resistente. Infatti, da quanto consta dalle dichiarazioni rese in sede di denuncia e dagli screenshot versati in atti, risulta che gli SMS sono stati inviati da due diverse utenze private e non si sono inseriti nella chat delle conversazioni genuine con l'intermediario.

Per quanto visto, è possibile formulare un giudizio di colpa grave a carico della parte ricorrente, la quale, fornendo al malfattore i codici di sicurezza personali, ha in fine dei conti consentito a quest'ultimo di effettuare l'*enrollment* della carta di pagamento sul proprio dispositivo e quindi di eseguire le operazioni di pagamento contestate mediante l'utilizzo della stessa.

D'altro canto, non si può però fare a meno di notare la mancata adozione, da parte dell'intermediario, delle misure di sicurezza tecniche necessarie per evitare che fossero poste in essere, in danno della parte ricorrente, le operazioni di pagamento contestate, che apparivano oggettivamente anomale. Nel caso di specie, sono state effettuate otto operazioni di pagamento online in rapida sequenza, in un brevissimo lasso di tempo, con una medesima carta di pagamento presso lo stesso sito e-commerce (la prima alle ore 19:13 del 24.06.2025 e l'ottava alle ore 20:20 dello stesso giorno). E non a caso, le stesse sono sussumibili nella fattispecie del rischio di frode normativamente tipizzato, in particolare in quella di cui all'art. 8, D.M. 30.04.2007, n. 112, lettera a) n. 2, (tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita).

Pertanto, il Collegio reputa sussistente un concorso di colpa delle parti nella causazione del danno e, in via equitativa, accerta il diritto della parte ricorrente ad ottenere dall'intermediario il rimborso per complessivi Euro 1.500,00.

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di Euro 1.500,00 (millecinquecento/00), oltre interessi legali dalla data del reclamo.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE