



COLLEGIO DI BOLOGNA

composto dai signori:

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

Relatore ANDREA GENOVESE

Seduta del 25/11/2025

FATTO

Insoddisfatta dell'interlocuzione con l'intermediario nella fase del reclamo, con ricorso n. 1308707 del 26.06.2025, la parte ricorrente si rivolge all'Arbitro al quale chiede di disporre il rimborso della somma di Euro 760,00, corrispondente all'importo di n. 2 operazioni di pagamento online fraudolentemente eseguite. A sostegno delle pretese, deduce che: (i) è titolare della carta prepagata H* n. *132; (ii) a partire dal 13.05.2025 si accorgeva di alcuni malfunzionamenti nell'App installata sul proprio smartphone e, pertanto, in data 15.05.2025, la disinstallava e reinstallava; (iii) al primo accesso in App, non ricordando la password, attivava la relativa procedura di recupero; (iv) riceveva quindi la mail e l'SMS contenenti le due parti del codice OTP necessari per il reset della password, che eseguiva con esito positivo; (iv) poco dopo avere impostato la nuova password ed effettuato l'accesso in App, riceveva un primo SMS con cui l'intermediario la informava che un pagamento di Euro 700,00 era stato eseguito il 15.05.2025, alle 18:24, a favore di X; (v) controllava pertanto il saldo e la lista movimenti. Scopriva, così, un ulteriore pagamento a favore del medesimo beneficiario X, di importo pari a Euro 60,00, eseguito alle 18:25 del 15.05.2025; (vii) tali transazioni venivano autorizzate da un indirizzo IP estero; (viii) disconosceva le due operazioni, bloccava immediatamente la carta e presentava reclamo all'intermediario, ricevendo riscontro negativo; (ix) contattava il beneficiario delle operazioni X, il quale

le riferiva che nessun pagamento con la carta n. *132 era stato registrato nei suoi sistemi. Pertanto, informava di tale circostanza la parte resistente; (x) non ha fornito a terzi le credenziali di accesso al suo account o altri dati riservati, né ha smarrito la carta o il suo dispositivo mobile.

Costituitosi, l'intermediario chiede all'Arbitro di rigettare il ricorso perché infondato, sul rilievo che: a) la parte ricorrente non descrive in modo puntuale l'episodio di cui è rimasta vittima. Ciò rende impossibile ricostruire in maniera univoca le modalità della truffa. Né il ricorrente ha prodotto una perizia comprovante una possibile intromissione di terzi malfattori nel suo *device*; b) è verosimile che la parte ricorrente abbia fornito le proprie credenziali a terzi, nell'ambito di un ordinario episodio di "*phishing/vishing*", ovvero abbia digitato le sue credenziali all'interno di un'App non ufficiale o, ancora, abbia utilizzato una rete *wifi* non sicura o scaricato un *malware* sul proprio *device*. Dalle verifiche effettuate emerge, infatti, che la stessa parte ricorrente ha consentito l'accesso al suo conto da un nuovo dispositivo mobile; d) in particolare, gli SMS contenenti i codici segreti (OTP), necessari per accedere all'applicazione, sono stati ricevuti sul numero di cellulare intestato alla parte ricorrente, con la conseguenza che la sua ricostruzione dei fatti non può considerarsi attendibile, rafforzando così l'ipotesi che la stessa sia rimasta vittima di un episodio di *phishing*; e) le operazioni di pagamento sono state eseguite tramite autenticazione "*challenge*", in *Strong Customer Authentication*; f) inviava alla parte ricorrente una puntuale informativa in ordine all'esecuzione delle operazioni, c.d. *Memoshop*, nonché una notifica *push* in corrispondenza del cambio del dispositivo, con i quali la avvisava espressamente di non comunicare a terzi i codici personali; g) realizza, a favore della propria clientela, campagne informative sulle frodi, attraverso l'invio di comunicazioni via mail, notifiche *push* sui *device* dei clienti, sezioni dedicate e articoli descrittivi sul proprio sito internet e sulle proprie pagine social; h) quanto alla lamentata non veridicità delle informazioni fornite con riguardo al nominativo dell'esercente beneficiario dei pagamenti, conferma la piena correttezza e attendibilità dei dati già comunicati al ricorrente.

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. 2 operazioni di pagamento online, effettuate in data 15.05.2025 con la carta di pagamento n.*132 intestata al ricorrente, dell'importo complessivo di Euro 760,00, così sintetizzate:

DATA GG/MM/AA	ORA	IMPORTO
15.05.2025	18:23	Euro 700,00

15.05.2025	18:24	Euro 60,00
------------	-------	------------

Per quanto riguarda l'autenticazione delle operazioni, la parte resistente ha versato in atti documentazione informatica (log accesso all'area riservata, log delle operazioni di pagamento) dalla quale si evince che l'onboarding del nuovo device, l'accesso all'*home banking* e le operazioni di pagamento *online* sono state tutte correttamente autenticate, eseguite e contabilizzate attraverso la SCA. In particolare, l'accesso all'*home banking* è avvenuto con un dispositivo mobile diverso da quello utilizzato dalla parte ricorrente, previa autenticazione forte SCA. L'accesso si è articolato in due passaggi: 1) inserimento della *password* conosciuta dal solo ricorrente (elemento della conoscenza) e successivo inserimento del codice dinamico OTP ricevuto tramite SMS al numero di cellulare della parte ricorrente registrato nell'anagrafica tenuta dall'intermediario (elemento del possesso); 2) secondo inserimento del codice dinamico OTP ricevuto tramite SMS, sempre al medesimo numero di cellulare (elemento del possesso), con il quale è stata ultimata l'associazione del nuovo *device* all'account del ricorrente. In seguito, l'esecuzione delle operazioni di pagamento online è stata autorizzata tramite autenticazione multifattoriale, ossia mediante la notifica *push* inviata al nuovo dispositivo associato (elemento del possesso) e successivo inserimento della *password* (elemento della conoscenza), previa azione di "*tap*" sulle notifiche *push*.

Per quanto osservato, è possibile affermare che l'intermediario ha assolto il 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"*.

Parte ricorrente, nel ricorso e in sede di denuncia, riferisce che, in data 15.05.2025, dopo alcuni giorni in cui aveva riscontrato alcuni malfunzionamenti dell'App dell'intermediario installata sul suo telefono mobile, la disinstallava e la scaricava nuovamente dalla cronologia Cloud delle applicazioni scaricate. Al momento del primo accesso, giacché non ricordava la password, attivava la procedura di recupero e riceveva una mail e un sms, apparentemente provenienti dall'intermediario, contenenti le due parti del codice OTP necessario per il reset della password. Impostato il nuovo codice personale, associava il suo dispositivo al conto, previa digitazione in App di un codice OTP ricevuto via SMS. Riceveva, inoltre, anche altri tre codici OTP. Poco dopo, perveniva sul suo cellulare un SMS che la informava dell'avvenuta disposizione di una operazione di pagamento di Euro 700,00 a favore di X. Controllando

la lista movimenti del conto, scopriva, infine, l'esistenza di un ulteriore pagamento di Euro 60,00, sempre a favore di X. La parte ricorrente afferma di non avere mai comunicato i propri codici o credenziali a terzi, di essere sempre rimasta in possesso del suo smartphone e della carta di pagamento, di non avere ricevuto messaggi contenenti link sospetti.

Ciò posto, come correttamente eccepito dall'intermediario, si osserva che la parte ricorrente: a) non ha circostanziato l'episodio truffaldino di cui è rimasta vittima, rendendo impossibile ricostruire in maniera univoca le modalità della truffa. In particolare, alla luce del fatto che in sede di denuncia ha dichiarato di aver sempre mantenuto il possesso del telefono mobile e della carta, nonché di non aver mai comunicato a terzi i propri codici personali, non ha neanche dimostrato (ad esempio mediante una perizia tecnico-informatica) di aver subito un'intromissione nel suo *device* da parte di terzi; b) non ha allegato in maniera specifica i fatti da cui poter ricostruire l'episodio truffaldino di cui è stata vittima. Rispetto a quanto prospettato non ha versato in atti idonea documentazione comprovante: (i) la disinstallazione dell'App dell'intermediario resistente e la reinstallazione dalla cronologia Cloud delle applicazioni scaricate; (ii) la procedura di ripristino della password, mediante l'inserimento di un codice OTP ricevuto in parte via sms e in parte via mail; (iii) l'SMS contenente il codice OTP con cui avrebbe associato il suo dispositivo al conto; (iv) gli altri tre codici OTP che avrebbe ricevuto.

La genericità del ricorso e il mancato assolvimento dell'onere della prova ex art. 2697 c.c. impediscono al Collegio di verificare l'attendibilità e la fondatezza di quanto dedotto e richiesto dal ricorrente. Ciò permette, peraltro, di formulare un giudizio di colpa grave a carico della parte ricorrente, che, presumibilmente, ha incautamente comunicato a terzi i propri codici personali, che avrebbe dovuto tenere per sé, partecipando, seppur involontariamente, alla consumazione della truffa a suo danno.

Non si rinviene, invece, alcun elemento che consenta di ravvisare una qualche colpa in capo all'intermediario, anche tenuto conto che: a) le operazioni contestate non integrano alcun parametro di cui all' art. 8 del D.M. 112/2007, relativo al "*Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento»*"; b) ha inviato al ricorrente le notifiche *push* e gli SMS *alert*, di cui è stata prodotta evidenza; c) ha anche dimostrato di aver promosso campagne informative della clientela, per renderla edotta del rischio di frodi, come quella perpetrata ai danni del ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE