

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) PLATANIA	Membro di designazione rappresentativa dei clienti

Relatore ANTONINO FRANCESCO PLATANIA

Seduta del 11/02/2026

FATTO

Il ricorrente chiede la restituzione della somma di euro 1.640,25, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati affermando che in data 04/04/2025 è stato vittima di una truffa causata dalla carenza di presidi di sicurezza predisposti dall'intermediario convenuto. Afferma che in data 08/04/2025 veniva effettuata una transazione non autorizzata, presso un esercente estero in Danimarca di importo pari ad euro 1.640,25, corrispondenti a 11.999,00 corone danesi) immediatamente disconosciuta anche nella considerazione che non si trovava all'estero all'epoca dei fatti né si era recato nei mesi precedenti in Danimarca. Rileva l'assenza di predisposizione di un sistema di sicurezza idoneo ad evitare l'intromissione di soggetti malintenzionati all'home banking del cliente, i quali hanno potuto associare la carta ad un proprio dispositivo, eseguendo di conseguenza in modo autonomo i pagamenti tramite riconoscimento biometrico. Contesta l'assenza di alcuna comunicazione circa l'accreditamento di un nuovo dispositivo. Inoltre dichiara di non aver ricevuto alcun codice per autorizzare l'operazione contestata. Rileva l'assenza di colpa in quanto non ha autorizzato l'accreditamento del riconoscimento biometrico del dispositivo con cui è stata effettuata l'operazione contestata. A ciò aggiunge di aver sempre custodito in segretezza le credenziali della carta, la quale, tra l'altro, prima dell'operazione contestata, non era mai stata utilizzata per alcuna operazione né in negozi fisici né online.

Costitutosi l'intermediario convenuto eccepisce che il ricorrente non fornisce elementi utili a ricostruire la vicenda, limitandosi ad affermare di non avere autorizzato le operazioni disconosciute. Eccepisce la

sussistenza dell'avvenuta adozione di un sistema di autenticazione a due fattori della transazione sconosciuta. Pertanto, in difetto di specifiche allegazioni della controparte circa le modalità della truffa, il ricorso non dovrebbe trovare accoglimento. Eccepisce che il ricorrente non ha adempiuto con diligenza ai propri obblighi di custodia e protezione delle credenziali. A ciò si aggiunga come non emergano elementi di particolare sofisticazione della truffa tali da escludere la colpa grave del ricorrente, che si presume avere comunicato ai soggetti frodatori, in data 04/04/2025, username e password statica, oltre che il codice OTP ricevuto tramite SMS.

Con repliche del 15/12/2025 parte ricorrente insiste nei motivi del ricorso ribadendo di non avere mai ricevuto alcun SMS menzionato dall'intermediario in sede di controdeduzioni, di non avere mai utilizzato (né prima né dopo le operazioni fraudolente) la carta di credito da cui è stata effettuata l'operazione e di non avere comunicato a nessuno i propri dati né le proprie credenziali.

DIRITTO

1) Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 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), entrato in vigore il 13/1/2018. Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare: a) l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. b) il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente. Parte ricorrente lamenta l'esecuzione fraudolenta di n. 1 operazione di acquisto *e-commerce* effettuata in data 08/04/2025 alle ore 13:27, verso un esercente estero (Danimarca) di importo pari ad euro 1.640,25 corrispondenti a 11.999,00 corone danesi.

Si rileva che l'operazione contestata è stata effettuata dai soggetti frodatori, in seguito all'*enrollment* dell'App dell'intermediario su dispositivo diverso rispetto a quello abitualmente in uso al ricorrente.

Con riferimento all'autenticazione delle operazioni e alle loro modalità si precisa che le fonti normative che regolano la *strong customer authentication* sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del d.lgs. 10/2011, 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 dall'EBA. Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Preliminarmente va rilevato che dalle evidenze prodotte in sede di controdeduzioni da parte resistente emerge come il dispositivo adoperato per autorizzare tramite App l'operazione fraudolenta sia del modello "X*** M*CG":

Tuttavia, in sede di repliche, la parte ricorrente afferma di non possedere né di avere mai posseduto tale dispositivo. L'intermediario produce i log e le legende relative alla fase di *enrollment* dell'App su altro dispositivo dimostrando la SCA e precisamente: l'accesso all'App scaricata sul nuovo *device* in cui si utilizza *username* e *password* statica alle ore 13:43:33 del 04/04/2025. B) la generazione di un codice OTP che è stato inoltrato tramite SMS all'utenza del cliente. C) inserito il codice OTP all'interno dell'App il sistema verifica la correttezza e la corrispondenza dei dati inseriti e il processo di SCA ha esito

favorevole. e) alle ore 13:43:52 viene effettuato l'accesso all'App e viene contestualmente certificato il nuovo dispositivo. F) Alle ore 13:44:53 viene abilitato il riconoscimento biometrico per il dispositivo certificato.

Da quanto rilevato, pertanto, emerge che per l'operazione di *enrollment* dell'App su altro dispositivo sia stato previsto l'utilizzo di un doppio fattore: Conoscenza: inserimento del nome utente e della *password* del cliente e Possesso: codice OTP inoltrato tramite SMS all'utenza telefonica del cliente. A conferma di quanto dichiarato produce evidenze unitamente alla legenda esplicativa delle operazioni.

L'intermediario produce evidenza dell'invio degli SMS per l'installazione dell'app e per l'attivazione della biometria e il Collegio rileva che Il numero coincide con quello indicato dal ricorrente in sede di denuncia:

Pertanto, sulla base delle evidenze prodotte e sopra riportate risulta che l'operazione di *enrollment* dell'App su altro dispositivo e di registrazione biometria sia stata effettuata nel rispetto della normativa in materia di *strong customer authentication*.

Con riferimento all'autenticazione forte relativa alla disattivazione del servizio di SMS *alert* dall'analisi dei log emerge come i truffatori, operando in seguito all'*enrollment* sul dispositivo a loro disposizione, hanno modificato un'impostazione all'interno dell'App. Così facendo è stato revocato il servizio di invio di SMS *alert* all'utenza telefonica registrata del cliente. In particolare, risulta che in data 07/05/2025, in seguito al *log-in* in App effettuato tramite riconoscimento biometrico, alle ore 12:34:31, i truffatori abbiano modificato il servizio di invio di SMS *alert*, revocandolo. L'operazione è stata autorizzata tramite fattore biometrico (inerenza), operando sul dispositivo precedentemente registrato (possesso). Da quanto descritto, pertanto, emerge che per l'operazione di *enrollment* dell'App su altro dispositivo sia stato previsto l'utilizzo di un doppio fattore: Possesso: l'operazione è stata disposta ed autorizzata adoperando il *device* registrato e inerenza: l'operazione è stata autorizzata tramite fattore biometrico. Anche in questo caso l'intermediario produce evidenze con relative legenda esplicativa. Pertanto, sulla base delle evidenze prodotte e sopra riportate risulta che tale operazione sia stata effettuata nel rispetto della normativa in materia di *strong customer authentication*.

Con riferimento all'autenticazione forte relativa all'esecuzione dell'operazione e-commerce l'intermediario illustra le evidenze prodotte, precisando che le stesse danno prova del sistema di autenticazione forte adoperato che, nel caso di specie, ha così funzionato: Tramite *Web browser* viene predisposto il pagamento in data 08/04/2025.-Per confermare il pagamento l'App genera automaticamente una notifica *push* che viene inviata al dispositivo autenticato.- L'operazione si conclude con la conferma con riconoscimento biometrico (impronta digitale o scansione del viso) tramite il *device* mobile precedentemente autenticato.

Da quanto descritto e documentato emerge che per l'operazione dispositiva del pagamento e-commerce sia stato previsto l'utilizzo di un doppio fattore: Possesso: notifica *push* inviata all'App installata sul *device* e Inerenza: utilizzo del fattore biometrico per autorizzare l'operazione di e-commerce. A conferma di quanto dichiarato produce evidenze e la legenda esplicativa.

Si tratta di un pagamento e-commerce (colonna "Posem"), autorizzato (colonna "Tiporis") nei confronti di un esercente estero, con sede in Danimarca (colonna "Nazmer").

Il pagamento contestato ha richiesto l'autenticazione (colonna "Pares") ed è stato effettuato in seguito ad autenticazione tramite fattore biometrico (colonna "Authmetod"), successivamente alla sua predisposizione tramite Browser (colonna "Devicetype").

La notifica inviata al dispositivo autenticato è del tipo "parlante", indicando l'importo (in valuta estera) e il beneficiario del pagamento.

Pertanto, sulla base delle evidenze prodotte e sopra riportate risulta che l'operazione di pagamento e-commerce è stata effettuata nel rispetto della normativa in materia di *strong customer authentication*.

In conclusione, sulla base delle evidenze prodotte e sopra riportate risulta che ognuna delle operazioni oggetto di contestazione nel presente ricorso è stata effettuata nel rispetto della normativa in materia di *strong customer authentication*.

Il Collegio ritiene la sussistenza della colpa grave del ricorrente. Parte ricorrente in sede di denuncia si limita ad affermare che: -In data 08/04/2025 riceveva una e-mail (non prodotta) che gli segnalava n. 3 pagamenti da lui non autorizzati, uno dei quali era non contabilizzato.- Contattava il numero verde per bloccare le operazioni eseguite fraudolentemente. Tuttavia, n. 2 operazioni risultavano già contabilizzate per un danno economico totale pari ad euro 3.155,25.- In seguito alla truffa provvedeva a bloccare la carta di credito e, in via precauzionale, anche tutte le altre carte di credito e di pagamento in suo possesso. In sede di ricorso all'ABF la parte ricorrente fa riferimento ad un'unica operazione, di importo pari ad euro 1.640,25. Infatti, come anche affermato e provato da parte resistente in sede di controdeduzioni, l'operazione che è andata a buon fine è esclusivamente una. Le altre due operazioni sono state precauzionalmente bloccate dal sistema di sicurezza dell'intermediario, che è costantemente presidiato da operatori specializzati nella valutazione delle transazioni. Il ricorrente né in sede di ricorso né in sede di repliche allega l'e-mail truffaldina ricevuta. Nei casi di phishing "tradizionale", l'orientamento condiviso dai Collegi ABF, a causa della diffusione del fenomeno e della sua conoscenza, è quello di ritenere che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa. Pertanto, il ricorrente è tenuto a sopportare – per colpa grave – tutte le perdite derivanti da operazioni di pagamento non autorizzate (cfr. Collegio di Coordinamento, Decisione n. 3498/2012). Da quanto riportato in sede di denuncia da parte ricorrente non è possibile ricostruire l'esatta dinamica della truffa subita.

Si osserva che, secondo l'orientamento condiviso dai Collegi territoriali, nel caso in cui:

i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute; ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA); iii. non risultano indizi di anomalia delle operazioni e/o ulteriori elementi; le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano elementi conducenti per affermare la colpa grave del ricorrente. Infine parte ricorrente in sede di ricorso riferisce di non aver ricevuto alcun *alert* circa le operazioni fraudolentemente eseguite. In particolare, egli dichiara, sia in sede di ricorso che di repliche, di non aver ricevuto alcuna comunicazione circa l'accredito di un nuovo dispositivo né di aver ricevuto la comunicazione di codici di sicurezza necessari per l'esecuzione delle operazioni. Tuttavia, parte resistente ha dato evidenza dell'invio un sms OTP "parlante" per la registrazione del nuovo device. Nello specifico, in data 04/04/2025 l'intermediario ha inoltrato alle 13:43 e alle 13:44 n. 2 messaggi SMS contenenti due codici OTP necessari, rispettivamente, per certificare il nuovo dispositivo e per abilitare il riconoscimento biometrico, evidenziando altresì come nel corpo del messaggio SMS fosse indicato di prestare massima attenzione alla comunicazione del codice OTP indicato in calce, in quanto si sarebbe potuto trattare di frode. Si rileva che, secondo l'orientamento del Collegio, in presenza di messaggi contenenti i codici autorizzativi (OTP) che avvisano l'utente del tipo, dell'importo e del destinatario dell'operazione che sta per autorizzare (c.d. SMS parlante), non rileva l'attivazione o meno di sistemi di *alert ex post* (Collegio di Palermo, decisione n. 13859/2022; Collegio di Palermo, decisione n. 5893/2023, Collegio di Torino, decisione n. 1344/2023). Inoltre, l'intermediario produce evidenza circa l'invio, in data 07/04/2025, di comunicazioni di *alert* con riferimento all'avvenuta cancellazione del servizio di invio degli sms alert. Infine, l'assistenza clienti dell'intermediario ha inviato in data 08/04/2025 n. 2 comunicazioni tramite e-mail che informavano il cliente della necessità urgente di un contatto, in seguito al blocco preventivo di n. 2 pagamenti.

Il Collegio per quanto sopra ritiene non meritevole di accoglimento la domanda proposta dal ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE