

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore ANTONIO FORGIONE

Seduta del 29/01/2026

FATTO

Parte ricorrente si rivolge all'ABF esponendo di intrattenere un rapporto di conto corrente con l'intermediario chiamato nel presente procedimento. In particolare, riferisce di aver riscontrato l'addebito sul proprio conto di un bonifico istantaneo, disposto a favore di un beneficiario sconosciuto e verso un IBAN riconducibile a un paese estero. La parte precisa di essere venuto a conoscenza dell'operazione fraudolenta esclusivamente a seguito della ricezione di un SMS di conferma inviato dalla banca e che, allarmata da tale notifica, contattava immediatamente l'assistenza telefonica dell'intermediario per disconoscere l'operazione e bloccare le credenziali. In ordine alla dinamica della frode, il ricorrente ricostruisce di essere stato vittima di una tecnica di *smishing*. In dettaglio, dichiara di aver ricevuto un messaggio SMS apparentemente proveniente dall'intermediario, privo di errori grammaticali o anomalie evidenti che potessero destare sospetto, contenente un *link*. Cliccando su tale collegamento, veniva reindirizzato su un sito internet "clone", graficamente identico al portale ufficiale della banca, all'interno del quale inseriva le proprie credenziali di accesso. Tali dati venivano successivamente carpiri dai frodatori e utilizzati per disporre il bonifico oggetto di contestazione. In diritto, il ricorrente lamenta la violazione da parte dell'intermediario del canone di diligenza professionale di cui all'articolo 1176, comma 2, cod. civ. Sostiene, infatti, che la banca avrebbe dovuto

adottare presidi di sicurezza più efficaci e cautele idonee a prevenire il compimento di operazioni fraudolente, specialmente a fronte di attacchi informatici noti e ricorrenti. Chiede, pertanto, la condanna dell'intermediario alla restituzione della somma indebitamente sottratta.

L'intermediario, costituendosi nel procedimento, contesta le pretese del ricorrente, chiedendo il rigetto del ricorso. Nel merito, l'intermediario eccepisce la piena conformità dei propri sistemi di sicurezza alla normativa vigente (PSD2) e agli standard tecnici regolamentari, e dichiara di adottare un sistema di autenticazione forte del cliente (*Strong Customer Authentication* – SCA) a due fattori per l'accesso all'area riservata e per l'autorizzazione delle disposizioni. L'intermediario rileva che il bonifico istantaneo oggetto di causa è stato disposto a seguito dell'attivazione dell'App mobile per la gestione in remoto del conto corrente su un nuovo dispositivo, diverso da quello abitualmente in uso a parte ricorrente. Tale procedura di associazione del nuovo *device* – attività necessaria per operare – richiede l'inserimento di un codice OTP (*One Time Password*) specifico, che è stato correttamente inviato via SMS al numero di telefono certificato del cliente. Ne consegue, secondo la prospettazione difensiva, che l'installazione della nuova App sul dispositivo in uso ai frodatori è stata resa possibile esclusivamente dalla condotta colposa del ricorrente, che ha comunicato a terzi il codice di sicurezza strettamente personale, violando gli obblighi di custodia delle credenziali. L'intermediario precisa, inoltre, che l'operazione dispositiva è stata eseguita con un bonifico istantaneo, con la conseguenza che l'ordine di pagamento è divenuto irrevocabile non appena ricevuto, rendendo tecnicamente impossibile per la banca procedere all'annullamento o al richiamo dei fondi data la lavorazione in tempo reale dell'operazione. Infine, l'intermediario sottolinea di aver assolto ai propri obblighi informativi e di diligenza, attuando periodiche campagne di sensibilizzazione contro le frodi informatiche. Conclude pertanto insistendo per il riconoscimento della colpa grave del ricorrente e il conseguente rigetto della domanda restitutoria.

Nelle proprie repliche, parte ricorrente contesta le eccezioni avversarie, negando di aver cooperato colposamente con i frodatori. Sottolinea che l'avvenuta installazione dell'applicazione su un dispositivo in uso a terzi non costituisce, di per sé, prova di una condotta gravemente negligente del cliente. Il ricorrente evidenzia l'elevata sofisticazione delle odierne tecniche di *phishing*, capaci di trarre in inganno l'utente medio tramite siti clone perfettamente identici agli originali. Pertanto, la deduzione dell'intermediario secondo cui il ricorrente avrebbe necessariamente comunicato l'OTP ai malfattori viene definita meramente congetturale e priva di riscontro probatorio. In diritto, la difesa di parte ricorrente osserva che la colpa grave non può essere presunta dalla sola circostanza che l'operazione risulti formalmente autenticata. Nel caso di specie, l'intermediario non avrebbe fornito elementi fattuali concreti a dimostrazione della negligenza del cliente. Circa l'irrevocabilità tecnica del bonifico istantaneo, il ricorrente osserva che tale circostanza non esonera l'intermediario dall'obbligo giuridico di rimborso delle operazioni non autorizzate previsto dal D.Lgs. n. 11/2010. Sotto il profilo tecnico, la parte lamenta inoltre gravi carenze nei sistemi di monitoraggio e di *alert* della banca a fronte di un'operazione anomala ed eccepisce l'inidoneità probatoria dei *log* informatici prodotti dall'intermediario, in quanto privi di sottoscrizione digitale o di marcatura temporale opponibile a terzi.

In sede di controrepliche, l'intermediario non ha introdotto nuovi elementi di fatto o di diritto, rimettendosi integralmente a quanto già dedotto, argomentato ed eccepito nella propria memoria di costituzione.

DIRITTO

Il ricorso ha ad oggetto il disconoscimento di un'operazione di pagamento eseguita su canale telematico, fattispecie rientrante nella disciplina del D.Lgs. n. 11/2010 (attuativo della direttiva PSD2).

In via preliminare, il Collegio osserva che, ai sensi dell'articolo 10 del citato decreto, qualora l'utente neghi di aver autorizzato un'operazione, l'onere di provare la genuinità della stessa e l'eventuale dolo o colpa grave dell'utente ricade interamente sull'intermediario.

Nel caso di specie, l'istruttoria ha evidenziato che l'operazione fraudolenta non è stata disposta direttamente dal dispositivo abituale della ricorrente, bensì è stata preceduta da una fase di attivazione dell'App di *remote banking* dell'intermediario su un nuovo dispositivo in uso ai frodatori. Dalla ricostruzione delle evidenze informatiche prodotte, tale procedura di associazione del nuovo *device* si è articolata, in sintesi, nelle fasi dell'inserimento nell'App scaricata sul nuovo dispositivo dei dati identificativi statici (Codice Cliente e data di nascita), nonché nella digitazione di una porzione del codice PIN (tre cifre) a conferma dell'identità e, infine, nell'inserimento di un codice OTP inviato via SMS al numero certificato del ricorrente, necessario per validare l'attivazione. Sotto il profilo della sicurezza informatica, il sistema adottato dall'intermediario ha dunque impiegato due fattori di autenticazione, ossia l'elemento della conoscenza e l'elemento del possesso.

Procedendo all'analisi della fase prettamente dispositiva del bonifico istantaneo, i tracciati informatici prodotti dall'intermediario descrivono una sequenza operativa che appare, sotto il profilo tecnico, formalmente corretta e lineare. Dalla ricostruzione dei *log* si evince infatti che, una volta effettuato l'accesso e inseriti i dati essenziali del pagamento, quali importo, causale, coordinate IBAN e beneficiario, il sistema ha proceduto alla validazione formale degli stessi, prospettando la schermata di riepilogo. L'autorizzazione finale all'addebito è stata quindi perfezionata mediante l'utilizzo del riconoscimento biometrico (impronta digitale), che era stata configurata e memorizzata sul dispositivo contestualmente alla precedente fase di attivazione. Anche in questa fase, pertanto, l'operazione risulta supportata dalla combinazione di due fattori di autenticazione distinti (SCA): il fattore dell'inerenza (impronta digitale) e il fattore del possesso, concretizzatosi nell'utilizzo dello specifico dispositivo mobile che, a seguito della procedura di associazione sopra descritta, risultava correttamente registrato presso i sistemi della banca.

Giova precisare che, a supporto della ricostruzione tecnica appena esposta, parte resistente ha prodotto i relativi *log* corredati da opportuna legenda esplicativa, rendendo intelligibili le tracce informatiche. Sulla scorta di tali evidenze, deve ritenersi accertato che l'operazione contestata è stata autenticata nel rispetto della normativa in materia di SCA, essendosi l'intermediario limitato a dare esecuzione a ordini impartiti mediante il corretto utilizzo delle credenziali di sicurezza. Ne discende, sul piano della causalità materiale, che l'operazione è stata resa possibile dalla cooperazione attiva del cliente, il quale ha fornito gli elementi necessari per il perfezionamento della procedura. Non può ritenersi condivisibile la contestazione di parte ricorrente circa l'attendibilità dei *log* informatici prodotti dall'intermediario, essendo questa del tutto analoga a quella usualmente presentata per le controversie di questo tipo (in senso conforme si veda Collegio ABF Milano, decisione 6265/25).

Circa la prospettata attenuazione della responsabilità del cliente per colpa grave in ragione della tipologia di truffa subita, va osservato che il ricorrente afferma di avere ricevuto un SMS "civetta" apparentemente riconducibile all'intermediario, ma non ne produce alcuna evidenza. Tale carenza impedisce a questo Collegio di qualificare l'episodio come *spoofing* e, soprattutto, di valutarne in concreto la sofisticazione e l'idoneità a ingenerare un legittimo affidamento circa la genuinità della comunicazione. In difetto di prova, l'assunto rimane meramente assertivo e non può fondare alcuna mitigazione del giudizio di rimproverabilità della condotta dell'utente. Ne consegue che non sussistono elementi per attenuare la responsabilità per colpa grave del cliente né per riconoscere l'invocata ripartizione del pregiudizio.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE