

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) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) PLATANIA	Membro di designazione rappresentativa dei clienti

Relatore ANTONIO FORGIONE

Seduta del 11/12/2025

FATTO

Parte ricorrente si rivolge all'ABF lamentando l'esecuzione fraudolenta di un'operazione di prelievo di contante senza carta (cosiddetto prelievo *smart*), addebitata sul proprio conto corrente. In dettaglio, la parte espone che la propria figlia era stata contattata telefonicamente da un soggetto interessato all'acquisto di un bene messo in vendita su una piattaforma *on line*. Stante l'impossibilità della figlia di ricevere il pagamento, il ricorrente accettava di riceverlo sul proprio conto e veniva contattato da un'utenza mobile sconosciuta. L'interlocutore proponeva una modalità di accredito tramite la scansione di un codice QR mediante l'applicazione mobile dell'intermediario per la gestione in remoto del proprio conto corrente. Il ricorrente, pur non conoscendo la procedura, riferisce di aver seguito le istruzioni del terzo: accedeva pertanto all'applicazione installata sul proprio dispositivo e inquadrava un QR *code* che il truffatore aveva inviato sul cellulare di un amico del ricorrente stesso, presente in quel momento. Immediatamente dopo tale attività, riceveva una *e-mail* dall'intermediario che lo informava dell'avvenuto prelievo di contante presso uno sportello ATM sito in località diversa da quella di residenza. Ritenendo sussistere una falla nei sistemi di sicurezza relativi al servizio di prelievo *smart*, il ricorrente chiede la restituzione della somma.

L'intermediario, costituitosi nel procedimento, chiede il rigetto del ricorso. Nelle proprie controdeduzioni, la parte rileva che l'operazione contestata è stata correttamente autenticata dal cliente, senza anomalie formali rilevabili. L'intermediario specifica che la funzionalità prelievo *smart* richiede una procedura più articolata rispetto a quella indicata dal ricorrente: accesso all'applicazione di *home banking* tramite riconoscimento biometrico, selezione della voce specifica, scelta dell'importo e

autorizzazione della prenotazione mediante nuovo riconoscimento biometrico. Solo successivamente si attiva la fotocamera per inquadrare il QR code necessario al prelievo che il truffatore ha inviato al ricorrente su un'altra utenza in modo che fosse inquadrata con la sua app di *mobile banking* dopo aver cliccato su un apposito tasto del dispositivo per autorizzare il prelevamento. L'intermediario produce, inoltre, *log* informatici dai quali risulterebbe che l'accesso e l'operazione sono stati eseguiti dal dispositivo associato al ricorrente e validati tramite fattore biometrico (impronta digitale). Parte resistente conclude eccependo la colpa grave del cliente, che ha collaborato attivamente con il truffatore, seguendo le istruzioni fornite telefonicamente e inquadrando un QR code fornito da terzi, finalizzando così l'operazione.

In sede di repliche, il ricorrente insiste, sostenendo che la possibilità di autorizzare il prelievo inquadrando una foto di un QR code (inviata su altro dispositivo) costituisca una lacuna di sicurezza della procedura.

Nelle controrepliche, l'intermediario ribadisce la regolarità tecnica dell'operazione e la negligenza del cliente.

DIRITTO

Il presente procedimento ha ad oggetto il disconoscimento di un'operazione di pagamento rientrante nell'ambito di applicazione del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 (di recepimento della direttiva PSD2). L'articolo 10 del d.lgs. 11/2010 dispone che, qualora l'utente neghi di aver autorizzato un'operazione, è onere del prestatore di servizi di pagamento (PSP) provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze di malfunzionamenti. L'autenticazione deve avvenire mediante procedura di *Strong Customer Authentication* (SCA), basata sull'uso di due o più fattori tra conoscenza, possesso e ineranza.

Nel caso di specie, l'intermediario ha prodotto i tracciati informatici (*log*) relativi all'operazione contestata. Dall'analisi della documentazione tecnica, corredata da legenda, emerge che l'accesso all'app di *mobile banking* è avvenuto dal dispositivo associato al ricorrente (fattore di possesso) ed è stato validato tramite riconoscimento dell'impronta digitale (fattore di ineranza/biometrico). La successiva disposizione di prelievo *smart* è stata anch'essa confermata mediante riconoscimento biometrico. Tale modalità di autenticazione risulta conforme ai requisiti di sicurezza previsti dalla normativa vigente (PSD2 e Regolamento Delegato UE 2018/389), garantendo l'univoca riconducibilità dell'operazione allo strumento e al cliente.

Da quanto osservato, in linea con l'orientamento consolidato dei Collegi (ad esempio, Collegio ABF Roma, decisione n. 3032/23), la modalità autorizzativa basata sull'utilizzo dell'applicazione su dispositivo certificato e del QR code è conforme alla SCA.

Va altresì osservato che non si rilevano, dai *log file* prodotti, evidenze di malfunzionamenti o accessi abusivi ai sistemi informatici.

Accertata la corretta autenticazione dell'operazione, occorre valutare la condotta del ricorrente ai fini della ripartizione della responsabilità ai sensi dell'articolo 12 del d.lgs. 11/2010.

Dalla ricostruzione dei fatti fornita dallo stesso ricorrente, sia in sede di reclamo che di denuncia alle autorità di polizia, emerge in modo inequivocabile che egli ha agito su istigazione del truffatore. Il ricorrente ammette di aver effettuato l'accesso alla propria applicazione di *home banking* e di aver inquadrato, su indicazione del terzo, un QR code ricevuto sul telefono di un terzo soggetto. Tale condotta integra gli estremi della colpa grave. L'operazione di prelievo *smart* è funzionale al ritiro di contante e non all'accredito di somme; l'aver seguito pedissequamente le istruzioni di uno sconosciuto, utilizzando una funzionalità di prelievo per una presunta operazione di incasso, denota un

comportamento imprudente. Inoltre, l'azione di scansionare un QR code fornito da un soggetto terzo esterno al circuito bancario (come osservato, inviato tramite messaggistica su un altro telefono), finalizzata ad autorizzare un'operazione sul proprio conto, rappresenta una violazione degli obblighi di custodia e corretto utilizzo dello strumento di pagamento.

Come affermato dalla giurisprudenza dell'ABF in casi analoghi (si veda, Collegio ABF Milano, decisione n. 9756/23), la collaborazione attiva del cliente con il truffatore, che consente il collegamento tra il dispositivo del cliente e l'ATM dove viene erogato il contante, interrompe il nesso causale tra l'eventuale sofisticatezza della frode e il danno subito.

L'intermediario, inoltre, non avrebbe potuto impedire un'operazione che, dal punto di vista formale, appariva come regolarmente disposta e confermata dal cliente stesso tramite i richiesti fattori di sicurezza.

Non essendo ravvisabili carenze nei sistemi di sicurezza della banca e sussistendo la colpa grave dell'utente per aver fattivamente agevolato la frode, la domanda di rimborso non può essere accolta.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE