

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore PAOLO DI STEFANO

Seduta del 26/02/2026

FATTO

Con ricorso del 3.8.2025 la ricorrente espone di essere stata vittima di una frode informatica durante un soggiorno all'estero. Deduce in particolare che in data 6.7.2025, dopo avere effettuato un'operazione di pagamento, ignoti eseguivano dal suo conto, tramite un dispositivo sconosciuto collegato alla propria app, alcuni prelievi di somme sottraendo inizialmente 450 euro tramite money transfer. Successivamente, i truffatori effettuavano sei ricariche fraudolente sulla carta prepagata della vittima rispettivamente di euro 300, 150, 500, 0,95, 0,95, 0,95, per poi addebitare un altro pagamento da 450 euro. Numerosi altri tentativi di bonifico verso iban esteri (Spagna e Francia) fallivano solo per esaurimento del plafond. Nonostante i ripetuti tentativi di contatto, la ricorrente riusciva a bloccare le carte collegate al conto solo alle 16:40. Al rientro in Italia, nonostante quattro formali disconoscimenti e la conferma del blocco del conto, il 13.7.2025 alle 22:00 registrava un ulteriore tentativo di bonifico non autorizzato verso lo stesso destinatario sconosciuto. Il giorno seguente, venivano effettuati due bonifici istantanei di euro 1,00 e 1.350,00, che azzeravano le somme disponibili sul conto. La ricorrente, quindi, si accorgeva nuovamente che era stato agganciato all'app un ulteriore device non riconosciuto dalla stessa ed ancora si rivolgeva all'intermediario richiedendo ulteriormente di bloccare il conto. In data 29.07.2025 riceveva un bonifico in entrata di euro 0,71 da un iban francese, evidentemente a riprova che il conto fosse operativo. A fronte dell'accaduto, parte ricorrente otteneva dall'intermediario rimborsi per complessivi euro 1.400,00 relativamente alle operazioni effettuate in data 06.07.2025, senza vedersi restituite la residua somma di euro 1.351,00, oggetto di ricorso

In sede di controdeduzioni, parte resistente, rimessa in termini con provvedimento della Presidente del Collegio del 12.11.2025, insta per il rigetto del ricorso deducendo che l'accaduto sia ascrivibile a colpa grave della cliente, considerato che per il tipo di operazioni descritte la banca adotta - come ha adottato nel caso di specie - un sistema di autenticazione forte di accesso all'area riservata e di autorizzazione delle disposizioni di pagamento nel rispetto delle previsioni normative. Precisa che le operazioni del 12 e del 14 luglio 2025 sono state assistite dal doppio fattore di autenticazione e, dunque, sono state autorizzate dalla ricorrente, evidenziando come la stessa nulla abbia riferito in merito ai fatti occorsi in dette giornate e come non abbia tenuto conto della notifica alert dell'installazione dell'App per due giorni. Nonostante i sistemi di autenticazione delle operazioni in esame non avessero registrato anomalie, la banca ha comunque dato tempestivamente seguito alle richieste di recall, che non hanno avuto alcun esito da parte della banca beneficiaria e, in riferimento al bonifico istantaneo, nulla si è potuto in ragione della lavorazione immediata dell'operazione. Infine, quanto al mancato intervento della banca per bloccare la truffa, parte resistente, dopo avere precisato di avere messo in atto campagne di sensibilizzazione volte a prevenire il rischio di frodi ai danni della clientela, rileva che non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle proprie somme.

La ricorrente contesta le difese di parte resistente con repliche e documenti depositati il 15.01.2026, deducendo in ordine ai fatti verificatisi in suo danno tra il 12.07.2025 e il 14.07.2025, ritenendoli collegati alla medesima truffa del 6.7.2025. Rispetto alla dinamica dei fatti, sostiene di non avere agito con colpa, tant'è che ha ripetutamente chiesto di bloccare non solo le proprie carte ma anche il proprio conto corrente, ma tale richiesta non è stata esaudita dall'intermediario, violando gli obblighi di diligenza professionale. Parte ricorrente afferma inoltre che la banca non avrebbe dovuto ignorare i plurimi indizi di anomalia che caratterizzavano le operazioni in questione, che il sistema di autenticazione seguito dalla banca non può annoverarsi come "forte" in quanto il codice OTP necessario all'installazione dell'app non è mai stato inviato all'utenza della ricorrente e che la scelta dell'alert inviato a mezzo e-mail non può reputarsi sicura, in quanto costringerebbe l'utente a tenere sempre sotto controllo la propria casella di posta elettronica.

Parte resistente, in sede controrepliche, si riporta a quanto argomentato in sede di controrepliche, ribadendo che l'installazione dell'app su altro dispositivo è stata possibile solo in ragione della colpevole cooperazione fornita dalla cliente al frodatore e che la truffa subita in data 06.07.2025 è differente da quella oggetto dell'odierno ricorso.

DIRITTO

La controversia è disciplinata dal 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 13/01/2018, 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, le fonti normative che regolano la strong customer authentication (cd. SCA) 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 (v. in particolare il parere dell'EBA del 21 giugno 2019).

L'intermediario ha quindi l'onere di fornire la prova dell'adozione delle procedure di autenticazione in linea con le suindicate disposizioni normative, salvo che l'operazione disconosciuta non sia stata direttamente autorizzata dal cliente.

Nella vicenda in esame, si contesta e disconosce l'esecuzione fraudolenta di due bonifici istantanei effettuati in data 14.07.2025, rispettivamente di importo pari ad euro 1,00 ed euro 1.350,00, per un totale complessivo di euro 1.351,00 (dalla lista movimenti in atti, emerge che l'esiguo importo di euro 1,00 non corrisponde ad un onere commissionale ma rappresenta un autonomo bonifico istantaneo). Dall'analisi dei log informatici correttamente prodotti dalla parte resistente sembra che le operazioni fraudolente (eseguite in data 14.07.2025) siano state effettuate dai soggetti malfattori in seguito all'enrollment dell'app dell'intermediario su un dispositivo in loro possesso (effettuato in data 12.07.2025).

Quanto alla procedura di autenticazione riferita alla fase di enrollment dell'app su nuovo dispositivo, l'intermediario produce evidenza informatica dei segmenti attuativi del meccanismo di autenticazione caratterizzato dalla sussistenza del doppio fattore: quello di conoscenza (codice cliente e data di nascita + tre cifre del PIN) e quello di possesso (codice OTP inviato all'utenza telefonica del ricorrente) di cui. L'utenza telefonica a cui è stato inviato il codice OTP tramite SMS corrisponde al numero di telefono indicato dalla ricorrente e della regolare consegna al destinatario vi è evidenza documentale. Quanto alla procedura di autenticazione riferita alle fasi dispositive dei due bonifici istantanei, i log informatici rivelano la corretta applicazione della SCA tramite l'applicazione dei fattori di autenticazione di inerenza (dato dall'utilizzo del fattore biometrico, ossia il riconoscimento facciale, registrato in sede di enrollment) e di possesso (si è operato sul device precedentemente validato in fase di enrollment).

L'analisi dei processi informatici dimostra, pertanto, che ognuna delle operazioni contestate è stata effettuata nel rispetto della normativa in materia di strong customer authentication (c.d. SCA).

Vista, quindi, la corretta adozione delle procedure di sicurezza che l'intermediario è tenuto a seguire nelle fasi di autenticazione, occorre rilevare eventuali profili di colpa grave della ricorrente, stante che, secondo il costante orientamento dei Collegi, la prova dell'autenticazione delle operazioni rappresenta un *prius* logico e giuridico rispetto alla valutazione del comportamento dell'utente (cfr. Collegio di Coordinamento ABF, decisione n. 22745/2019).

Dalla descrizione dei fatti fornita dalla ricorrente in sede di ricorso emerge esclusivamente che: a) la ricorrente, in conseguenza della precedente truffa subita in data 06.07.2025, aveva chiesto all'intermediario il blocco del proprio conto, per evitare l'esecuzione di ulteriori operazioni fraudolente; b) l'intermediario non aveva provveduto ad effettuare il blocco richiesto; c) in data 14.07.2025 alle ore 15:50 prendeva visione di un alert di un bonifico istantaneo in uscita dal proprio conto di euro 1,00, verso destinatario sconosciuto con IBAN francese, cui seguiva immediatamente un secondo bonifico istantaneo in uscita di euro 1.350,00, pari all'ammontare rimasto sul conto della ricorrente; d) in conseguenza di ciò, la ricorrente richiedeva ulteriormente il blocco del proprio conto e, anche in questo caso, la banca non eseguiva tale ordine, tant'è che in data 29.07.2025 veniva effettuato un bonifico in entrata di euro 0,71 proveniente da un iban francese, a riprova che il conto fosse attivo ed operativo.

La sequela dei fatti sopra riportati non consente di ricostruire l'esatta dinamica della truffa oggetto dell'odierno ricorso, ma porta a ritenere che da parte della ricorrente vi sia stata una reazione allarmistica che l'ha indotta a formulare una richiesta di chiusura del conto sia in occasione della prima truffa subita (di tale richiesta - invero - non vi è evidenza), sia in occasione dei fatti occorsi successivamente (richiesta - questa sì - documentata dalla nota di posta elettronica del 14.07.2025 relativa al conto che l'intermediario ha continuato a mantenere attivo).

Sull'attivazione dei sistemi di alert le allegazioni difensive non appaiono lineari, poiché, se da un lato la ricorrente deduce di aver avuto notizia dell'esecuzione dei bonifici fraudolenti in seguito alla ricezione di alcune comunicazioni, dall'altro lato la stessa rileva di non aver ricevuto sms o email contestuali alle fasi di enrollment e di pagamento.

Tuttavia, avuto riguardo agli esiti dell'analisi informatica condotta sui processi di attivazione dei sistemi di alert delle singole operazioni, risulta che: della fase di enrollment (avvenuta alle ore 18:06 del 12.07.2025) è stata inviata una comunicazione alla cliente tramite canale e-mail, in un momento immediatamente successivo a quello della registrazione dell'app sul nuovo dispositivo, come da

allegati seguenti; della fase relativa al bonifico istantaneo di euro 1,00 delle ore 16:08 del 14/07/2025 non vi sono attivi sistemi di alert; del bonifico istantaneo di euro 1.350,00 delle ore 16:34 del 14/07/2025 vi è traccia di comunicazioni recapitate alla ricorrente tramite SMS delle ore 16:38 ed email delle ore 01:47.

Emerge, dunque, che il sistema di alert si sia attivato tardi, considerato peraltro che l'email risulta trasmessa la notte, mentre i due bonifici, oggetto di truffa, sono stati effettuati rispettivamente alle ore 16:08 e alle 16:34.

Secondo gli orientamenti condivisi dai Collegi la mancata attivazione ovvero il mancato funzionamento del servizio di sms-alert (o servizio assimilabile) sono irrilevanti nell'ipotesi in cui le operazioni risultino effettuate a breve distanza di tempo l'una dall'altra ovvero si tratti di una sola operazione, in quanto l'invio dell'sms non avrebbe potuto, in concreto, impedire o contenere la perdita relativa alle operazioni non autorizzate dal titolare dello strumento di pagamento.

In particolare, questo Collegio ritiene che in caso di mancato invio del sms alert, non sussiste responsabilità dell'intermediario qualora le operazioni sconosciute siano avvenute entro l'arco temporale di cinque minuti (cfr., ex plurimis decisioni nn. 4125/2025, 2495/2024, 13261/2020).

Di conseguenza, parte resistente, vista la mancata tempestiva attivazione del sistema di alert, avvenuta oltre il lasso temporale individuato dalla giurisprudenza arbitrale, è tenuta a rimborsare alla ricorrente la somma relativa alla seconda operazione, fraudolentemente sottratta, per l'importo di euro 1.350,00.

La responsabilità dell'intermediario rileva anche sotto il profilo del mancato rilevamento degli indici di anomalia ex DM 11/2007 [ossia: tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, di cui al punto 2 della lett. a) dell'art. 8], giacché in data 14.07.2025 oltre al bonifico andato a buon fine, sono stati effettuati anche tre tentativi di bonifici verso uno stesso beneficiario.

In continuità con la posizione del Collegio, le operazioni effettuate in presenza di indici anomalia, vanno restituite al 20% salvo una diversa distribuzione in concreto del concorso di colpa tra le parti (Collegio di Palermo, n. 4200/2024) e, in caso di simultanea sussistenza dell'obbligo dell'intermediario di restituire l'importo integrale delle operazioni compiute in difetto di alert, è onere della banca rimborsare anche il 20% della prima operazione per la presenza dell'indice di anomalia che la banca non ha valorizzato (Collegio di Palermo, n. 12488/2024).

In applicazione dei suesposti principi parte resistente è tenuta a rimborsare la somma di € 1.350,20, dovuta quanto a euro 0,20 (20% di euro 1,00) per via della violazione dell'indice di anomalia e quanto a euro 1.350,00 per via dell'intempestivo funzionamento del servizio di alert.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 1.350,20.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE