

COLLEGIO DI MILANO

composto:

- nella parte del ricorso relativa ai “consumatori”, dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti “Consumatori”

- nella parte del ricorso relativa ai “ non consumatori”, dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti “Non Consumatori”

Relatore (MI) DELL ANNA MISURALE

Seduta del 17/03/2026

PARTE RELATIVA AI SOGGETTI "CONSUMATORI"

FATTO

Con il ricorso del 7 ottobre 2025, integrato da quanto dedotto nel modulo di disconoscimento, dal reclamo e dalla denuncia in atti, il cliente espone quanto segue:

- alle ore 13:26 del 29/08/2025 riceveva una chiamata e un sedicente operatore della banca si presentava come nuovo addetto al controllo di movimenti sospetti sulle carte dei clienti;
- la chiamata proveniva da un numero di cellulare privato al numero di linea fissa della sua azienda durante l'orario di chiusura della banca;
- con la chiamata gli veniva comunicato che erano stati registrati dei movimenti sospetti su due carte di debito e una carta di credito su una nota piattaforma di e-commerce. Una carta di debito era intestata al cliente, mentre le altre alla ditta;
- il sedicente operatore gli chiedeva la conferma dei dati anagrafici e delle cifre delle carte per poter accedere al servizio di blocco carte e procedere con l'avvio della procedura assicurativa per il rimborso del denaro sottratto;
- a questo punto l'operatore provvedeva a chiedergli i codici inviati via sms al cellulare, ma egli non riusciva subito a comunicarglieli, in quanto non avvezzo all'impiego della tecnologia e in particolare alla spedizione e ricezione dei messaggi;
- afferma infatti di possedere un cellulare senza connessione internet e di servirsi dell'aiuto della figlia per poter inviare e leggere i messaggi;
- il sedicente operatore lo guidava fornendogli le istruzioni per leggere i messaggi tramite una combinazione dei tasti;
- una volta ottenuti i codici, il truffatore gli comunicava che tutte le carte erano state bloccate e che bisognava passare alla seconda fase utile a richiedere il rimborso all'estero (in Romania);
- i truffatori utilizzavano sia i dati delle carte sia i codici comunicati per creare nuove carte virtuali intestate a lui sul loro dispositivo ed effettuavano movimenti di danaro su propri conti o carte all'estero;
- una volta conclusa la lunga telefonata, chiamava la propria banca dopo l'orario di apertura e scopriva quindi di essere stato vittima di una truffa;
- procedeva, tramite l'aiuto della figlia a bloccare la carta e a presentare denuncia presso le Autorità;
- presentava tre distinti moduli di disconoscimento, che ricevevano riscontro negativo;
- ritiene di essere stato vittima di una truffa di "ingegneria sociale", tramite manipolazione telefonica;
- afferma di aver sempre conservato segretamente i PIN e le credenziali di sicurezza delle carte e di non aver autorizzato le operazioni eseguite dal truffatore.

Chiede, pertanto, il rimborso dei movimenti oggetto di truffa.

L'intermediario, riportato il fatto, espone quanto segue:

- in via preliminare occorre eccepire che nel ricorso il cliente si è qualificato come consumatore, laddove tuttavia due delle carte oggetto di truffa sono intestate alla ditta;
- il cliente ritiene di essere stato vittima di cd. vishing, da lui definito come "truffa di ingegneria sociale";
- le operazioni sono state correttamente contabilizzate, registrate e autenticate con il sistema di autenticazione forte (SCA);

- sussiste la colpa grave del cliente che non ha fornito in merito alcuna allegazione specifica circa la modalità in cui si è svolta la truffa e nemmeno l'estratto conto, limitandosi a negare di aver autorizzato le predette operazioni, ma riconoscendo di avere comunicato i codici ricevuti dall'intermediario; ha peraltro ignorato gli alert ricevuti;
- il blocco della carta è stato richiesto dopo le ore 16:00 (italiane) e quindi successivamente alle operazioni disconosciute dal cliente;
- non sarebbero rilevabili indici di frode, anomalia e sospetto;

Chiede, pertanto, il rigetto del ricorso, in subordine l'applicazione delle franchigie di legge.

Il cliente, richiamati i propri scritti, replica che:

- premette di essersi avvalso dell'aiuto della figlia (procuratrice) per poter esporre le proprie istanze in maniera più appropriata dal punto di vista lessicale e tecnico in tutte le fasi antecedenti alle repliche;
- l'intermediario dovrebbe prendere provvedimenti volti a tutelare la fascia di popolazione che, data l'anzianità, non è avvezza all'uso di dispositivi informatici e strumenti di pagamento digitali;
- è un uomo di 81 anni che si dice estraneo al mondo digitale;
- sono ravvisabili forti indici di anomalie che l'intermediario non ha riscontrato e riconosciuto in relazione al comportamento tenuto solitamente da lui;
- egli si considera un cliente con un profilo alquanto abitudinario e che si avvale di strumenti di pagamento tradizionali, ed effettua operazioni della medesima tipologia ed importo;
- le operazioni sono state effettuate in un intervallo temporale di 50 minuti e hanno riguardato tre carte di credito/debito contemporaneamente delle quali sono stati innalzati i massimali di spesa;
- non è ravvisabile alcuna negligenza in merito alla gestione delle carte fisiche e dei pin relativi, in quanto conservati segretamente e separatamente dalle carte;
- l'intermediario avrebbe dovuto rilevare dei forti indici di anomalia in quanto, nei giorni in cui sono state eseguite le transazioni, sono stati attivati ed utilizzati strumenti digitali mai impiegati prima;
- sebbene il blocco delle tre carte sia tempestivo da parte sua, l'intermediario non gli ha fornito indicazioni su come "fermare, bloccare, congelare" le operazioni eseguite dal truffatore;
- il suo comportamento non può essere qualificato negligente in quanto non ha mai ceduto le proprie carte e i rispettivi PIN a terzi;
- ha riferito solo dati parziali delle carte perché gli altri erano già possesso del truffatore;
- a testimonianza della sua estraneità dal mondo digitale, possiede un telefono di una nota marca destinata ad anziani;
- non c'è stata alcuna omissione nella ricostruzione dei fatti, in quanto nel ricorso si è evidenziato che il truffatore ha conquistato la fiducia del cliente grazie alla conoscenza di alcuni dati personali e in virtù di un atteggiamento rassicurante;
- la qualificazione come consumatore nel ricorso è dovuta al fatto che la truffa è stata compiuta a suo danno come persona fisica e non come titolare della società che peraltro è stata chiusa definitivamente per pensionamento il 31/07/2025;
- è importante sottolineare che la chiamata è avvenuta di venerdì e durante l'orario di chiusura della filiale, il che è stata una scelta strategica del truffatore per evitare che egli potesse contattare l'intermediario;
- il tempestivo blocco delle carte da parte sua ha evitato che i truffatori eseguissero altre operazioni approfittando del weekend e quindi della chiusura della filiale;
- in merito alla mancata allegazione della truffa subita, non è stato richiesto alcun estratto conto in sede di reclamo e di disconoscimento;
- parimenti in sede di reclamo e disconoscimento non è stato richiesto alcun documento comprovante la chiamata e gli sms ricevuti, i quali sono invece stati richiesti nelle controdeduzioni;

- i tabulati sono stati richiesti al numero di competenza, mentre per quanto concerne gli sms si insiste sull'incapacità del ricorrente a non saper né inviare né leggere i messaggi recapitati;
- non può aver autorizzato operazioni di cui non conosce la terminologia e alle quali il truffatore non ha mai fatto nemmeno riferimento;
- non possiede un telefono con connessione internet su cui effettuare l'enrollment dell'app e non possiede un proprio indirizzo e-mail;
- l'indirizzo e-mail utilizzato nell'ambito delle transazioni è sconosciuto e non riconducibile al cliente;
- risulta anomalo che in un lasso temporale assai breve sia stato eseguito l'enrollment di un'applicazione, associato un nuovo numero di telefono, innalzato il limite massimale di spesa di tutte e tre le carte ed eseguite delle transazioni in Irlanda con importi non irrisori.

Con le repliche il cliente, rispetto alla domanda formulata in sede di ricorso, chiede altresì che venga offerta maggiore tutela alla clientela di età avanzata, non abituata ad utilizzare strumenti di pagamento digitali e pertanto più facilmente manipolabili tramite truffe.

L'intermediario, riportandosi alle conclusioni in atti, controreplica che:

- il cliente non può addurre a giustificazione dell'accaduto l'età, in quanto, come dimostrato dall'intestazione di due delle carte alla ditta, trattasi di persona attiva a livello professionale che dovrebbe conoscere il funzionamento anche online degli strumenti di pagamento;
- la continua affermazione di non servirsi del mondo digitale è irrilevante in quanto egli stesso afferma di aver comunicato gli OTP ai truffatori;
- la lamentela circa "il mancato blocco delle operazioni in transito" è erronea e infondata in quanto il cliente confonde l'operazione di blocco della carta con la revoca delle transazioni, la quale non può avvenire una volta che esse siano state correttamente autenticate;
- per quanto concerne la qualifica di consumatore, è irrilevante l'affermazione circa la cessazione dell'attività per pensionamento;
- il richiamo a futuri interventi legislativi è infondato dato che si tratta di proposte ancora in itinere e non ancora vigenti;
- la collaborazione da parte del cliente nel comunicare i dati al truffatore è da qualificare come colpa grave;
- è pacifico che l'orario in cui sono state eseguite le operazioni sia tra le 13:31 e le 13:51, con riferimento a luogo dell'esercente situato in Irlanda;
- è pacifico che il blocco carta sia stato disposto alle ore 16:02 (orario italiano);
- il cliente ammette di aver letto e riferito al truffatore i codici OTP senza sapere di cosa si trattasse, ignorando gli avvisi dell'intermediario sull'indicazione di inserire i detti codici solo in app.

L'intermediario richiama le precedenti difese e insiste per l'accoglimento delle precedenti conclusioni.

DIRITTO

Oggetto di controversia è il diritto al rimborso di n. 7 operazioni disconosciute relative a rapporti facenti capo al ricorrente personalmente, quale persona fisica, nonché nella sua qualità di rappresentante legale di una società in nome collettivo cancellata.

Ai fini della corretta composizione del Collegio, si evidenzia che nel modulo di ricorso il cliente si qualifica come "consumatore".

Sulla base delle evidenze in atti risulta che:

- il ricorrente dichiara di essere stato amministratore della società in nome collettivo e fornisce evidenza (visura camerale e atto notarile) di aver ricoperto la carica di rappresentante legale fino al 31/07/2025, data di cancellazione della s.n.c.;
- il ricorrente dichiara che gli strumenti di pagamento su cui sono state compiute le operazioni fraudolente, comprese le carte aziendali, sono a lui intestati;
- il ricorrente, nella denuncia, ha erroneamente indicato la carta di debito ****0977 come intestata alla società, quando in realtà è intestata a lui stesso come persona fisica; è infatti la carta di debito ****5928 ad essere intestata alla società.

Ne segue che il ricorrente agisce nella duplice qualità di consumatore, per quanto concerne il proprio conto corrente personale, e di non consumatore, per ciò che attiene al conto corrente intestato alla propria attività aziendale.

Ebbene, con riferimento alle domande relative a più rapporti rispetto ai quali il ricorrente rivesta, nel complesso, sia la qualifica di “consumatore” sia di “non consumatore”, i Collegi hanno condiviso l’orientamento secondo cui - alla luce del principio di economia processuale e al fine di assicurare una tutela effettiva della clientela - in questi casi il ricorso debba essere considerato ammissibile e deciso nel merito con riferimento a tutti i rapporti dedotti in giudizio.

Considerato che, in base alle richiamate Disposizioni, è necessario assicurare “che la composizione dell’organo decidente sia adeguata alla tipologia delle parti coinvolte nel ricorso oggetto di trattazione”, è stato ritenuto che in simili casi la composizione del Collegio debba variare in base alla qualifica rivestita dal ricorrente con riguardo alla domanda esaminata, trattando quindi il ricorso nell’ambito di due Collegi diversi con l’adozione di due dispositivi distinti.

Oggetto della presente controversia sono, ora, n. 3 operazioni disconosciute compiute con la carta di debito personale ***0977:

1. in data 29/08/2025 alle ore 13:49 – operazione di euro 1000,00;
2. in data 29/08/2025 alle ore 13.49 – operazione di euro 500,00;
3. in data 29/08/2025 alle ore 13:50 – operazione di euro 500,00.

Le fonti normative applicabili alla fattispecie in esame sono rinvenibili negli artt. 97 e 98 della PDS2, nell’articolo 10 bis del D. Lgs. n. 11/2010, 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). Nello specifico è richiesta l’autenticazione forte (SCA) 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.

Al riguardo, giova precisare che l’art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell’onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l’operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l’operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell’esonero dalla responsabilità (comma 2) che l’uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell’utilizzatore rispetto agli obblighi di condotta imposti a quest’ultimo dall’art. 7 dell’anzidetto decreto. Dalle

dichiarazioni rese dal cliente nella denuncia/nel ricorso risulta che il cliente abbia confermato al sedicente operatore i dati relativi al codice fiscale, numero dei conti correnti e numeri iniziali delle carte di debito/credito.

Solo per scrupolo, si sottolinea che sebbene il cliente affermi di aver riferito i codici OTP arrivati al proprio cellulare sotto la guida dell'operatore, non per questo le operazioni possono considerarsi eseguite personalmente dal cliente. I Collegi sono infatti fermi nel ritenere che, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Pertanto, si procederà di seguito ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010.

Ebbene, rispetto alle dette operazioni non è stata raggiunta la prova della SCA.

Infatti, se per la fase di enrollment dell'App, l'intermediario produce evidenze dalle quali può ricavarsi il doppio fattore autenticazione: username + password (elemento di conoscenza); OTP SMS (elemento di possesso), fa invece difetto la prova della SCA con riferimento alla fase di tokenizzazione delle carte. In proposito, l'intermediario afferma che in data 29/09/2025 il soggetto possessore del device su cui è stata installata l'app, ha aggiunto al wallet (A**** P** = 103) la carta di credito personale del cliente n. ***0977. Per ogni carta aggiunta al digital wallet il circuito assegna un numero Token, ossia un numero di carta virtuale.

Dopo che tale carta è stata aggiunta al digital wallet, sono state autorizzate ed eseguite le operazioni che il cliente chiede di disconoscere.

Ebbene, dalle evidenze prodotte, risulta che:

- la carta digitalizzata precedentemente era utilizzata come carta fisica dal cliente ("non digitalizzata" sotto la voce stato iniziale);
- durante la fase di tokenizzazione è stato associato un numero token (numero di carta virtuale) che generalmente viene considerato un elemento di possesso;
- non è chiaro tuttavia tramite quale canale sia stata tokenizzata la carta, se con app riconducibile all'intermediario o al wallet provider. Sul punto, l'intermediario si limita a dire che il Circuito M*** (di gestione della carta in esame) assegna un numero token.

L'intermediario, quindi, si limita a riportare l'associazione della carta al numero token fornito dal circuito, senza specificare quale sia stato l'iter di autenticazione per la fase di tokenizzazione. In particolare, anche a voler considerare che l'autenticazione sia avvenuta nell'ambito della app di banca, dunque con elemento di possesso (anche se comunque circostanza non provata) non è chiaro quale altro fattore di autenticazione (inerenza/conoscenza) sia intervenuto in tale fase.

Invero, la gestione effettuata dal *wallet provider* nella disposizione di operazioni di pagamento tramite carta digitalizzata non esime il prestatore di servizi di pagamento dalla piena responsabilità per quanto attiene all'adozione delle prescritte misure di sicurezza e, quindi, per la conformità delle modalità di autenticazione anche della fase di tokenizzazione ai requisiti della SCA (in questo senso v. Collegio Milano, decisione n. 143/2023).

Vi è poi che la prova della SCA non sia stata fornita neppure per la fase di innalzamento dei massimali per la carta di pagamento perché l'intermediario si limita a riportare i log degli SMS alert che sono stati inviati al riguardo al numero di cellulare del cliente, senza nulla riferire in merito ai fattori di autenticazione che sono intervenuti in tale fase.

I fattori di autenticazione mancano, infine, anche in relazione alla fase di esecuzione delle singole operazioni.

Dalle evidenze risulta che le operazioni siano state autorizzate tramite l'App del wallet su cui erano state digitalizzate le carte, che può costituire l'elemento di possesso ma l'intermediario non ha prodotto evidenze informatiche circa un secondo fattore di autenticazione (conoscenza e/o inerenza). Peraltro, riportando che le operazioni sono state autenticate tramite lo stesso device su cui la carta era stata digitalizzata e l'APP del wallet l'intermediario fa riferimento a due fattori della stessa natura, vale a dire a fattori qualificabili entrambi come di possesso.

Come da insegnamento consolidato dei Collegi la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

L'importo relativo alle operazioni disconosciute deve, dunque, essere rimborsato integralmente, perché nel caso di specie non è applicabile la franchigia invocata dall'intermediario.

L'orientamento condiviso dai Collegi territoriali è infatti nel senso di ritenere che nel caso di utilizzi fraudolenti on line, la richiesta di applicazione della franchigia formulata dall'intermediario *"non può essere accolta [...] in quanto la stessa è prevista in ipotesi di 'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n.11/2010)"* (cfr. decisione del Collegio di Coordinamento n. 22745 del 10 ottobre 2019; cfr. altresì pronuncia n. 24366/19).

PER QUESTI MOTIVI

Il Collegio, rilevato che il ricorso ha ad oggetto domande relative a più rapporti rispetto ai quali il ricorrente riveste, rispettivamente, la qualifica di consumatore e quella di non consumatore, accoglie la domanda proposta in qualità di consumatore e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.000,00.

Relativamente alle domande formulate dal cliente quale non consumatore, ne rimette l'esame al Collegio nella composizione per tale tipologia di clienti.

PARTE DEL RICORSO RELATIVA AI SOGGETTI “NON CONSUMATORE”.

FATTO

Con il ricorso del 7 ottobre 2025, integrato da quanto dedotto nel modulo di disconoscimento, dal reclamo e dalla denuncia in atti, il cliente espone quanto segue:

- alle ore 13:26 del 29/08/2025 riceveva una chiamata e un sedicente operatore della banca si presentava come nuovo addetto al controllo di movimenti sospetti sulle carte dei clienti;
- la chiamata proveniva da un numero di cellulare privato al numero di linea fissa della sua azienda durante l'orario di chiusura della banca;
- con la chiamata gli veniva comunicato che erano stati registrati dei movimenti sospetti su due carte di debito e una carta di credito su una nota piattaforma di e-commerce. Una carta di debito era intestata al cliente, mentre le altre alla ditta;
- il sedicente operatore gli chiedeva la conferma dei dati anagrafici e delle cifre delle carte per poter accedere al servizio di blocco carte e procedere con l'avvio della procedura assicurativa per il rimborso del denaro sottratto;
- a questo punto l'operatore provvedeva a chiedergli i codici inviati via sms al cellulare, ma egli non riusciva subito a comunicarglieli, in quanto non avvezzo all'impiego della tecnologia e in particolare alla spedizione e ricezione dei messaggi;
- afferma infatti di possedere un cellulare senza connessione internet e di servirsi dell'aiuto della figlia per poter inviare e leggere i messaggi;
- il sedicente operatore lo guidava fornendogli le istruzioni per leggere i messaggi tramite una combinazione dei tasti;
- una volta ottenuti i codici, il truffatore gli comunicava che tutte le carte erano state bloccate e che bisognava passare alla seconda fase utile a richiedere il rimborso all'estero (in Romania);
- i truffatori utilizzavano sia i dati delle carte sia i codici comunicati per creare nuove carte virtuali intestate a lui sul loro dispositivo ed effettuavano movimenti di danaro su propri conti o carte all'estero;
- una volta conclusa la lunga telefonata, chiamava la propria banca dopo l'orario di apertura e scopriva quindi di essere stato vittima di una truffa;
- procedeva, tramite l'aiuto della figlia a bloccare la carta e a presentare denuncia presso le Autorità;
- presentava tre distinti moduli di disconoscimento, che ricevevano riscontro negativo;
- ritiene di essere stato vittima di una truffa di “ingegneria sociale”, tramite manipolazione telefonica;
- afferma di aver sempre conservato segretamente i PIN e le credenziali di sicurezza delle carte e di non aver autorizzato le operazioni eseguite dal truffatore.

Chiede, pertanto, il rimborso dei movimenti oggetto di truffa.

L'intermediario, riportato il fatto, espone quanto segue:

- in via preliminare occorre eccepire che nel ricorso il cliente si è qualificato come consumatore, laddove tuttavia due delle carte oggetto di truffa sono intestate alla ditta;
- il cliente ritiene di essere stato vittima di cd. vishing, da lui definito come “truffa di ingegneria sociale”;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate con il sistema di autenticazione forte (SCA);
- sussiste la colpa grave del cliente che non ha fornito in merito alcuna allegazione specifica circa la modalità in cui si è svolta la truffa e nemmeno l'estratto conto, limitandosi a negare di aver autorizzato

le predette operazioni, ma riconoscendo di avere comunicato i codici ricevuti dall'intermediario; ha peraltro ignorato gli alert ricevuti;

- il blocco della carta è stato richiesto dopo le ore 16:00 (italiane) e quindi successivamente alle operazioni disconosciute dal cliente;

- non sarebbero rilevabili indizi di frode, anomalia e sospetto;

Chiede, pertanto, il rigetto del ricorso, in subordine l'applicazione delle franchigie di legge.

Il cliente, richiamati i propri scritti, replica che:

- premette di essersi avvalso dell'aiuto della figlia (procuratrice) per poter esporre le proprie istanze in maniera più appropriata dal punto di vista lessicale e tecnico in tutte le fasi antecedenti alle repliche;

- l'intermediario dovrebbe prendere provvedimenti volti a tutelare la fascia di popolazione che, data l'anzianità, non è avvezzata all'uso di dispositivi informatici e strumenti di pagamento digitali;

- è un uomo di 81 anni che si dice estraneo al mondo digitale;

- sono ravvisabili forti indizi di anomalie che l'intermediario non ha riscontrato e riconosciuto in relazione al comportamento tenuto solitamente da lui;

- egli si considera un cliente con un profilo alquanto abitudinario e che si avvale di strumenti di pagamento tradizionali, ed effettua operazioni della medesima tipologia ed importo;

- le operazioni sono state effettuate in un intervallo temporale di 50 minuti e hanno riguardato tre carte di credito/debito contemporaneamente delle quali sono stati innalzati i massimali di spesa;

- non è ravvisabile alcuna negligenza in merito alla gestione delle carte fisiche e dei pin relativi, in quanto conservati segretamente e separatamente dalle carte;

- l'intermediario avrebbe dovuto rilevare dei forti indizi di anomalia in quanto, nei giorni in cui sono state eseguite le transazioni, sono stati attivati ed utilizzati strumenti digitali mai impiegati prima;

- sebbene il blocco delle tre carte sia tempestivo da parte sua, l'intermediario non gli ha fornito indicazioni su come "fermare, bloccare, congelare" le operazioni eseguite dal truffatore;

- il suo comportamento non può essere qualificato negligente in quanto non ha mai ceduto le proprie carte e i rispettivi PIN a terzi;

- ha riferito solo dati parziali delle carte perché gli altri erano già possesso del truffatore;

- a testimonianza della sua estraneità dal mondo digitale, possiede un telefono di una nota marca destinata ad anziani;

- non c'è stata alcuna omissione nella ricostruzione dei fatti, in quanto nel ricorso si è evidenziato che il truffatore ha conquistato la fiducia del cliente grazie alla conoscenza di alcuni dati personali e in virtù di un atteggiamento rassicurante;

- la qualificazione come consumatore nel ricorso è dovuta al fatto che la truffa è stata compiuta a suo danno come persona fisica e non come titolare della società che peraltro è stata chiusa definitivamente per pensionamento il 31/07/2025;

- è importante sottolineare che la chiamata è avvenuta di venerdì e durante l'orario di chiusura della filiale, il che è stata una scelta strategica del truffatore per evitare che egli potesse contattare l'intermediario;

- il tempestivo blocco delle carte da parte sua ha evitato che i truffatori eseguissero altre operazioni approfittando del weekend e quindi della chiusura della filiale;

- in merito alla mancata allegazione della truffa subita, non è stato richiesto alcun estratto conto in sede di reclamo e di disconoscimento;

- parimenti in sede di reclamo e disconoscimento non è stato richiesto alcun documento comprovante la chiamata e gli sms ricevuti, i quali sono invece stati richiesti nelle controdeduzioni;

- i tabulati sono stati richiesti al numero di competenza, mentre per quanto concerne gli sms si insiste sull'incapacità del ricorrente a non saper né inviare né leggere i messaggi recapitati;
- non può aver autorizzato operazioni di cui non conosce la terminologia e alle quali il truffatore non ha mai fatto nemmeno riferimento;
- non possiede un telefono con connessione internet su cui effettuare l'enrollment dell'app e non possiede un proprio indirizzo e-mail;
- l'indirizzo e-mail utilizzato nell'ambito delle transazioni è sconosciuto e non riconducibile al cliente;

- risulta anomalo che in un lasso temporale assai breve sia stato eseguito l'enrollment di un'applicazione, associato un nuovo numero di telefono, innalzato il limite massimale di spesa di tutte e tre le carte ed eseguite delle transazioni in Irlanda con importi non irrisori.

Con le repliche il cliente, rispetto alla domanda formulata in sede di ricorso, chiede altresì che venga offerta maggiore tutela alla clientela di età avanzata, non abituata ad utilizzare strumenti di pagamento digitali e pertanto più facilmente manipolabili tramite truffe.

L'intermediario, riportandosi alle conclusioni in atti, controreplica che:

- il cliente non può addurre a giustificazione dell'accaduto l'età, in quanto, come dimostrato dall'intestazione di due delle carte alla ditta, trattasi di persona attiva a livello professionale che dovrebbe conoscere il funzionamento anche online degli strumenti di pagamento;
 - la continua affermazione di non servirsi del mondo digitale è irrilevante in quanto egli stesso afferma di aver comunicato gli OTP ai truffatori;
 - la lamentela circa "il mancato blocco delle operazioni in transito" è erronea e infondata in quanto il cliente confonde l'operazione di blocco della carta con la revoca delle transazioni, la quale non può avvenire una volta che esse siano state correttamente autenticate;
 - per quanto concerne la qualifica di consumatore, è irrilevante l'affermazione circa la cessazione dell'attività per pensionamento;
 - il richiamo a futuri interventi legislativi è infondato dato che si tratta di proposte ancora in itinere e non ancora vigenti;
 - la collaborazione da parte del cliente nel comunicare i dati al truffatore è da qualificare come colpa grave;
 - è pacifico che l'orario in cui sono state eseguite le operazioni sia tra le 13:31 e le 13:51, con riferimento a luogo dell'esercente situato in Irlanda;
 - è pacifico che il blocco carta sia stato disposto alle ore 16:02 (orario italiano);
 - il cliente ammette di aver letto e riferito al truffatore i codici OTP senza sapere di cosa si trattasse, ignorando gli avvisi dell'intermediario sull'indicazione di inserire i detti codici solo in app.
- L'intermediario richiama le precedenti difese e insiste per l'accoglimento delle precedenti conclusioni.

DIRITTO

Oggetto di controversia è il diritto al rimborso di n. 7 operazioni disconosciute relative a rapporti facenti capo al ricorrente personalmente, quale persona fisica, nonché nella sua qualità di rappresentante legale di una società in nome collettivo cancellata.

Ai fini della corretta composizione del Collegio, si evidenzia che nel modulo di ricorso il cliente si qualifica come "consumatore".

Sulla base delle evidenze in atti risulta che:

- il ricorrente è stato amministratore e rappresentante legale della società in nome collettivo di cui fornisce evidenza (visura camerale e atto notarile);
- gli strumenti di pagamento su cui sono state compiute le operazioni fraudolente, comprese le carte aziendali, sono a lui intestati;
- nella denuncia, ha erroneamente indicato la carta di debito ****0977 come intestata alla società, quando in realtà è intestata a lui stesso come persona fisica; è infatti la carta di debito ****5928 ad essere intestata alla società.

Ne segue che il ricorrente agisce nella duplice qualità di consumatore, per quanto concerne il proprio conto corrente personale, e di non consumatore, per ciò che attiene al conto corrente intestato alla propria attività aziendale.

Ebbene, con riferimento alle domande relative a più rapporti rispetto ai quali il ricorrente rivesta, nel complesso, sia la qualifica di “consumatore” sia di “non consumatore”, i Collegi hanno condiviso l’orientamento secondo cui - alla luce del principio di economia processuale e al fine di assicurare una tutela effettiva della clientela - in questi casi il ricorso debba essere considerato ammissibile e deciso nel merito con riferimento a tutti i rapporti dedotti in giudizio.

Considerato che, in base alle richiamate Disposizioni, è necessario assicurare “che la composizione dell’organo decidente sia adeguata alla tipologia delle parti coinvolte nel ricorso oggetto di trattazione”, è stato ritenuto che in simili casi la composizione del Collegio debba variare in base alla qualifica rivestita dal ricorrente con riguardo alla domanda esaminata, trattando quindi il ricorso nell’ambito di due Collegi diversi con l’adozione di due dispositivi distinti.

Oggetto della presente controversia sono, ora, quattro operazioni disconosciute di cui n. 3 sulla carta di debito intestata alla società n. ***5928:

- 1) in data 29/08/2025 alle ore 13:33- operazione di euro 1000,00;
- 2) in data 29/08/2025 alle ore 13:33 - operazione di euro 1000,00;
- 3) in data 29/08/2025 alle ore 13:40-operazione di euro 500,00

e n. 1 sulla carta di credito intestata alla società n. ****6012:

- 1) in data 29/08/2025 alle ore 13:31- operazione di euro 2.500,00.

Le fonti normative applicabili alla fattispecie in esame sono rinvenibili negli artt. 97 e 98 della PDS2, nell’articolo 10 bis del D. Lgs. n. 11/2010, 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). Nello specifico è richiesta l’autenticazione forte (SCA) 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.

Al riguardo, giova precisare che l’art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell’onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l’operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l’operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell’esonero dalla responsabilità (comma 2) che l’uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell’utilizzatore

rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto. Dalle dichiarazioni rese dal cliente nella denuncia/nel ricorso risulta che il cliente abbia confermato al sedicente operatore i dati relativi al codice fiscale, numero dei conti correnti e numeri iniziali delle carte di debito/credito.

Solo per scrupolo, si sottolinea che sebbene il cliente affermi di aver riferito i codici OTP arrivati al proprio cellulare sotto la guida dell'operatore, non per questo le operazioni possono considerarsi eseguite personalmente dal cliente. I Collegi sono infatti fermi nel ritenere che, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Pertanto, si procederà di seguito ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010.

Ebbene, rispetto alle dette operazioni non è stata raggiunta la prova della SCA.

Infatti, se per la fase di enrollment dell'App, l'intermediario produce evidenze dalle quali può ricavarsi il doppio fattore di autenticazione: username + password (elemento di conoscenza); OTP SMS (elemento di possesso), fa difetto la prova della SCA con riferimento alla fase di tokenizzazione delle carte.

In proposito, l'intermediario afferma che in data 29/09/2025 il soggetto possessore del device su cui è stata installata l'app, ha aggiunto al wallet (A**** P** = 103) la carta di debito ***5928 e la carta di credito ***6012. Per ogni carta aggiunta al digital wallet il circuito assegna un numero Token, ossia un numero di carta virtuale.

Dopo che le carte sono state aggiunte al digital wallet, sono state autorizzate ed eseguite le operazioni che il cliente chiede di disconoscere.

Ebbene, dalle evidenze prodotte, risulta che:

- sono state digitalizzate le carte ***6012 e ***5298, le quali precedentemente erano solamente utilizzate come carte fisiche dal cliente ("non digitalizzata" sotto la voce stato iniziale);
- durante la fase di tokenizzazione è stato associato un numero token (numero di carta virtuale) che generalmente viene considerato un elemento di possesso;
- non è chiaro tuttavia tramite quale canale siano state tokenizzate le carte, se con app riconducibile all'intermediario o al wallet provider. Sul punto, l'intermediario si limita a dire che il Circuito M*** (di gestione delle carte in esame) assegna un numero token.

L'intermediario, quindi, si limita a riportare l'associazione delle carte al numero token fornito dal circuito, senza specificare quale sia stato l'iter di autenticazione per la fase di tokenizzazione. In particolare, anche a voler considerare che l'autenticazione sia avvenuta nell'ambito della app di banca, dunque con elemento di possesso (anche se comunque circostanza non provata) non è chiaro quale altro fattore di autenticazione (inerenza/conoscenza) sia intervenuto in tale fase.

Invero, la gestione effettuata dal *wallet provider* nella disposizione di operazioni di pagamento tramite carta digitalizzata non esime il prestatore di servizi di pagamento dalla piena responsabilità per quanto attiene all'adozione delle prescritte misure di sicurezza e, quindi, per la conformità delle modalità di autenticazione anche della fase di tokenizzazione ai requisiti della SCA (in questo senso v. Collegio Milano, decisione n. 143/2023).

Vi è poi che la prova della SCA non sia stata fornita neppure per la fase di innalzamento dei massimali per le carte di pagamento perché l'intermediario si limita a riportare i log degli SMS alert che sono stati inviati al riguardo al numero di cellulare del cliente, senza nulla riferire in merito ai fattori di autenticazione che sono intervenuti in tale fase.

I fattori di autenticazione mancano, infine, anche in relazione alla fase di esecuzione delle singole operazioni.

Dalle evidenze risulta che le operazioni siano state autorizzate tramite l'App del wallet su cui erano state digitalizzate le carte, che può costituire l'elemento di possesso ma l'intermediario non ha prodotto evidenze informatiche circa un secondo fattore di autenticazione (conoscenza e/o inerenza). Peraltro, riportando che le operazioni sono state autenticate tramite lo stesso device su cui le carte erano state digitalizzate e l'APP del wallet, l'intermediario fa riferimento a due fattori della stessa natura, vale a dire a fattori qualificabili entrambi come di possesso.

Come da insegnamento consolidato dei Collegi la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

L'importo relativo alle quattro operazioni disconosciute deve, dunque, essere rimborsato integralmente, perché nel caso di specie non è applicabile la franchigia invocata dall'intermediario.

L'orientamento condiviso dai Collegi territoriali è infatti nel senso di ritenere che nel caso di utilizzi fraudolenti on line, la richiesta di applicazione della franchigia formulata dall'intermediario *"non può essere accolta [...] in quanto la stessa è prevista in ipotesi di 'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n.11/2010)"* (cfr. decisione del Collegio di Coordinamento n. 22745 del 10 ottobre 2019; cfr. altresì pronuncia n. 24366/19).

PER QUESTI MOTIVI

Il Collegio, preso atto che il ricorso ha ad oggetto domande relative a più rapporti rispetto ai quali il ricorrente riveste, rispettivamente, la qualifica di consumatore e quella di non consumatore, accoglie la domanda proposta in qualità di non consumatore e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.000,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE