

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 14/04/2026

FATTO

La ricorrente rappresenta di essere stata vittima, in data 30.09.2025, di una truffa perpetrata attraverso una nota piattaforma di vendite *on-line*, a seguito della quale veniva eseguita sulla sua carta di debito una operazione totalmente non autorizzata per l'importo di € 499,00. Riferisce di aver immediatamente provveduto al disconoscimento dell'operazione e di aver presentato denuncia alle autorità competenti. La banca, dopo aver inizialmente riaccreditato l'importo disconosciuto, provvedeva al successivo riaddebito, adducendo motivazioni che la ricorrente ritiene non condivisibili.

L'intermediario, nelle proprie controdeduzioni, riporta che nella denuncia la ricorrente dichiara di aver messo in vendita, in data 29.09.2025, alcuni oggetti su una piattaforma *on-line*, ricevendo poco dopo un messaggio da un sedicente potenziale acquirente nella chat del portale, che la invitava a contattarlo tramite un'applicazione di messaggistica istantanea. Dopo aver preso contatto con il medesimo, questi si dichiarava interessato all'acquisto e le trasmetteva un'immagine richiedendole la propria *e-mail* personale; la ricorrente gliela forniva e riceveva immediatamente un *link*, accedendo al quale le veniva chiesto di inserire i dati completi della propria carta di pagamento. La ricorrente eseguiva quanto richiesto e, di lì a poco, veniva eseguita l'operazione per l'importo di € 499,00. L'intermediario evidenzia che la ricorrente ammette di aver inserito i dati della propria carta di debito sul sito truffaldino, al quale aveva avuto accesso mediante un *link* trasmessole via *e-mail* dal frodatore, nell'erronea convinzione che tale operazione fosse funzionale all'incasso del prezzo dell'oggetto messo in vendita. Ritiene pertanto che l'operazione debba intendersi personalmente autorizzata dalla cliente e che non sia applicabile la disciplina di cui al D.lgs. n. 11/2010; in ogni caso, sostiene che l'operazione risulta correttamente autenticata mediante il corretto inserimento delle credenziali, come da documentazione informatica prodotta. Eccepisce altresì la sussistenza della colpa grave della ricorrente, la quale avrebbe: dato credito a una comunicazione evidentemente fraudolenta; inserito i dati della propria carta su un sito truffaldino; ignorato del tutto la notifica *push* ricevuta, dal contenuto inequivocabile.

DIRITTO

L'operazione oggetto di contestazione rientra nell'ambito di applicazione del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13.01.2018) del D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno e alla disciplina in materia di *strong customer authentication* (SCA).

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave in capo all'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, nell'art. 10 bis del D. lgs. 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, 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.

Nel caso in esame, l'operazione disconosciuta consiste in un pagamento, per l'importo di € 499,00, eseguito tramite carta di debito in data 30.09.2025 alle ore 11:02.

Dalla denuncia presentata dalla ricorrente sempre in data 30.09.2025 emerge che la ricorrente aveva messo in vendita alcuni oggetti su una piattaforma *on-line* ed era stata contattata da un presunto acquirente nella *chat* del portale, che la invitava a proseguire la comunicazione tramite un'applicazione di messaggistica esterna. In tale sede aveva ricevuto un *link*, accedendo al quale le veniva richiesto di inserire i dati completi della propria carta di pagamento, operazione che la ricorrente eseguiva, nella convinzione di dover compiere tale passaggio per ricevere il corrispettivo dell'oggetto messo in vendita. L'intermediario eccepisce l'inapplicabilità del regime di protezione di cui al D.lgs. n. 11/2010, sostenendo che l'operazione sarebbe da intendersi personalmente disposta dalla ricorrente.

Tuttavia, il Collegio rileva che, nella denuncia e nel ricorso, la cliente ha unicamente riferito di aver inserito sul sito truffaldino i dati della propria carta di debito, e non anche di aver inserito fattori di autenticazione o comunque autorizzato l'operazione, che è stata formalmente disconosciuta. Secondo l'orientamento consolidato ABF, 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. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010.

Riguardo alla prova della autenticazione forte, l'intermediario ha precisato che la cliente, codice utente n. *486, si connette prevalentemente usando un *device iPhone* identificato con il codice univoco. L'operatività contestata è stata eseguita con tale *device*, mediante la carta di debito n. *785 intestata alla cliente.

Dalle evidenze informatiche prodotte dall'intermediario emerge che, in data 30.09.2025 alle ore 11:02:47, dopo l'inserimento della disposizione di pagamento e delle credenziali della carta nel sito dell'esercente, dal dispositivo in uso alla ricorrente veniva confermato il pagamento di € 499,00 a mezzo carta di debito. La transazione è stata validata con il codice OTP virtuale, mediante riconoscimento biometrico. Risulta anche evidenza della notifica *push* del seguente tenore: “*Stai autorizzando il pagamento di 499.00 EUR presso M* del 30/09/2025 11:02 con la carta xxx785*”, vale a dire con indicazione esplicita dell'importo, del beneficiario e della carta utilizzata. La validazione dell'OTP, generata dall'APP installata sul *device* della cliente alle ore 11:02:47, mediante validazione biometrica porta all'esecuzione dell'operazione di pagamento alle ore 11:02:57. La notifica risulta essere stata correttamente consegnata sul dispositivo intestato alla ricorrente.

L'operazione disconosciuta risulta essere stata autorizzata mediante invio di notifica *push* sul dispositivo della cliente con successiva generazione di OTP virtuale (elemento di possesso), generato e validato tramite riconoscimento biometrico-impronta digitale (elemento di inerenza). Viene dunque raggiunta la prova dell'autenticazione forte ai sensi della PSD2 e del D.lgs. n. 11/2010.

In merito alla condotta delle parti e ai profili rilevanti per la valutazione della sussistenza o meno della colpa grave dell'utente, risulta che la truffa ha avuto luogo mediante canali in nessun modo riconducibili all'intermediario. Dall'esame congiunto delle dichiarazioni della ricorrente e dei log prodotti dall'intermediario, emerge che l'operazione fraudolenta è stata di fatto disposta dalla stessa ricorrente per il tramite del dispositivo nella sua esclusiva disponibilità, del quale non ha mai dichiarato di aver perso il possesso. La ricorrente ha segnatamente: fornito credito alle indicazioni di un sedicente acquirente; inserito i propri dati di pagamento su un sito truffaldino; validato mediante riconoscimento biometrico la notifica *push* recapitata sul proprio dispositivo, la quale recava l'indicazione esplicita e non ambigua del pagamento che si stava per autorizzare. La condotta complessiva così descritta integra gli estremi della colpa grave ai sensi dell'art. 12 del D.Lgs. n. 11/2010, ravvisabile nella macroscopica violazione degli obblighi di diligenza e cautela che devono presiedere all'utilizzo degli strumenti di pagamento.

Con riferimento al profilo delle notifiche di avvenuta esecuzione delle operazioni, agli atti non vi è evidenza di attivazione di un servizio di SMS-*alert* o di servizio assimilabile (v. Collegio di coordinamento, decisione n. 8672/2024). Sul punto, tuttavia, i Collegi hanno condiviso un'interpretazione sostanzialistica di tale presidio di sicurezza *ex post*, ritenendo che la mancata attivazione ovvero il mancato funzionamento del servizio di SMS-*alert* siano irrilevanti nelle ipotesi di esecuzione di una sola operazione fraudolenta — come nel caso in esame — in quanto la tempestiva ricezione dell'*alert* non avrebbe potuto in concreto limitare il pregiudizio dell'utente (*ex multis*, Collegio di Milano, decisione n. 1110/2023).

Alla luce delle considerazioni che precedono, il ricorso deve essere rigettato.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE