

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PICARO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore DANIELA CONCETTA NOTARO

Seduta del 13/02/2026

FATTO

Con ricorso del 1.08.2025 (preceduto da rituale reclamo negativamente riscontrato dall'intermediario), l'istante si è rivolta a codesto Collegio rappresentando che il 16/07/2024, visionando l'estratto conto, si accorgeva di un movimento fraudolento da lei mai autorizzato, ossia un pagamento POS estero effettuato il 16/07/2024 in favore di Nike di euro 1.081,63 (comprensivo di commissioni di conversione valuta).

La truffa, in realtà, ha avuto origine da un sms ricevuto il pari data, nel quale era scritto *"la consegna del pacco è sospesa a causa del numero civico. Per favore, aggiorna le informazioni qui: ***"*.

Poiché era in attesa della consegna di alcuni acquisti online, in buona fede cliccava sul link, che reindirizzava ad una pagina web simile a quella di un altro intermediario, dove inseriva i dati mancanti; successivamente si apriva una pagina nella quale veniva chiesto l'inserimento dei dati della carta per coprire i costi di consegna.

La ricorrente inseriva i dati richiesti, senza sospettare lo *smishing*.

Ritenendo sussistere una responsabilità dell'intermediario, ha richiesto il rimborso dell'importo sottratto. Nel costituirsi con apposite controdeduzioni, l'intermediario ha osservato che la ricorrente è titolare della carta di debito collegata con al suo conto corrente n.ro **, in essere presso la filiale di Roma ***, abilitato al servizio di Internet Banking.

Tramite detto servizio, alle ore 22:34 del giorno 16.07.2024, è stato effettuato un pagamento su commercio elettronico presso la Nike di Hong Kong dell'importo di euro 1.060,32.

Il valore complessivo di addebito sul conto della cliente è di euro 1.081,63 perché maggiorato delle commissioni per complessivi euro 21,31 di cui: euro 10,60 di "conversion fee" ed euro 10,71 di "optional fee".

Tale complessivo addebito in origine era in 8.995,00 dollari hongkonghesi (HKD), cioè la divisa originaria della transazione, a cui è stato applicato il tasso di cambio di 0,120247.

Per accedere ai servizi online della Banca è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice Titolare (password statica) il codice PIN (password statica) e il codice O* (OTP

cioè la password dinamica). Il codice OTP, oltre che per l'operazione di login al portale, è utilizzato per l'autorizzazione delle singole operazioni di tipo dispositivo. Il Codice O* (OTP) è il codice che viene generato: via software dall'App della Banca, per i clienti che hanno attivato O* Smart; via SMS (inoltrato sul numero di telefono certificato), per i clienti che hanno attivato O* SMS. Con l'utilizzo dell'O* Smart, i codici O* dinamici per accedere ai servizi di banca online e per autorizzare le operazioni sono generati a seguito della selezione della notifica ricevuta sullo smartphone o tablet su cui è stato attivato O* Smart e della successiva digitazione su tale smartphone o tablet del PIN oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale. In caso di smartphone o tablet con connessione dati assente o momentaneamente non funzionante, il codice O* dinamico è inviato tramite SMS al numero di cellulare certificato. Infine, per aumentare ancora il livello di sicurezza di alcune disposizioni di pagamento, oltre la consueta autenticazione e conferma con codice dinamico, è richiesto al cliente l'inserimento di un secondo codice inviato via SMS.

La Banca fornisce alla propria clientela ampia informativa sul proprio sito internet dove viene sempre sottolineato di prestare attenzione alle e-mail, sms e telefonate sospette e di diffidare da link che prevedano l'inserimento di password. Sul sito della Banca vi è una apposita sezione denominata "Sicurezza" in cui vengono fornite specifiche indicazioni per difendersi dai tentativi di truffa. In tale sezione, oltre ad essere indicati i corretti comportamenti da adottare per prevenire le frodi, vengono riportati graficamente degli esempi di tentativi di truffa perpetrati via sms, e-mail e web. Più nello specifico, il cliente viene esplicitamente invitato a prestare attenzione al contenuto dei messaggi ricevuti e a non comunicare codici personali (che non vengono mai chiesti dalla banca).

Al fine di dimostrare la corretta autenticazione delle operazioni e l'assenza di anomalie è stato prodotto l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta riportante i log estratti, in formato non editabile, dagli archivi informatici della Banca.

Nel caso in esame, la ricorrente si connette prevalentemente usando uno smartphone del tipo Android, identificato con il codice univoco: "****bb5".

Il 16/07/2024 alle ore 22:34 risulta disposto dalla APP un pagamento di 8.995,00 dollari hongkonghesi (HKD) presso "Nike". La transazione è stata autorizzata, con la validazione del codice OTP, previo inserimento del pin.

In particolare, nella ricostruzione emergerebbe la colpa grave desumibile dalle sotto riportate circostanze:

- A) l'operazione di pagamento disconosciuta è stata autorizzata con il corretto inserimento delle credenziali del servizio di internet banking della cliente;
- B) in sede di disconoscimento e nel reclamo la cliente ha ammesso di aver ricevuto in data 16/07/2024 sul proprio telefono un sms contenente un link su cui ha cliccato, di aver poi risposto alle informazioni che le venivano richieste;
- C) l'operazione di pagamento contestata è stata eseguita subito dopo;
- D) la cliente ha consentito l'esecuzione dell'operazione contestata, cadendo vittima di una truffa piuttosto semplice e assumendo dunque una condotta non scusabile (si veda, per tutte, la decisione del Collegio di Roma, n. 7088, del 21/7/2025);
- E) infine, la ricorrente non allega lo screenshot dell'SMS che dichiara di aver ricevuto, impedendo di fatto di valutare sussistenza ed entità del tipo di truffa subita. In ogni caso il link non è in alcun modo riconducibile alla Banca (*ex multis* decisione del Collegio di Napoli n.108/2025);

Da ciò si confermerebbe che la ricorrente è stata vittima di una truffa di tipo *smishing*, che esula dalla responsabilità della banca.

Alla luce di quanto precede, l'intermediario ha richiesto di respingere il ricorso e, in subordine, di riconoscere il concorso di colpa tra le parti.

In sede di repliche, la ricorrente ricapitola i fatti e ribadisce di aver cliccato sul link in buona fede, in quanto era effettivamente in attesa della consegna di alcuni acquisti.

Nelle controrepliche la banca ribadisce che la ricorrente non ha allegato l'sms truffaldino e che, in ogni caso, il link ivi contenuto non è riconducibile alla banca.

DIRITTO

Come noto, l'utilizzo fraudolento è disciplinato dal 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, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 correlata alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Sul punto si rammenta che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo *“ispirata al principio del “rischio d'impresa”, e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente “pericolose”, che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi”* (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 (*infra* riportato) prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

- A. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Nello specifico, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;
- B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Nel merito, parte ricorrente chiede il rimborso della somma di euro 1.081,63, corrispondente all'importo distratto con l'operazione disconosciuta.

In ordine agli elementi di fatto, la ricorrente dichiara di aver ricevuto un sms che la informava dell'impossibilità di portare a termine una spedizione a lei destinata; dichiara, inoltre, di aver fatto accesso al link contenuto nel messaggio e di aver inserito i dati della carta di debito per pagare il corrispettivo richiesto per il perfezionamento della spedizione.

Nella denuncia la ricorrente ha solo disconosciuto l'operazione.

Ciò posto, si precisa che quella in esame potrebbe essere un'operazione autorizzata dalla ricorrente, nella convinzione di pagare i costi di spedizione, così come indicato nel link truffaldino.

In ogni caso, avendo la ricorrente dichiarato di non aver autorizzato l'operazione, verranno esaminate le modalità di autenticazione nel rispetto degli elementi richiesti dalla normativa di settore ai fini della c.d. *strong customer authentication*, cui si aggiunge l'ulteriore eventuale rilevanza causale del contegno della parte ricorrente, così come richiesto dal d.lgs. 11/2010.

In tale contesto, l'intermediario afferma di aver adottato un sistema di autenticazione forte, illustrato più dettagliatamente nelle controdeduzioni.

In particolare, quanto alle modalità di funzionamento del servizio di home banking, l'intermediario evidenzia come sia necessario l'inserimento di due codici statici (codice titolare e codice PIN) e di un codice dinamico (Codice O***).

Il codice dinamico può essere generato attraverso due diversi canali: a) via software dall'App, per i clienti che hanno attivato O*** Smart; b) via SMS (inoltrato sul numero di telefono certificato), per i clienti che hanno attivato O*** SMS.

Con l'utilizzo dell'O*** Smart, i codici dinamici per accedere ai servizi di banca online e per autorizzare le operazioni sono generati a seguito della: i) selezione della notifica ricevuta sullo smartphone o tablet su cui è stato attivato O*** Smart; ii) digitazione su tale smartphone o tablet del PIN oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale.

In caso di smartphone o tablet con connessione dati assente o momentaneamente non funzionante, il codice O* dinamico è inviato tramite SMS al numero di cellulare certificato.

L'intermediario precisa che l'operazione, dunque, è stata disposta tramite il device in uso della ricorrente.

Ed in proposito, ha rilevato che il giorno 16/07/2024 alle ore 22:34 è stata disposta l'operazione disconosciuta. La transazione è stata autorizzata, con la validazione del codice OTP [fattore di possesso] previo inserimento del pin [fattore di conoscenza].

In tale direzione, l'operazione appare conforme alla SCA.

Quanto, poi, alla valutazione della condotta di parte ricorrente, quest'ultima riferisce che la truffa ha avuto origine da un sms che la invitava ad aggiornare le informazioni necessarie per la consegna di un pacco. Il mittente è un'utenza privata non riconducibile alla banca.

In tale contesto, va precisato che dalla documentazione agli atti, si evince la ricezione di un sms da un numero di cellulare sconosciuto alla ricorrente contenente un link.

Dunque, la truffa è stata perpetrata mediante il fenomeno del c.d. *smishing*, tipo particolare di *phishing*, caratterizzato dalla ricezione del messaggio ingannevole tramite SMS.

Il phishing operato tramite e-mail o sms è ritenuto fenomeno diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso dell'home banking, dovrebbero conoscere.

L'orientamento cristallizzato nelle pronunce dei Collegi Territoriali (e dello stesso Collegio di Coordinamento) evidenzia che soltanto il ricorrente vittima di truffe particolarmente insidiose e difficili da individuare è esente da colpa grave.

Viceversa, il ricorrente vittima di truffe tramite phishing o, come nel caso di specie, smishing, è gravemente negligente nella custodia dei codici di accesso, circostanza questa che comporta la responsabilità dell'utilizzatore ai sensi dell'art. 12, comma 3, D.Lgs. n. 11/2010, e non consente di accogliere la richiesta di rimborso delle somme indebitamente sottratte.

Il Collegio osserva altresì che, nel caso di specie, la ricorrente ammette di aver dato seguito alle istruzioni contenute nel messaggio ricevuto sulla propria utenza telefonica, che erroneamente credeva provenire dall'intermediario resistente.

Ne deriva che la domanda di parte ricorrente non può essere accolta.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE