COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 06/02/2025

FATTO

Dall'atto introduttivo emerge che il 05/10/2024 la ricorrente è stata avvisata dalla propria banca di n. 6 bonifici istantanei sospetti in uscita dal suo conto il 04/10/2024 e il 05/10/2024, per un totale di 2.580,00 euro. Questi bonifici in uscita si accompagnavano ad alcuni accrediti di piccolo importo, per un totale di €.143,00.

La ricorrente afferma di non aver mai fornito a terzi le proprie credenziali e di non aver cooperato neppure involontariamente in alcun modo all'effettuazione di queste operazioni.

Ciò premesso, al ricorrente domanda il rimborso di 2.437,00 € (pari alla differenza tra operazioni in uscita e in entrata).

Nelle controdeduzioni l'intermediario eccepisce quanto segue.

• L'autenticazione delle operazioni disconosciute è avvenuta attraverso i seguenti passaggi.

o In primo luogo, alle 14:13 del 04/10/2024 il truffatore ha effettuato l'accesso all'home banking via browser inserendo codice cliente, data di nascita e PIN (elemento di conoscenza).
A questo punto, la ricorrente ha cliccato sulla notifica push ricevuto sull'app token installata sul suo smartphone (elemento di possesso), digitando il PIN (elemento di conoscenza) per generale l'OTP in via silente sul dispositivo.
o Il truffatore ha quindi disposto un bonifico tramite home banking, che è stato autenticato dalla ricorrente sull'app token (elemento di possesso), previa ricezione di una notifica push e digitazione del PIN (elemento di conoscenza).
o Lo stesso processo (accesso via browser e autenticazione di un bonifico) si è poi ripetuto per tutte le altre operazioni, alle 18:33 e alle 18:56 del 04/10/2024, nonché 10:00, alle 11:16 e alle 12:05 del 05/10/2024.
• Dopo ciascuna operazione, l'intermediario ha trasmesso SMS alert al numero di cellulare della ricorrente.
• Quanto alla colpa grave, il fatto che nella fase di autenticazione si stato utilizzato lo smartphone della ricorrente — attivato come dispositivo token il 16/08/2020, ben prima della frode — attesta la sua cooperazione della frode, nonostante l'assenza di elementi sul punto nel ricorso.
• Successivamente alla frode, il 12/10/2024, sul conto della ricorrente è pervenuto un ulteriore accredito di 20,00 €.
• Una volta venuto a conoscenza della natura fraudolenta delle operazioni, l'intermediario ne ha tentato il recall, che si è però concluso negativamente.
Ciò posto, l'intermediario chiede il rigetto del ricorso.
Nelle repliche, la parte ricorrente contesta di aver cooperato colpevolmente nell'autenticazione delle operazioni, suggerendo che le operazioni siano state effettuate tramite la violazione dei sistemi informatici dell'intermediario.
Afferma che, in ogni caso, la banca avrebbe dovuto bloccare preventivamente le operazioni in quanto sospette.
Con le controrepliche, l'intermediario si riporta a quanto già dedotto.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite nei giorni del 4 e 5 ottobre 2024. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".
Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the*

European Banking Authority on the elements of strong customer authentication under PSD2 del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

4.- Le operazioni contestate sono n. 6 bonifici istantanei disposti tra il 04/10/2024 e il 05/10/2024: bonifico di 20,00 € del 04/10/2024 ore 14:28; bonifico di 50,00 € del 04/10/2024 ore 18:35; bonifico di 20,00 € del 04/10/2024 ore 18:58; bonifico di 100,00 € del 05/10/2024 ore 10:02; bonifico di 490,00 € del 05/10/2024 ore 11:19; bonifico di 1900,00 € del 05/10/2024 ore 12:07.

Ai bonifici in uscita si sono intervallati da bonifici in entrata per un totale di 163,00 € (di 143,00 € dà conto già la ricorrente nel ricorso e ad ulteriori 20,00 € fa riferimento l'intermediario nelle controdeduzioni). La ricorrente detrae il valore dei bonifici in entrata dall'oggetto della domanda.

5.- Quanto all'autenticazione delle operazioni, dai log in atti, risulta che ciascuna delle operazioni è stata preceduta da un separato accesso all'home banking via browser tramite codice cliente, data di nascita e PIN (elemento di conoscenza) e generazioni di OTP in via silente sullo smartphone della ricorrente (elemento di possesso) — configurato come dispositivo token il 16/08/2020 —, previa ricezione di una notifica push e la digitazione del PIN (elemento di conoscenza).

Dopo ciascun accesso è stato disposto un bonifico, autenticato previa ricezione della notifica push sull'app token installata sullo smartphone della ricorrente (elemento di possesso) e la digitazione del PIN (elemento di conoscenza) per generale l'OTP in via silente sul dispositivo.

Sono presenti agli atti i log relativi all'accesso all'home banking delle 14:13 del 04/10/2024, da cui risulta l'impiego delle credenziali statiche e la generazione di OTP in via silente tramite app token tramite push e digitazione del PIN.

L'intermediario produce log analoghi anche per le altre operazioni, attestanti la stessa modalità di autenticazione (accesso via browser e autenticazione di un bonifico) per ciascuna di esse, alle 18:33 e alle 18:56 del 04/10/2024, nonché 10:00, alle 11:16 e alle 12:05 del 05/10/2024.

Produce, altresì, il log attestante che il token impiegato nell'autenticazione è quello attivato dalla ricorrente il 16/08/2020.

6.- La parte ricorrente lamenta il mancato blocco preventivo da parte dell'intermediario delle operazioni di pagamento contestate, a fronte della loro natura anomala.

Sul tema del monitoraggio preventivo delle operazioni di pagamento si osserva che l'art. 2 del Regolamento Delegato (UE) n. 2018/389 della Commissione prevede che gli intermediari predispongano meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. Peraltro, in base all'interpretazione fornita dall'EBA, non è necessario che questi meccanismi operino in tempo reale – vagliando le operazioni prima della loro esecuzione –, potendo limitarsi a un monitoraggio delle frodi ex post (cfr. ex plurimis Collegio di Roma, decisione n. 2534 del 10/02/2022, decisione n. 707/2022, decisione n. 180/2022).

Peraltro, nel caso di specie, ciascuna operazione è stata seguita da un SMS alert tramesso al numero di cellulare della ricorrente. La circostanza non è controversa.

7.- In ogni caso, occorre rilevare che nella denuncia alle forze dell'ordine, come nel ricorso, la parte ricorrente non ha ricostruito le modalità della truffa, limitandosi ad affermare di essere venuta a conoscenza il 05/10/2024 dell'effettuazione, tra il 04/10/2024 e il 05/10/2024, di n. 6 bonifici istantanei non autorizzati a valere sul suo conto corrente, per l'importo complessivo di 2.580,00 €.

In caso di laconica ricostruzione del fatto, questo Collegio ritiene verosimile che la frode sia riconducibile ad un caso di "phishing" classico, caratterizzato dalla colpa grave dell'utente (Collegio di Roma, decisione n. 471/2020).

Invero, ferma restando l'allocazione dell'onere della prova a carico dell'intermediario, questo Collegio ritiene che sussista in capo al ricorrente un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare (Coll. Roma, dec. n. 10723/19).

8.- Per cui il Collegio osserva che, ai sensi dell'art. 10 del D. Lgs. 27 gennaio 2010, n. 11, come in vigore dal 13 gennaio 2018, grava sul prestatore di servizi l'onere di dimostrare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Nel caso di specie, l'intermediario ha prodotto evidenza della corretta autorizzazione delle operazioni contestate con rispetto degli standard di sicurezza (SCA) indicati dalla PSD2.

Come già ritenuto in diverse occasioni da questo Collegio, il ricorso ad un sistema di autenticazione a doppio fattore, in assenza di malfunzionamento del sistema, consente di ritenere che l'intermediario abbia assolto all'onere della prova che la legge gli impone in caso di disconoscimento di una operazione di pagamento.

Infatti, a fronte di una allegazione generica di disconoscimento delle operazioni della parte ricorrente, l'intermediario ha documentato che l'operazione contestata è stata correttamente autenticata, registrata e contabilizzata. A ciò si aggiunga che nonostante la ricezione degli SMS alert il ricorrente non si è attivato tempestivamente per il blocco della carta.

Non si ravvisano, d'altro canto, elementi idonei ad imputare una qualche responsabilità in capo all'intermediario resistente.

9.- Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA