COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 28/06/2023

FATTO

La parte ricorrente espone quanto segue:
- è titolare e cointestataria del conto corrente n. 22***, che può essere gestito anche da app, essendo attivo il servizio di internet banking;
- in data 7/12/2022, alle ore 10,17, riceveva sul proprio numero di cellulare 349*** un sms dal circuito dell'intermediario emittente, il cui sistema è posto a protezione della carta prepagata collegata al conto anzidetto, con cui si chiedeva di cliccare sul link allegato per aggiornare la carta/conto;
- tratta in inganno dalla provenienza del messaggio e dal relativo contenuto, procedeva come indicato;
- immediatamente dopo, veniva contattata da un sedicente impiegato del "Dipartimento di aggiornamento", il quale le chiedeva di accedere al proprio conto e verificare se l'applicazione fosse funzionante; terminata la telefonata, eseguiva la verifica richiesta con esito positivo;
- Lo stesso sms veniva rinotificato anche alle ore 11.29, ma non veniva visualizzato;
- Alle ore 15,22, la banca inviava un sms con cui si avvisava dell'esecuzione di un bonifico di euro 2.224,00;
- Allarmata, chiamava il numero verde dell'istituto e l'operatrice segnalava che in realtà erano stati disposti due bonifici ordinari, ma che potevano essere bloccati nel caso in cui la cliente non li avesse autorizzati;

- intorno alle 17,00 il vicedirettore della filiale di riferimento contattava la cliente per avvisarla che era stato eseguito un terzo bonifico istantaneo di 4.200,00;
- a dire dello stesso direttore lo stesso bonifico non poteva essere revocato, nonostante nella Lista movimenti vi fosse espressa l'annotazione che si trattava di "operazioni non definitive, stornabili";
- Lo stesso giorno, sporgeva formale querela nei confronti di ignoti.

La ricorrente eccepisce inoltre:

- di essere caduta vittima di un'azione fraudolenta riconducibile alla pratica del c.d. phishing, nella forma del c.d. spoofing, essendo ignoti riusciti ad indurla in errore tramite l'invio di un link apparentemente riconducibile alla resistente, ovvero al referente per la sicurezza del proprio circuito, così consentendo che fossero elusi i sistemi di sicurezza informatici dell'Istituto medesimo;
- l'anomala gestione dell'operatività fraudolenta da parte dell'intermediario, in quanto dopo la revoca di ben due bonifici e il blocco del conto veniva disposto un ulteriore bonifico di euro 4.200,00;
- la mancata adozione da parte della resistente di tutte le misure idonee a garantire la sicurezza del servizio, che espone la clientela al rischio di subire operazioni come quella di cui è stata vittima, posto che non ha rivelato ad alcuno le proprie credenziali.

L'intermediario contesta che sia stata la stessa ricorrente a dichiarare, in sede di denuncia-querela, di aver fornito tutte le proprie credenziali cliccando sul link allegato all'SMS ricevuto.

Ricostruisce come segue i fatti per cui è ricorso:

- In data 7 dicembre 2022, alle ore 10.13, è stato eseguito il login all'Internet Banking della ricorrente, tramite Desktop. Precisa che per accedere all'Internet Banking tramite Desktop è necessario inserire (i) il codice utente e la password personale e (ii) il PIN personale impostato dal cliente. Tale accesso è stato eseguito (presumibilmente) dalla stessa ricorrente;
- alle ore 10.28.00 è stata attivata una nuova "licenza smartphone" presumibilmente dal terzo truffatore (sul proprio dispositivo mobile), il quale per attivare la predetta licenza (e quindi l'APP) ha dovuto necessariamente inserire correttamente "Utenza + Password + OTP ricevuto via SMS sul cellulare certificato dal cliente. Da ciò ne consegue indefettibilmente che la ricorrente ha espressamente comunicato al terzo frodatore l'OTP di installazione dell'App;
- alle ore 10.28.51 i sistemi della Banca hanno registrato un secondo accesso all'Internet Banking della Cliente tramite APP; ritiene che questo secondo accesso sia stato eseguito (presumibilmente) dal frodatore;
- alle ore 13.23 della medesima giornata è stato autorizzato un bonifico di importo pari a Euro 4.200,00; per l'autorizzazione dell'operazione di pagamento è stato necessario inserire il codice utente e la password personale e il PIN personale impostato dal cliente;
- veniva contestualmente indirizzato via mail un alert relativo all'operazione effettuata;
- successivamente, alle ore 13.30 e alle ore 15.21 sono state inserite ed autorizzate due operazioni di bonifico SEPA, rispettivamente di importo pari ad Euro 3.540,00 ed Euro 2.254,00 le quali, come indicato anche in sede di denuncia da parte della Cliente sono state dalla stessa revocate;
- sostiene che la truffa sia stata perpetrata grazie alla collaborazione della cliente, posto che per l'installazione dell'APP è necessario inserire codice utente, password e OTP che solo la cliente poteva conoscere;
- ritiene infondate le contestazioni avversarie, considerato che il bonifico oggetto del presente ricorso è stato disposto prima della revoca dei due bonifici ordinari di importo

3.540,00 ed Euro 2.254,00 ed evidenzia le contraddizioni tra quanto dichiarato dalla ricorrente in sede di prima denuncia ed in sede di integrazione e di reclamo;
- difatti, in sede di prima denuncia all'Autorità Giudiziaria, la cliente ha ammesso di aver fornito le proprie credenziali, salvo poi ritrattare nell'integrazione successiva ed in sede di reclamo;
- ritiene pertanto integrata la colpa grave della ricorrente, considerato che ha cliccato su di un link truffaldino ignorando gli errori grammaticali presenti nel messaggio "esca" ed ha fornito le proprie credenziali;
- rappresenta di aver inviato apposita informativa alla cliente circa i rischi insiti nelle frodi online;
- eccepisce l'inammissibilità e l'infondatezza della domanda avente ad oggetto le spese legali, che non sono state oggetto di reclamo e cita sul punto giurisprudenza ABF.

Con le repliche la ricorrente, richiamate in gran parte le argomentazioni difensive svolte in sede di ricorso, contesta l'avversa ricostruzione dei fatti di causa, eccependo di aver ricevuto soltanto quattro mail da parte dell'intermediario che la informavano dei bonifici ordinari in esecuzione, poi revocati dalla stessa cliente.
In secondo luogo, riferisce che quanto dichiarato nella prima denuncia in ordine alla circostanza di aver fornito "tutte le credenziali" sarebbe frutto della "vulnerabilità psicologica" in cui versava immediatamente dopo la truffa, mentre deve ritenersi che con "credenziali" abbia inteso riferirsi a nome, cognome e codice utente, usualmente richiesti dalle banche.
Contesta l'efficacia probatoria dei LOG informatici prodotti ex adverso, sostenendo che gli stessi non sono idonei a provare l'assolvimento degli obblighi gravanti sull'intermediario.
Nelle controrepliche l'intermediario ribadisce che la truffa si è realizzata solo grazie alla collaborazione della cliente, colpevole di aver comunicato a terzi le proprie credenziali, consentendo così l'installazione dell'app sul device del frodatore.
D'altra parte, ribadisce che nel link inviato tramite sms "esca" vi sono evidenti errori grammaticali.
Ritiene pertanto integrata la colpa grave della ricorrente, anche in ragione del sistema di autenticazione utilizzato nel caso di specie, conforme alla disciplina in materia.
Ribadisce l'eccezione di inammissibilità della domanda di condanna alla refusione delle spese legali.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 7 dicembre 2022. Risulta pertanto effettuata 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 tale operazione è altresì successiva 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)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- Il ricorso ha ad oggetto un'operazione di bonifico BIR online per l'importo di € 4.200,00, effettuata alle ore 13.23 del 7.12.2022.

A tale operazione sono seguiti ulteriori due bonifici, parimenti disconosciuti, dei quali la ricorrente ha disposto la revoca con successo: in particolare alle ore 13:30 è stato disposto bonifico Sepa (ordinario) di euro 3.450,00 ed alle ore 15:21 bonifico Sepa (ordinario) di euro 2.224,00.

La ricorrente si duole della mancata ottemperanza all'ordine di revoca del bonifico di € 4.200,00, primo ad essere stato disposto in ordine temporale e che, a dire della banca, sarebbe stato irrevocabile.

Sul punto, l'intermediario precisa che il bonifico "BIR" di euro 4.200,00 è stato autorizzato (dal terzo frodatore) alle ore 13:23, ossia prima della revoca dei due bonifici ordinari SEPA - avvenuta rispettivamente, alle ore 15:38 per il bonifico di euro 2.224,00 e alle ore 15:39 per quello di euro 3.540,00 - e comunque prima del blocco dell'utenza, disposto alle ore 15:51, come si evince dalle notifiche di conferma inviate all'indirizzo mail della cliente.

L'intermediario non si sofferma invece sui tempi di processamento ai fini di una possibile revocabilità della tipologia di bonifici in questione, né riferisce alcunché su un eventuale tentativo di recall non andato a buon fine. Invero, trattandosi di un bonifico di importo rilevante (BIR), dovrebbero essere previsti tempi più rapidi, rispetto al bonifico ordinario, per l'accredito definitivo sul conto corrente del beneficiario.

Dal ricorso emerge che la parte ricorrente è rimasta vittima di una truffa riconducibile al fenomeno dello *spoofing* seguito da *vishing*.

La ricorrente produce lo screenshot che contiene il messaggio ricevuto da cui è partita la frode. Da tali evidenze si evince che: il messaggio si è inserito in una chat intestata all'intermediario terzo emittente della carta prepagata associata al proprio conto corrente; non contiene significativi errori grammaticali; il link contiene la denominazione dell'emittente la carta di pagamento.

Dichiara di aver poi ricevuto una telefonata da un sedicente operatore della resistente, che la invitava a verificare il corretto funzionamento dell'App.

Dalla denuncia querela sporta lo stesso giorno della truffa, si evince che la cliente ha cliccato sul link ed ha fornito tutte le credenziali al frodatore.

5.- Con riguardo all'autenticazione l'intermediario ricostruisce l'operatività fraudolenta verificatasi in data 7.12.2022 come segue:

- alle ore 10:13 è stato eseguito un accesso, presumibilmente dalla cliente, al proprio intermet baning tramite Desktop; a tal fine è stato necessario inserire: i) il codice utente e la password e ii) il PIN personale impostato dalla cliente;
- successivamente, alle ore 10:28 è stata attivata una nuova "licenza smartotp", presumibilmente dal terzo frodatore sul proprio dispositivo mobile; il frodatore, per attivare la nuova licenza smartotp, ha dovuto inserire "Utenza + Password + OTP ricevuto via SMS sul cellulare certificato dalla cliente.
- Immediatamente dopo i frodatori hanno fatto accesso all'Internet banking della cliente tramite l'App Dmobile installata sul proprio cellulare, inserendo il codice utente/password e il Pin personale impostato dalla cliente.
- In orari successivi, dalle ore 13:23 alle ore 15:21, il frodatore ha potuto disporre e autorizzare le operazioni oggetto di contestazione.

Da tali elementi fattuali l'intermediario deduce che la cliente abbia comunicato al terzo frodatore sia l'OTP necessario all'installazione dell'App Dmobile sia le credenziali personali (ossia, codice utente, password e PIN) necessarie per completare l'accesso all'Internet banking.

Con riguardo al processo di *enrollment* l'intermediario riporta nella legenda il sistema di autenticazione utilizzato (utenza+password+OTP ricevuto via sms), specificando che in data 7.12.2023 è stato attivato un nuovo device dallo stesso IP utilizzato per effettuare l'accesso e disporre la transazione.

Si rileva, tuttavia, che dai log prodotti non si evince l'inserimento dei menzionati fattori di autenticazione né vi è evidenza dell'invio dell'OTP sul dispositivo certificato della cliente.

Pertanto, ad avviso del Collegio l'intermediario non ha adeguatamente dimostrato, tramite la documentazione fornita, la corretta autenticazione e la formale regolarità dell'operatività contestata.

6.- Ciò posto, deve altresì precisarsi che l'art. 10, comma 1, del D. Lgs. n. 11/2010, nel caso di disconoscimento di un'operazione da parte dell'utilizzatore, stabilisce che "è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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".

Secondo l'orientamento dei Collegi, solo a seguito dell'assolvimento di tale onere probatorio assume rilievo la valutazione della sussistenza della colpa grave in capo all'utilizzatore prevista dall'art. 12, comma 3 del D. Lgs. n. 11/2010, con conseguente spostamento della responsabilità in capo a quest'ultimo. Nel caso in esame, l'intermediario resistente non allega la prova dell'autenticazione, registrazione e contabilizzazione dell'operazione, con la conseguenza che non rileva l'eventuale comportamento gravemente colposo del cliente e la richiesta di accertamento del disconoscimento dell'operazione deve essere accolta, con conseguente obbligo di rimborso da parte dell'intermediario dell'importo ad essa relativo, senza applicazione della franchigia prevista dalla legge (Coll. Roma, dec. n. 26738/2019; Coll. Milano, dec. n. 6339/2016 e 682/2016; più recentemente dec. n. 6057/2023 e n. 6060/2023).

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 4.200,00. Respinge nel resto.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA