COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PROTO	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 12/07/2022

FATTO

La parte ricorrente espone quanto segue:
- in data 02.09.2021 il ricorrente riceveva un SMS apparentemente proveniente dalla banca resistente, che gli chiedeva di seguire un link per evitare il blocco della propria utenza;
- precisa che proprio in quei giorni era in atto l'aggiornamento della piattaforma digitale della banca;
- di lì a poco il ricorrente riceveva una telefonata da cellulare, da parte di una persona che si qualificava come funzionario dell'intermediario e gli chiedeva di controllare l'accesso al portale, dato che era in corso l'aggiornamento alla nuova piattaforma di internet banking;
- il ricorrente effettuava l'operazione senza comunicare all'interlocutore i codici di accesso, e terminava la telefonata senza avere dubbi a riguardo;
- in data 08.09.2021, alle ore 18:00, il ricorrente veniva poi contattato dalla banca, che gli comunicava l'addebito di un bonifico anomalo di € 7.950,00;
- il ricorrente disconosceva l'operazione e provvedeva a bloccare immediatamente il conto;
- fa presente che il link ricevuto aveva il prefisso "https://", riportava il nome dell'intermediario e rimandava a una pagina corrispondente a quella della nuova piattaforma appena aggiornata della banca;
- chiede il rimborso dell'importo di € 7.950,00.

L'intermediario resiste al ricorso ed eccepisce quanto segue:

- dai log relativi all'operazione risulta che essa sia stata correttamente autorizzata, e afferma che la frode si è potuta perpetrare in quanto il ricorrente stesso ha fornito ai frodatori le proprie credenziali statiche e dinamiche, che hanno permesso loro di installare l'app della banca sul proprio device e di disporre successivamente il bonifico disconosciuto;
- in particolare, alle 14:54:42 del giorno 02.09.2021 (tre minuti dopo la ricezione dell'SMS civetta) si registrava l'installazione dell'app della banca su un nuovo device, autorizzata mediante inserimento di un codice di attivazione inviato sul cellulare certificato del cliente e di un O-Key SMS per completare l'operazione;
- dopo alcuni giorni, l'8.09.2021, il truffatore accedeva all'home banking del cliente ed effettuava il bonifico disconosciuto;
- la banca fa presente che per accedere all'Home banking è necessario inserire tutti i seguenti codici:
    - il Codice Titolare, codice statico che identifica ogni cliente, unico codice ad essere conosciuto dalla Banca, indicato dalla banca con apposita comunicazione inviata al cliente in busta chiusa all'indirizzo di contratto;
    - il Codice PIN, codice statico creato dal cliente al primo accesso e solo da questi conosciuto;
    - il Codice O-Key, codice temporaneo monouso, trasmesso al cliente da un sistema automatizzato. Tale codice viene generato dall'app O-Key Smart e quindi definito anche come codice OTP.
- in caso di mancata attivazione dell'O-Key Smart, il codice O-Key è ricevuto dal cliente via SMS sul numero di cellulare certificato (e in questo caso esso viene definito oltre che OTP anche come codice O-Key SMS o OTS); in talune specifiche circostanze (ad esempio in caso di caduta di linea o difficoltà d ricezione dell'OTP) anche in presenza della app O-Key Smart il codice O-Key può essere inviato in forma di OTS via SMS sul numero di cellulare certificato;
- in ogni caso il codice O-Key (sia esso OTP o OTS) consiste in un numero di 6 cifre, avente una validità operativa di pochi secondi ed utilizzabile una sola volta, ed è sempre necessario per disporre istruzioni alla Banca di qualsiasi natura (impartire un addebito in conto per bonifici, pagamento utenze, acquisto titoli, o anche la variazione delle informazioni di contatto quali la e-mail o il numero di cellulare certificato ai sensi della normativa PSD2);
- inoltre, quale ulteriore garanzia per la clientela, laddove una singola operazione abbia caratteristiche tali da essere identificata quale "sospetta" dal motore antifrode della banca, per completare l'autenticazione viene richiesto l'inserimento, oltre che del codice O-Key, anche di un ulteriore codice inviato sempre sull'utenza telefonica certificata (e quindi denominato sempre OTS) ovvero, in alternativa, l'inserimento delle corrette risposte - preimpostate dal cliente- alle domande di sicurezza che gli vengono poste.

L'intermediario conclude quindi chiedendo il rigetto del ricorso, o in subordine il riconoscimento di un concorso di colpa tra le parti.

Con le repliche il ricorrente sostiene che il link ricevuto fosse altamente ingannevole, e ritiene che il bonifico avrebbe dovuto essere tempestivamente bloccato dalla banca; precisa di non avere comunicato a terzi le proprie credenziali, ed insiste per l'accoglimento del ricorso.

Nelle controrepliche l'intermediario ribadisce che l'*enrollment* del nuovo device è avvenuto in data 02.09.2021 alle ore 14:54:42, ed è stato correttamente autorizzato mediante inserimento di un codice di attivazione e di un O-Key SMS inviati sul numero di cellulare del cliente;

- successivamente, è stato eseguito l'accesso all'home banking attraverso un nuovo dispositivo, completato attraverso le credenziali statiche del cliente e la conferma di una push sul device, e anche l'operazione di bonifico di € 7.950,00 è stata autorizzata mediante push;
- afferma che la vicenda fraudolenta non si configura come una truffa particolarmente sofisticata, ma fa emergere la colpa grave del ricorrente come già evidenziato in sede di controdeduzioni;
- insiste quindi per il rigetto del ricorso.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 7 maggio 2021. 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)*".
4.- Nel caso di specie, il ricorrente precisa che, alle ore 14:51 del 02.09.2021, riceveva un SMS apparentemente proveniente dalla banca convenuta, che si inseriva in una preesistente conversazione contenente messaggi legittimi.
Afferma di avere seguito il link, ingannato dalla presenza del prefisso "https://" e della denominazione della banca sul link.
Di lì a poco riceveva una telefonata da un numero di cellulare, da parte di un soggetto che si qualificava come funzionario della banca e gli chiedeva di "controllare l'accesso al portale dato che si stava aggiornando la nuova piattaforma di internet banking".
Il ricorrente effettuava le operazioni richieste e chiudeva la telefonata, senza nutrire sospetti.
Alcuni giorni dopo, e precisamente l'8.09.2021, veniva contattato telefonicamente dalla banca che lo informava dell'esecuzione di una operazione di bonifico di € 7.950,00, da lui non autorizzata.
Il ricorrente afferma di avere provveduto a bloccare il conto in data 08.09.2021, subito dopo essere stato informato dell'operazione disconosciuta.
L'operazione contestata consiste in un bonifico online di € 7.950,00 disposto in data 08.09.2021 alle ore 17:12.
L'intermediario produce i log relativi all'operazione, precisando quanto segue:
• alle ore 14:54 del 02.09.2021 veniva eseguito l'enrollment di un nuovo dispositivo, autorizzato con inserimento delle credenziali statiche di accesso al conto e di due codici OTS tramessi via SMS sul numero di cellulare del ricorrente:
• alle ore 17:03 dell'8.09.2021 veniva effettuato l'accesso all'home banking dal nuovo dispositivo, mediante inserimento delle credenziali statiche di accesso al conto e dell'OTP generato da app a seguito di tap su notifica push:
• alle 17:12 veniva disposto il bonifico disconosciuto, autorizzato mediante OTP generato da app a seguito di tap su notifica push.
5.- Secondo la più recente posizione condivisa da tutti i Collegi territoriali, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, "a meno che non si rinvengano […] indici di inattendibilità o anomalia del messaggio; in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di *phishing* e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario".

Nel caso in esame, la parte ricorrente produce copia del messaggio truffaldino, dalla quale si evince che: 1. il linguaggio sembra caratterizzato da un tono formale e non contiene errori grammaticali; 2. il link contenuto si riferisce all'intermediario e si inserisce una schermata che reca il riferimento all'acronimo del gruppo bancario di cui è parte l'intermediario; 3. il messaggio risulta essersi inserito nello storico delle conversazioni genuine precedentemente intercorse con l'intermediario.

6.- Pertanto, alla luce delle risultanze istruttorie, il Collegio ritiene che non sussistano profili di colpa grave del cliente.

Infatti, il truffatore ha adottato un sistema tecnicamente sofisticato, tale da concretare un'ipotesi di malfunzionamento del servizio di pagamento o altro inconveniente connesso al servizio di disposizione di ordine di pagamento, pur inteso in senso ampio, destinato a ricadere nella sfera del rischio di impresa dell'intermediario. Non è dubbio, infatti, che le operazioni siano un effetto di tale malfunzionamento.

8.- Alla luce di quanto sopra esposto il Collegio la domanda proposta con il ricorso è fondata. Peraltro, alla luce della eccezione proposta dall'intermediario che in via subordinata chiede di riconoscersi il concorso di colpa, tenuto conto delle previsioni richiamate del d.lgs. n. 11 del 2010, si deve ritenere che la responsabilità per l'operazione di pagamento oggetto di contestazione gravi sull'intermediario e che parte ricorrente abbia diritto ad ottenere il rimborso dell'importo complessivo ad esse corrispondente, al netto della franchigia di cui all'art. 12, comma 3, d.lgs. 11/2010.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 7.900,00.

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