COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore - FRANCESCA VESSIA

Seduta del 27/07/2023

FATTO

La ricorrente, titolare di un conto corrente acceso presso l'intermediario, riferisce di aver ricevuto in data 26/05/2022, alle ore 15:24 circa, un sms proveniente dall'intermediario, con cui veniva invitata a cliccare su un link per evitare la sospensione del proprio conto corrente. Evidenzia che il messaggio in questione non è estato identificato come spam dal relativo servizio di monitoraggio delle comunicazioni moleste, attivo sul proprio device telefonico.
Allarmata dal tenore della comunicazione, parte ricorrente effettuava una ricerca su internet per reperire informazioni sulla portata della comunicazione e verificare se altri clienti dello stesso intermediario avessero riscontrato lo stesso disservizio. Avendo reperito numerosi articoli che riportavano la veridicità della notizia, la cliente dava corso alle indicazioni contenute nel sms, aprendo il collegamento convinta della serietà dell'avviso ricevuto.
Afferma di essere stata indirizzata su una pagina web identica al sito dell'intermediario convenuto, di aver inserito il proprio indirizzo mail e codice PIN, senza inserire il terzo elemento di sicurezza, ossia il codice token stampigliato su una carta fisica fornita dall'intermediario.
Riceveva una telefonata da un presunto operatore dell'intermediario che effettuava alcuni controlli sul suo conto corrente; durante la chiamata, la ricorrente non ha comunicato alcun dato associato o riferibile al rapporto bancario in questione nella propria disponibilità, necessario per l'autorizzazione al compimento delle operazioni. Nell'arco di pochi minuti la

telefonata si interrompeva bruscamente; in quel momento, la ricorrente veniva a conoscenza dell'effettuazione di un bonifico dal proprio conto corrente in favore di un terzo sconosciuto, per l'importo di € 29.450,00, dalla stessa mai autorizzato, superiore al tetto massimo di spesa preimpostato.
Allarmata da quanto appena accaduto, parte ricorrente provava immediatamente a contattare il servizio clienti dell'istituto di credito per parlare con un operatore ma si accorgeva dell'indisponibilità di tale opzione; utilizzava quindi la chat collegata all'app dell'intermediario, dove spiegava quanto verificatosi poco prima, disconosceva la disposizione del bonifico e ne chiedeva l'imminente revoca, riuscendo ad ottenere unicamente il cambio delle impostazioni della carta ed il suo blocco.
Il giorno successivo, in data 27/05/2022, l'intermediario inoltrava alla correntista conferma del bonifico per l'importo di € 29.450,00, in favore del beneficiario sconosciuto, su un IBAN incardinato presso l'istituto di credito convenuto.
Evidenzia che nel documento ricevuto, era indicato che si trattasse di una "semplice conferma della richiesta di bonifico" e non di una "prova dell'avvenuta esecuzione della transazione" e che l'intermediario avrebbe eseguito il bonifico all'esito del processo di verifica obbligatorio.
Riferisce inoltre: di aver reiterato nella stessa giornata l'istanza di annullamento dell'operazione disconosciuta e contestata; di aver presentato denuncia con richiesta di sequestro urgente della somma sottratta e di aver presentato reclamo verso l'intermediario, riscontrato negativamente; che, all'esito delle indagini espletate dalle autorità competenti, è emerso che il terzo beneficiario è stato, a sua volta, inconsapevole vittima di truffa, per aver ricevuto l'accredito dell'importo sottratto alla ricorrente sul proprio conto corrente, da cui sono stati poi eseguiti 9 pagamenti da lui mai disposti.
Riguardo alle operazioni contestate, compiute fra il 26 e il 27/05/2022, richiama la normativa di settore, lamentando di essere stata vittima di smishing e di vishing, perpetrati attraverso il metodo dello spoofing.
Soggiunge che il tenore dell'sms e le notizie sulla chiusura dei conti correnti presso l'intermediario, insieme alla riferibilità del link all'intermediario, hanno indotto la ricorrente in errore sul carattere ingannevole della comunicazione.
Evidenzia la debolezza dei sistemi di difesa dell'intermediario, il quale non avrebbe neppure intercettato l'evidente anomalia delle plurime disposizioni intervenute subito dopo la truffa in questione verso nuovi beneficiari, dal conto corrente del primo beneficiario, definito dormiente dal suo titolare.
Ritiene che le circostanze descritte fossero da sole idonee a rappresentare l'anomalia dei pagamenti e avrebbero dovuto essere rilevate da un sistema di vigilanza interno o dall'eventuale algoritmo preimpostato di un efficiente sistema di sicurezza dei pagamenti tramite home banking.
La carenza funzionale del sistema interno dell'intermediario sulla verifica delle operazioni di conto corrente assume rilievo decisivo e determinante sotto il profilo causale, rendendo irrilevante ogni altra condotta eventualmente imputabile al fruitore del servizio.
La ricorrente chiede, pertanto:
1) DISPORRE che l'Intermediario (…), in persona del legale rappresentante pro tempore, corrisponda in favore della Ricorrente (…) la somma di €. 29.450,00 (Euro ventinovemila quattrocentocinquanta/00), oltre interessi legali dalla data dell'occorso (26/05/2022) e fino al soddisfo;
2) DISPORRE – altresì – che l'Intermediario (…), in persona del legale rappresentante pro tempore, corrisponda in favore della Ricorrente (…) l'ulteriore somma di €. 20,00 a titolo di rimborso per la presentazione del Ricorso.

Costituitosi, l'intermediario fa preliminarmente presente che la ricorrente non ha descritto le modalità della frode subita nemmeno in sede di denuncia alle autorità, descrivendola sommariamente durante le proprie interlocuzioni col Servizio Clienti dell'intermediario, e limitandosi comunque ad affermare di non aver autorizzato l'operazione oggetto di disconoscimento, della quale si sarebbe avveduta in data 26 maggio 2022, alle ore 16.30 circa, a frode conclusa.
Precisa che la ricorrente, nel corso di una live-chat intercorsa alle ore 16:32 del 26 maggio 2022, dichiarava a un operatore del Servizio Clienti dell'intermediario di avere cliccato sul link di reindirizzamento collegato al suddetto messaggio truffaldino, inserendovi le proprie credenziali di accesso all'home-banking (e-mail e password) oltre al proprio PIN dispositivo e il codice token della propria carta di debito. Al riguardo, i log informatici in possesso dell'intermediario dimostrano che parte ricorrente ha comunicato al frodatore le proprie credenziali di accesso al conto corrente e la stessa ha provveduto autonomamente ad autorizzare l'operazione di bonifico contestata.
In particolare, poco prima che l'operazione di bonifico disconosciuta venisse eseguita, il frodatore effettuava l'accesso al conto della ricorrente da un dispositivo mobile con device token (*e63) utilizzando i dati di login - e-mail e password - normalmente in uso e precedentemente impostati dalla stessa ricorrente e a seguito della conferma da parte di quest'ultima di un codice OTP/notifica push inviatale al suo dispositivo mobile con device token (*24) associato al conto della medesima.
Rammenta che la ricorrente era stata tempestivamente e regolarmente resa edotta circa gli accessi anomali eseguiti da soggetti terzi al proprio conto corrente per mezzo di n. 2 e-mail inviate all'indirizzo di posta elettronica collegato al proprio conto in data 26 maggio 2022 alle ore 15:28, orario coincidente col verificarsi della frode in analisi.
In merito, rileva altresì che, allorquando un cliente esegue l'accesso al conto da un dispositivo non associato, gli viene chiesto di confermare una notifica push sul proprio dispositivo associato o, in alternativa, può richiedere la ricezione di un codice via SMS sul numero di telefono registrato al proprio conto corrente per confermare l'accesso al medesimo. Questa procedura di autenticazione a due fattori garantisce che soltanto il titolare del conto possa accedervi.
Deduce pertanto che la ricorrente ha consentito al malfattore di accedere al proprio conto, comunicandogli le proprie credenziali di accesso al conto e il codice OTP ricevuto sulla propria utenza telefonica, permettendo altresì al malfattore di attuare tutte le ulteriori azioni necessarie a finalizzare la frode; inoltre la ricorrente era stata debitamente informata degli accessi anomali effettuati dal frodatore tramite le n. 2 email già menzionate ed aveva ricevuto le relative notifiche push per confermare l'accesso dal dispositivo non associato del frodatore.
L'operazione di bonifico è stata predisposta e autorizzata in autonomia dalla ricorrente, che ha inserito il c.d. PIN di conferma, un codice a quattro cifre creato personalmente dai clienti in fase di prima associazione del device personale al proprio conto corrente e, pertanto, non è un codice originato dall'intermediario.
Difatti, le tracciature in possesso dell'intermediario dimostrano che l'ordine di bonifico in analisi è stato autorizzato dallo smartphone con device token (*024) riferibile alla ricorrente, con inserimento del PIN di conferma, da questa creato e modificato in date ben antecedenti alla frode.
Segnatamente, evidenzia che il bonifico in esame è stato predisposto dal frodatore da un cellulare con device token (*e63) e, infine, autorizzato con lo smartphone con device token (*024) riferibile alla ricorrente. La voce "certified" presente nei log comprova che l'operazione di bonifico in disputa è stata autorizzata a seguito di corretta identificazione dell'utente con le proprie credenziali di accesso all'app, tramite una procedura di Strong Customer

Authentication, basata sull'uso congiunto di fattori di diversa natura (inserimento del PIN e notifica push da device associato), tra loro indipendenti.
Fa presente che da tempo l'intermediario ha intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela in merito al generale fenomeno del phishing e alle sue possibili declinazioni.
L'intermediario ribadisce che la ricorrente ha sempre mantenuto il pieno ed esclusivo controllo dell'App installata sul proprio dispositivo mobile personale associato al conto corrente. Precisa che la ricorrente non ha mai denunciato lo smarrimento o il furto del proprio device; ritiene di particolare rilievo la circostanza che, in data 26 maggio 2022, la data di ultima associazione del device personale della ricorrente al proprio conto corrente risaliva al giorno 1 marzo 2022 alle ore 19:57, data di molto antecedente al giorno in cui la frode in questione si consumava. Ciò dimostra che l'operazione di bonifico in questa sede contestata non poteva che verificarsi esclusivamente previo accesso al conto da parte della ricorrente tramite la propria App. A ulteriore riprova del contegno colpevole tenuto dalla ricorrente, sottolinea che ai fini della conclusione della frode si è resa assolutamente necessaria la collaborazione da parte della stessa: in particolare, prima delle ore 13:28 del 26 maggio 2022, in nessun momento il frodatore ha avuto completo accesso al conto corrente in parola; egli ha dovuto contattare telefonicamente la ricorrente e persuaderla a porre in essere tutte le azioni necessarie per portare a compimento la frode in analisi; non si è verificato pertanto alcun "data breach" dei dati relativi alla ricorrente.
Sostiene che la procedura di accesso al proprio conto corrente da parte del singolo cliente si basa sull'uso di due o più elementi di sicurezza consistenti nell'inserimento delle credenziali personali, costituite dal proprio indirizzo e-mail registrato e dalla password personale, e nell'utilizzo dell'applicazione mobile installata sul dispositivo associato in via esclusiva al titolare del conto, oppure richiedendo in aggiunta un codice SMS inviato esclusivamente all'utenza telefonica presente in anagrafica.
In relazione all'sms civetta ricevuto dalla ricorrente, rileva che nel relativo screenshot non compare il numero telefonico dell'intermediario, bensì solo la denominazione.
Con riferimento all'inattendibilità del messaggio, evidenzia che risulta formulato in tono elementare e generico; inoltre, il link presente nel messaggio truffaldino non è palesemente riconducibile all'intermediario né il messaggio SMS si colloca in coda a messaggi genuini; il messaggio truffaldino non appare sintatticamente coerente, in quanto risulta formulato in terza persona singolare. Inoltre, l'SMS contiene gravi errori di sintassi e di grammatica (illogica alternanza della seconda e della terza persona singolare, assenza di punteggiatura, la preposizione "Su" con l'apostrofo e un incoerente uso delle lettere maiuscole).
Ritiene pertanto pacifico che nel contesto sopra descritto - anche in ragione delle n. 2 e-mail di alert inviate dall'intermediario il giorno 26 maggio 2022 alle ore 13:28 che la informavano in merito agli accessi anomali effettuati dal frodatore al proprio conto – la ricorrente avrebbe dovuto contattare immediatamente la banca al fine di sincerarsi in merito all'attività anomala rilevata sul proprio conto, provvedendo prontamente a bloccare l'operatività del conto corrente tramite la linea telefonica di emergenza dedicata.
Afferma che la ricorrente sarebbe stata vittima di una tipologia di truffa denominata social hacking, basata sull'impartire telefonicamente istruzioni manipolative al titolare dello strumento di pagamento, lasciando che sia lo stesso titolare ad autenticare le singole transazioni. Desume che, nel caso di specie, l'operazione è stata autorizzata dalla ricorrente, nel contesto delle operazioni autorizzate dall'utilizzatore.
Osserva che tali ipotesi esulano dal regime di protezione previsto dal menzionato d.lgs. 11/2010 in caso di operazioni non autorizzate, posto che non difetta il requisito del consenso dell'utilizzatore.

Ritiene di aver fornito prova della corretta autorizzazione dell'operazione di bonifico in esame, resa possibile dalla condotta incauta e dalla piena collaborazione della ricorrente che ha dato credito alle indicazioni del frodatore e chiede di respingere il ricorso.
Riferisce, infine che, pur essendosi immediatamente adoperata al fine di stornare l'operazione disconosciuta, il tentativo di recupero della somma non è andato a buon fine in virtù del fatto che la stessa aveva formato oggetto di ulteriori operazioni dispositive effettuate da parte del frodatore in stretta successione temporale.
In sede di repliche, la ricorrente eccepisce l'assenza di conformità agli originali dei documenti allegati alle controdeduzioni e la mancanza di corrispondenza tra il contenuto dei documenti e i fatti, ai sensi dell'art. 2719 e 2712 c.c.
Evidenzia di aver descritto in modo compiuto la vicenda, di aver presentato istanza di accesso agli atti dell'intermediario il 20/10/2022 e che questi avrebbe evaso la richiesta nel mese di aprile 2023, in pendenza della procedura ABF, a distanza di sei mesi dalla richiesta.
Rappresenta che parte resistente non ha fornito la prova della corretta implementazione di un sistema di autenticazione forte nella fase di accesso al conto corrente della ricorrente; inoltre, la legenda esplicativa a corollario dei log informatici, il cui contenuto disconosce e contesta, reca diverse incongruenze e, nello specifico, non consente di capire il significato delle espressioni "MFA_REQUIRED", "MFA_OTP", utilizzate.
Ribadisce di non aver comunicato a nessuno i propri codici PIN, OTP e OTS, contestando le allegazioni dell'intermediario, nella parte relativa alla prova dell'autenticazione forte e dell'invio delle notifiche push sul device della ricorrente; rileva la debolezza del sistema dell'intermediario, il quale non avrebbe intercettato i pagamenti disposti dal conto corrente del beneficiario della somma sottratta alla ricorrente.
Pertanto, la ricorrente insiste per l'accoglimento del ricorso.
In sede di controrepliche, l'intermediario eccepisce la genericità e l'inconferenza delle contestazioni della ricorrente riferite alle tracciature informatiche, riconosciute dalla giurisprudenza ABF.
Ribadisce che parte ricorrente ha rilasciato dichiarazioni reticenti spesso contraddittorie e non rispondenti alle risultanze informatiche acquisite.
Rammenta che la ricorrente è sempre rimasta in possesso del device associato al proprio conto corrente; evidenzia che dalle tracciature prodotte emerge la prova dell'invio dell'SMS contenente il codice OTP autorizzativo per l'accesso al conto, correttamente trasmesso allo smartphone associato al conto e verificato dalla ricorrente.
Ritiene quindi chiaro che l'accesso al conto da parte del frodatore è stato correttamente autenticato con inserimento di un fattore di conoscenza rappresentato dalla digitazione delle credenziali del cliente (email e password) e di un fattore di possesso quale secondo fattore di autenticazione (il codice OTP).
Ad avviso dell'intermediario, le suddette credenziali sarebbero state condivise dalla ricorrente poiché, con leggerezza, ella avrebbe prestato fede a comunicazioni con profili di anomalia e ha comunicato le credenziali di sicurezza necessarie per la predisposizione e l'esecuzione dell'operazione di pagamento non autorizzata. In merito, l'intermediario ritiene incontroverso che la ricorrente abbia consentito al truffatore di accedere all'area riservata del proprio home-banking, comunicando a un terzo le proprie credenziali di login e il codice OTP ricevuto sulla propria utenza telefonica, permettendo così al frodatore di portare a compimento il suo piano criminoso. L'intermediario rileva di aver informato la ricorrente circa l'accesso anomalo di un soggetto terzo al proprio conto corrente tramite due mail inviate all'indirizzo di posta elettronica collegato al conto in data 26 maggio 2022, alle ore 15:58, in coincidenza con il momento della frode. Produce i log delle modifiche effettuate dalla ricorrente ai propri dati personali associati al conto corrente, a riprova del fatto che tutte le comunicazioni trasmesse sono state correttamente ricevute dalla ricorrente alla propria

email riferibile al provider hotmail e alla propria utenza mobile registrata in anagrafica, dati che non hanno mai formato oggetto di variazione nel corso del lasso temporale coincidente con la frode. Sottolinea che l'indirizzo e-mail della ricorrente è stato modificato solo il giorno 26 maggio 2022 alle ore 16:55, successivamente al verificarsi della frode.
A riprova della ricezione da parte della ricorrente delle notifiche push sul proprio dispositivo mobile, rileva che questa non ha mai denunciato lo smarrimento o il furto del proprio device (*024); inoltre, la data di ultima associazione del device personale della ricorrente al proprio conto corrente, era di molto risalente, essendo avvenuta il 1 marzo 2022 alle ore 19:57.
Al riguardo, richiama l'orientamento ABF che assimila le notifiche push agli sms alert, ove vengano inviate all'utilizzatore come nella fattispecie in questione (ex multis, Coll. Milano, decisione n.13320/22; decisione n. 329 del 13 gennaio 2020 relativa a un caso analogo a quello in esame).
Rammenta che, una volta che l'operazione di bonifico contestata era stata autorizzata, la resistente era impossibilitata a provvedere al relativo blocco, poiché la richiesta di sospensione era stata avanzata da parte della ricorrente quando la transazione in questione risultava ormai irrevocabile ai sensi e per gli effetti dell'art. 17 del D.Lgs. n. 11/2010.
La resistente esclude che la frode subita dalla ricorrente sia riconducibile a una fattispecie particolarmente sofisticata; fa presente che la ricorrente ha tenuto una condotta incauta e gravemente negligente, consentendo al frodatore di accedere all'area riservata del conto corrente della medesima e di predisporre l'ordine di bonifico oggetto di contestazione che la stessa ricorrente, infine, ha provveduto ad autorizzare all'interno della App installata sul proprio device personale associato al conto corrente.
La resistente conferma la propria disponibilità a collaborare con le autorità competenti qualora interpellata riguardo ai fatti oggetto del presente ricorso, insistendo per il rigetto.

DIRITTO

Il ricorso ha ad oggetto una frode online, in cui il cliente è risultato vittima di una truffa perpetrata tramite SMS spoofing, phishing, smishing e vishing, e chiede all'intermediario la restituzione della somma illecitamente sottratta, pari a € 29.450,00, attraverso una operazione di bonifico online eseguita tramite intrusione sulla App del telefono della ricorrente, in data 26/05/2022 alle ore 15:24 circa, e successivamente disconosciuta dalla ricorrente.
L'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018.
Va detto che la ricorrente ha sempre negato di aver autorizzato l'operazione e affermato di non aver comunicato a nessuno i dati associati o riferibili al rapporto bancario in questione nella propria disponibilità, necessari per l'autorizzazione al compimento delle operazioni. Viene pertanto in rilievo, innanzitutto, l'art. 10, comma 1, D.lgs. n. 11/2010 (e successive modifiche), secondo cui il prestatore dei servizi di pagamento, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già eseguita, ha l'onere di provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione. Inoltre, ai sensi dell'art. 10-bis, comma 1, D.lgs. n. 11/2010, l'intermediario ha altresì l'onere di dimostrare che vi sia stata aderenza della procedura di pagamento utilizzata dall'intermediario resistente alla SCA (Strong Customer Authentication). In mancanza di

dette prove l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute, senza alcuna limitazione o franchigia.
In seconda battuta occorre verificare se l'intermediario abbia fornito la prova della colpa grave o del dolo in capo all'utilizzatore ricorrente, come prescritto dall'art. 10, comma 2, D.lgs. n. 11/2010, ed anche di questo l'intermediario deve fornire la prova.
Quanto al primo profilo, occorre dunque verificare se, nel caso di specie, l'intermediario abbia provato che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che l'operazione contestata sia stata attuata mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".
Avuto riguardo alla documentazione prodotta in atti dall'intermediario, quest'ultimo ha rappresentato, e prodotto evidenze, del fatto che: i) il frodatore effettuava l'accesso al conto della ricorrente da un dispositivo mobile con device token ****e63 utilizzando i dati di login - e-mail e password - normalmente in uso e precedentemente impostati dalla stessa ricorrente e a seguito della conferma da parte di quest'ultima di un codice OTP/notifica push inviatale al suo dispositivo (tanto risulta dalle schermate dei Logs informatici relativi agli SMS inviati dalla Banca alla ricorrente in data 26.5.2022 contenenti i codici OTP di verifica di conferma dell'identità per accedere al conto); ii) la cliente ha effettuato l'accesso al proprio conto nel corso della chiamata intercorsa con il frodatore "tra le ore 13:28 UTC+2 (ora locale 15:28) e le ore 14:09 UTC+2 (ora locale 16:09)" per mezzo del dispositivo mobile con device token ****024 (ulteriore allegazione dell'intermediario); iii) detti accessi sono avvenuti in conformità con l'autenticazione a due fattori, mediante inserimento delle credenziali di sicurezza (username e password - elemento di conoscenza) e del codice OTP inviato via SMS alla cliente alla propria utenza telefonica associata al conto (elemento di possesso) (tanto risulta dalle schermate dei Logs informatici comprovanti gli accessi effettuati dalla ricorrente in data 26.5.2022 riportanti la dicitura password, certified e transaction SCA approved).
Per quanto concerne il processo di associazione di un nuovo dispositivo al conto corrente della cliente, in sede di controrepliche, l'intermediario specifica che la voce "MFA_OTP" ivi riportata alla colonna "Process", indica che il secondo fattore di autenticazione applicato al caso di specie è costituito da un codice OTP.
Le evidenze sopra riportate sembrano confermare quanto sostenuto dall'intermediario, relativamente agli accessi al conto effettuati dal frodatore, l'inserimento di credenziali statiche (v. dicitura LOGIN WITH PASSWORD) e dinamiche (MFA_OTP).
L'intermediario allega, inoltre, logs informatici relativi all'operazione di bonifico per dimostrare che, alle ore 15:39 del 26/05/2022, il bonifico in esame è stato predisposto dal device del frodatore *e63 (cfr. voce Transfer creation authentication) e, infine, autorizzato con il device della ricorrente *024 (cfr. voce User ID e Unique Device Token).
Pertanto, dalla documentazione prodotta, si evince che l'operazione di bonifico è stata autorizzata mediante un sistema di autenticazione forte e grazie alla collaborazione della ricorrente che ha fornito ai frodatori fattori di diversa natura e tra loro indipendenti (inserimento del PIN e notifica push da device associato). L'intermediario ha, inoltre, prodotto in atti la schermata attestante che il PIN utilizzato per confermare le operazioni è quello creato dal ricorrente in data 20 settembre 2018 e modificato in data 11 novembre 2019, nonché fornito evidenza della notifica push autorizzativa inviata alla cliente e da questa confermata (logs relativi alle notifiche push inviate il giorno 26.05.2022 e associate al conto della ricorrente).
Il Collegio, all'esito di tali fonti documentali prodotte dall'intermediario, ritiene provato sia che l'operazione sia stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua

esecuzione, sia dimostrata l'applicazione alla procedura di pagamento della c.d. "autenticazione forte" o SCA.
Quanto, invece, al secondo profilo della colpa grave del cliente, si deve ricordare che il Collegio di coordinamento, con pronuncia n. 22745/2019, ha enunciato il seguente principio di diritto: "[…] la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l' "autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente".
A tale proposito, l'intermediario rileva che il link presente nel messaggio truffaldino è palesemente non riconducibile all'intermediario né il messaggio SMS si colloca in coda a messaggi autentici generati dalla resistente; e inoltre che il messaggio è caratterizzato da un tono elementare e non appare sintatticamente coerente, in quanto gli SMS generati dalla resistente sono sempre formulati alla seconda persona singolare mentre nell'SMS "civetta" inviato dal frodatore si ricorre alla terza persona singolare. Non vi sarebbe, pertanto, alcuna parvenza che consenta di ricondurre il messaggio civetta all'intermediario.
Inoltre l'intermediario ha provato (mediante esibizione dei Logs informatici relativi alle e-mail inviate il giorno 26.05.2022 all'indirizzo di posta elettronica associata al conto) che la ricorrente era stata tempestivamente e regolarmente resa edotta circa gli accessi anomali eseguiti da soggetti terzi al proprio conto corrente per mezzo di n. 2 e-mail inviate all'indirizzo di posta elettronica collegato al proprio conto in data 26 maggio 2022 alle ore 15:28 (ora locale), orario coincidente col verificarsi della frode in analisi.
Pertanto, il sistema di alert predisposto dall'intermediario ha funzionato regolarmente, assolvendo al suo compito di avviso tempestivo al cliente in ordine alle operazioni anomali registrate sul suo conto.
Nella valutazione della colpa grave, si deve ricordare il recente orientamento del Collegio di Milano, decisione n. 230/23, secondo il quale «sia quando il messaggio civetta si inserisca in una "conversazione" o "chat" contenente precedenti messaggi genuini provenienti dall'intermediario, sia quando sussista un singolo messaggio civetta che risulti apparentemente proveniente dall'intermediario in relazione alla simulazione del nome del mittente, occorre valutare caso per caso eventuali profili di colpa grave del cliente, non potendosi ipotizzare automatismi di sorta circa il riparto di responsabilità tra le parti. Nella fattispecie si rileva che l'assenza di errori nel testo del messaggio e la sua formale riferibilità all'Intermediario, la urgenza insita nella comunicazione palesatasi prima facie attendibile, ha consentito l'installazione dell'app Home banking sul device del malfattore così escludendo la ricorrente poi dalla fase conclusiva dell'operazione fraudolenta. Ritiene il Collegio che al comportamento della ricorrente non possa quindi nel caso in esame riconoscersi una determinante ed inescusabile colpa nella produzione del fatto illecito altrui, da ricondursi invece integralmente nell'area del rischio professionale del prestatore dei servizi di pagamento.»
Il caso qui in discussione si presenta molto simile a quello deciso dal Collegio di Milano: anzitutto, il messaggio civetta non era anomalo né presentava errori ortografici ed anzi risultava ineccepibile sul piano testuale "ATTENZIONE!!! Il Suo Conto Viene Sospeso Per Evitare la Sospensione Clicca su" con un successivo link seguito dall'indicazione ****, ossia contenente la denominazione della banca. Esso, pur non presentandosi nella chat normalmente usata dall'intermediario, appariva genuino poiché conteneva una comunicazione al cliente sulla funzionalità (rectius disfunzionalità) del suo conto, e il nome **** dell'intermediario che consentiva la apparente riferibilità del messaggio allo stesso.

Non può assumere rilevanza, per contro, la circostanza evidenziata dall'intermediario, secondo cui la banca non ricorre normalmente alla terza persona singolare ma alla seconda persona singolare (dettaglio privo di rilievo perché generalmente non noto ai clienti).
Inoltre, il sito su cui la ricorrente è stata instradata appariva talmente simile a quello proprio dell'intermediario da non far sorgere alcun dubbio sulla sua autenticità e le richieste formulate telefonicamente di fornire le credenziali (PIN e OTP) da parte di sedicenti operatori della banca dovevano servire, secondo la ricorrente e secondo quanto dichiarato telefonicamente alla stessa dai truffatori, a ripristinare la interrotta funzionalità del conto corrente, e non per perfezionare un bonifico da altro dispositivo; operazione di cui la ricorrente era completamente all'oscuro nel momento in cui veniva compiuta. Infatti, la schermata apparsa alla ricorrente non era certamente quella dell'ordine di bonifico, il quale è stato invece concluso presso un diverso device direttamente dal frodatore.
Deve a ciò aggiungersi che il sistema di alert dell'intermediario, che ha inviato due mail alla ricorrente contestualmente alle attività anomale registrate sul suo conto, ha certamente attirato l'attenzione della ricorrente rendendola edotta del bonifico fatto dal suo conto che aveva svuotato lo stesso dell'intera provvista di denaro, tanto vero che la stessa ha contattato il servizio clienti meno di un'ora dopo l'operazione contestata chiedendo l'annullamento del bonifico, ed usando nella chat con l'intermediario toni chiaramente allarmati che hanno provocato un'immediata reazione dell'intermediario. L'intermediario, infatti, ha riferito di essersi "immediatamente" adoperato al fine di stornare l'operazione disconosciuta, ma il tentativo di recupero della somma non è andato a buon fine in virtù del fatto che la stessa aveva formato oggetto di ulteriori operazioni dispositive effettuate da parte del frodatore in stretta successione temporale, probabilmente ricorrendo a bonifici istantanei.
Dunque, l'efficiente sistema di alert, pur avendo assolto alla sua funzione di avviso tempestivo, non è bastato ad impedire il perfezionamento della truffa, cosa di cui non può essere considerata responsabile la ricorrente.
Per tutte queste ragioni, ossia assenza di errori nel testo del messaggio, l'apparente riferibilità all'Intermediario dell'sms, l'urgenza insita nella comunicazione palesatasi prima fase attendibile e infine l'esclusione della ricorrente dalla fase terminale della operazione, unitamente alla celerità dell'azione dei truffatori che ha coinvolto anche altri conti correnti e diverse operazioni dispositive compiute in rapidissima sequenza temporale, il Collegio ritiene che non sia ravvisabile nella condotta della ricorrente una inescusabile colpa grave nella produzione del fatto illecito altrui, bensì una colpa lieve, essendo di fronte ad una frode informatica tanto sofisticata e subdola da poter trarre in inganno anche persone normalmente avvedute, e dovendo per contro ricondursi tale frode integralmente nell'area del rischio professionale del prestatore dei servizi di pagamento (cfr. Collegio di Milano, decisione n. 230/23).

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 29.450,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI