

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARIANELLO

Seduta del 18/12/2025

FATTO

La ricorrente, titolare di un conto corrente presso l'intermediario, riferisce di avere ricevuto in data 16, 17 e 19 dicembre 2024 sulla propria utenza mobile tre *sms*, inseritisi nella *chat* genuina con l'intermediario, mediante i quali veniva invitata a contattare con urgenza un numero telefonico fisso. La stessa, data l'attendibilità delle comunicazioni, il 19/12/2024 contattava telefonicamente il suddetto recapito, a cui rispondeva un sedicente addetto. Durante la conversazione le veniva comunicato che il bancomat aveva subito una clonazione e che vi erano stati diversi tentativi di intrusione nel suo *home banking*. Al fine di bloccare illegittime operazioni poste in essere da terzi l'interlocutore chiedeva conferma di alcuni movimenti, effettivamente posti in essere dalla cliente nei giorni precedenti, a riprova dell'avvenuta violazione dei sistemi di sicurezza dell'istituto, nonché del conseguente "*data breach*". L'operatore le comunicava la necessità di sostituire la carta di debito per ragioni di sicurezza. Per tale motivo la correntista si rendeva disponibile a spedire la carta che, come comunicatole tramite *sms*, sarebbe stata ispezionata dal *team security check* della banca, secondo le istruzioni ricevute mediante consegna in busta chiusa ad un corriere. Successivamente l'istante riceveva un ulteriore *sms*, con cui le venivano fornite le presunte nuove credenziali. Nel contempo, l'interlocutore telefonico le chiedeva di fornire le precedenti credenziali, al fine di bloccarle ed evitare ulteriori tentativi di accesso. Tramite *sms* la ricorrente riceveva il codice *pin* della presunta nuova carta di debito, che le sarebbe stata inviata il giorno successivo tramite corriere, nonché forniva le credenziali richieste. La correntista riceveva, poi, ulteriori *sms* che confermavano l'avvenuto blocco di presunte transazioni sospette.

Ogni attività richiesta dall'operatore telefonico, infatti, veniva sempre preceduta da un *sms* apparentemente genuino. Tuttavia, il giorno successivo, ovvero il 20/12/2024, la correntista riceveva tramite messaggistica istantanea, da un contatto riconducibile alla banca ed avente quale immagine del profilo il logo ufficiale della stessa, una comunicazione con cui veniva informata del fatto che le consegne delle carte avrebbero subito ritardi. Insospettita da tale circostanza, contattava il Servizio clienti, il quale la informava che, previo aumento del massimale, erano stati effettuati alcuni prelievi non autorizzati in data 19/12/2024 di € 2.500,00 e € 1.500,00 e, in data 20/12/2024, presso una differente filiale, di € 4.990,00, € 2.500,00 e € 1.500,00, per un totale di € 12.990,00. Inoltre il 27/12/2024 venivano contabilizzate alcune transazioni POS (€ 4.467,00 eseguita il 19/12/2024; € 4.467,00 e € 506,39 eseguite il 20/12/2024) per € 9.440,39.

La correntista chiedeva il blocco immediato della carta e procedeva a sporgere denuncia. La stessa ritiene l'intermediario contrattualmente responsabile, sia in ragione del "*data breach*" avvenuto in proprio danno, sia per la violazione degli obblighi, sullo stesso gravanti, di protezione e di controllo, inclusa la mancata attivazione degli *sms alert* (mai ricevuti) e la mancata predisposizione di sistemi di blocco automatico. Il caso di specie integrerebbe gli estremi della frode ai sensi dell'art. 8 del d.m. n. 112/2007, lett. a), n. 3 e lett. b), in ragione di plurime transazioni, effettuate in tempi brevi, di importi superiori a quelli di solito prelevati/spesi dalla correntista. In conclusione, insoddisfatta dell'interlocuzione avuta in sede di reclamo, la ricorrente chiede all'Arbitro: - in via principale di accertare la responsabilità dell'istituto di credito e, per l'effetto, condannarlo al rimborso integrale delle somme illecitamente sottratte mediante la truffa (del tipo *spoofing* mista a *vishing*), per il complessivo importo di € 22.430,39, oltre rivalutazione monetaria ed interessi legali dalla data dell'avanzato reclamo sino all'effettivo soddisfo, oltre al ristoro delle spese legali e rimborso del contributo versato; - in via subordinata, di accertare la responsabilità contrattuale e, per l'effetto, condannare lo stesso al rimborso, nella misura dell'80% ovvero nella maggiore o minore misura ritenuta di giustizia, delle somme illecitamente sottratte, oltre rivalutazione monetaria, interessi legali, spese legali e rimborso del contributo.

L'intermediario, regolarmente costituito nel presente procedimento, rappresenta che la ricorrente collocava la carta di pagamento originale, poi ritirata da un sedicente "*corriere*", all'interno della propria cassetta condominiale, rivelando telefonicamente sia il *pin* che credenziali di accesso alla banca via *internet*. Tale comportamento consentiva ai truffatori di eseguire, tra il 19 ed il 20 dicembre 2024, otto operazioni (prelevamenti ATM e pagamenti POS) con la carta di debito, per l'importo complessivo di € 22.430,39.

Il resistente eccepisce preliminarmente l'infondatezza delle richieste risarcitorie concernenti le spese legali in quanto non documentate, non quantificate e non giustificate, attesa la facoltatività dell'assistenza difensiva nel procedimento ABF.

In ogni caso le operazioni contestate risultano correttamente autenticate con le credenziali e il PIN personale, comunicati dalla ricorrente ai malfattori per sua stessa ammissione.

In particolare, risultano eseguite le seguenti operazioni in data 19/12/2024:

- ore 16:22, prelevamento di € 2.500,00 presso ATM, autorizzato con carta e PIN;
- ore 16:23, prelevamento di € 1.500,00 presso ATM, autorizzato con carta e PIN;
- ore 16:56, pagamento POS di € 4.467,00, autorizzato con carta e PIN;

ed in data 20/12/2024:

- ore 08:27, prelevamento presso cassa veloce di € 4.990,00, autorizzato con carta, PIN e OTP (inviata dalla banca all'utenza telefonica della ricorrente);
- ore 08:28, prelevamento presso ATM di € 2.500,00, autorizzato con carta e PIN;
- ore 08:29, prelevamento di € 1.500,00 presso ATM, autorizzato con carta e PIN;
- ore 09:12, pagamento POS di € 4.467,00, autorizzato con carta e PIN;
- ore 10:04, pagamento POS di € 506,39 autorizzato con carta e PIN.

L'intermediario precisa che in data 19/12/2024, alle ore 16:21, dopo l'accesso all'*home banking* via

browser autenticato tramite *token* (utilizzo di *password* usa e getta prodotta su *token* fisico), venivano aumentati i massimali della carta (pagamento POS giornaliero a € 5.000,00 e mensile a € 15.000,00; pagamento *e-commerce*; prelievo a € 10.000,00), autorizzati mediante uso di *password* usa e getta prodotta su *token* fisico.

L'utilizzo della carta presso la cassa veloce funge da strumento di autenticazione e, nel caso in esame, l'importo prelevato rientra nel massimale di € 5.000,00, di cui alla proposta di modifica unilaterale, a suo tempo inviata alla ricorrente a mezzo estratto conto del 30/09/2016 (di cui produce evidenza di trasmissione nella sezione documenti *on-line*, cui la cliente aderiva per la ricezione delle comunicazioni).

Ne deriva che tutte le operazioni risultano eseguite nel rispetto dei massimali, che gli ATM non hanno registrato anomalie (come risulta dai giornali di fondo) e che la progressione del contatore ATC risulta corretta.

Dagli atti si evince che la ricorrente non soltanto ha consegnato la carta, ma ha anche reso noto il PIN e le credenziali di accesso all'*home banking*, consentendo ai malfattori di effettuare le operazioni e di aumentare i massimali, oltre ad avere comunicato il codice OTP.

La banca, inoltre, rappresenta di avere inviato all'utenza della ricorrente, coincidente con quella indicata nel ricorso, la notifica di tutte le operazioni contestate, contenente il riepilogo dei dati dei prelievi/pagamenti effettuati ed il numero verde della banca. Purtuttavia la stessa segnalava l'occorrenza e chiedeva, tramite numero verde, il blocco della carta solo in data 20/12/2024 alle ore 17:27 (dopo oltre un giorno rispetto alla prima operazione).

L'utenza con cui controparte si metteva in contatto, così come quella dei messaggi civetta, non appartengono alla banca, come risulta facilmente verificabile consultando i riferimenti della stessa. Inoltre il testo dei messaggi in questione appariva grossolano, inconsueto, grammaticalmente errato e privo di personalizzazione (nome del cliente e della banca, dati operazione, numero verde) e anche la numerazione della carta ivi indicata non corrispondeva in alcuni casi a quella reale.

Il resistente rileva altresì come non sia consueto chiedere alla clientela di depositare la carta di debito, per di più attiva, all'interno della cassetta pubblicitaria condominiale, di facile accesso a qualsiasi estraneo e, comunque, di ritirare carte dei clienti a domicilio, piuttosto che in agenzia.

L'intermediario, richiamate alcune decisioni dell'Arbitro e della Giurisprudenza di merito, chiede di accogliere l'eccezione preliminare e, in seconda istanza, di respingere il ricorso.

In sede di repliche la ricorrente sottolinea la responsabilità contrattuale dell'istituto per l'avvenuto illegittimo "*data breach*" dei propri dati, in relazione al quale la banca non offriva spiegazioni, né prove contrarie, per la mancata adozione di misure di sicurezza e di protezione volte ad evitare azioni fraudolente, nonché per la mancata attivazione di misure di controllo sulle transazioni mediante sistemi di *alert* e blocco automatico, a fronte di movimentazioni anomale per entità e rapida successione cronologica. La stessa evidenza che, alla luce del contesto di grave inganno e pressione psicologica, tipico delle tecniche di "*social engineering*" finalizzate a carpire la buona fede dell'utente, non rilevarebbe la circostanza della comunicazione delle credenziali, trattandosi di un comportamento indotto mediante raggiri particolarmente sofisticati e realizzati con modalità tali da non consentire un'effettiva percezione del rischio. L'affidamento nella stessa ingenerato non sarebbe ascrivibile a propria colpa grave, essendo la stessa stata tratta in inganno dall'apparente riconducibilità alla banca degli innumerevoli *sms* ricevuti, nonché dal fatto che l'asserito operatore conosceva, in ragione del *data breach*, alcune operazioni effettivamente poste in essere antecedentemente. Nel caso di specie la banca non ha fornito la prova della corretta autorizzazione delle operazioni illecite, essendosi limitata a rilevare che le stesse sarebbero avvenute tramite le credenziali della cliente, nonché a comprovare, mediante la produzione in atti della progressione dell'ATC, la mera esecuzione tecnica e la cronologia delle transazioni, senza fornire elementi idonei a dimostrare la riconducibilità delle operazioni fraudolente alla volontà della correntista. L'istante contesta anche l'asserita presenza di errori ortografici nei messaggi ricevuti, in quanto essi erano redatti in lingua italiana corretta e con uno stile

coerente con quello utilizzato ordinariamente dall'intermediario, nonché la documentazione che l'intermediario ritiene idonea a dimostrare l'invio di *sms alert*, in quanto priva di qualsivoglia efficacia probatoria in ordine all'effettivo inoltro e alla ricezione dei suddetti messaggi sul proprio dispositivo. Anche la presunta eccezione circa la tardività della segnalazione delle operazioni fraudolente, rispetto alle asserite notifiche delle operazioni inviate dalla banca risulterebbe priva di fondamento. Non corrisponde al vero, infine, l'assunto di controparte secondo cui non sarebbe stata prodotta in atti la documentazione relativa agli *screenshot* delle chiamate intercorse con il truffatore, già accluse al ricorso e di nuovo prodotte in allegato. L'istante insiste per l'accoglimento delle richieste avanzate in sede di ricorso.

L'intermediario, nelle controrepliche, rileva che le doglianze di controparte e, tra queste, la contestazione inerente l'asserito *data breach*, introdotta per la prima volta in sede di repliche, risultano palesemente infondate e non pertinenti, in quanto sformite di qualsiasi supporto probatorio. La consegna da parte della ricorrente, come dalla stessa ammesso, delle credenziali per l'accesso alla banca via *internet*, del codice PIN, della carta di debito originale (lasciata incustodita, alla portata di tutti, all'interno della cassetta della pubblicità comune al condominio, aperta senza serratura), nonché del codice OTP, laddove previsto, consentiva al truffatore di operare come il vero titolare. Il resistente, dopo avere rimarcato la circostanza che il mancato blocco della carta subito dopo avere ricevuto i primi messaggi avrebbe impedito le successive operazioni, insiste per il rigetto del ricorso.

DIRITTO

Si evidenzia preliminarmente, pur in assenza di eccezioni sul punto da parte dell'intermediario, che in tema di violazione di normativa sulla *privacy*, è stata affermata dai Collegi la competenza dell'Arbitro qualora la denunciata violazione sul trattamento dei dati personali dei clienti sia collegata alla prestazione di servizi bancari e finanziari (*ex plurimis*, Collegio ABF Palermo, n. 10395/2023; Collegio ABF Bologna, n. 23238/2021; Collegio ABF Milano, n. 5185/2015; Collegio ABF Roma, n. 11412/2016). Nel caso di specie le asserite violazioni (*data breach*) lamentate dalla ricorrente riguardano il trattamento di dati personali, comunque inerenti a rapporti di conto corrente bancario. La predetta contestazione, diversamente da quanto asserito dal resistente, non è stata introdotta per la prima volta in sede di repliche, ma risulta già proposta in sede di ricorso ad ulteriore fondamento della domanda risarcitoria.

La presente controversia attiene alla richiesta di parte ricorrente relativa al disconoscimento di otto operazioni, per un importo complessivo di € 22.430,39 e, precisamente:

- due prelievi presso ATM (di € 2.500,00 alle ore 16:22 e € 1.500,00 alle ore 16:23), effettuati in data 19/12/2024;
- un pagamento POS (di € 4.467,00 alle ore 16:56), effettuato in data 19/12/2024;
- un prelievo cassa veloce (di € 4.990,00 alle ore 8:27), effettuato in data 20/12/2024;
- due prelievi presso ATM (di € 2.500,00 alle ore 8:28 e € 1.500,00 alle ore 8:29), effettuati in data 20/12/2024;
- due pagamenti POS (di € 4.467,00 alle ore 9:12 e € 506,39 alle ore 10:04), effettuati in data 20/12/2024.

Occorre rilevare che le operazioni contestate risultano essere state eseguite tra il 19/12/2024 ed il 20/12/2024 e, pertanto, ricadono nell'ambito di applicazione del D.lgs. 27/01/2010, n. 11, di attuazione della Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal D.lgs. 15/12/2017, 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.

In particolare, le fonti normative che regolano la *strong customer authentication* (c.d. SCA) sono rinvenibili negli artt. 97 e 98 della PSD 2, nell'articolo 10-bis del D.lgs. n. 10/2011, nelle norme tecniche

di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14/09/2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, il parere dell'EBA del 21/06/2019).

Come costantemente rilevato da questo Arbitro, la normativa novellata ha rafforzato il regime di speciale protezione e di *favor probatorio* a beneficio degli utenti, introdotto dal D.lgs. n. 11/2010 *ante* modifica, ripetutamente evidenziato da numerose decisioni dell'ABF (*ex plurimis*, Collegio di Coordinamento ABF, n. 21285/2021; n. 991/2014; n. 5304/2014; n. 3498/2012).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo o della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, D. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia del 05/07/2011.

Il ricorso è infondato e non merita accoglimento per le considerazioni che seguono.

La ricorrente in sede di denuncia ammette di avere ricevuto un messaggio, apparentemente proveniente dalla banca, contenente un recapito telefonico che provvedeva a contattare, nonché di avere fornito il codice *pin* della carta e di avere depositato la medesima all'interno della cassetta condominiale, come indicatole dal truffatore.

La carta risulta essere stata bloccata alle ore 17:27 del 20/12/2024.

Premesso quanto sopra, a fronte del disconoscimento di operazioni fraudolente da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi degli artt. 10, c. 1 e 2 e 10-*bis* del d.lgs. n. 11/2010. In mancanza di tale dimostrazione, l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute. Nel caso di specie, l'intermediario ricostruisce i singoli passaggi esecutivi, fornendo le relative evidenze informatiche. Al riguardo, anche con riferimento alle contestazioni della ricorrente, circa l'efficacia probatoria della documentazione tecnica prodotta, si rammenta che, secondo gli orientamenti condivisi dei Collegi, tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico *standard* per l'inserimento e la tracciatura dei fattori di autenticazione forte, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai *log*) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. Eventuali dichiarazioni confessorie della cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

L'accesso al browser risulta autorizzato con doppio fattore di conoscenza (validazione *pin*) e di possesso (*update token ok*).

Con riferimento all'operazione di modifica dei massimali, autorizzata "*tramite token fisico*" - fattore di possesso - alla luce delle schermate depositate in atti, nonché della sequenza temporale ravvicinata delle operazioni, sembrerebbe essere stato riutilizzato il primo fattore.

Al riguardo l'EBA (nel Q&A 2018-4141) ritiene riutilizzabile il primo fattore (fattore di conoscenza) purché - come nel caso di specie - l'azione avvenga nell'ambito della medesima sessione.

La modifica dei massimali (di pagamento POS, di prelievo, di pagamento *e-commerce*) risulta intervenuta prima delle operazioni contestate, ovvero alle ore 16:21 del 19/12/2024.

Successivamente risultano effettuati (alle ore 16:22 e alle ore 16:23 del 19/12/2024) due prelievi presso il medesimo ATM di € 2.500,00 e € 1.500,00, entrambi autorizzati tramite *chip* e *pin*, di cui la banca produce i relativi *log*.

Alle ore 16:56 del 19/12/2024, invece, risulta effettuato un pagamento POS di € 4.467,00 sempre mediante doppio fattore di autenticazione.

Con riferimento al prelievo cassa veloce di € 4.990,00 del giorno successivo (avvenuto alle ore 08:27) l'intermediario evidenzia che lo stesso era stato oggetto di modifica unilaterale in data 30/09/2016 e tale circostanza non risulta contestata dall'istante.

Anche la predetta operazione risulta autorizzata con doppio fattore (*pin* e OTP), rispettivamente di conoscenza e di possesso.

Risultano effettuati con le medesime modalità anche le altre quattro operazioni compiute nel medesimo giorno, ovvero i due prelievi ATM (alle ore 08:28 di € 2.500,00 ed alle ore 08:29 di € 1.500,00) e i due pagamenti POS (alle ore 09:12 di € 4.467,00 ed alle ore 10:04 di € 506,39).

Ne consegue che tutte le operazioni contestate, pertanto, risultano eseguite in conformità dell'art. 10-*bis* del D. lgs. n. 11/2010, in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti rispettivamente alle categorie della conoscenza (qualcosa che solo l'utente conosce) e del possesso (qualcosa che solo l'utente possiede) e, pertanto, risultano *compliant* alla SCA.

Risultano prodotti anche il giornale di fondo e la progressione del contatore ATC, alla luce dei quali non risulta emergere alcuna anomalia.

Per quanto attiene al comportamento della ricorrente, nel caso di specie la stessa è incorsa in una fattispecie di colpa grave sia per quanto attiene alla custodia dello strumento di pagamento che delle relative credenziali di sicurezza. Alla luce delle dichiarazioni di natura confessoria rese in sede di denuncia, infatti, l'istante ammette di avere rivelato ai truffatori le relative credenziali di sicurezza nonché di avere consegnato la carta integra all'interno della cassetta della pubblicità (in senso conforme, Collegio di Coordinamento ABF, n. 5304/2013).

Inoltre la chiamata in uscita con il sedicente operatore risulta effettuata nei confronti di un numero non riconducibile all'intermediario ed anche le interlocuzioni effettuate tramite messaggistica istantanea risultano poste in essere con un canale comunicativo non utilizzato dalla banca per i contatti con la clientela.

Gli elementi sopra indicati consentono, quindi, di ricondurre la presente fattispecie alla truffa effettuata tramite il c.d. *smishing/vishing*, per la quale i Collegi sono soliti ritenere che "*il cliente è vittima di una colpevole credulità*" (in senso conforme, Collegio di Coordinamento ABF, n. 3498/2012).

In tale ipotesi l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente si realizzano con metodi ormai piuttosto noti (*e-mail*, *sms* e telefonate civetta, false comunicazioni di scadenza, invito all'aggiornamento di *database*) che il cliente, dispiegando un minimo di diligenza, sarebbe oggettivamente in grado di schivare, anche per le accresciute campagne di informazione e di sensibilizzazione che i *media* e gli stessi intermediari hanno da tempo attuato.

Alla luce degli estratti-conto versati in atti e dell'entità delle relative operazioni non sembrano sussistere neppure gli indici di frode identificati dall'art. 8 del D.M. n. 112/2007 che, tuttavia, non hanno un valore precettivo diretto ma rappresentano degli utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.

Per quanto concerne l'attivazione di sistemi di *alert*, si evidenzia che: "*Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto*" (Collegio di Coordinamento ABF, n. 24366/2019).

A tale riguardo il convenuto ha prodotto evidenza sia dell'invio di *sms alert* che di notifiche *push* per ciascuna delle operazioni contestate, che risultano consegnati al numero di telefono indicato dalla ricorrente. Quest'ultima ha provveduto al blocco della carta soltanto alle ore 17:27 del 20/12/2024, dopo oltre un giorno dall'effettuazione della prima operazione non autorizzata.

Tutte le considerazioni sopra evidenziate portano ad escludere un apporto causale dell'intermediario nell'esecuzione della frode, la quale risulta ascrivibile esclusivamente al comportamento gravemente colposo tenuto da parte ricorrente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE