Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) MANENTE	Membro di designazione rappresentativa degli intermediari
(MI) FALCE	Membro di designazione rappresentativa dei clienti

Relatore (MI) DENOZZA

Seduta del 21/01/2021

FATTO

Parte ricorrente espone:
di essere stata vittima di una frode informatica a lei non imputabile e di agire per ottenere la restituzione dell'importo sottratto, l'accesso alla documentazione inerente le operazioni contestate, oltre al risarcimento dei danni subiti e alle spese legali.

Dalla documentazione allegata si evince che la cliente:

- ha disconosciuto due operazioni di bonifico istantaneo effettuate in data 27 e 28.03.2020 per l'importo complessivo di € 29.900,00;
- l'intermediario non ha accolto la sua richiesta di produzione di tutta la documentazione inerente le operazioni, in particolare dei log relativi agli accessi al conto e alle operazioni effettuate dal 01.01.2020 al 31.03.2020, completi di indirizzo IP e *legenda*;

La Cliente chiede il rimborso della somma di € 29.900,00 pari al valore della somma sottratta, l'accesso alla documentazione inerente le operazioni contestate, oltre al risarcimento dei danni subiti e delle spese legali.

L'Intermediario afferma:

- che le due operazioni contestate sono state disposte tramite home banking mediante l'APP dell'intermediario;
- che l'operatività tramite home banking è stata attivata dalla cliente in occasione della sottoscrizione del contratto del 03.02.2020;
- che per accedere all'home banking è necessario digitare l'identificativo cliente e il codice pin, per effettuare le singole operazioni è necessario digitare inoltre un codice OTP tramite APP (mobile token) o tramite token fisico (fino al 14.09.2019);
- che lo schema delineato integra un sistema di autenticazione a due fattori;
- che la scrivente banca da tempo raccomanda la massima cautela nell'utilizzo dei canali telematici;
- che in presenza di un sistema a due fattori è lecito presumere che la cliente abbia tenuto un comportamento gravemente colposo;
- che verosimilmente la cliente è stata vittima di un episodio di phishing per effetto del quale ha fornito tutti i dati necessari ad effettuare le operazioni ai frodatori;
- che tutte le operazioni sono state regolarmente autorizzate e si è provveduto ad inviare alla cliente gli sms recanti le informazioni del caso;
- che gli sms sono stati consegnati alla cliente e che l'attività informatica riconducibile all'operazione è stata disposta dall'Id utente riconducibile alla cliente;
- che lo scrivente intermediario si è tempestivamente attivato con la banca beneficiaria per recuperare le somme, senza tuttavia riuscirvi a causa della natura di bonifico istantaneo delle operazioni contestate;
- che non è possibile accedere al mobile token con la sola conoscenza delle credenziali statiche, in quanto è necessario disporre del codice OTP inviato via sms al cliente per attivare il servizio;
- che, nel caso in cui il frodatore cambi il numero di telefono associato al conto, al titolare vengono inviate varie notifiche, tra cui una tramite sms;
- che la cliente non ha contestualizzato in denuncia la dinamica della frode;
- che il sistema di autenticazione adottato è conforme anche a quanto previsto dal Codice della privacy;

Chiede il rigetto del ricorso.

La ricorrente in sede di repliche afferma:

- che l'intermediario non ha assolto l'onere della prova di cui è onerato;
- che in particolare non risultano IMEI e utenza associata al dispositivo con cui stata effettuata l'operazione;
- che per il dispositivo utilizzato in occasione della frode non è stata effettuata la stessa operazione di attivazione compiuta in data 11.03.2020 per la prima attivazione dell'APP;
- che nel frangente di tempo durante il quale sono state effettuate le operazioni, il suo telefono cellulare era spento;
- che in occasione della frode sono state registrate ben 10 attività effettuate con un dispositivo differente da quello da lei utilizzato;
- che l'intermediario non ha inviato l'sms alert relativo quando il frodatore ha modificato il numero di telefono associato all'utenza, attraverso il quale ha poi utilizzato l'APP per autorizzare le operazioni;

L'intermediario afferma:

- che i dati forniti sono sufficienti a provare la corretta autenticazione delle operazioni, mentre IMEI e utenza rientrano tra i dati sensibili di cui non è concessa la divulgazione;
- che la cliente non prova che il device utilizzato dalla cliente fosse spento al momento delle operazioni e che nulla esclude che la stessa cliente abbia utilizzato un altro dispositivo, attività consentita senza che sia necessaria una ulteriore comunicazione alla banca medesima;
- che lo scrivente intermediario ha tempestivamente informato la banca in merito a ciò che stava accadendo;
- che la relazione allegata dall'intermediario è inattendibile e priva di fondamento;
- che è la stessa cliente ad affermare che è stato adottato un sistema di autenticazione a due fattori;
- che il sistema permette di scaricare l'APP e di accedere al proprio device da più dispositivi;

DIRITTO

Le operazioni contestate sono state effettuate il 27. 03.2020 alle ore 23.12 e il 28.03.2020 alle ore 00.11. Le operazioni poste in essere sono costituite da due operazioni di bonifico istantaneo dell'importo di € 14.950,00 ciascuna effettuate tramite home banking.
In denuncia è indicata una terza operazione, di bonifico ordinario, dell'importo di € 14.800,00, restituito dall'intermediario.

La cliente allega la denuncia del 28.03.2020, in cui disconosce le operazioni e riferisce di essersi accorta delle operazioni grazie a degli sms di allerta arrivati sulla sua utenza telefonica.

L'intermediario espone di aver predisposto un livello di sicurezza rafforzato *a più fattori* come sarebbe evincibile da quanto affermato nelle controdeduzioni e nei relativi allegati.

La cliente, di contro, produce una relazione tecnica (*cfr. all. al ricorso relazione tecnica*) volta ad evidenziare l'inadeguatezza del sistema di autenticazione predisposto dall'intermediario. In detta relazione si contesta tra l'altro la tempestiva ricezione delle notifiche di *alert* inviate via APP, relative alle operazioni in questione. Sul punto la cliente allega uno *screenshot* delle notifiche delle operazioni che sarebbero pervenute sul suo dispositivo soltanto alle ore 08.42 del 28.03.2020. Le notifiche riguardano una delle operazioni disconosciute e il bonifico dell'importo di € 14.800,00, rimborsato dalla banca e non oggetto di domanda.

L'intermediario afferma che l'operazione di accesso all'home banking necessita dell'inserimento del codice identificativo del cliente e del codice pin da quest'ultimo conosciuto.
L'autorizzazione delle singole operazioni, ove disposta da APP, come nel presente caso, richiede l'inserimento di un codice OTP, generato dalla stessa APP (mobile token).
L'intermediario produce un allegato (*all. 4 ctd*.) all'interno del quale sono riportate tutte le notifiche inviate all'utenza della cliente e il dispositivo a cui sono state inviate.

Le notifiche di *alert* dei due bonifici contestati sembrerebbero essere state inviate tanto al disposavo *Android* della cliente quanto a quello *ios* con cui sono state effettuate le operazioni. La cliente contesta però di averle ricevute.
La ricorrente riferisce che ha appreso del compimento dell'altro bonifico istantaneo soltanto dopo aver richiesto la nuova attivazione dell'APP in quanto, nonostante fossero presenti le notifiche, non riusciva ad effettuare l'accesso all'applicazione della banca. Per questa operazione non sarebbe pervenuta alcuna notifica, pur essendo presente nell'APP un resoconto della stessa. Attesta il *reset* dell'APP allegando l'sms contenente l'OTP all'uopo inviato.
Venendo all'esame della disciplina nella fattispecie applicabile, va richiamato il disposto del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della Direttiva 2015/2366/EU (PSD II), che deve essere ovviamente interpretato alla luce delle finalità perseguite dalla Direttiva stessa.
Significativo a questo riguardo risulta il disposto dell'Art.72 di detta Direttiva ai sensi del quale:

Art 72 *1 Gli stati membri dispongono che qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che l'operazione di pagamento non è stata correttamente eseguita, spetti al prestatore di servizi di pagamento fornire la prova del fatto che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti del servizio fornito dal prestatore di servizi di pagamento.*
2 Se l'utente di servizi di pagamento nega di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso se del caso il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione di pagamento sia stata autorizzata dal pagatore né che questi abbia agito in modo fraudolento o non abbia adempiuto, dolosamente o con negligenza grave, a uno o più degli obblighi di cui all'articolo 69. Il prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornisce gli elementi di prova che dimostrano la frode o la negligenza grave da parte dell'utente di servizi di pagamento".
Deve essere qui sottolineato, in particolare, quanto disposto nell'ultimo periodo del secondo comma, e cioè che è onere del prestatore di servizi di pagamento quello di fornire elementi di prova che dimostrino la frode o la negligenza grave del cliente.
A questo riguardo la dottrina oltre a ricordare che la colpa grave è nozione che va molto al di là della semplice violazione dell'obbligo di avere cura degli strumenti di pagamento e implica "*… un grado significativo di mancanza di diligenza…*" (così testualmente il considerando 72 della Direttiva) sottolinea che l'intermediario non può limitarsi ad affermare di avere operato correttamente, ma deve fornire " *supporting evidence* " atta a provare la colpa grave del cliente (v. ad es. R. STEENNOT, *Reduced payer's liability for unauthorized payment transactions under the second Payment Service Directive (PSD2),* in 34 *Computer law and security review,* 954,962).
In sostanza, sembra evidente che la *ratio* complessiva della disciplina è nel senso che le perdite per le quali non venga data la prova positiva della colpa grave del cliente, sono destinate a restare a carico degli intermediari, anche quando essi abbiano operato in assoluta conformità alle regole, e non vi sia alcuna negligenza che sia loro specificamente rimproverabile.

Questa precisa indicazione normativa sembra già di per sé idonea ad orientare la decisione del presente caso, dove nessuna prova positiva di una eventuale colpa grave della ricorrente è stata fornita dal convenuto.
A ciò si può aggiungere che, anche se si volesse considerare accettabile una sorta di prova indiretta, nel senso di accettare come prova l'adozione da parte dell'intermediario di sistemi di protezione non solo conformi a quelli richiesti dalla disciplina vigente, ma addirittura tali da rendere assolutamente improbabile la loro violazione se non per malfattori che abbiano potuto di fatto approfittare di gravi negligenze del cliente, deve essere comunque osservato che nella specie una simile prova indiretta non potrebbe ritenersi raggiunta.
Va intanto premesso che ai fini della sicurezza dei pagamenti, non rilevano solo i presidi adottati per l'autenticazione della singola transazione, ma anche le procedure seguite, e i presidi adottati, dall'intermediario per la consegna delle credenziali o dello strumento e la protezione dell'ambiente per l'utilizzo di strumenti e credenziali (APP dispositiva, sito Internet, dispositivi POS e ATM). Eventuali frodi in queste fasi possono infatti compromettere la sicurezza dello strumento o delle credenziali. A questi fini rilevano, ad esempio, l'installazione di una APP che abilita ai pagamenti su un dispositivo telefonico o su un computer, la tokenizzazione della carta, la memorizzazione del numero di telefono il cui possesso costituisce uno dei fattori di autenticazione.
Il Regolamento delegato (UE) 2018/389 del 27 novembre 2017 che integra la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri) precisa che gli intermediari devono assicurare:
a) la creazione delle credenziali di sicurezza in un ambiente protetto (art. 23);
b) l'associazione univoca, in un ambiente protetto (es. home banking, siti web, sito di pagamento, ATM), del cliente alle credenziali di sicurezza e ai software di autenticazione, tenendo presente anche i rischi che derivano dai dispositivi utilizzati durante il processo di associazione, che non sono sotto la diretta responsabilità dell'intermediario; se effettuata "a distanza" l'associazione va garantita con SCA (art. 24);
c) che le credenziali di sicurezza personalizzate, i dispositivi e il software di autenticazione siano consegnati all'utente dei servizi di pagamento in un modo sicuro volto a far fronte ai rischi connessi al loro utilizzo non autorizzato conseguente a perdita, furto o copia (art.25); che la distruzione, la disattivazione o la revoca nonché il rinnovo o la riattivazione delle credenziali di sicurezza personalizzate avvengano nel rispetto delle procedure per la creazione, l'associazione e la consegna delle credenziali e dei dispositivi di autenticazione (artt. 26 e 27).
Ciò premesso, a parte quanto osservato nella relazione tecnica prodotta dalla ricorrente in ordine agli aggiornamenti dei programmi utilizzati, va rilevato che già il fatto di consentire la coesistenza di due esemplari dell'applicazione funzionanti su apparecchi diversi appare un ovvio fattore di debolezza del sistema, così come ancora di più appare fattore di debolezza l'eccessivo affidamento sulle credenziali statiche, cosa che, se addirittura non esclude, sicuramente indebolisce l'autenticazione a due fattori e che comunque rende tutto il sistema estremamente vulnerabile, stante la notoria possibilità che i codici statici vengano intercettati (possibilità che è del resto alla base della richiesta del secondo fattore, e che è dovuta, tra l'altro, alla notoria esistenza di *malware* in grado di installarsi nei *browser* e di leggere i codici non criptati).
Non facilmente spiegabile risulta poi nella specie l'intervenuto blocco di cui sembra avere sofferto l'applicazione "legittima", così come non si può non notare l'inutilità della rilevazione dei codici IMEI se in caso di necessità di loro utilizzazione al fine di accertare

quanto effettivamente accaduto, si riesce solo a constatare che la protezione della *privacy* ne impedisce ogni utile impiego.
In definitiva il Collegio ritiene che, anche a voler ammettere la possibilità di ricorrere a quella che abbiamo indicato come prova indiretta della colpa grave del cliente, nella specie non si può ritenere che le circostanze accertate impongano di presumere che l'esistenza di detta colpa grave sia da considerare come l'unica possibile spiegazione dell'accaduto.
L'accoglimento della domanda principale determina l'assorbimento delle domande strumentali.
Non possono esser accolte né la domanda relativa al risarcimento dei danni, che non sono peraltro dimostrati, né, data la natura del giudizio avanti all'ABF, quella relativa al rimborso delle spese legali.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 29.900,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA