Lo Spoofing e la corresponsabilità della banca nelle frodi ai sistemi di *home banking*. Commento ad una recente e innovativa decisione dell'Arbitrato Bancario Finanziario

A cura dell'Avv. Cino Raffa Ugolini, Lègister Avvocati

Si segnala una interessante decisione dell'ABF, che sembra discostarsi per alcuni aspetti dalla prevalente giurisprudenza del suddetto organismo in un caso di frode, denominato "caller Id spoofing", emessa in data 5 maggio 2021.

I FATTI

Vediamo i fatti della controversia.

Un correntista di una primaria banca italiana venne contattato dal numero verde della banca stessa, ma non riuscì a prendere la chiamata. Pochi minuti dopo, venne contattato da un numero di cellulare sconosciuto. Egli rispose quindi al telefono e chi chiamava si identificò come operatore della banca, comunicandogli che stava avvenendo una operazione di hackering ai suoi danni, per cui lo sollecitava a rispondere alla chiamata del numero verde della banca. Il cliente riagganciava e il numero verde della banca richiamò immediatamente. Questa volta egli prese la telefonata, che proveniva dalla stessa persona, con cui aveva parlato poco prima. Questo funzionario gli comunicò che un hacker era riuscito a entrare nel suo conto online e che stava cercando di autorizzare delle operazioni di prelievo. Lo stesso funzionario gli disse che per bloccarlo era necessario comunicargli i codici che la banca gli avrebbe inviato di lì a poco via sms. Ogni codice era associato a un'operazione di prelievo e, stando all'operatore, attraverso quei codici la banca avrebbe potuto bloccare quelle operazioni di prelievo.

Nella convinzione di parlare con un operatore autorizzato della banca, che lo chiamava dal numero verde dell'istituto, il cliente comunicò all'apparente funzionario i codici speditigli tramite sms dalla banca. Tale procedura proseguì per 9 (nove) volte nell'arco di pochi minuti, sempre mentre il cliente comunicava telefonicamente con l'incaricato, che chiamava dal numero verde della banca.

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

Per effetto di tale frode, il cliente subì un ammanco di diverse migliaia di euro.
La banca, prontamente informata, avviò le indagini del caso e all'esito non ritenne di riconoscere alcun ristoro alla vittima, che fu costretta ad adire l'ABF.

IL PROCEDIMENTO DAVANTI ALL'ABF

Nel suddetto procedimento, su richiesta del cliente, la banca ha esibito copia in formato leggibile degli "*Inquiry LOG*" relativi all'accesso ai sistemi informatici dei canali digitali della banca dedicati al cliente.
Tale acquisizione probatoria si è rivelata fondamentale.

1. **L'inadeguatezza del sistema di sicurezza**

Come noto, le frodi più comuni nei servizi di home banking riguardano l'abuso delle credenziali di accesso e dispositive assegnate al cliente.
Gli intermediari si raccomandano di trattare i codici di accesso (codice titolare e PIN) con estrema cautela e di non condividerli con nessuno. In genere, i terzi vengono in possesso di questi dati tendenzialmente riservatissimi per la disattenzione dell'utente.
Un discorso diverso deve farsi per i codici dispositivi, che oggi sono costituiti essenzialmente da password dinamiche, che vengono generate automaticamente da dispositivi abbinati al conto o di volta in volta spedite via SMS al cliente (OTP o OTS, one time password) o generate via software dall'APP della banca o costituite dalla digitazione del PIN sull'APP stessa.
Infatti, per poter effettuare le operazioni di prelievo abusivo dei fondi del correntista vittima della frode è necessario, ma non sufficiente, procurarsi le sue credenziali di accesso, in quanto occorre anche procurarsi il codice dispositivo per validare l'operazione.
È astrattamente possibile che le misure di sicurezza adottate dall'intermediario vengano aggirate da terzi particolarmente esperti, ma spesso ciò accade (anche) in conseguenza della partecipazione colposa del cliente vittima della manovra fraudolenta.
La prima anomalia che viene segnalata nella decisione in commento riguarda il comportamento dell'intermediario, che sia consapevole dell'accesso abusivo da parte di terzi e sia rimasto

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

inerte, omettendo di informare il cliente della necessità di cambiare le sue credenziali in quanto violate da terzi.

Nella fattispecie è emerso dai LOG dell'intermediario che il malfattore era già riuscito ad accedere al sistema, evidentemente essendosi procurato le credenziali del cliente all'insaputa di questi.

In particolare, prima dell'inoltro degli SMS di conferma delle operazioni contestate, vennero effettuate, sul canale collegato al conto del cliente, ulteriori operazioni tipicamente riconducibili all'intrusione del malfattore, quali l'accesso da un indirizzo IP mai utilizzato dal cliente, il cambio del PIN, il blocco delle notifiche via SMS.

L'intermediario non poteva non esserne a conoscenza, in quanto è sua responsabilità monitorare i LOG. Nonostante ciò, la banca non ha avvisato il cliente.

Per perpetrare la frode, al malfattore non bastava essere in possesso delle credenziali di acceso al conto, in quanto gli servivano i codici dispositivi, che è riuscito a farsi comunicare via telefono dalla vittima, facendogli credere che fosse in atto un tentativo di attacco al suo conto corrente.

Si badi bene che durante le telefonate che provenivano dal numero verde della banca, il malfattore non chiese mai al cliente il numero di PIN (che evidentemente già possedeva), ma solo i codici dispositivi.

L'accesso al sistema tramite le credenziali abusivamente ottenute potrebbe essere riconducibile ad una falla nei sistemi di sicurezza adottati dalla banca.

Non sono chiare le modalità attraverso cui tale accesso sia avvenuto. Ciò che rileva è che la banca è stata censurata non per l'abusivo ottenimento delle credenziali da parte di terzi, ma per il **mancato avviso** al cliente della violazione delle sue credenziali.

È evidente che un cliente di media diligenza, ove fosse stato informato da parte della banca di questo accesso abusivo al suo conto on line, avrebbe tempestivamente modificato le sue credenziali (soprattutto il PIN) e non sarebbe certo caduto vittima della frode successiva.

Un ulteriore profilo di (cor)responsabilità dell'intermediario investe le modalità di comunicazione al cliente della violazione delle sue credenziali.

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

La banca ha, infatti, sostenuto di aver inviato, all'utenza cellulare del cliente, una comunicazione OTP (sotto forma di una notifica PUSH), con la quale lo avvisava che era stato eseguito un accesso da un browser non normalmente utilizzato dal cliente.Il cliente riferiva invece di non aver mai ricevuto tale messaggio OTP e dai LOG della banca sembrerebbe che ci sia stato un malfunzionamento del sistema.

Cionondimeno, l'ABF ha ritenuto tale sistema di sicurezza non adeguato, in quanto utilizza lo stesso canale, potenzialmente compromesso, sul quale il cliente ha già ricevuto l'OTP dispositiva. Esso difetta dell'indispensabile requisito dell'indipendenza dei diversi fattori, imposta dalla normativa europea (*regulatory technical standards dell'European Banking Authority*).

Ricordiamo che la sicurezza dei modelli di home banking si fonda essenzialmente sul sistema "a due fattori", ovvero sulla previsione di due distinti livelli per accedere al sistema ed effettuare le operazioni, come sopra indicato, quello delle credenziali d'accesso, costituite da password statiche, e quello dei codici dispositivi, che sono password dinamiche.

In altre parole, è necessario che l'intermediario contatti il cliente tramite un **canale diverso** da quello utilizzato nel momento in cui viene posta in essere l'operatività sospetta.

Questo ulteriore requisito di sicurezza comporta per l'intermediario conseguenze molto rilevanti, che potrebbero obbligarlo a rivedere le procedure di sicurezza in essere.

Infatti, l'ABF afferma espressamente che: *"in caso di sospetto di frode, quindi, l'intermediario dovrebbe adottare **altre misure** che assicurino un effettivo controllo dell'identità del soggetto che ha eseguito l'operazione attraverso un fattore aggiuntivo indipendente da quelli già utilizzati per la sua autenticazione (per esempio, prendere contatto direttamente con il cliente e, qualora ciò non sia possibile, bloccare cautelativamente l'operazione)".*

Appare evidente che un sistema di sicurezza adeguato avrebbe dovuto prevedere l'invio di una mail, un contatto telefonico o altro canale di comunicazione diverso dall'OTP.

In questa affermazione si ravvisa forse il punto più importante della decisione in commento: qualora l'intermediario non riesca a contattare il cliente per verificare l'identità del soggetto disponente, ad esempio perché la linea telefonica è occupata, è necessario bloccare cautelativamente l'operazione.

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

Si può immaginare come sia difficile, se non impossibile, in un sistema automatizzato e comunque governato dall'intelligenza artificiale, quale quello sottostante alle operazioni digitali di pagamento, mettere in atto delle misure di sicurezza, che consentano all'intermediario, 24 ore al giorno e sette giorni alla settimana, di verificare l'identità del cliente in concomitanza con il compimento di operazioni in apparenza sospette.

Appare molto più ragionevole e prudente un sistema automatico di blocco delle operazioni in presenza di sospetta frode (ad esempio quando venga posta in essere a distanza ravvicinata una pluralità di operazioni verso conti mai utilizzati in precedenza dal cliente), adottando un presidio attivo 24 ore al giorno per ottenere l'autorizzazione allo sblocco delle operazioni sospette. Tale presidio esiste già per le carte di credito e potrebbe essere esteso alle fattispecie qui discusse.

La mancata adozione di misure di sicurezza adeguate per prevenire questo genere di rischi è considerata prova della negligenza dell'intermediario e, come in seguito vedremo, causa del concorso colposo della banca nella prodizione del danno.

Si ritiene che questa carenza delle misure di sicurezza sia già di per se' idonea ad interrompere il nesso causale fra negligenza del cliente e il danno dallo sesso subito.

2. Recenti forme di frode informatica dal "vishing" allo "spoofing"

La terza esimente del cliente riguarda il cuore della frode, ovvero l'essenza del "vishing" che è una forma di truffa simile al più noto phishing.

Il phishing è una truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.

Il vishing è effettuata tramite servizi di telefonia, in particolare, sfruttando la tecnologia VoIP, per esempio viene effettuata una telefonata simulando l'esistenza di un call center e chiedendo alla vittima di fornire i propri dati ad un operatore.

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

Più specificatamente, per spoofing, nel linguaggio informatico, s'intende la manipolazione dei dati trasmessi in una rete telematica, consistente nella falsificazione del proprio indirizzo IP, oppure nell'utilizzo abusivo di user name e password di altri utenti. In particolare, lo spoofing dell'ID chiamante è la pratica di far sì che la rete telefonica indichi al destinatario di una chiamata che l'originatore della chiamata è una stazione diversa dalla vera stazione di origine.

Il cliente aveva ricevuto una chiamata dal numero verde della banca e da lì erano iniziate le comunicazioni col malfattore, al quale il cliente ha comunicato i codici dispositivi credendo di conferire col funzionario dell'intermediario, a suo dire intervenuto per impedire un accesso abusivo al suo conto corrente.

Sotto questo profilo, l'ABF non ritiene imputabile al consumatore l'ignoranza, circa il funzionamento dei cd. numeri verde e, in particolare, circa l'abilitazione degli stessi alla sola ricezione delle telefonate; al contrario, sarebbe onere (in tal caso, disatteso) dell'Intermediario mettere la clientela al corrente di tali informazioni.

Quindi, la banca avrebbe dovuto avvisare gli utenti di questa circostanza. Risulta invece che tale informativa sia stata diffusa dall'istituto di credito coinvolto ai propri utenti solo dopo i fatti in contestazione.

3. La decisione

In conclusione, l'ABF censura i sistemi di sicurezza dell'intermediario, che considera corresponsabile del danno subito dal cliente e in quanto tale tenuto a rifondere al correntista la metà delle somme distratte dal malfattore.

In punto di diritto, l'ABF ha ritenuto di fissare un concorso di colpa dell'intermediario nella misura del 50%. E' stato quindi riconosciuto che la banca ha contribuito causalmente alla realizzazione dell'evento dannoso, che non può essere addossato in via esclusiva alla colpa del cliente.

È infatti indubbio che il cliente non avrebbe dovuto, contro ogni avvertimento dell'intermediario, comunicare i codici dispositivi a terzi, ma tale negligenza si è accompagnata ad un malfunzionamento del servizio di pagamento o altro inconveniente connesso ai sistemi di sicurezza dell'intermediario, contribuendo

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

alla realizzazione del danno, che altrimenti non si sarebbe prodotto.

Le operazioni dispositive fraudolentemente poste in essere dal malfattore sono quindi state causate sia dall'ingenuità del cliente, sia dal malfunzionamento e dall'inadeguatezza dei sistemi di sicurezza della banca, sui quali si è innestata la colpa del cliente.

Senza l'inadeguatezza del sistema, la colpa del cliente sarebbe stata irrilevante, di qui la condivisione del nesso causale e la compartecipazione alla produzione dell'evento dannoso, che viene posto a carico delle parti in egual misura.

CONSIDERAZIONI FINALI

Ricordiamo che, secondo il disposto dell'art. 10 del d.lgs. 11/2010, come modificato dal d.lgs. 218/2017, qualora l'utilizzatore neghi di aver autorizzato un'operazione di pagamento eseguita, grava sull'intermediario l'onere di provare l'avvenuta autenticazione della medesima operazione, la sua corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Tale prova –precisa il comma 2 del citato articolo- non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi sul medesimo gravanti, essendo onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente.

Nel caso di mancato assolvimento dell'onere probatorio di cui si è detto, l'intermediario è obbligato a riaccreditarne l'importo sul conto del cliente, ai sensi dell'art. 11 del medesimo d.lgs. n. 11/2010.

Secondo la prevalente giurisprudenza dell'ABF, il sistema a due fattori induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, che la banca abbia assolto all'onere sulla stessa gravante ai sensi della disposizione sopra citata, e che il cliente si sia reso gravemente inadempiente all'obbligo di custodire con la dovuta diligenza i dispositivi personali per l'utilizzo del sistema di pagamento.

Quindi, una volta dimostrato che il cliente abbia comunicato a terzi i dispositivi personali di accesso all'home banking, si presume la sua colpa grave.

LÈGISTER AVVOCATI MILANO
Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it

In questo caso si è invece riusciti a vincere tale presunzione di colpa.

Infatti, con l'ausilio dei LOG della banca, sono stati forniti elementi utili e decisivi per individuare le modalità con le quali è stata realizzata la truffa informatica a danno del cliente.

Questa decisione si discosta dall'orientamento formatosi nella vigenza del sistema "a due fattori" fra loro indipendenti, che si è rivelato necessario ma non sufficiente a prevenire frodi e danni allorché la banca abbia compromesso uno dei due livelli di salvaguardia. Il cliente non può quindi essere ritenuto il solo responsabile se la compromissione del sistema sia frutto della reciproca negligenza.

Sembra una soluzione salomonica, ma essa appare equa e corretta anche dal punto di vista strettamente giuridico.

LÈGISTER AVVOCATI MILANO

Via Amedei, 15
20123 Milano
Tel. +39 02 43980804
Fax +39 02 43980825
info@legister.it

www.legister.it