AZIENDABANCA

PAESE :Italia
PAGINE :40;41
SUPERFICIE :196 %
PERIODICITÀ :Mensile□□

DIFFUSIONE :(4000)
AUTORE :Andrea Puccio

► 1 aprile 2024

Spoofing, smishing, vishing. Le nuove frontiere della truffa e i rischi per gli intermediari

Chi si fa carico del danno economico causato dalle truffe telematiche? L'impianto normativo è a favore del cliente e le pronunce dell'ABF sottolineano l'importanza dell'adozione di sistemi di monitoraggio delle potenziali frodi

Da un esame delle più recenti pronunce dell'Arbitro Bancario Finanziario (ABF), emerge come siano ormai sempre più diffuse, nell'ambito dei servizi bancari, tipologie di frodi contraddistinte da una condotta di spoofing, smishing o vishing.
Con spoofing si intende una forma di aggressione informatica che consiste nella sostituzione del numero originario da cui proviene un sms con un testo alfanumerico riconducibile a quello utilizzato dall'intermediario per i propri messaggi genuini.
Lo smishing è una forma di phishing che viene attuata attraverso messaggi di testo con cui le vittime vengono indotte a fornire informazioni sensibili a un terzo aggressore.
Il vishing, invece, ricorre quando la chiamata telefonica effettuata dal falso operatore appare riferibile ad una utenza della banca. In questo caso, purtroppo, accade che alla realizzazione di tali condotte truffaldine concorra il dipendente infedele dell'istituto bancario.

La difficile individuazione degli autori del reato

Fermo restando la rilevanza penale di tali condotte, riconducibili all'alveo delle fattispecie delittuose di truffa e sostituzione di persona ex artt. 640 e 494 c.p., nella maggior parte dei casi l'individuazione degli autori del reato ad opera del Pubblico Ministero, nel corso delle indagini preliminari, risulta di fatto impossibile, con la conseguenza che il danaro sottratto non può essere recuperato. Così, per l'utente/cliente residua solo la possibilità di far valere la responsabilità della Banca.
La disciplina dei servizi di pagamento è, dunque, stata di recente oggetto di molteplici pronunce della giurisprudenza dell'ABF, che si è preoccupata di precisare i principi guida nell'individuazione del soggetto che, di volta in volta, è chiamato a farsi carico del danno economico derivante dalla commissione delle condotte fraudolente.
Il tema non è di secondaria rilevanza: ogni qual volta la condotta di sottrazione delle somme di denaro può dirsi agevolata dal cliente, questi non potrà chiedere la restituzione delle somme asportate. Negli altri casi, invece, l'istituto di credito sarà chiamato a rifondere gli importi oggetto delle condotte delittuose.

Le fonti normative

È, innanzitutto, importante ricordare che le operazioni di pagamento (nello specifico, il trasferimento di fondi senza la consegna materiale del denaro) sono oggetto di una disciplina ad hoc, contenuta nelle Direttive PSD 1 e PSD 2.
Il primo provvedimento - recepito nel nostro ordinamento mediante il d.lgs. n. 11/2010, che ha apportato modifiche al d.lgs. n. 385/1993 - è espressione della volontà delle istituzioni europee di predi-

@ Andrea Puccio,
Founding Partner Puccio Penalisti Associati

AZIENDABANCA

PAESE : Italia
PAGINE :40;41
SUPERFICIE :196 %
PERIODICITÀ : Mensile□□

DIFFUSIONE :(4000)
AUTORE : Andrea Puccio

► **1 aprile 2024**

sporre regole uniformi in ordine ai pagamenti elettronici dell'Eurozona per dare vita ad un mercato unico europeo dei pagamenti al dettaglio (c.d. SEPA).
Alla luce dell'evoluzione tecnologica che ha interessato (anche) il settore degli strumenti di pagamento, si è reso necessario un ulteriore intervento del legislatore comunitario, volto a introdurre livelli di sicurezza idonei a garantire la tutela della clientela mediante la previsione di standard di verifica più elevati, diretti a prevenire un utilizzo fraudolento di tali sistemi.
Queste le ragioni che hanno portato all'emanazione della Direttiva 2015/2366/UE che, come noto, è stata recepita a livello nazionale con il d. lgs. 15 dicembre 2017, n. 218 e ha modificato talune disposizioni del Testo Unico Bancario e del citato d.lgs. 27 gennaio 2010, n. 11.

La giurisprudenza dell'ABF: oneri probatori e criteri di attribuzione del danno economico cagionato dal reato

In base alla normativa in questione, così come interpretata e applicata dall'ABF, due sono i passaggi ineludibili in materia.
In primo luogo, è l'intermediario a dover provare la corretta registrazione e contabilizzazione delle operazioni di pagamento, dovendo, in particolare, fornire evidenza dell'adozione, da parte dell'istituto, di un sistema di autenticazione a due fattori - c.d. "sistema di autenticazione forte" (SCA) - per poter procedere all'effettuazione delle movimentazioni di denaro.
Secondariamente, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può vedersi ascritte le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
Al riguardo, il Collegio di Bari, con decisione n. 388 del 9 gennaio 2024, ha ricordato come la disciplina in esame istituisca "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema".
In altre parole, l'ascrivibilità al cliente dell'onere economico derivante dalle condotte criminose, resta circoscritta ai casi di comportamento fraudolento del medesimo, ovvero all'inadempimento doloso o gravemente colposo, da parte sua, degli obblighi previsti dall'art. 7 del d. lgs. 11/2010, fermo restando che l'onere della prova fa capo all'intermediario.
Tale orientamento dell'ABF ha trovato ripetuto riscontro nella giurisprudenza della Corte di Cassazione, secondo cui è necessario verificare l'adozione, da parte dell'istituto bancario, delle misure idonee a garantire la sicurezza del servizio. Infatti, la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi, come parametro, la figura dell'accorto banchiere.

Adozione di sistemi di monitoraggio e alert

Talune pronunce, come la decisione del Collegio di Bari, n. 12345 del 7 dicembre 2023, pongono l'accento su un ulteriore elemento di carenza spesso ravvisato nell'analisi ex post della condotta tenuta dalla banca, vale a dire la mancata adozione di sistemi di monitoraggio e di alert che dovrebbero essere adottati per intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.d. sospette, in aderenza alle indicazioni contenute nel d.m. 30 aprile 2007, n. 112, adottato in attuazione della l. 17 agosto 2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento".
In conclusione, nonostante non sia possibile stabilire, a priori, se il danno economico ricada in capo all'istituto di credito - con conseguente obbligo alla restituzione della somma fraudolentemente sottratta da terzi al cliente - piuttosto che in capo a quest'ultimo, è, tuttavia, evidente come l'impianto normativo in materia sia stato costruito dal legislatore in maniera favorevole al cliente, seguendo il fin troppo noto schema secondo cui si alloca sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento.

@ Carola Panicali,
Associate Puccio Penalisti Associati

Andrea Puccio
Founding Partner Puccio Penalisti Associati
e **Carola Panicali**
Associate Puccio Penalisti Associati