FERNANDEZADVOCATS

EL FRAU BANCARI DIGITAL: QUI EN SUPORTA LES CONSEQÜÈNCIES?

El *phishing*, el *smishing*, el *vishing* o el *SIM swapping* ja no són paraules estranyes. Cada cop més persones reben missatges de text, correus electrònics o trucades que imiten amb una precisió inquietant la comunicació del seu banc, i moltes acaben cedint les seves credencials o autoritzant transferències que mai haurien volgut fer. Quan això passa, la pregunta que inevitablement es planteja és: qui suporta les pèrdues?

La resposta, afortunadament, és clara en el nostre ordenament jurídic: la legislació espanyola i europea ofereix una protecció sòlida al consumidor. En aquest article expliquem com funciona i per què, en la majoria dels casos, és el banc qui se n'ha de fer càrrec.

1. **El punt de partida: la càrrega de la prova recau sobre el banc.**

El principi estructural del sistema europeu és contundent: quan es produeix una transferència no autoritzada, és el banc qui ha de demostrar que l'operació era legítima, no el consumidor.

L'article 44 del Reial Decret-llei 19/2018, que transposa la Directiva europea PSD, estableix que, quan el client nega haver autoritzat una operació, correspon al proveïdor de serveis de pagament acreditar que l'operació va ser autenticada correctament i que no hi va haver cap fallada tècnica o deficiència del servei. El simple fet que el sistema informàtic del banc hagi registrat l'operació com a completada no és suficient per demostrar ni que el client la va autoritzar ni que va actuar amb negligència greu.

Així ho ha ratificat el Tribunal Suprem en la Sentència 571/2025, de 9 d'abril, que és avui el pronunciament de referència en la matèria. I el mateix principi és compartit, amb matisos, per la jurisprudència francesa, italiana i d'altres ordenaments europeus: el proveïdor de serveis de pagament no pot limitar-se a invocar el registre informàtic de la transacció per negar el reemborsament.

2. Un règim de responsabilitat quasi objectiva.

El sistema europeu estableix el que la doctrina anomena responsabilitat quasi objectiva del banc. Quan un client nega haver autoritzat una operació, la presumpció legal és que, efectivament, no ho va fer. L'entitat bancària té l'obligació de reemborsar l'import, com a màxim, el dia hàbil següent a tenir-ne coneixement, llevat que pugui demostrar que el client va actuar fraudulentament o amb negligència greu.

A més, el Tribunal Suprem ha aclarit que la "*deficiència del servei*" va molt més enllà dels errors tècnics estrictes: inclou no reaccionar davant senyals evidents de frau, com ara transferències d'import inusual realitzades de forma repetitiva en un període molt breu, accessos des de dispositius desconeguts, o modificacions de claus en horaris atípics. El banc ha d'actuar amb la diligència pròpia d'un "*ordenat i expert comerciant*", un estàndard molt superior al del ciutadà mitjà, i les advertències genèriques a la pàgina web o els missatges informatius estereotipats no satisfan aquesta exigència.

El Reglament Delegat (UE) 2018/389, que complementa la PSD2 en matèria d'autenticació reforçada de client, és igualment exigent: els proveïdors de serveis de pagament han d'implementar mecanismes de supervisió que analitzin el comportament transaccional habitual de l'usuari, el dispositiu utilitzat, l'import de les operacions i els patrons de frau coneguts. Si un banc no detecta que un client que mai ha fet transferències internacionals n'envia repentinament milers d'euros a l'estranger, incompleix el seu deure de supervisió tècnica.

3. La negligència greu: un concepte interpretat molt restrictivament.

La negligència greu és gairebé l'única excusa que pot al·legar el banc per no reemborsar. I els tribunals la interpreten de forma molt restrictiva, pràcticament equiparant-la al dol o al descuit inexcusable.

La pròpia Directiva PSD2 ja ho anticipa: la negligència grava "ha de significar quelcom més que la mera negligència", i l'exemple que n'ofereix el text normatiu és il·lustratiu: guardar les credencials d'accés juntes al dispositiu de pagament, en un format obert i fàcilment detectable per tercers.

Els tribunals espanyols han descartat la negligència greu en supòsits com: fer clic en un enllaç rebut per SMS al mateix fil de missatges legítims del banc, introduir credencials en una pàgina web que reprodueix fidelment l'aparença de l'entitat, proporcionar un codi OTP a qui es fa passar per empleat bancari des d'un número aparentment oficial, o accedir a l'aplicació del banc des d'un dispositiu desconegut en un moment d'alarma fabricat per l'estafador.

El paràmetre de referència és el d'una persona ordinària que confia en l'entorn digital que el seu banc li ha facilitat, no el d'un expert en ciberseguretat. Només en supòsits veritablement extrems, com podrien ser lliurar voluntàriament i conscientment les claus a un tercer de forma reiterada, sense cap element d'engany o amb un engany burd, els tribunals han apreciat negligència greu.

Cal destacar, a més, que aquest estàndard no és uniforme per a tothom: s'adapta al perfil real de cada víctima. L'edat avançada, la manca de formació tecnològica o la poca familiaritat amb la banca digital són factors que els tribunals prenen en consideració per valorar si la reacció davant l'engany era la que s'esperaria d'aquella persona concreta. Una persona gran sense coneixements informàtics que segueix les instruccions de qui es presenta com a empleat del seu banc no pot ser jutjada amb el mateix criteri que un professional del sector tecnològic.

4. Reflexió final.

El marc jurídic espanyol i europeu situa el banc, com a arquitecte i beneficiari del sistema de pagaments digitals, en la posició de garant últim de la seva integritat. Aquesta no és una opció, sinó una obligació legal que dimana directament de la Directiva PSD2 i de la seva transposició a l'ordenament intern.

El disseny del sistema parteix d'una premissa raonable: les entitats financeres són les que desenvolupen, mantenen i lucren d'una infraestructura tecnològica complexa que el consumidor utilitza però no controla. Per tant, han de ser elles qui implementin els mecanismes de detecció i prevenció del frau, i qui n'assumeixin les conseqüències quan

aquests mecanismes fallen o resulten insuficients. El risc tecnològic no es pot traslladar sistemàticament a l'usuari.

Ara bé, aquest marc normatiu, per sòlid que sigui sobre el paper, no sempre es tradueix en una resposta immediata i satisfactòria per part de les entitats bancàries. En la pràctica, no és infreqüent que els bancs deneguin les reclamacions al·legant la negligència del client o simplement invocant que l'operació consta com a autenticada en els seus sistemes. Que la normativa i la jurisprudència s'inclinin per oferir majors garanties a la posició del consumidor no significa que el procés de reclamació sigui sempre senzill o automàtic.

** El present article té caràcter merament divulgatiu i no suposa assessorament jurídic ni compromís d'actualització.*

Per a més informació o assessorament, contacteu amb info@fernandezadvocats.es.