TOSCANA TODAY
ITALIA WEB MAGAZINE

Italian



Frodi bancarie online: come difendersi e quando la banca deve rimborsare

08/09/2026 12:00 · Alberto Foggia

Preferenze privacy

di ALBERTO FOGGIA –

Le frodi digitali non sono più episodi occasionali né truffe grossolane riconoscibili a colpo d'occhio. Oggi si presentano con SMS che sembrano arrivare davvero dalla banca, telefonate da numeri apparentemente ufficiali, link inseriti in conversazioni già esistenti, app malevole, siti clonati e richieste costruite per sfruttare urgenza, paura e fiducia. Le tecniche più diffuse – phishing, smishing, vishing e spoofing – hanno tutte un tratto comune: spingere il cliente a collaborare inconsapevolmente alla sottrazione di denaro o credenziali.

Ma essere caduti in una trappola ben congegnata non significa, automaticamente, perdere ogni tutela. La normativa sui servizi di pagamento e la giurisprudenza più recente impongono infatti alla banca obblighi stringenti di sicurezza, autenticazione e controllo, e non le consentono di scaricare con leggerezza sul correntista il peso economico della frode.

Non basta alla banca dire: "l'operazione risulta correttamente eseguita"

Questo è il primo punto da chiarire. Quando il cliente nega di aver autorizzato un pagamento, la legge stabilisce che è la banca – o comunque il prestatore di servizi di pagamento – a dover provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata, e che non vi sono stati malfunzionamenti o inconvenienti del sistema.

La normativa al riguardo è ancora più netta laddove precisa che il semplice utilizzo delle credenziali o dello strumento di pagamento non basta, da solo, a dimostrare che il cliente abbia davvero autorizzato l'operazione, né che abbia agito con dolo o colpa grave. Anche la prova della frode o della grave negligenza dell'utente grava sull'intermediario.

In altre parole, se il correntista disconosce un bonifico, un prelievo o un pagamento, la banca non può cavarsela limitandosi a dire che "risultano usati i codici giusti" oppure che "l'accesso è avvenuto dal dispositivo del cliente". Deve fornire una prova più completa e dimostrare di aver adottato tutte le misure richieste dalla diligenza tecnica dell'accorto banchiere.

La responsabilità della banca rientra nel suo rischio professionale

La Suprema Corte di Cassazione è da tempo chiara: nelle operazi
strumenti elettronici, il rischio che terzi riescano a utilizzare co

Preferenze privacy

del cliente rientra, in linea generale, nell'area del rischio professionale dell'intermediario, salvo il caso in cui emerga il dolo del cliente o un comportamento talmente incauto da non poter essere prevenuto in anticipo.

Questo orientamento ha una conseguenza pratica molto importante. La banca, quale professionista del settore, è tenuta a predisporre sistemi idonei non solo a registrare formalmente l'operazione, ma anche a verificare se quell'operazione sia davvero riconducibile alla volontà del cliente. La sua diligenza è una diligenza tecnica, qualificata, più intensa di quella richiesta al normale utente.

Quando scatta il diritto al rimborso

Se un'operazione è non autorizzata, il prestatore di servizi di pagamento deve rimborsare il cliente immediatamente e, comunque, entro la fine della giornata operativa successiva a quella in cui viene a conoscenza dell'operazione o riceve la contestazione, salvo motivato sospetto di frode da comunicare per iscritto.

Questo significa che, sul piano normativo, il sistema è costruito in favore del cliente vittima di un'operazione abusiva. Naturalmente, perché la tutela possa essere fatta valere in modo efficace, occorre che il correntista contesti tempestivamente i movimenti e ricostruisca quanto accaduto con la massima precisione possibile.

La "colpa grave" del cliente non si presume

È proprio qui che si gioca gran parte del contenzioso. La banca, per sottrarsi all'obbligo di rimborso, tende spesso a sostenere che il cliente abbia agevolato il truffatore: cliccando su un link, comunicando un OTP, autorizzando un accesso in app, seguendo istruzioni telefoniche o ignorando segnali sospetti.

Tuttavia la colpa grave non può essere affermata in automatico. La PSD2 e il d.lgs. 11/2010 richiedono un accertamento concreto, caso per caso, e impongono comunque alla banca di provare la negligenza grave dell'utente.

Per questo la giurisprudenza ha dato risposte differenziate.

Ci sono casi in cui il cliente ottiene il rimborso pieno

Accade quando la banca non prova in modo rigoroso la corretta autenticazione o non dimostra di aver predisposto adeguati sistemi di sicurezza e di controllo.

Ci sono casi in cui viene riconosciuto un concorso di colpa

È la soluzione oggi molto frequente nei casi più insidiosi, specie quando il correntista è stato agganciato da messaggi apparentemente genuini o da telefonate

Preferenze privacy

provenienti da numeri che sembravano riconducibili alla banca. In queste ipotesi, il cliente può aver tenuto una condotta imprudente, ma anche l'intermediario può aver contribuito causalmente al danno per carenze organizzative o per mancato rilievo di evidenti anomalie.

E ci sono casi in cui il rimborso viene negato

Soprattutto quando emerge una cooperazione decisiva del cliente alla frode, come l'inserimento volontario di codici o l'autorizzazione di operazioni in un contesto che avrebbe dovuto apparire chiaramente sospetto, e quando la banca riesce a dimostrare la piena regolarità del proprio sistema di autenticazione forte.

Il punto centrale: che cosa deve dimostrare davvero la banca

La banca deve vincere una duplice prova.

Da un lato, deve dimostrare che le operazioni sono state autenticate, registrate e contabilizzate correttamente, senza malfunzionamenti.

Dall'altro lato, se vuole attribuire il danno al cliente, deve provare che quest'ultimo abbia violato con dolo o colpa grave i propri obblighi di custodia e corretto utilizzo dello strumento di pagamento.

È qui che molti contenziosi si aprono davvero. Perché dimostrare la mera regolarità "tecnica" dell'accesso non equivale a provare la genuina volontà del cliente. Lo ha ribadito anche la giurisprudenza europea: l'apparente regolarità formale della procedura non basta, se manca la prova che il consenso sia stato realmente espresso secondo le modalità concordate.

L'autenticazione forte aiuta la banca, ma non la salva sempre

L'autenticazione forte del cliente – la cosiddetta SCA – rappresenta uno degli snodi principali. La normativa richiede normalmente almeno due fattori tra conoscenza, possesso e inerenza.

Se la banca non esige un'autenticazione forte, il cliente – salvo frode – non sopporta alcuna perdita.

Ma anche quando la SCA esiste, non sempre questo chiude la partita a favore dell'intermediario. Le decisioni più avvertite chiariscono che la prova dell'autenticazione forte è necessaria, ma non sempre sufficiente: occorre sempre verificare il contesto concreto, il tipo di frode, la presenz

Preferenze privacy

dispositivo usato, la comparsa di nuovi device, l'anomalia dell'operatività e la capacità del sistema di intercettare movimenti sospetti.

Le operazioni anomale devono far scattare controlli e protezioni

Un altro tema decisivo riguarda l'operatività palesemente anomala. Più bonifici in pochi minuti, importi ripetuti, beneficiari sconosciuti, causali seriali, movimenti verso l'estero o svuotamento improvviso del conto sono tutti indici che, in molte decisioni, hanno portato a riconoscere almeno una responsabilità concorrente della banca.

È vero che non esiste un obbligo assoluto di blocco preventivo di ogni operazione inconsueta; ma quando gli indici di frode diventano macroscopici, l'intermediario non può rimanere passivo. In tali casi vengono in rilievo gli obblighi di protezione, correttezza e buona fede nell'esecuzione del rapporto.

Attenzione: non tutte le frodi sono trattate allo stesso modo

Sul piano pratico, è utile distinguere almeno tre situazioni.

1. Operazione eseguita interamente dal truffatore

È l'ipotesi classica di sottrazione di credenziali, accesso abusivo, SIM swap, installazione di app malevole o presa di controllo del conto. Qui il cliente, se contesta tempestivamente e la banca non prova la colpa grave, ha generalmente buone possibilità di ottenere il rimborso.

2. Operazione eseguita dal cliente, ma sotto raggiro

È il caso più complesso: il cliente viene convinto a fare lui stesso il bonifico o a confermare dispositivi e operazioni in app. In questo scenario alcune decisioni negano la tutela propria delle operazioni "non autorizzate", ritenendo che l'ordine sia stato comunque disposto personalmente dall'utente, sia pure con volontà viziata. Altre, invece, valorizzano la sofisticazione del raggiro e il comportamento della banca, arrivando a riconoscere un rimborso almeno parziale per concorso di colpa.

3. Operazione seguita da contestazione tardiva

Anche il tempo conta. La comunicazione alla banca deve avvenire senza indugio e comunque entro 13 mesi dall'addebito. Una protratta inerzia del cliente, specie se avrebbe potuto accorgersi prima dell'anomalia controllando il co
può incidere pesantemente sulla decisione e, nei casi più gravi, e

Preferenze privacy

Che cosa deve fare subito il correntista truffato

Sul piano concreto, il comportamento immediatamente successivo alla frode è spesso determinante. Le prime mosse corrette sono queste:

- bloccare subito carte, app, token e accessi all'home banking;
- contattare immediatamente la banca e formalizzare il disconoscimento;
- conservare ogni prova, senza cancellare SMS, email, screenshot, URL, registro chiamate e notifiche push;
- presentare denuncia con una ricostruzione cronologica dei fatti;
- inviare un reclamo scritto alla banca, preferibilmente in forma documentabile.

Questa attività non è un mero formalismo: serve a cristallizzare il fatto, a dimostrare la tempestività della reazione e a mettere l'intermediario di fronte ai propri obblighi di rimborso e di prova.

Quali difese può far valere il cliente

Dal punto di vista pratico e giuridico, il cliente che contesta una frode bancaria può far leva su alcuni argomenti ricorrenti:

- contestare la mancata prova rigorosa dell'autenticazione;
- contestare la mancata prova della colpa grave;
- eccepire l'assenza o l'inadeguatezza di alert e sistemi di sicurezza;
- evidenziare il carattere sofisticato e ingannevole della truffa;
- valorizzare la tempestività del reclamo e della denuncia;
- mettere in luce l'eventuale anomalia dell'operatività contestata.

Spesso la differenza fra rigetto e accoglimento della domanda sta proprio nella qualità della ricostruzione documentale: chi conserva gli SMS civetta, gli screenshot della chat, il numero del chiamante, i log del telefono e le notifiche ricevute si trova in una posizione molto più forte rispetto a chi si limita a un generico disconoscimento.

In conclusione

Le frodi bancarie online non sono un terreno senza regole, né un ambito in cui il cliente resta sempre e comunque soccombente. Il sistema normativo vigente pone a carico della banca obblighi precisi: deve garantire sicurezza, pretendere autenticazione forte, rimborsare le operazioni non autorizzate e, se vuole negare il ristoro, provare davvero la frode o la colpa grave del cliente.

Preferenze privacy

Per il correntista, la regola pratica resta una: agire subito. Bloccare, documentare, contestare. Perché nelle frodi digitali il danno economico nasce in pochi istanti, ma la possibilità di recuperarlo dipende quasi sempre da ciò che si fa nelle ore immediatamente successive.

Per approfondire tutti gli aspetti giuridici e pratici legati alle frodi telematiche e alla tutela del correntista, si consiglia la lettura di ***«La rete che inganna: truffe online, come difendersi – aspetti pratici e giuridici»****, scritto dall'Avv. Alberto Foggia unitamente ad altri colleghi dell'Associazione ADUSBEF. Il volume è disponibile su Amazon al seguente link:https://www.amazon.it/inganna-difendersi-aspetti-pratici-giuridici/dp/8894863158*



Alberto Foggia

Alberto Foggia è avvocato esperto di diritto bancario e di composizione delle crisi da sovraindebitamento.

Privacy Policy

Cookie Policy
Termini e
Condizioni

TOSCANA TODAY

Edito da Toscana Today News & Media con sede a Zurigo (Svizzera), Dolderstrasse 62 (8031) VAT/P.IVA= CHE 219.143.708 - Impresa editoriale iscritta al Registro delle Imprese di Zurigo Designed by WPZOOM

Privacy Policy Cookie Policy Termini e Condizioni

Preferenze privacy