

Furto d'identità e frodi social: come riconoscerli, come difendersi e cosa fare se sei vittima

Autore: redazione

Data: 03/10/2026



di Alberto Foggia

Pisa, 3 ottobre 2026. Ogni giorno, migliaia di cittadini italiani si trovano a fare i conti con una realtà sempre più diffusa e insidiosa: qualcuno ha usato il loro nome, la loro foto, i loro documenti per aprire un conto corrente, disporre bonifici, contrarre debiti o commettere truffe ai danni di terzi. In altri casi, la vittima si accorge – spesso troppo tardi – che i propri risparmi sono stati sottratti attraverso un SMS apparentemente inviato dalla propria banca, o che un finto operatore bancario l'ha convinta a comunicare i propri codici di accesso.

Questo articolo si propone di spiegare in modo chiaro e accessibile cosa sono il furto d'identità e le frodi social, quali tutele offre l'ordinamento a chi ne è vittima, e come prevenire questi fenomeni grazie anche a indicazioni pratiche ricavabili dalla giurisprudenza più recente.

Cos'è il furto d'identità

Il furto d'identità consiste nella raccolta e nell'utilizzo illecito di dati personali altrui – nome, cognome, data di nascita, codice fiscale, foto, documenti d'identità – allo scopo di commettere frodi. Le modalità sono molteplici: apertura di conti correnti a nome della vittima, richiesta di finanziamenti, acquisti online, clonazione di profili social, operazioni bancarie non autorizzate.

Ciò che rende questo fenomeno particolarmente pericoloso è che la vittima spesso non si accorge di nulla finché non riceve una comunicazione da un istituto di credito, un atto giudiziario o una notifica di addebito per operazioni che non ha mai compiuto. In alcuni casi, la scoperta avviene addirittura nel momento in cui si viene iscritti in banche dati dei cattivi pagatori o si viene raggiunti da un avviso di garanzia.

Le principali tecniche di frode: smishing, vishing, spoofing e social engineering

È fondamentale conoscere le tecniche più diffuse per poterle riconoscere.

Smishing

Si tratta di un SMS fraudolento che induce l'utente a cliccare su un link, chiamare un numero o inserire dati riservati su un sito clone della propria banca. Il messaggio può apparire nella stessa conversazione degli SMS genuini dell'istituto di credito (il c.d. SMS spoofing), rendendo il raggirio particolarmente credibile.

Vishing

Contatto telefonico in cui il truffatore si presenta come operatore bancario o come "funzionario dell'ufficio antifrode" della banca per ottenere codici OTP, PIN o credenziali di accesso. Spesso la chiamata proviene da un numero che sul telefono della vittima appare identico a quello ufficiale della banca (caller ID spoofing).

Spoofing

Contraffazione del mittente di un messaggio o di una telefonata. Il messaggio sembra provenire dalla propria banca; in realtà, è opera di truffatori. Il meccanismo può estendersi alla registrazione di un nuovo dispositivo sull'app di mobile banking della vittima, con conseguente piena disponibilità del conto da parte del frodatore.

Social engineering e frodi sui social

Sui social network il furto può avvenire tramite profili falsi (catfishing), quiz e contest che raccolgono risposte alle domande di sicurezza, link o QR code malevoli che conducono a siti clone per rubare credenziali, messaggi privati contenenti richieste di documenti o selfie

per false opportunità di lavoro. L'utilizzo sempre più diffuso di deepfake e intelligenza artificiale generativa aumenta ulteriormente la capacità di inganno.

Un caso emblematico, analizzato dalla giurisprudenza dell'Arbitro Bancario Finanziario, è quello in cui ignoti hanno aperto due conti correnti online a nome di una persona completamente ignara, utilizzando una foto con documenti ottenuta mediante un annuncio di lavoro fasullo pubblicato sui social. La vittima si è poi trovata coinvolta in procedimenti penali per le truffe commesse dai malfattori a suo nome.

Il quadro normativo: le tutele previste dalla legge

Il D.Lgs. n. 11/2010 e la PSD2: la protezione delle operazioni di pagamento

La principale tutela per il cittadino vittima di operazioni bancarie non autorizzate è contenuta nel D.Lgs. 27 gennaio 2010, n. 11, che ha recepito la direttiva europea sui servizi di pagamento (PSD) e che è stato poi aggiornato con il D.Lgs. n. 218/2017 in attuazione della PSD2 (Direttiva UE 2015/2366).

Il principio fondamentale è chiaro: quando un utente disconosce un'operazione di pagamento, l'onere della prova grava sulla banca, non sul cliente. L'art. 10 del D.Lgs. n. 11/2010 stabilisce: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti."

Ma non basta: anche quando la banca dimostra la corretta autenticazione formale dell'operazione, ciò non è sufficiente ad escludere la propria responsabilità. Il comma 2 dello stesso articolo precisa che la banca deve anche fornire la prova della frode, del dolo o della colpa grave dell'utente. Il Collegio di Coordinamento dell'ABF, con la decisione n. 22745/2019, ha chiarito in modo definitivo che: "La produzione documentale diretta a fornire la dimostrazione dell'autenticazione e della formale regolarità dell'operazione contestata non esaurisce, di per sé, l'onere probatorio, in quanto è indispensabile che l'intermediario provveda specificatamente ad indicare una serie di elementi di fatto caratterizzanti le modalità esecutive dell'operazione, sulla cui base possa trarsi la prova della colpa grave dell'utente."

In altre parole: la banca non si libera dalla responsabilità semplicemente mostrando i propri log informatici. Deve provare concretamente che il cliente ha agito con grave negligenza.

La Strong Customer Authentication (SCA)

La PSD2 ha introdotto l'obbligo di autenticazione forte del cliente (Strong Customer Authentication – SCA), che impone alla banca di verificare l'identità dell'utente tramite almeno due elementi indipendenti tra loro, appartenenti alle categorie di: conoscenza (qualcosa che solo l'utente sa, come il PIN), possesso (qualcosa che solo l'utente ha,

come il dispositivo mobile), inerenza (qualcosa che caratterizza l'utente, come il riconoscimento biometrico).

L'art. 12, comma 2-bis del D.Lgs. n. 11/2010 è esplicito: "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Se la banca non ha attivato la SCA, la perdita è interamente a suo carico.

Quando il cliente perde la tutela: la colpa grave

La protezione dell'utente viene meno quando questi abbia agito con dolo o colpa grave. In tal caso, ai sensi dell'art. 12, comma 4, del D.Lgs. n. 11/2010, l'utente sopporta tutte le perdite derivanti dall'operazione non autorizzata.

La giurisprudenza ha progressivamente definito cosa costituisce colpa grave. Sono esempi tipici:

- Comunicazione di codici OTP o PIN a terzi che si spacciano per operatori bancari.
- Clic su link in SMS il cui URL non è riconducibile al dominio ufficiale della banca.
- Conservazione congiunta di carta e PIN nel portafoglio.

Diversamente, quando la frode è tecnicamente sofisticata – come nel caso del caller ID spoofing combinato con SMS spoofing che inserisce il messaggio nella chat genuina della banca – la giurisprudenza tende ad escludere la colpa grave del cliente. Il Tribunale di Monza (Sentenza n. 91/2026) ha condannato la banca al rimborso di 40.000 euro, rilevando che i log della banca non dimostravano la corretta autenticazione e che la sofisticazione della truffa (reindirizzamento delle comunicazioni, registrazione di un nuovo dispositivo) non era riconducibile a un comportamento negligente del correntista (cfr. Tribunale di Monza, Sez. I, 20 gennaio 2026, n. 91).

Il furto d'identità e gli obblighi antiriciclaggio delle banche

Un profilo spesso trascurato riguarda il caso in cui il furto d'identità porti all'apertura di conti a nome della vittima da parte di ignoti. In questa ipotesi, la tutela del cittadino si fonda sugli obblighi di adeguata verifica della clientela imposti alle banche dal D.Lgs. n. 231/2007 (normativa antiriciclaggio).

Gli artt. 18 e 19 del D.Lgs. n. 231/2007 obbligano gli intermediari a identificare e verificare l'identità del cliente prima di instaurare qualsiasi rapporto. Quando il cliente non è fisicamente presente (apertura del conto online), le banche devono adottare misure rafforzate di identificazione a distanza, che possono includere riconoscimento biometrico affidabile, selfie verificato contestualmente con procedure tecnologicamente robuste, o bonifico proveniente da un conto precedentemente identificato di persona.

Il Collegio di Coordinamento dell'ABF, con la decisione n. 6070/2024, ha stabilito un principio di fondamentale importanza: "Integra una 'controversia con la clientela' ai sensi dell'art. 128-bis t.u.b. – e, quindi, rientra nella competenza dell'Arbitro Bancario Finanziario – l'ipotesi nella quale la parte ricorrente chiedi il risarcimento dei danni subiti per effetto di

una truffa che abbia comportato l'apertura a suo nome di un conto corrente fittizio mediante furto di identità.”

Questo significa che anche chi non ha mai avuto alcun rapporto con la banca può rivolgersi all'ABF per ottenere il risarcimento, se l'intermediario ha aperto un conto a suo nome con procedure inadeguate. La vittima di furto d'identità è considerata “cliente” ai fini della tutela, poiché nei suoi confronti esistono specifici obblighi di protezione da parte dell'intermediario.

Il ruolo degli SMS alert e la responsabilità della banca

Un ulteriore profilo di responsabilità dell'intermediario riguarda l'attivazione del servizio di SMS alert (o notifiche equivalenti). Il Collegio di Coordinamento ABF ha chiarito, con la decisione n. 24366/2019, che la banca ha l'obbligo di fornire il servizio di SMS alert, da cui può essere esonerata solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene.

Quando la banca non attiva tali avvisi, e le operazioni fraudolente si susseguono nel tempo, essa non può andare esente da responsabilità per le operazioni successive alla prima. L'ABF (Decisione n. 2427/2026) ha applicato questo principio condannando la banca a rimborsare le operazioni compiute a partire dalla seconda tranche di prelievi illeciti, avvenuti il giorno successivo al furto della carta, poiché la disponibilità degli alert avrebbe consentito al cliente di segnalare tempestivamente l'accaduto.

L'Arbitro Bancario Finanziario: uno strumento rapido ed efficace

L'Arbitro Bancario Finanziario (ABF) è un sistema di risoluzione stragiudiziale delle controversie in materia bancaria e finanziaria, gratuito per l'utente (salvo il versamento di € 20 come contributo spese, rimborsato in caso di accoglimento del ricorso). È competente per controversie fino a € 200.000 e costituisce spesso il primo strumento da attivare.

Le sue decisioni non sono vincolanti come le sentenze di un tribunale, ma gli intermediari che non vi ottemperano vengono esposti alla pubblicazione del proprio inadempimento sul sito dell'ABF, uno strumento reputazionale molto efficace. In molti casi, la pronuncia favorevole dell'ABF precede o sostituisce l'azione giudiziaria.

Cosa fare prima, durante e dopo

Prima: prevenzione

a) Non comunicare mai codici OTP, PIN, password o credenziali di accesso a nessuno, nemmeno a chi si presenta come operatore della vostra banca: nessuna banca li chiede per telefono, SMS o email.

- b) Non cliccare mai su link contenuti in SMS o email che sembrano provenire dalla banca. Digitate sempre manualmente l'indirizzo ufficiale o usate l'app ufficiale scaricata dagli store certificati.
- c) Verificate l'URL prima di inserire dati su qualsiasi sito: anche se il messaggio è arrivato nella chat "vera" della banca, il link potrebbe condurre a un sito clone.
- d) Non condividete foto dei vostri documenti sui social o in risposta ad annunci di lavoro non verificati: potrebbero essere usate per aprire conti a vostro nome.
- e) Attivate gli SMS alert e le notifiche push per ogni operazione sul conto: sono fondamentali per accorgersi tempestivamente di movimenti non autorizzati.
- f) Controllate periodicamente l'estratto conto e verificate che non esistano rapporti bancari aperti a vostro nome che non riconoscete.
- g) Tenete aggiornati il sistema operativo del telefono e del PC, e usate un antivirus affidabile.

Come riconoscere la truffa

- Un messaggio o una telefonata crea un senso di urgenza: "Il suo conto è a rischio, agisca subito". Questo è il primo segnale di allarme.
- Vi viene chiesto di installare un'app o di fornire un codice ricevuto via SMS. Non fatelo.
- Qualcuno vi contatta per avvertirvi di "movimenti sospetti" e vi chiede di "mettere in sicurezza" il denaro trasferendolo su un altro conto. È una truffa classica.

Dopo: cosa fare immediatamente se siete vittima

- a) Bloccate immediatamente la carta, il conto o lo strumento di pagamento compromesso, chiamando il numero verde della banca.
- b) Raccogliete tutte le prove: screenshot di messaggi, SMS, email, chiamate (numeri e orari), URL visitati. Non cancellate nulla.
- c) Presentate denuncia-querela alla Polizia Postale, con la cronologia precisa di tutti gli eventi. La tempestività è essenziale.
- d) Inviare un reclamo formale alla banca (preferibilmente via PEC o raccomandata A/R), allegando la denuncia e richiedendo il rimborso ai sensi degli artt. 10 e 12 del D.Lgs. n. 11/2010. La banca ha 30 giorni per rispondere (15 giorni per i casi più semplici).
- e) Se la risposta è negativa o assente, presentate ricorso all'ABF entro 12 mesi dalla data del reclamo.
- f) In caso di furto d'identità con apertura di conti a vostro nome, segnalate l'accaduto anche al Garante per la protezione dei dati personali.

La distribuzione dell'onere della prova: un elemento cruciale

La Corte di Cassazione ha più volte ribadito che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici ha natura contrattuale e viene esclusa solo se ricorre una situazione di colpa grave dell'utente. Questo significa che:

- se la banca non riesce a provare né la corretta autenticazione né la colpa grave del cliente, deve rimborsare integralmente le somme sottratte;
- se la banca prova la corretta autenticazione ma non la colpa grave, la responsabilità rimane sua;
- solo se la banca dimostra entrambi gli elementi è possibile escludere il rimborso o ridurlo proporzionalmente al concorso di colpa delle parti.

Il Tribunale di Trieste (Sentenza n. 704/2024) ha condannato la banca a restituire euro 27.998, sottolineando che “la responsabilità del prestatore del servizio viene affermata anche quando non sia individuabile la causa dell'addebito perché dalle prove acquisite non emergano elementi utili per ricostruire la dinamica dell'operazione non autorizzata (c.d. 'ignoto tecnologico')”.

Conclusione: la consapevolezza è la prima difesa

Il furto d'identità e le frodi social sono fenomeni sempre più sofisticati, ma non inarrestabili. La conoscenza delle tecniche utilizzate dai truffatori, la comprensione delle proprie tutele legali e l'adozione di comportamenti prudenti nella vita digitale quotidiana rappresentano gli strumenti più efficaci di prevenzione.

L'ordinamento italiano, in linea con quello europeo, offre una tutela significativa: la banca non può limitarsi a dimostrare di aver rispettato le procedure tecniche, ma deve provare concretamente la colpa grave del cliente. Se non ci riesce, rimborsa. Chi invece, nonostante tutto, dovesse cadere vittima di una frode, ha a disposizione strumenti rapidi ed efficaci – a partire dal reclamo alla banca e dal ricorso all'ABF – per ottenere giustizia senza necessariamente intraprendere una lunga battaglia giudiziaria.

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>