

Crypto-truffe e piattaforme abusive di trading: la prima difesa è una denuncia immediata, completa e tecnicamente costruita

Autore: redazione

Data: 17/10/2026



di Alberto Foggia

Pisa, 17 ottobre 2026. Nelle frodi finanziarie online il tempo è tutto. Prima ancora della causa civile, conta agire subito con banca, autorità giudiziaria e organi di vigilanza.

Perché quando il denaro prende la via di conti esteri, società-schermo o wallet in criptovalute, ogni giorno perso può rendere il recupero molto più difficile.

Il copione è quasi sempre lo stesso.

Una telefonata, un annuncio sui social, un sito dall'aspetto professionale, un sedicente broker che promette rendimenti elevati e assistenza continua. La vittima versa una prima somma, poi un'altra, poi ancora. Sullo schermo compaiono grafici, profitti apparenti, saldi in crescita. Ma quando arriva la richiesta di prelevare, iniziano gli ostacoli: servono altre commissioni, altre imposte, altri versamenti "per sbloccare il conto". A quel punto, spesso, il denaro è già stato disperso.

La vera urgenza non è la causa civile: è fermare la dispersione del denaro

Quando si scopre di essere stati truffati, l'istinto porta a chiedersi se si possa fare subito causa. La risposta giuridica è sì, ma quella strategica è più prudente: la prima mossa decisiva, nella maggior parte dei casi, è una denuncia-querela tempestiva, dettagliata e ben argomentata, non l'azione civile.

La ragione è concreta. Nelle truffe di trading online i fondi vengono spesso:

- a) trasferiti su conti esteri;
- b) smistati verso più beneficiari;
- c) convertiti in crypto-attività;
- d) fatti transitare su wallet o piattaforme di scambio;
- e) dispersi in tempi brevissimi attraverso una rete di soggetti, prestanome e società di comodo.

Per questo la tempestività non è un dettaglio: è la condizione che può consentire alla Polizia Giudiziaria ed al Pubblico Ministero di intervenire quando i flussi finanziari sono ancora ricostruibili e, in alcuni casi, aggredibili.

Perché la denuncia-querela deve essere costruita bene

Una denuncia generica, limitata a dire “sono stato truffato”, rischia di arrivare tardi e male. In questo tipo di frodi, invece, serve un atto che metta subito gli investigatori nella condizione di lavorare.

In concreto, la denuncia dovrebbe contenere:

- a) la cronologia completa dei fatti;
- b) l'indicazione di date, importi, causali, IBAN e beneficiari dei bonifici;
- c) i nomi usati dai presunti broker;
- d) numeri di telefono, indirizzi email, chat WhatsApp o Telegram;
- e) screenshot della piattaforma e del conto utente;
- f) ricevute dei pagamenti;
- g) eventuali richieste di ulteriori somme per “sblocchi”, “tasse” o “commissioni”;
- h) ogni riferimento a domini web, wallet, società destinatarie e canali di contatto utilizzati dai truffatori.

L'obiettivo non è soltanto formalizzare la notizia di reato, ma offrire una base operativa immediata per ricostruire il percorso del denaro e preservare le prove digitali.

Il valore decisivo di una relazione tecnica informatica allegata alla denuncia

La denuncia dovrebbe essere accompagnata da una relazione tecnica di un esperto del settore informatico o informatico-forense. Il che consente di supportare l'attività investigativa con competenze idonee a leggere flussi bancari, dati telematici e passaggi verso il mondo crypto.

Infatti, una relazione tecnica ben fatta può aiutare a: (i) ricostruire il percorso dei bonifici; (ii) individuare eventuali passaggi verso exchange o wallet di criptovalute; (iii) mappare domini, hosting, provider, server, email e numeri VoIP; (iv) conservare e classificare chat, metadati, screenshot e header delle comunicazioni; (v) segnalare quali dati debbano essere richiesti urgentemente a banche, provider e piattaforme; (vi) orientare le richieste investigative su log di accesso, autenticazioni e tracciati informatici.

Il punto è semplice: il tecnico non sostituisce la Polizia Giudiziaria, ma può fornire un supporto specialistico che rende l'indagine più rapida, più precisa e più utile nella fase iniziale, quella in cui il tempo conta davvero.

Sequestro preventivo, log informatici e cooperazione internazionale: perché la via penale viene prima

La sede penale ha un vantaggio operativo evidente: il Pubblico Ministero dispone di strumenti che il privato non ha.

Tra questi:

- a) la richiesta di sequestro preventivo ex art. 321 c.p.p. su conti, wallet, domini e proventi del reato;
- b) l'acquisizione di documentazione bancaria e telematica;
- c) l'attivazione di canali di cooperazione giudiziaria internazionale;
- d) la possibilità di rivolgere richieste urgenti a intermediari, piattaforme, provider e autorità estere;
- e) la valorizzazione investigativa dei log informatici e dei dati di autenticazione, particolarmente importanti nelle operazioni digitali.

Sono utili anche segnalazioni all'Interpol, in funzione dell'attivazione di canali di rapido congelamento internazionale dei fondi, nonché agli organismi europei e alle autorità di vigilanza estere competenti.

In una truffa transnazionale, questo è spesso il vero spartiacque: bloccare subito è più utile che vincere tardi.

Le prime mosse pratiche: cosa fare nelle prime ore

Chi sospetta di essere caduto in una crypto-truffa o in un finto investimento online dovrebbe attivarsi senza ritardo su più piani.

- a) Raccogliere tutto

Bisogna conservare immediatamente:

- email;
- messaggi;
- chat;
- screenshot del sito e dell'area riservata;
- documenti inviati dai presunti broker;
- contabili dei bonifici;
- registri delle chiamate e ogni prova dei contatti.

b) Contattare la banca

Occorre chiedere subito il recall del bonifico. Se il pagamento è avvenuto con carta, va valutata la procedura di chargeback, che secondo la guida operativa può essere attivata entro 13 mesi dall'estratto conto.

c) Presentare denuncia-querela

La denuncia va sporta presso Polizia Postale, Carabinieri, Guardia di Finanza o Procura, allegando tutta la documentazione utile e, se possibile, una relazione tecnica di supporto.

d) Fare segnalazioni alle autorità di vigilanza

La frode va segnalata a Consob, e nei casi transnazionali anche a ESMA e alle autorità estere competenti. Questo può agevolare oscuramenti, blacklist e circolazione delle informazioni.

I reati ipotizzabili

Sul piano penale, i fatti possono integrare diverse fattispecie:

- truffa ex art. 640 c.p., spesso con possibili aggravanti ex art. 61 n. 5 e n. 7 c.p.;
- abusivismo finanziario ex art. 166 TUF quando vengono prestati servizi di investimento senza autorizzazione;
- nei casi più complessi, anche ipotesi di frode informatica e di associazione per delinquere. Questa qualificazione non è solo teorica: incide sulle misure cautelari reali e sugli strumenti investigativi attivabili.

E la banca del cliente? Non sempre risponde

Molte vittime, comprensibilmente, si rivolgono anche alla propria banca, sostenendo che avrebbe dovuto bloccare i pagamenti o segnalare l'anomalia. Ma l'orientamento dell'Arbitro Bancario Finanziario è, in larga parte, sfavorevole quando le operazioni sono state personalmente disposte dal cliente, anche se indotto in errore da un raggiro.

La linea ricorrente è questa: se il pagamento è stato autorizzato dal cliente, non si applica la disciplina delle operazioni non autorizzate di cui al d.lgs. n. 11/2010; inoltre non esiste, in via generale, un obbligo della banca di ingerirsi nelle scelte di investimento del correntista.

La Cassazione con decisione del 2023 ha chiarito che la banca non ha un dovere generale di monitorare tutte le operazioni ordinate dal cliente; un obbligo di protezione può sorgere solo quando ricorrano cumulativamente due presupposti: che l'operazione sia *ictu oculi* anomala e che appaia non rispondente all'interesse del cliente: "nonostante la banca non

abbia alcun dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente, nondimeno, in presenza di circostanze anomale idonee a ledere l'interesse del correntista, questa, in applicazione dei doveri di esecuzione del mandato secondo buona fede, deve rifiutare l'esecuzione o almeno informare il cliente”.

E ancora: “tale obbligo di protezione si attiva alla ricorrenza cumulativa di due presupposti: che l'operazione sia *ictu oculi* anomala e che non risponda agli interessi del cliente”.

Questo significa che l'azione contro la propria banca non è impossibile, ma è spesso difficile, soprattutto se il cliente ha effettuato i bonifici o i pagamenti con piena operatività personale.

Il giudizio civile esiste, ma viene dopo

La via civile resta assolutamente praticabile, ma nella strategia concreta va spesso collocata in secondo piano rispetto all'urgenza penale. Il motivo è operativo: anche quando si ottiene una sentenza favorevole, resta poi da eseguirla contro società estere, conti già svuotati, prestanome o veicoli societari creati solo per raccogliere denaro.

Ciò detto, gli strumenti civilistici ci sono e stanno trovando crescente riconoscimento nei tribunali.

a) Ripetizione dell'indebito ex art. 2033 c.c.

Quando il denaro è stato versato senza un valido titolo giuridico, la vittima può chiedere la restituzione delle somme come pagamento indebito.

b) Nullità del contratto ex art. 23 TUF

Quando viene prospettato un rapporto di investimento, entra in gioco anche l'art. 23 TUF: i contratti relativi alla prestazione di servizi di investimento devono rispettare precisi requisiti formali a pena di nullità.

Ma il vero problema è trasformare la sentenza in denaro recuperato

Qui sta il punto centrale. Sul piano del diritto, l'azione civile può essere solida. Sul piano pratico, però, il risultato dipende dalla possibilità di:

- rintracciare un soggetto realmente esistente e solvibile;
- notificare efficacemente all'estero;
- evitare che la società sia una mera scatola vuota;
- trovare beni o conti ancora capienti al momento dell'esecuzione.

Ecco perché, nelle truffe finanziarie online, la via civile è spesso complementare o successiva, mentre la vera partita si gioca all'inizio, quando la Procura può ancora chiedere sequestri, acquisire tracciati e agire sui canali internazionali.

Il messaggio finale: reagire bene, non solo reagire in fretta

Le crypto-truffe e le piattaforme abusive di trading non si combattono con una sola mossa. Servono rapidità, metodo e qualità della documentazione. Ma soprattutto serve capire che,

in questi casi, la denuncia-querela non è un atto formale: è il perno attorno a cui ruotano le possibilità concrete di recupero.

La raccolta delle prove, il recall bancario, l'eventuale chargeback, la segnalazione a Consob e alle autorità internazionali, il supporto di un tecnico informatico, la richiesta di sequestro dei flussi e delle infrastrutture digitali: tutto questo deve partire subito, in modo coordinato.

La causa civile resta uno strumento importante, soprattutto per far valere la nullità del rapporto o la ripetizione dell'indebito. Ma, nella concreta economia di queste vicende, arriva spesso dopo. E arriva su un terreno già reso difficile dalla volatilità del denaro e dalla dimensione internazionale della frode.

In altre parole: prima si aiuta l'autorità giudiziaria a inseguire il denaro, poi si valuta come consolidare il recupero in sede civile. Nelle truffe online, questa non è solo una scelta tecnica. È, molto spesso, l'unica strategia realistica.

Alberto Foggia, avvocato cassazionista, è alla guida dello Studio Legale Foggia-Americo di Pisa (fondato nel 1965). Specializzato in diritto bancario e finanziario, truffe digitali e procedure di sovraindebitamento, è delegato ADUSBEP per Pisa e provincia, co-curatore della collana "Diritto e Diritti" (Arancia Publishing) e autore di numerosi articoli giuridici. Contatti: foggiamerico@gmail.com | Tel. 050.542786. sito: www.avvocatipisa.com

CATEGORIE

Agenda politica

Consumatori e Allerta Truffe

Cronaca

Giornalisti

I nostri diritti

l'Agenda

L'istruzione e la salute

Lavori in corso

Lavoro e sindacati

Libri
