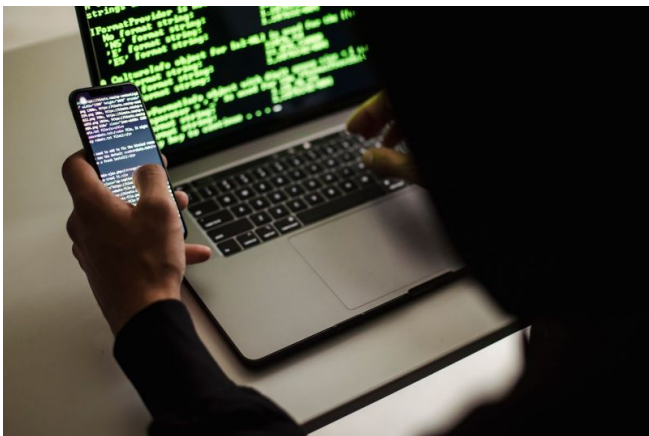


Il bonifico truffa: quando la banca deve restituire i soldi

Autore: redazione

Data: 19/09/2026



di Alberto Foggia

Pisa, 19 settembre 2026. Avete ricevuto via email una fattura dal vostro fornitore di sempre. L'intestazione è quella solita, il logo è identico, persino l'indirizzo email sembra uguale. Solo che qualcuno, nel frattempo, ha modificato il codice IBAN sul quale effettuare il pagamento. Voi pagate, convinti di saldare un debito genuino. Qualche giorno dopo, il vostro fornitore vi chiama: non ha ricevuto nulla. Siete stati vittima di una truffa informatica nota come Business Email Compromise (BEC) o truffa della fattura.

Come funziona la truffa

Il meccanismo è semplice quanto insidioso. Un criminale informatico si inserisce nella corrispondenza email tra due soggetti (ad esempio tra un'azienda e un suo fornitore), intercetta o imita una comunicazione autentica, e modifica l'IBAN indicato nella fattura, sostituendolo con quello di un conto controllato dai truffatori. La vittima, ignara, dispone un bonifico e lo autorizza personalmente. I fondi vengono immediatamente prelevati dal conto del truffatore, spesso svuotato nel giro di poche ore.

Come evidenziato in più pronunce recenti, la peculiarità di questa frode sta nel fatto che l'intrusione avviene prima del pagamento: il cliente dispone il bonifico volontariamente,

inserendo egli stesso l'IBAN (sbagliato) che gli è stato comunicato con l'inganno. I sistemi informatici della banca non vengono violati; è la vittima a eseguire l'operazione.

Il nodo giuridico: il bonifico era “autorizzato”?

Qui si apre la questione centrale. La normativa europea e italiana sui servizi di pagamento (il D.Lgs. n. 11/2010, attuazione della cosiddetta PSD2) distingue in modo netto tra:

- a. operazioni autorizzate: quelle eseguite con il consenso del pagatore;
- b. operazioni non autorizzate: quelle eseguite senza tale consenso.

Solo nel secondo caso la banca è obbligata a rimborsare immediatamente il cliente (cfr. art. 11, D.Lgs. n. 11/2010).

Nel caso della truffa della fattura, il cliente ha personalmente disposto e autorizzato il bonifico, anche se lo ha fatto sulla base di un inganno. Per questo motivo, la giurisprudenza consolidata dell'Arbitro Bancario Finanziario (ABF) e dei Tribunali ha stabilito che queste operazioni non rientrano nella categoria delle “operazioni non autorizzate” e dunque non beneficiano automaticamente del regime di rimborso obbligatorio.

La regola dell'IBAN: la banca non è tenuta a verificare il nome

Un secondo aspetto fondamentale riguarda il ruolo delle banche nell'esecuzione del bonifico. L'art. 24 del D.Lgs. n. 11/2010 stabilisce che, se un ordine di pagamento è eseguito conformemente all'identificativo unico (cioè l'IBAN), esso si ritiene eseguito correttamente, anche se il nome indicato del beneficiario non corrisponde al titolare del conto.

Questo principio – confermato sia dal Collegio di Coordinamento dell'ABF (decisione n. 162/2017) sia dalla Corte di Giustizia dell'Unione Europea (sentenza 21 marzo 2019, causa C-245/18) – vale per entrambe le banche coinvolte: quella dell'ordinante e quella del beneficiario. Nessuna delle due è tenuta, nella vigente normativa, a verificare che il nome indicato nell'ordine di pagamento corrisponda al titolare del conto identificato dall'IBAN.

Questo spiega perché, in molti casi, i ricorsi contro le banche vengono respinti: la banca ha semplicemente eseguito l'ordine del cliente, nel rispetto della normativa.

Del resto, il Regolamento UE 2024/886, già in vigore, introduce l'obbligo per le banche di attivare un servizio di verifica della corrispondenza tra IBAN e nome del beneficiario (Verification of Payee – VOP) prima di eseguire un bonifico. L'intermediario è tenuto ad avvisare il cliente in caso di mancata corrispondenza. Le banche hanno già attivato questo servizio: come ha rilevato l'ABF in una decisione del 2026, l'utente che riceve un avviso di discrepanza e decida comunque di procedere con il bonifico se ne assume la responsabilità (cfr. ABF, Decisione n. 4437/2026).

Quando la banca può rispondere

Nonostante il quadro generale sia sfavorevole per il cliente, esistono situazioni in cui è possibile far valere una responsabilità dell'intermediario. Vediamole.

a) Violazione degli obblighi di adeguata verifica (antiriciclaggio)

Se la banca del beneficiario ha aperto un conto a un soggetto senza effettuare i controlli prescritti dalla normativa antiriciclaggio (D.Lgs. 231/2007), permettendo così che il conto venisse utilizzato per la frode, può rispondere dei danni causati. Secondo l'ABF, Collegio di Napoli, decisione 11 ottobre 2023, n. 9801, l'intermediario non può limitarsi a un'affermazione generica di conformità alla normativa AML, ma deve fornire prova concreta dell'effettiva identificazione del titolare del conto. La mancata adeguata verifica viola, oltre alla normativa antiriciclaggio, i doveri di sana e prudente gestione (artt. 5 e 127 TUB) e i doveri di protezione derivanti dalla buona fede oggettiva e correttezza, e può fondare un nesso causale con il danno subito dall'ordinante, soprattutto laddove l'omissione renda di fatto impossibile rintracciare il truffatore o recuperare le somme.

b) Anomalie manifeste e sistemi antifrode ignorati

Quando l'operazione non è "normale" ma presenta segnali concreti di rischio, la banca non può limitarsi a eseguire meccanicamente l'ordine. Il Tribunale di Torino, con la sentenza n. 4708/2026, ha affermato che l'intermediario è tenuto ad attivarsi quando emergano circostanze idonee a rendere l'operazione sospetta, anomala o incoerente rispetto al profilo del correntista, e che in tali ipotesi i doveri di diligenza professionale (art. 1176, comma 2, c.c.), correttezza e buona fede impongono di effettuare verifiche ulteriori e di instaurare un'interlocuzione con il soggetto legittimato a esprimere la volontà del cliente. La banca che ignori i propri sistemi antifrode interni – i quali avevano già "acceso una spia" – non può poi invocare la regola dell'identificativo unico per sottrarsi a responsabilità.

c) Mancato rispetto degli obblighi di recall e cooperazione

Anche quando la banca non sia responsabile per l'esecuzione originaria del bonifico, rimane comunque tenuta a compiere sforzi ragionevoli per il recupero delle somme attraverso le procedure interbancarie di richiamo (recall) ed a fornire al cliente le informazioni utili per un'eventuale azione di tutela. Il mancato o tardivo avvio della procedura di recall dopo la segnalazione della frode può configurare una responsabilità autonoma dell'intermediario, distinta e indipendente rispetto a quella relativa all'esecuzione dell'ordine.

d) Vulnerabilità del sistema informatico e divergenza tra ordine impartito e ordine eseguito

Vi è infine una fattispecie tecnica distinta dal BEC "puro": quella in cui l'alterazione delle coordinate bancarie non avviene nella fase di comunicazione esterna (via email), ma all'interno del canale di home banking, per effetto di un attacco di tipo *man-in-the-middle*. In questi casi – in cui ciò che il cliente ha ordinato e ciò che la banca ha effettivamente eseguito non coincidono – l'ABF ha ritenuto che la corretta autenticazione tramite OTP non sia sufficiente a escludere la responsabilità dell'intermediario se il sistema presentava vulnerabilità tali da consentire la manipolazione dell'IBAN nella fase di esecuzione (cfr.

ABF, Collegio di Bologna, 21 gennaio 2022, n. 1439). In queste ipotesi, il profilo di responsabilità si sovrappone a quello delle operazioni non autorizzate, con oneri probatori più gravosi per la banca.

Il caso del bonifico disposto “sotto dettatura”

Esiste una fattispecie distinta: quella in cui il truffatore contatta telefonicamente la vittima spacciandosi per un operatore bancario (cosiddetto *vishing* o *spoofing*) e la convince a eseguire bonifici “per bloccare operazioni sospette”. In questo caso, se il pagamento è stato eseguito mentre la vittima stava di fatto seguendo le istruzioni del frodatore – e non era pienamente consapevole di disporre un vero trasferimento di denaro – si può sostenere che il consenso fosse viziato e l’operazione non propriamente “autorizzata” ai sensi della PSD2.

In questi casi la normativa (art. 10 e 12 del D.Lgs. n. 11/2010) impone alla banca di provare che l’operazione sia stata correttamente autenticata con autenticazione forte (SCA), ossia con almeno due fattori indipendenti tra conoscenza, possesso e inerenza. Se la banca non riesce a fornire questa prova, deve rimborsare il cliente indipendentemente da qualsiasi valutazione di colpa.

Tuttavia, se la banca prova l’autenticazione forte, occorre verificare se il cliente abbia agito con colpa grave: ad esempio, comunicando i propri codici OTP a terzi, ignorando avvisi palesemente anomali, o non verificando la genuinità del numero telefonico del presunto operatore.

La posizione del debitore verso il suo creditore

Va affrontata anche un’altra prospettiva: quella del debitore che ha pagato l’IBAN sbagliato. Il pagamento non estingue il debito verso il creditore originario, il quale potrà comunque agire per riscuotere quanto dovuto.

Il debitore può invocare l’art. 1189 c.c. – il pagamento al creditore apparente – per ottenere la liberazione dall’obbligazione, ma solo se prova:

- a. di essere stato in buona fede;
- b. che la sua buona fede era fondata su circostanze univoche (es. email dall’indirizzo esatto del creditore, con documenti identici a quelli abituali);
- c. che il suo errore è stato determinato da un comportamento colposo del creditore stesso (ad esempio per non aver adottato misure di sicurezza informatica adeguate).

Alcuni tribunali hanno applicato questo principio a favore del debitore (cfr. Tribunale di Viterbo, sentenza n. 1172/2024), mentre altri lo hanno negato in presenza di segnali di allerta ignorati (cfr. Tribunale di Ferrara, sentenza n. 15/2026; Tribunale di Rovigo, sentenza n. 372/2026). In quest’ultimo caso, il debitore incauto dovrà pagare due volte – al truffatore e al creditore legittimo – salvo riuscire eventualmente a recuperare le somme in sede penale.

Consigli pratici: come non cadere nella trappola

Prima di eseguire qualsiasi bonifico su coordinate bancarie ricevute via email:

- a. verificate telefonicamente l'IBAN: chiamate il vostro fornitore/creditore su un numero che conoscete già (non quello eventualmente indicato nella stessa email sospetta) e chiedete conferma delle coordinate bancarie;
- b. controllate l'indirizzo email del mittente: i truffatori utilizzano indirizzi quasi identici a quelli reali, con variazioni minime (es. "@mailo.com" invece di "@gmail.com", o un punto aggiunto). Controllate lettera per lettera;
- c. insospettitevi di ogni variazione improvvisa dell'IBAN: un fornitore che non ha mai cambiato le coordinate bancarie e improvvisamente lo fa via email deve essere contattato direttamente. Diffidate anche di IBAN esteri insoliti rispetto alla prassi consolidata;
- d. non fidatevi dei link e degli allegati in email con oggetto sospetto o provenienti da mittenti non verificati: se la vostra casella segnala "{Spam?}" nell'oggetto, questa è già una bandiera rossa;
- e. attivate il servizio di verifica del beneficiario (VOP) con la vostra banca, ove disponibile: se l'IBAN inserito non corrisponde al nome del beneficiario, il sistema vi avviserà prima di confermare il bonifico;
- f. agite immediatamente in caso di frode: se vi accorgete dell'errore, contattate subito la vostra banca per attivare la procedura di *recall* (richiamo del bonifico). Ogni ora è preziosa: i truffatori svuotano i conti in poche ore dall'accredito. Sporgete altresì denuncia-querela presso le autorità giudiziarie o la Polizia Postale;
- g. conservate tutta la documentazione: le email originali e quelle fraudolente, le fatture, le ricevute di bonifico, i log delle comunicazioni: saranno essenziali per qualsiasi azione legale;
- h. per le aziende: adottate procedure interne che prevedano la doppia autorizzazione per i pagamenti sopra soglia e la verifica fuori banda (canale diverso dall'email, es. telefono) di qualsiasi variazione delle coordinate di pagamento di un fornitore.

Conclusione

La truffa della fattura è un fenomeno in crescita che si nutre della nostra fiducia nella tecnologia e nelle comunicazioni digitali. Il diritto offre tutele, ma spesso limitate: la normativa sui servizi di pagamento è costruita per favorire la velocità e l'automazione dei bonifici, non per proteggere chi – anche involontariamente – ha inserito un IBAN sbagliato.

La prevenzione resta lo strumento più efficace. E quando la truffa è già avvenuta, l'intervento immediato – verso la propria banca, verso l'autorità giudiziaria – può fare la differenza tra recuperare i propri soldi e perderli definitivamente.

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 ADUSBEF 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

*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>*

(Foto di Sora Shimazaki da Pexels: <https://www.pexels.com/it-it/foto/ritaglia-lo-sviluppatore-irricoscibile-utilizzando-laptop-e-smartphone-5926389/>)