Diritto del Risparmio

LA MANIPOLAZIONE DEL PAGATORE: IL RISCHIO DELLE FRODI ALLO SPORTELLO.

di Federico CORALLO*

Approfondimenti
fascicolo 3/2025

*Addetto reclami e contenzioso stragiudiziale presso primario Gruppo Bancario. La presente opera viene redatta a titolo puramente personale e non riguarda e/o fa riferimento a casi trattati in ambito professionale.

ISSN 2785-3004

Rivista di Diritto del Risparmio

APPROFONDIMENTI

La manipolazione del pagatore: il rischio delle frodi allo sportello*

di Federico CORALLO**

Settembre
fascicolo 3/2025

---

* Contributo approvato dai *referee*.
** Addetto reclami e contenzioso stragiudiziale presso primario Gruppo Bancario. La presente opera viene redatta a titolo puramente personale e non riguarda e/o fa riferimento a casi trattati in ambito professionale.

La manipolazione del pagatore: il rischio delle frodi allo sportello.

A cura di Federico CORALLO.

SOMMARIO: 1. Tecniche di approccio – 1.1. Il messaggio SMS – 1.2. La telefonata – 1.2.1. Cenni sullo spoofing – 2. L'arrivo in Filiale – 2.1. I sintomi della truffa – 2.2. I controlli da parte della Banca – 2.2.1. La disciplina antiriciclaggio – 2.2.2. Il rifiuto dell'operazione – 3. La truffa svelata: rimedi e consigli – 4. Orientamenti dell'ABF – 4.1. Pagatore vs. Banca ordinante – 4.1.1. Sugli indici di anomalia – 4.2. Pagatore vs. Banca beneficiaria – 4.2.1. Il conto fittizio – 4.2.2. La diversa intestazione del rapporto beneficiario – 4.2.3. Il nuovo servizio di verifica del beneficiario.

Premessa

"Che cos'è l'onestà'" disse Rambert, con aria d'un tratto seria.
"Non so cosa sia in generale. Ma nel mio caso, so che consiste nel fare il mio lavoro".
La peste – Albert Camus (1947)

Chi scrive prende a prestito le parole del saggista francese nel tentativo di dar loro una veste più attuale, spostata su di un piano unicamente finanziario, inquadrando le nuove tipologie di truffe come pestilenze che ciclicamente si ripresentano e, proprio come una patologia, sono connotate da sintomi comuni.

A far luce sul tema in oggetto, riguardante per l'appunto i casi di "*manipolazione del pagatore*", sovvengono gli ultimi dati rilasciati da Banca d'Italia nel "*Rapporto sulle operazioni di pagamento fraudolente in Italia*" (Febbraio 2025[1]).

Preliminarmente, occorre dare una definizione del fenomeno che si verifica quando "*l'utente pagatore viene indotto dal frodatore a impartire un'istruzione di pagamento al PSP, in buona fede, su un conto che egli ritiene appartenere a un beneficiario legittimo*"[2] ovvero a se stesso (*ndr*).

[1] https://www.bancaditalia.it/media/notizie/2025/Rapporto-sulle-operazioni-di-pagamento-fraudolente.pdf.
[2] Pag. 11 del Rapporto.

Sul punto, così come l'improvvisa moria di ratti rappresentò un monito per la città di Orano negli anni '40, analogamente, nel primo semestre dell'anno trascorso si è registrato un significativo aumento delle frodi attuate tramite la '*semplice*' manipolazione del pagatore, ossia convincendo quest'ultimo, tramite abili raggiri, alla personale esecuzione del pagamento in ogni sua fase, senza alcuna cessione di credenziali e/o dati personali a soggetti terzi e, di conseguenza, senza alcuna violazione dei sistemi online (*home banking).*

Per quanto concerne i bonifici, il dato in questione è passato dalla media oscillante tra il 32 e 48% – presente negli anni 2022 e 2023 – al 65% nel primo semestre del 2024 in termini di volume, ossia di numero di operazioni. In aggiunta, tutt'altro che secondario, è il dato indicante il valore sul totale delle frodi, che per la fattispecie in esame rappresenta un decisivo 74% per il comparto bonifici[3].

Premesso quanto precede, l'analisi verrà condotta affrontando una tipologia di truffa diffusasi soprattutto nel corso dell'ultimo anno e che coinvolge clienti indotti da sedicenti operatori bancari e/o delle Forze dell'ordine ad eseguire bonifici urgenti allo sportello fisico nella convinzione di mettere in sicurezza i propri risparmi.

Chi scrive, nonostante le truffe dilaghino proprio come periodiche pestilenze, non a caso parla di onestà quale mezzo di cura e/o – soprattutto – di prevenzione, sottolineando l'importanza dell'azione concreta del dovere che non solo è professionale, ma anche umano.

Ma che cos'è allora l'onestà a cui si fa cenno e invocata dal Dottor Rieux? Chi scrive cercherà di darne un tratto univoco e completo, a partire dal primo allarme del fenomeno sino ai possibili antidoti.

Probabilmente tutto questo perché "*io non so quale sia il mio lavoro* – proseguì Rambert – *E infatti forse sono colpevole a scegliere l'amore*". Ed è solo quest'ultimo che può essere utilizzato ai fini di una ricerca della cura.

[3] Pag. 12 del Rapporto.

1. Tecniche di approccio.

1.1. Il messaggio SMS.

Nella maggior parte dei casi studiati e oggetto di giurisprudenza, il primo contatto tra cliente della Banca e truffatore avviene tramite l'inoltro da parte di quest'ultimo di un messaggio SMS.

Questo è il primo amo che viene gettato e che, a seconda dei casi, può presentare diversi caratteri di insidiosità non sempre facilmente riconoscibili.

Indubbiamente, i messaggi più sofisticati sono quelli presentati sottoforma di "*spoofing*", ossia che riescono ad inserirsi direttamente all'interno della cronologia genuina dell'intermediario bancario e per i quali è necessario soffermarsi sul tenore letterale del testo riportato all'interno del messaggio. Molto spesso, infatti, questo si presenta in stile generico, senza fare riferimento specifico a rapporti propri del cliente, segnalando meramente la presenza di un'operazione sospetta per un certo importo e di richiamare un numero di telefono – solitamente proprio di un cellulare – qualora la transazione non sia riconosciuta.

In questi casi, chi riceve il messaggio, qualora dubbioso, deve sostanzialmente limitarsi ad un paio di azioni:

a) verificare l'effettiva esistenza di un'operazione in uscita (es., tramite controllo *home banking* e/o contatto con la propria Filiale di fiducia o del Servizio Clienti);
b) controllare il numero di telefono riportato nel messaggio tramite contatto telefonico con il Servizio Clienti e/o anche su un qualsiasi motore di ricerca onde comprenderne immediatamente la natura truffaldina e la sua non riconducibilità alla Banca.

In altri casi, i messaggi si presentano in maniera meno subdola, recando addirittura l'intestazione di altro intermediario bancario o di società emittenti carte di pagamento. Altre volte, ancora, il numero mittente è chiaramente visibile e non si presente con l'ID dell'intermediario, il cui nome è presente al limite nel solo testo del messaggio.

1.2. La telefonata.

La seconda fase della truffa si sviluppa in una conversazione telefonica tra il cliente ed il truffatore che si finge un operatore bancario oppure delle FF.OO.

O meglio. Può esserci il caso in cui sia il cliente a contattare direttamente il numero di cellulare riportato all'interno del messaggio SMS ricevuto oppure che sia questi ad essere chiamato dal truffatore. In quest'ultimo caso, è bene distinguere il tipo di numero chiamante.

Infatti, anche la telefonata può essere oggetto di camuffamento (*spoofing*) e il cliente può veder comparire sul proprio display quello che – effettivamente – sembra il numero o l'ID Caller della propria Banca.

Sicuramente in questi casi l'azione da parte del truffatore ha una maggiore carica persuasiva in quanto l'interlocutore riceve quella che, *prima facie*, sembra essere una telefonata da parte della propria Banca.

Di recente, onde contrastare detto fenomeno, alcuni intermediari hanno introdotto la verifica della chiamata direttamente "*in app*", ossia un servizio gratuito che conferma all'utente, tramite notifica *push* trasmessa allo smartphone certificato, di essere in linea con un (vero) operatore della Banca. A quel punto, l'utente che riceve una chiamata – apparentemente dalla propria Banca – ma senza conferma della verifica tramite app, avrebbe l'onere di nutrire un fondato sospetto.

Ma vi è comunque di più, perché nella maggior parte dei casi l'opera di raggiro è coordinata in *tandem*. Ossia la telefonata inizia con quello che sembra essere un operatore bancario – di solito dell'ufficio antifrode – e, successivamente, prosegue con un secondo soggetto, preannunciato dal primo, che si palesa quale Maresciallo, Ispettore o altro operatore delle FF.OO.

Anche nel caso di telefonata da parte delle FF.OO, spesso i truffatori riescono a camuffarne il relativo numero di telefono (es., Carabinieri o Questura del luogo in questione) ,rendendo così più convincente l'opera di persuasione nei confronti del destinatario.

Successivamente, durante il corso della conversazione, l'utente viene via via convinto dal malfattore di essere vittima di una potenziale frode in corso, specificando quasi sempre che:

1. è in atto un'indagine a carico di alcuni dipendenti '*infedeli*' della Banca che starebbero trafugando i conti dei correntisti (magari proprio della Filiale di fiducia);
2. a seguito di quanto sopra, è strettamente necessario non farne parola con i medesimi né prendere contatti diretti con la Filiale;
3. onde annullare la presunta operazione in uscita (segnalata a mezzo SMS), sarà necessario eseguire un bonifico urgente di pari importo così da destinare i fondi su altro rapporto definito come '*sicuro*'.

Ad ogni modo, per quanto persuasive possano essere le parole e i tecnicismi usati dai sedicenti operatori – e che, talvolta, sono a conoscenza anche di dati personali dei clienti – è bene rammentare principalmente che:

i. qualora vi fosse realmente un'operazione sospetta in uscita, il servizio antifrode della Banca, presi contatti con il titolare del rapporto onde verificarne la legittimità, opererebbe già in autonomia in osservanza dei protocolli in uso tra intermediari nonché di concerto con la Filiale di riferimento;
ii. inoltre, nessun servizio bancario '*passerebbe*' la telefonata e relative operazioni da eseguire per la tutela del cliente alle FF.OO.;
iii. infine, nessun operatore bancario e/o delle FF.OO. farebbe mai condurre al cliente, in prima persona, le operazioni di messa in sicurezza del capitale e/o coinvolgerebbe questi nelle indagini a carico di esponenti dell'intermediario.
iv. E ancora, a livello tecnico-contabile, qualora vi fosse effettivamente un bonifico in uscita, questo non può essere stornato da alcun bonifico di pari importo eseguito contestualmente, bensì è necessario azionare i rimedi pattuiti contrattualmente in base alla natura del pagamento e relative tempistiche (es., revoca; *recall*).

1.2.1. Cenni sullo spoofing.

In conclusione, un breve accenno circa l'ormai noto fenomeno dello *spoofing*, che possiamo definire quale tecnica di truffa informatica finalizzata a far credere alla vittima che la fonte di un messaggio (come *e-mail*, SMS o telefonata) sia affidabile, mentre in realtà è contraffatta. In pratica, l'attaccante manipola l'indirizzo mittente o il numero di telefono per far apparire la comunicazione come proveniente dall'istituto di credito o da un'altra fonte legittima.

Con particolare riferimento al camuffamento del numero chiamante e/o dell'ID Caller, si segnala come tale dato sia gestito dalla rete telefonica e di conseguenza dal relativo operatore di chi effettua la telefonata, il quale ha l'onere di inviare informazioni circa il mittente. Questa informazione (CLI – *Calling Line Identification*) viene quindi passata alle reti interconnesse fino ad arrivare al destinatario.

In altri casi, la telefonata camuffata viene effettuata tramite VoIP (*Voice over Internet Protocol*) e per il truffatore l'azione può presentare meno ostacoli rispetto ad una rete tradizionale poiché la chiamata viaggia come pacchetti dati su Internet e taluni provider VoIP non

verificano se il numero inserito è reale; pertanto, il destinatario vede il numero scelto dal chiamante, anche se falso.

Sul tema in questione, con la Delibera n. 106/25/CONS, AGCOM ha recentemente approvato un regolamento che stabilisce disposizioni per la trasparenza nell'offerta dei servizi di comunicazione elettronica e nella presentazione del numero chiamante a carico delle compagnie telefoniche. Tale regolamento include specifiche tecniche per il blocco delle chiamate che utilizzano numeri identificativi illegittimi o non conformi alle raccomandazioni internazionali[4]. In tale documento, da notare come le proposte e ammonimenti abbiano come destinatari esclusivi gli operatori telefonici – e non gli intermediari bancari, i quali, quindi, non hanno modo di limitare a monte il fenomeno – nonché i gestori dei servizi di chiamate vocali (VoIP). Per questi ultimi, è stato proposto il Protocollo STIR/SHAKEN, ossia un modello che autentica l'identità del chiamante all'inizio della chiamata e la verifica alla fine del percorso, utilizzando un meccanismo basato su firme digitali (ma al momento sembra essere di difficile attuazione per difficoltà tecniche e costi elevati).

Ad ogni modo, l'AGCOM ritiene necessario e non più procrastinabile procedere (quantomeno) con il blocco delle illegittime chiamate internazionali in entrata con CLI nazionale.

2. L'arrivo in Filiale.

Una volta giunta presso la Filiale, alla vittima viene intimato da parte del sedicente operatore di non riferire alcunché ai dipendenti presenti circa l'operazione in corso al fine di non comprometterne le indagini.

Solitamente, il sedicente operatore cerca di restare in diretto contatto telefonico con la vittima onde poterle fornire istruzioni qualora sorgessero domande da parte dei dipendenti della Filiale circa la natura dell'operazione.

In questi casi, da parte del (vero) operatore bancario, è bene prestare attenzione all'atteggiamento del cliente, il quale potrebbe risultare con il telefono direttamente all'orecchio e/o con un auricolare collegato *bluetooth* al dispositivo lasciato in tasca o in borsa. Nel primo caso, indubbiamente, l'essere al telefono durante un'operazione di bonifico

[4] Delibera 106-25-CONS.pdf.

potrebbe (dovrebbe) rappresentare un primo campanello d'allarme da valutare unitamente ad altri elementi (es., importo, causale, natura dell'operazione; etc.).

2.1. I sintomi della truffa.

Istruito il cliente circa i passaggi da compiere, questi porta a termine il bonifico firmando di proprio pugno l'ordine di pagamento. La maggior parte dei pagamenti oggetto di frode presenta diversi tratti comuni, tali da rendere ormai sintomatica la truffa in parola.

In particolare, senza pretese di esaustività, i fattori comuni possono essere così riassunti:

1. importo anomalo e/o c.d. "*svuotaconto*";
2. natura istantanea o urgente dell'operazione così da rendere irrevocabile l'ordine di pagamento;
3. causale generica non supportata da adeguati giustificativi durante il pagamento (es., acquisto auto senza contratto di vendita e/o numero di targa; acquisto immobile senza copia del rogito e/o del preliminare; etc.). Talvolta le causali hanno natura più '*personale*', quali un possibile aiuto familiare e/o un prestito ad un conoscente o parente per cui diventa più difficile ottenere un adeguato supporto probatorio.
4. Con riferimento sempre al punto precedente, ancora, è stato appurato che a diversi clienti viene ordinato di utilizzare la causale "*giroconto*" per quanto sia – nella stragrande maggioranza dei casi – un bonifico verso altro intermediario[5]. In questo caso particolare, pertanto, il cliente crede di fare un bonifico a favore di se stesso su coordinate bancarie "*di sicurezza*" accese all'uopo. Conseguentemente, il nominativo beneficiario, che sarà riportato nella relativa contabile di pagamento, non potrà che essere quello dello stesso ordinante.

   Allo stato attuale, stando a quanto previsto dall'art. 24 D.lgs. 11/2010, è sufficiente che le coordinate bancarie del beneficiario siano corrette (esistenti) sebbene – si badi bene – il conto acceso presso la Banca ricevente abbia diversa intestazione[6].

[5] Il "giroconto", infatti, consiste in un trasferimento di fondi tra conti intestati al medesimo soggetto e presso il medesimo intermediario bancario.

[6] In particolare, "*1. Se un ordine di pagamento è eseguito conformemente all'identificativo unico, esso si ritiene eseguito correttamente per quanto concerne il beneficiario e/o il conto indicato dall'identificativo unico. (…) 3. Il prestatore di servizi di pagamento è responsabile solo dell'esecuzione dell'operazione di pagamento in conformità con l'identificativo unico fornito dall'utente anche qualora quest'ultimo abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'identificativo unico.*"

Anche in tali casi può risultare arduo per la Banca identificare il tentativo di truffa, a fronte dell'inestimabile mole di operazioni nel mercato avente tale motivazione – e che, pertanto, non può essere considerata bloccante o sospetta – nonché nel fatto che, sebbene il cliente non abbia mai bonificato prima d'ora somme verso quel determinato Iban, non è detto che non possa essere un conto acceso recentemente per proprie ragioni personali, anche di natura commerciale.

Di conseguenza, in tali situazioni richiedere una prova all'ordinante della titolarità del conto presso il diverso intermediario può sembrare eccessivo, anche perché questi dovrebbe avere con sé un documento contrattuale.

A parer di chi scrive, dunque, il sospetto vero e proprio, prima che lato Banca, dovrebbe essere coltivato proprio dal cliente, il quale dovrebbe domandarsi come sia possibile l'accensione di un conto corrente a suo nome senza l'apposizione di alcuna firma. È anche vero che lo stesso cliente potrebbe obiettare – in sede di reclamo o contenzioso – la conoscenza del citato art. 24 e, pertanto, di aver eseguito il bonifico consapevole che sarebbe andato a buon fine sulla base delle sole coordinate, nonostante sapesse dell'impossibilità che potesse essere acceso a suo nome. Tutte valutazioni, comunque, che vanno commisurate al caso concreto.

5. Ulteriore causale che può destare sospetto è il riferimento ad una presunta "*gestione patrimoniale*". Infatti, nel caso di un cliente (apparentemente) privo di significative giacenze presso l'Istituto, è sicuramente un elemento che può destare perplessità, ma anche una volontà da parte del titolare di intraprendere investimenti finanziari contenuti presso intermediari specializzati proprio in quel segmento di mercato.

   Qualora, invece, il cliente fosse classificato come ad elevata patrimonialità (c.d. "*private*"), il congenito spirito commerciale, a seconda dei casi, potrebbe portare il personale di Filiale a sconsigliare l'operazione, offrendo occasioni migliori e quindi indagando sulle condizioni offerte dal diverso intermediario (che non esistono).

È bene rammentare, comunque, che i tratti sopra riportati non devono considerarsi determinanti ai fini dell'inquadramento della fattispecie, bensì quali meri segnali da unire ad altri elementi e da rapportare sempre all'intera vicenda.

2.2. I controlli da parte della Banca.

2.2.1. La disciplina antiriciclaggio.

In prima battuta, escludendo i casi di "*operazioni occasionali*"[7] pari o superiori a 15.000,00 euro e per le quali è necessario procedere all'adeguata verifica ex art. 17, comma 1, lett. b), D.lgs. 231/2007 (decreto antiriciclaggio), la Banca, per quanto riguarda i clienti già profilati, ai sensi del successivo terzo comma, deve comunque tenere conto dei seguenti criteri generali:

"*a) con riferimento al cliente:*

1) la natura giuridica;

2) la prevalente attività svolta;

3) il comportamento tenuto al momento del compimento dell'operazione o dell'instaurazione del rapporto continuativo o della prestazione professionale;

4) l'area geografica di residenza o sede del cliente o della controparte;

b) con riferimento all'operazione, rapporto continuativo o prestazione professionale:

1) la tipologia dell'operazione, rapporto continuativo o prestazione professionale posti in essere;

2) le modalità di svolgimento dell'operazione, rapporto continuativo o prestazione professionale;

3) l'ammontare dell'operazione;

4) la frequenza e il volume delle operazioni e la durata del rapporto continuativo o della prestazione professionale;

5) la ragionevolezza dell'operazione, del rapporto continuativo o della prestazione professionale, in rapporto all'attività svolta dal cliente e all'entità delle risorse economiche nella sua disponibilità;

6) l'area geografica di destinazione del prodotto e l'oggetto dell'operazione, del rapporto continuativo o della prestazione professionale".

In altri termini, i soggetti obbligati devono sempre provvedere all'adeguata verifica del cliente nei seguenti casi:

a) presenza di sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
b) esistenza di dubbi sulla veridicità o sull'adeguatezza dei dati ottenuti precedentemente per l'identificazione di un cliente.

[7] L'operazione è definita occasionale quando non è riconducibile a un rapporto continuativo in essere (cfr., art. 1, comma 2, lett. z), D.lgs. 231/2007.

Il decreto in esame, inoltre, dispone obblighi anche a carico del cliente stesso (art. 22). In particolare, all'atto dell'identificazione, i clienti forniscono per iscritto, sotto la propria responsabilità, tutte le informazioni necessarie ed aggiornate per l'individuazione dei soggetti per conto dei quali operano. Va rammentato, sul punto, che la firma del cliente su detta modulistica comporta eventuali responsabilità penali[8].

Pertanto, nel caso non sia possibile adempiere ai citati obblighi, l'intermediario ha l'obbligo di astenersi dall'effettuare l'operazione (art. 42). Tali disposizioni, tra l'altro, sono applicabili anche in caso di rapporti già instaurati, sempre che l'intermediario non pregiudichi diritti dei clienti[9].

Sul tema, infine, fondamentale è quanto previsto dall'art. 35 della normativa in esame e concernente l'obbligo di segnalazione delle operazioni sospette. In merito, la Banca, prima di compiere l'operazione, invia senza ritardo alla UIF[10], una segnalazione di operazione sospetta quando sa, sospetta o ha motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa. Il sospetto è desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita.

In presenza degli elementi di sospetto, dunque, la Banca non compie l'operazione fino al momento in cui non ha provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In dette ipotesi, la Banca, dopo aver eseguito l'operazione, ne dà notizia immediata alla UIF.

Per quanto ovvio, la SOS è valevole anche nei confronti di clienti storici e già profilati, siccome possono comunque verificarsi operazioni incoerenti con il loro profilo economico.

[8] Vd. art. 55, comma 3, D.lgs. 231/2007.

[9] Sul tema, cfr. anche R. Razzante, "*Manuale di legislazione e prassi dell'antiriciclaggio*", 2020, pp. 135 – 147.

[10] La UIF (Unità di Informazione Finanziaria) è l'organo italiano deputato a ricevere, analizzare e segnalare operazioni sospette alle Autorità competenti ai fini della prevenzione del riciclaggio e del finanziamento del terrorismo.

2.2.2. Il rifiuto dell'operazione.

Addentrandoci più intensamente all'interno della normativa riguardante i pagamenti, al di là dei ragionevoli sospetti che possono essere nutriti dalla Banca in forza della disciplina antiriciclaggio, questa può comunque rifiutarsi di eseguire l'ordine di pagamento ricevuto in presenza di giustificati motivi – *in primis*, in caso di sospetta frode – informandone tempestivamente il cliente se possibile.

Al riguardo, l'art. 16 D.lgs. 11/2010[11] dispone proprio che qualora il prestatore di servizi di pagamento rifiuti di eseguire o di disporre un ordine di pagamento, il rifiuto e, ove possibile, le relative motivazioni sono comunicati all'utente, salvo che tale informazione non debba essere fornita in quanto in contrasto con obiettivi di ordine pubblico o di pubblica sicurezza, individuati ai sensi dell'art. 126 del D.lgs. 385/1993 (Testo unico bancario), o ricorrano giustificati motivi ostativi in base alle disposizioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo, di legge o di regolamento. Il prestatore di servizi di pagamento ha l'onere di segnalare quindi la comunicazione di rigetto secondo le modalità previste nel contratto quadro e, comunque, con la massima sollecitudine.

A parer di chi scrive, forse, tale ultimo dettato sembra lasciare maggiore carta bianca all'intermediario bancario in sede di valutazione circa la natura dell'operazione. È anche vero che la normativa sui pagamenti e quella antiriciclaggio non si debbono escludere a vicenda e, anzi, devono '*correre insieme*' in quello che deve essere un approccio unitario.

Indubbiamente, in presenza di un modulo di adeguata verifica sottoscritto dal cliente, difficilmente quest'ultimo potrà obiettare nei confronti della Banca un comportamento incauto a tutela dei suoi risparmi.

Infine, visto il recente prosperare del fenomeno fraudolento in questione, ruolo fondamentale è recitato dalle campagne di sensibilizzazione attivate dagli intermediari in tema antifrode.

Oltre all'ormai nota diffusione a livello *web* sui siti istituzionali degli intermediari, per quanto riguarda la fattispecie in esame che riguarda un canale '*tradizionale*' quale è appunto lo sportello fisico, è consigliabile spostare l'attenzione della clientela proprio in tali luoghi, attuando una campagna mirata sul fenomeno in discussione tramite, ad es., locandine informative e facilmente comprensibili per un pubblico '*non tecnico*', nonché modulistiche

[11] Che 'discende' dall'art. 79 PSD2 (Direttive UE 2015/2366).

create *ad hoc* – alternative a quelle già esistenti (es., adeguata verifica) – e rappresentanti una sorta di manleva a favore della Banca, la quale, prima di ricevere l'ordine di pagamento – considerato più o meno non coerente con il profilo del pagatore – riepiloga per iscritto quelli che sono i rischi derivanti dalle truffe più in voga del momento e sotto quale forma si manifestano.

3. La truffa svelata: rimedi e consigli.

Terminata l'operazione allo sportello, è d'uso che il sedicente operatore delle FF.OO. richieda copia del pagamento a mezzo *chat* istantanea al cliente, vuoi per creare una finta convinzione in controparte circa la veridicità di tutta la messa in scena, vuoi per meri fini di verifica dei dati di pagamento a favore del conto beneficiario, poiché, una volta ricevuti i fondi, sarà necessario spostarli immediatamente onde disperderne le tracce.

Circa il prosciugamento contabile del rapporto beneficiario, le tecniche sono le più disparate e dipendono sostanzialmente dagli strumenti di pagamento in mano al truffatore e relativi massimali previsti (es., bonifici verso conti terzi; prelievi presso ATM e/o su altri sportelli; operazioni *e-commerce* a favore di *account* aperti su piattaforme finanziarie).

Infine, ultimo atto solitamente compiuto dai malfattori, consiste nel dare un appuntamento fittizio al malcapitato presso la stazione o caserma locale onde verbalizzare quanto successo e riottenere possesso dei propri risparmi. Giunto sul posto concordato, poi, il cliente prende coscienza della truffa, fatte salve altre circostanze del caso che ne anticipino il momento.

In questa fase, la truffa può dirsi conclusa e molto dipende dal tempo trascorso dall'esecuzione del bonifico nonché dalla sua natura.

Infatti, in caso di bonifico avente natura "*istantanea*", il termine di accredito a favore del rapporto beneficiario avviene nell'arco di massimo 10 secondi. Pertanto, premessa la sua innata caratteristica di irrevocabilità una volta eseguito, l'unica speranza non può che consistere in un blocco '*a valle*' presente sulla Banca ricevente, la quale magari ha apprestato ulteriori controlli imposti dalle normative vigenti e/o dalle proprie politiche interne.

Normalmente, tuttavia, proprio per ragioni di sicurezza, il bonifico istantaneo, pur se effettuato allo sportello, presenta massimali più contenuti rispetto agli altri tipi di bonifico. Pertanto, a seconda della giacenza presente sul conto da addebitarsi, con il pretesto di dover spostare il prima possibile i fondi onde metterli in sicurezza, nel caso questi superino il massimale consentito per il bonifico istantaneo, il truffatore potrebbe anche '*rischiare*' di

convincere il cliente ad optare per un bonifico "*urgente*", ossia non avente le caratteristiche dell'immediatezza, ma con possibilità di massimali decisamente più alti (se non del tutto assenti talvolta).

Anche in tale situazione, una volta eseguito il bonifico urgente, questo è da ritenersi irrevocabile lato Banca del cliente; tuttavia, i tempi di accredito sono variabili a secondo delle *policy* previste dagli intermediari. Di base, se il bonifico è eseguito entro l'orario di sportello, è garantito l'accredito in giornata sulla Banca beneficiaria. I tempi possono variare da pochi minuti a qualche ora a seconda dei casi.

Un primo ed imprescindibile rimedio che può attuare il cliente, consiste nel segnalare il prima possibile l'evento alla propria Banca, la quale – com'è d'uso per tutti i bonifici eseguiti – attiverà la procedura di c.d. "*recall*", ossia di richiamo del pagamento.

Tale azione rimediale è normativamente consacrata, siccome, ai sensi dell'art. 24, comma 2, D.lgs. 11/2010 "*(…) Il prestatore di servizi di pagamento del pagatore compie tuttavia sforzi ragionevoli per recuperare i fondi oggetto dell'operazione di pagamento. Il prestatore di servizi di pagamento del beneficiario è tenuto a collaborare, anche comunicando al prestatore di servizi di pagamento del pagatore ogni informazione utile. Se non è possibile il recupero dei fondi, il prestatore di servizi di pagamento del pagatore, su richiesta scritta del pagatore, è tenuto a fornirgli ogni informazione disponibile che sia utile ai fini di un'azione di tutela.*".

Ma gli "*sforzi ragionevoli*" non dovrebbero esaurirsi nella semplice attivazione di una procedura interbancaria. Questi, nella prassi, comprendono azioni parallele attuate anche da altre funzioni della Banca, quali il servizio Antifrode che deve trasmettere la segnalazione al corrispondente reparto ubicato presso l'intermediario beneficiario sui canali a disposizione (posta elettronica; contatti telefonici; etc.).

Analogo compito potrebbe (*rectius*, dovrebbe) essere portato avanti dalla Filiale che, essendo a conoscenza dell'ABI e del CAB delle coordinate beneficiarie, può facilmente risalire alla Filiale ove è acceso il rapporto e provare a prendere contatti urgenti tramite i canali sopra accennati. La ricerca si complica in presenza di intermediari privi di filiali fisiche sul territorio e per i quali è necessario attendere i tempi dei *call center*.

È bene evidenziare, comunque, che la procedura di *recall* non dà garanzia di rientro dei fondi. Anzi, qualora si riesca a bloccare anche solo parzialmente la somma bonificata sul conto del beneficiario, la restituzione è necessariamente subordinata al consenso di quest'ultimo ex art. 17 D.lgs. 11/2010. Consenso che, per quanto ovvio, sarà assai difficile ottenere visto che

dall'altra parte vi è un malfattore, che, una volta scoperto il blocco sul proprio conto, si renderà irreperibile.

Di conseguenza, qualora la somma o parte di questa fosse ancora presente sul rapporto di accredito, il cliente dovrà necessariamente attivarsi giudizialmente per ottenere il sequestro della somma. Tuttavia, è bene precisare che non per forza quello che si riesce a '*congelare*' sul conto del truffatore è di spettanza del cliente truffato, in quanto può benissimo trattarsi di un residuo di altrettanti bonifici fraudolenti pervenuti su quel rapporto e, pertanto, la somma dovrà essere ripartita tra gli aventi diritto in sede giudiziale.

In altre situazioni, soprattutto qualora gli importi non siano significativi e i costi delle procedure giudiziali siano antieconomici, taluni intermediari richiedono una lettera di "*indemnity*" alla Banca del pagatore, la quale, a fronte del rientro della somma, seppur senza consenso del beneficiario (malfattore), dovrà assumersi ogni ed esclusiva responsabilità qualora un domani questa risultasse non dovuta, manlevando così la Banca beneficiaria. A cascata, poi, la Banca del pagatore è solita chiedere un'ulteriore lettera di manleva al richiedente, valevole solo tra le parti, qualora il beneficiario dovesse un giorno reclamarla giudizialmente (improbabile comunque nei casi di frode acclarata).

Quanto argomentato finora può, quindi, essere annoverato nella categoria delle azioni '*ufficiali*' che gli intermediari devono concretizzare non appena ricevuta – o scoperta – la truffa ai danni del proprio cliente.

Nulla esclude, ovviamente, che anche il materiale esecutore del bonifico possa fare la sua parte e nel proprio interesse. *In primis*, è consigliabile che il contatto con la Banca beneficiaria lo prenda anche l'ordinante del bonifico per quanto possibile.

Il primo contatto, in particolare, qualora non ancora prestato dalla propria Banca, può (*rectius*, deve) essere nei confronti della Filiale della Banca ricevente. In caso di Banca '*tradizionale*', ossia dotata di sportelli fisici, la dipendenza interessata è individuabile grazie al "CAB" presente nelle coordinate che segue immediatamente il codice "ABI" che, invece, identifica l'intermediario[12]; il numero di telefono e/o talvolta anche indirizzo *e-mail* possono essere facilmente reperiti sui motori di ricerca. In alternativa, rimangono sempre disponibili i canali istituzionali disponibili notoriamente sui relativi siti *web*.

[12] A mero titolo esemplificativo: "*IT* (sigla nazionale) *01* (codice di controllo internazionale) *A* (codice di controllo nazionale) *23456* (ABI) 78910 (CAB) *123456789012*".

Perché chi scrive consiglia quanto sopra? Il motivo risiede nel fatto che, come spesso capita, qualsiasi tipo di comunicazione pervenuta all'intermediario subisce dei '*processi*' interni e la sua lettura o conoscenza può non essere tempestiva. In questo frangente, può succedere che, ad esempio in presenza di un bonifico urgente, il cliente prenda coscienza dopo pochi minuti del raggiro perpetrato ai suoi danni ed una comunicazione tempestiva potrebbe fare la differenza, meglio se scritta, ma anche orale tramite il numero del Servizio Clienti, in quanto la telefonata viene comunque registrata.

Ergo, se, nonostante le suddette segnalazioni, la somma non dovesse essere bloccata per tempo dalla Banca beneficiaria, il pagatore manterrà comunque il diritto di interpellare quest'ultima circa gli esatti orari di ricezione e contabilizzazione della somma nonché delle successive fasi in cui è stata sottratta. Qualora la risposta non dovesse risultare soddisfacente, convincente o priva di supporti probatori, il pagatore conserva la facoltà di andare in *escalation* e adire gli organi previsti (Arbitro Bancario Finanziario; Autorità Giudiziaria; etc.); se effettivamente risultasse che la somma è stata sottratta – in tutto o in parte – in un momento successivo la comunicazione del pagatore, a seconda dei casi, l'intermediario può esserne chiamato a risponderne.

Analogo discorso deve essere applicato alla Banca del pagatore in presenza di un *recall* tardivo, qualora ciò abbia pregiudicato il blocco tempestivo dei fondi presso l'intermediario beneficiario.

4. Orientamenti dell'ABF.

In questo paragrafo si cercheranno di esaminare le più recenti decisioni assunte dall'Arbitro Bancario Finanziario (ABF) principalmente sullo specifico tema delle frodi attuate presso lo sportello bancario a seguito di manipolazione del pagatore.

Si anticipa già che, allo stato attuale, l'orientamento maggioritario propende per riconoscere una responsabilità esclusiva a carico del cliente che ha effettuato l'operazione, salvo taluni casi in cui è possibile individuare un concorso di colpa insieme all'intermediario coinvolto.

Con l'occasione verranno fatti accenni anche a principi ormai '*generali*' ed applicabili anche ai casi di bonifici personalmente eseguiti da remoto (*home banking*) a seguito di truffa ("*scam*") con l'utilizzo di tecniche di "*social engineering*".

Infine, verranno analizzate anche le decisioni in materia riguardanti contenziosi intercorsi non solo tra il cliente e la propria Banca, bensì anche tra il primo e la Banca ricevente per quanto non sia sussistente un rapporto '*diretto*'.

4.1. Pagatore vs. Banca ordinante.

Questo primo gruppo di decisioni, numericamente più nutrito rispetto a quello che verrà affrontato nei paragrafi successivi, riguarda contenziosi stragiudiziali attivati dal pagatore nei confronti della propria Banca, ove è radicato il conto corrente dal quale è partito il bonifico a favore del truffatore.

Innanzitutto, è bene rilevare che, il fattore comune sottostante le decisioni dei Collegi territoriali è rappresentato dal fatto che il bonifico, personalmente effettuato dal cliente presso lo sportello, non rientra nella categoria delle c.d. "*operazioni non autorizzate*", per la quale, diversamente, si applica l'art. 10 D.lgs. 11/2010 (c.d. procedimento di "*disconoscimento*"[13]).

In queste circostanze, infatti, siccome la coartazione delle volontà avviene '*a monte*' dell'esecuzione del bonifico, che viene portato a termine direttamente dal cliente, non si applicano le disposizioni sui pagamenti "*non autorizzati*", essendo qualificati come tali, ex art. 5 D.lgs. 11/2010, solo quelli effettuati senza il consenso del pagatore[14]. Sono, quindi, considerate autorizzate anche quelle eseguite dal pagatore seguendo le indicazioni del frodatore[15] per quanto "*sulla base di un consenso viziato dagli artifizi e dai raggiri posti in essere dal truffatore anche per mezzo di sms o chiamate civetta apparentemente provenienti dall'intermediario resistente.*"[16]

Partendo dal Collegio di Torino, in un caso ove sono stati effettuati tre bonifici urgenti per l'importo complessivo di 16.000,00 euro, disposti allo sportello fisico di due distinte filiali del medesimo intermediario (di cui uno richiamato con successo), è stato precisato che la banca "*non poteva accorgersi della truffa perpetrata ai danni del cliente posto che ha assolto l'obbligo di verifica dell'identità del cliente disponente, attraverso un documento di riconoscimento, ma non ha obbligo di indagare le motivazioni delle operazioni di pagamento ordinate, né di chiedere il giustificativo del bonifico, in questo*

[13]Ciò vale anche nei casi di bonifici interamente disposti dal cliente da remoto, ossia inseriti ed autorizzati, per i quali, in caso di contestazione, allo stato attuale non è richiesta all'intermediario la prova dei *log*, ossia di dimostrazione della *strong customer authentication* (c.d. "SCA") o, in lingua nostrana, autenticazione a due fattori.

[14] A mero titolo di completezza, vd. F. Corallo, "*Indagine sul consenso nei pagamenti non autorizzati*", in Rivista di Diritto del Risparmio, Fascicolo 2/2024.

[15] Vd., Collegio di Torino, decisione n. 2685/2025; Collegio di Milano, decisione n. 631/2025.

[16] Vd., Collegio di Bologna, decisione n. 9631/2025 (cfr., anche decisione n. 2290/2023).

caso la fattura indicata nella causale, peraltro compatibile con la tipologia di cliente consumatore quale è parte ricorrente. (…) In ogni caso, in situazioni simili a quella in oggetto – disposizione di bonifico istantaneo presso sportello fisico –, il Collegio di Torino è solito escludere la possibilità di vagliare ulteriori elementi di rischio frode (decisione n. 7413/2024)" (decisione n. 794/2025).

Detto orientamento fa seguito a quello già assunto dalla medesima sezione territoriale qualche mese prima, ove, a fronte della doppia telefonata da parte di sedicenti operatori bancari e delle FF.OO. da numeri apparentemente reali, previa ricezione di SMS sottoforma di *spoofing*, è stato chiarito che "*parte ricorrente con l'aver direttamente disposto allo sportello l'operazione contestata trasferendo tutta la liquidità disponibile, dando così credito al racconto stravagante dei truffatori (trasferire direttamente sul conto di una sconosciuta dipendente dell'intermediario resistente la somma in contestazione, senza nulla riferire in filiale a motivo di indagini in corso nei confronti di altro dipendente della banca), ha assunto comportamenti talmente incauti e di colpevole credulità da non poter essere fronteggiati in anticipo da parte del resistente.*" (decisione n. 10067/2024).

Tuttavia, da rilevare come il Collegio di Torino, già a luglio 2024, in un caso di bonifico di 14.000,00 euro disposto dalla ricorrente su indicazione telefonica di un presunto operatore dell'intermediario, nella convinzione di mettere in sicurezza i fondi del proprio conto a fronte di un presunto rischio di frode informatica, ha dato qualche segnale di '*apertura*'. Ossia, il Collegio può rilevare una "*responsabilità concorrente del PSP* (ndr, Prestatore Servizi di Pagamento) *sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto, dalla documentazione in atti, un apporto causale dell'intermediario alla frode come, ad esempio, nel caso di mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, a cui il pagatore si sia rivolto esponendo le richieste del frodatore.*" (decisione n. 8332/2024).

Principio quello testé accennato che è stato ripreso anche dal Collegio di Milano, nella decisione n. 3498/2025[17], per cui "*È principio consolidato che, in caso di operazioni compiute direttamente dal cliente, l'intermediario è esonerato dalla prova di autenticazione e non è configurabile una sua responsabilità oggettiva dovendosi valutare una sua eventuale responsabilità concorrente solo secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:*

[17] In senso analogo, vd. anche Collegio di Bari, decisione n. 10990/2024; Collegio di Palermo, decisione n. 791/2025. In quest'ultimo caso, il Collegio ha rilevato in particolar modo che "*il richiamo all'anomalia dell'importo oggetto del bonifico, corrispondente all'intero saldo del conto corrente, non può portare all'accoglimento neanche parziale del ricorso poiché il cliente dichiara di aver effettuato l'operazione presso gli uffici dell'intermediario ed in quella sede ha consapevolmente omesso di chiedere chiarimenti all'addetto allo sportello ed in ogni caso non risulta prodotto un estratto conto da cui poter trarre conferma in ordine alla straordinarietà del valore dell'importo oggetto di bonifico e della corrispondenza con l'intero ammontare del deposito*".

a) *mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;*
b) *mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;*
c) *mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.*".

Sempre nella medesima pronuncia, considerata l'assenza di particolari elementi di anomalia, compreso il fatto che ormai per lo *spoofing* telefonico "*è noto come la circostanza non sia di per sé sufficiente a determinare la responsabilità dell'intermediario, essendo oggi facile far apparire come mittente di una telefonata o di un messaggio un utente diverso da quello effettivo*", va osservato che, "*in assenza di domande o richieste di chiarimenti ovvero di altri particolari segnali di anomalia, l'esecuzione di un ordine di pagamento con sottoscrizione del relativo modulo sia pure per un ammontare come quello di specie* (ndr, 29.200,00 euro) *non integra comportamento che debba di per sé allertare l'operatore, essendo per contro obbligo dell'intermediario dare esecuzione agli ordini ricevuti*"[18].

Al riguardo, il Collegio napoletano ha evidenziato che il dipendente dell'intermediario, cui la parte attrice si sia rivolta esponendo le richieste del frodatore, omettendo di identificare il tentativo di frode in corso, rassicurando anzi il ricorrente circa la bontà dell'operazione, comporta una corresponsabilità nella misura del 50% sull'intera somma sottratta (decisione n. 5465/2024).

I criteri di cui ai sopra citati punti a), b) e c) sono stati ripresi anche dal Collegio di Bologna, seppur in un caso parzialmente difforme di bonifico allo sportello a fronte di una truffa meglio nota come "*family emergency scam*". Ovvero quando la vittima, convinta di esaudire una richiesta proveniente da un parente stretto, si determina ad effettuare il pagamento richiesto[19] (decisione n. 2634/2025; in senso conforme, anche Collegio di Roma, decisione n. 2409/2025).

Interessante, per quanto riguarda i casi di "*scam*", ma applicabile in generale a tutte le fattispecie, l'accoglimento integrale del ricorso da parte del Collegio di Napoli nei confronti

[18] Vd., anche Collegio di Milano, decisione n. 3635/2025.
[19] Non vi è quindi presenza di falsi operatori bancari e/o delle FF.OO. e relativi meccanismi di *spoofing* multicanale.

del ricorrente una volta accertato il comportamento tardivo della Banca nell'attivazione della procedura di *recall* (decisione n. 1673/2025).

Sui possibili segnali di anomalia rilevabili, il Collegio di Roma si è soffermato in particolar modo sul tenore delle causali. Nel merito:

- in presenza di una causale riportante "*Anticipo Acquisto Terreno*", la somma di 28.000,00 euro bonificata allo sportello è stata ritenuta coerente con l'operazione, nonostante l'assenza di giustificativi documentali (decisione n. 12813/2024);
- analogamente, in un altro caso di bonifici per importo di 27.250,00 euro, la causale "*giroconto personale*" non può ritenersi riconoscibile *ictu oculi* da parte della Filiale (decisione n. 385/2025).

Il Collegio capitolino[20], ad ogni modo, ha manifestato segnali di aperture *pro consumer* in un caso di doppio bonifico allo sportello per l'importo complessivo di 30.000,00 euro. Nello specifico, è stato innanzitutto statuito che, ribaditi i noti principi di cui ai punti a), b) e c) *ut supra* richiamati, "*nel caso di specie viene in rilievo la possibile violazione da parte dell'intermediario finanziario dei più elementari obblighi di diligenza professionale dell'accorto banchiere ex art. 1176, comma 2, c.c., nonché di correttezza e di buona fede nell'esecuzione del contratto. Si può in effetti ritenere che l'intermediario, alla luce degli obblighi appena richiamati, debba adottare sistemi idonei a impedire operazioni e trasferimenti che manifestino già* prima facie *carattere anomalo e fraudolento o quantomeno, trattandosi di operazioni disposte dal titolare allo sportello, attivarsi per chiedere altre ulteriori informazioni in merito alle operazioni anomale che questi intende compiere. Nel caso in esame, si tratta di due bonifici istantanei, e dunque non revocabili, di importo complessivamente rilevante. A ciò si aggiunge la circostanza che la ricorrente – secondo quanto rilevato dallo stesso intermediario – non si era mai presentata in filiale prima di allora e ha eseguito i due bonifici istantanei mentre parlava al telefono. Il Collegio ritiene dunque che, a prescindere dalla richiesta proveniente dalla cliente, la natura anomala delle operazioni di pagamento, riconoscibile* ictu oculi*, avrebbe dovuto indurre l'impiegato dell'intermediario ad attivarsi per approfondire la natura genuina e la ragione delle operazioni, il che avrebbe potuto evitare il compimento della frode ai suoi danni o almeno ridurne le conseguenze dannose (nel medesimo senso v. già Collegio di Roma, decisioni nn. 5955/2024; 5646/2024 e 4808/2024)*".

Secondo il Collegio, poi, è degna di nota la pronuncia della Corte di Cassazione, 31 marzo 2010, n. 7956, secondo cui "*è difficilmente contestabile che rientri nei doveri di esecuzione di buona fede*

[20] Decisione n. 10302 del 02/10/2024.

gravanti sul mandatario (e quindi sulla banca alla quale la società abbia affidato i propri depositi stipulando una convenzione di assegno) il rifiuto di operazioni ictu oculi *anomali, quando esse siano tali da compromettere palesemente l'interesse della correntista*".

Nel caso di specie, in conclusione, il Collegio ha riconosciuto una responsabilità concorrente a carico del PSP da quantificarsi nella misura di 7.500,00 euro (25% del *petitum*) determinato in via equitativa ex art. 1226 c.c.

Da rilevare come tale pronuncia, ad una prima lettura, si attesti quale parziale cambio di pensiero rispetto ad un precedente analogo giudicato nel giugno del medesimo anno. In particolare, in un caso di doppio bonifico per l'importo complessivo – decisamente più contenuto – di 6.700,00 euro, nonostante la presenza di uno *spoofing* multicanale apparentemente riconducibile alla banca resistente (documentato dal ricorrente), sebbene il cliente sia rimasto collegato al telefono con il frodatore durante l'esecuzione del pagamento e, nonostante la resistente non abbia contestato la sua condotta tardiva nell'attivazione della procedura di *recall*, senza nulla produrre in merito, il Collegio ha comunque respinto il ricorso *in toto*[21].

Da ricordare, infine, da parte del Collegio di coordinamento, la decisione n. 8671/2024 secondo la quale "*i pagamenti interamente eseguiti dal titolare dello strumento di pagamento non rientrano, secondo il consolidato orientamento dell'Arbitro, nella fattispecie della responsabilità oggettiva del prestatore di servizi di pagamento per le operazioni non autorizzate dai clienti: fattispecie che, come ha sottolineato la Corte di Giustizia nella decisione del 2 settembre 2021, causa C-337/20 (DM, LR contro Caisse régionale de Crédit agricole mutuel (CRCAM) – Alpes-Provence), è disciplinata in via esclusiva dal d. lgs n. 11/2010. Ciò non impedisce, tuttavia, che proprio in quanto sottratti al perimetro di operatività della normativa ora citata, i danni subiti dal cliente per i pagamenti da lui "*autorizzati*" possano, in astratto, essere risarciti ai sensi dell'art. 1218 c.c., qualora sia dimostrata la negligenza dell'intermediario nell'adempimento di obblighi contrattuali. Ciò può verificarsi, in particolare, se sia accertata l'omessa adozione di misure di sicurezza e di monitoraggio adeguate a contrastare scenari di truffa dotati di una tipicità sociale (per esempio, in caso di mancata valorizzazione di indici di frode, là dove il cliente sia stato indotto dal truffatore a disporre dei pagamenti nella convinzione di effettuare accrediti in conto, mentre la ricezione di* alert *o la sospensione delle transazioni gli avrebbe consentito di acquisire consapevolezza della frode e di evitarne il perfezionarsi). Nel caso di specie, tuttavia, non si ravvedono evidenti profili di negligenza nella*

[21] Collegio di Roma, decisione n. 6884/2024; in senso conforme, vd. anche Collegio di Napoli, decisione n. 2330/2024.

condotta dell'intermediario, mentre il fatto colposo della parte ricorrente - recatasi di persona a effettuare i versamenti in filiale, presso uno sportello presidiato da un dipendente e omettendo di esporre a quest'ultimo le richieste del frodatore - assorbe il rilievo causale di qualsiasi inadempimento della banca.".

4.1.1. Sugli indici di anomalia.

Un discorso a se stante merita la giurisprudenza arbitrale sulla possibile presenza dei c.d. "*indici di anomalia*".

Una recente e significativa pronuncia del Collegio milanese[22], ha stabilito che gli indici di frode di cui all'art. 8 del D.M. n. 112/2007 – originariamente concepiti per le carte di pagamento in modalità "*card present*" (utilizzi su POS fisico) – possono costituire un parametro di valutazione del comportamento dell'intermediario bancario anche con riguardo ad operazioni effettuate con altri strumenti di pagamento, quali bonifici, ricariche *online* o presso ATM, in funzione dell'unicità della *ratio* sottesa a tale normativa.

Proprio per tale motivo, i principi in parola non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, bensì sono espressione di un generale obbligo di monitoraggio delle transazioni.

Gli Arbitri, inoltre, possono far emergere indici di frode ulteriori rispetto a quelli di cui al decreto in questione, ad esempio in presenza di una movimentazione anomala non coerente con la storicità pregressa del cliente. In questi casi, è possibile fare riferimento anche ai seguenti parametri:

- numero di operazioni;
- tipologia (*id est*, differenza tra operazioni aventi natura immediata/urgente e ordinaria; etc.);
- importo (qualora oltre una certa soglia rispetto alla disponibilità del conto corrente);
- frequenza (sono da considerarsi sospette le operazioni eseguite in tempi ravvicinati o comunque in rapida sequenza temporale);

[22] Collegio di Milano, decisione n. 323 del 14/01/2025. In particolare, la decisione riguardava quattordici bonifici personalmente eseguiti da remoto dal ricorrente, previo raggiro telefonico tramite *spoofing* da parte di sedicente operatore bancario e per un totale di 14.344,00 euro. Al riguardo, è stata riconosciuta la responsabilità concorsuale a carico dell'intermediario nella misura di 1/3 del *petitum*, siccome è stato valutato l'indice di anomalia rappresentato dalla frequenza con cui sono stati fatti i pagamenti ravvicinati, quasi tutti di pari importo (900,00 euro ca.) e a favore di diversi beneficiari. Ne è scaturita, così, una responsabilità concorrente dell'intermediario in relazione agli obblighi di protezione su di esso gravanti ex art. 1375 c.c.

- riconducibilità delle operazioni al medesimo beneficiario.

L'art. 8 in questione, rubricato per l'appunto "*Rischio di frode*"[23], dispone che questo si configura ogni qualvolta venga raggiunto almeno uno dei seguenti parametri:

a) con riferimento ai punti vendita (esercizi commerciali):
    1. cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;
    2. tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;
    3. richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto vendita;
b) riguardo alle carte di pagamento:
    1. sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;
    2. una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del *plafond* della carta di pagamento;
    3. due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di 60 minuti.

Per esperienza giurisprudenziale, è possibile affermare che i criteri più utilizzati – ed estesi anche da qualche tempo a tutti i tipi di operazioni di pagamento – sono quelli di cui alla lett. a), n. 2 e lett. b) nn. 1-2.

Applicando tali principi ai bonifici, il primo criterio di anomalia può essere individuato, per esempio, nell'effettuazione di tre bonifici a favore del medesimo beneficiario nell'arco di 24 ore; i restanti si possono configurare, in ipotesi, nell'esecuzione di sette bonifici – anche a favore di sette diversi beneficiari – nell'arco di 24 ore oppure nell'esecuzione di un bonifico a quasi totale azzeramento del conto. Tendenzialmente, anche il criterio di cui alla lett. b), n. 3, può essere individuato nell'esecuzione di due bonifici esteri nell'arco di un'ora (da valutare se questo poi debba essere interpretato nel senso di due bonifici verso due diversi Stati oppure sia sufficiente il mero accredito oltre '*confine*', seppur verso il medesimo Paese).

[23] DECRETO 30 aprile 2007, n. 112 - Normattiva.

Di non facile attuazione, invece, il criterio di cui alla lett. a), n. 3, soprattutto se in sede di contenzioso non viene sollevato dall'attore e/o in assenza degli estratti conto utili ad effettuarne il calcolo algebrico.

Ad ogni modo, l'eventuale ripartizione di responsabilità tra ricorrente ed intermediario deve essere determinata caso per caso, analizzando le circostanze di fatto, siccome le previsioni del D.M. n. 112/2007 costituiscono solo un parametro per la formulazione di un giudizio in concreto della "*negligenza tecnica*" dell'intermediario.

Si badi bene. La trattazione di questi indici di frode è stata volutamente separata rispetto al precedente paragrafo in quanto, come precisato dall'ABF, vi è un fondamento di valutazione squisitamente '*tecnico*', o meglio, quasi '*matematico*' siccome è necessario effettuare dei conteggi.

I criteri, invece, visti nel paragrafo precedente – da leggere comunque congiuntamente a quelli tecnici – hanno una natura decisamente più '*intuitiva*' (i.e., *ictu oculi*), soprattutto in forza del fatto che vi è l'incontro tra due persone. Per quanto, quindi, un cassiere non possa di certo valutare nell'immediatezza un parametro matematico, se non supportato da idonee procedure, può tuttavia cogliere aspetti sensoriali che appunto una macchina non è in grado di fare, quali l'atteggiamento del cliente, la sua eventuale reticenza o agitazione durante l'operazione, a maggior ragione se conosciuto e, realisticamente, diverso dal solito (ovviamente, entro quelli che sono anche i limiti della riservatezza e/o discrezione).

I criteri tecnici, a parere del Collegio, dovrebbero imporre alla Banca l'adozione di adeguati presidi automatici di sicurezza, che consentano il blocco delle operazioni non in linea con una normale operatività.

La decisione n. 6732 del 09/07/2025 del Collegio di Milano parrebbe invece collocarsi, *à rebours*, rispetto all'orientamento consueto, ma, leggendola a fondo, non si può certo definirla una pronuncia di *huysmansiana* memoria.

In tale seduta, infatti, è stata decretata l'insussistenza di un obbligo di monitoraggio preventivo in capo all'intermediario e, di conseguenza, l'impossibilità da parte sua di disporre un blocco delle operazioni. In particolare, "*il fatto che dette operazioni nel loro complesso non rientrassero nella normale operatività sia per importi che per destinatari non è di per sé significativo sia perché non si può escludere che vi siano occasioni in cui un cliente debba effettuare operazioni diverse dalle sue abitudini in relazione a esigenze specifiche (…) né che debba bonificare per la prima volta soggetti a cui favore non ha mai effettuato in precedenza operazioni di pagamento sia, infine, perché non è dato comprendere quali siano gli elementi che possano determinare il momento e il contesto in cui l'intermediario avrebbe dovuto*

bloccare l'operatività del conto, se si considera che ogni bonifico aveva un destinatario ed un importo diverso[24]. *In conclusione, non ritiene il Collegio che l'obbligo di protezione che grava sull'intermediario si debba estendere sino al punto di procedere* ex ante *a blocchi automatici al superamento di un certo numero di operazioni o di un determinato ammontare in assenza di precisi indici di frode*"[25].

Ma il caso appena discusso, indagando nella sezione "*Fatto*" della decisione, non riguarda propriamente una '*manipolazione*' del pagatore a fronte di un presunto pericolo imminente, bensì una truffa perpetrata da un finto *broker* finanziario ai danni del ricorrente, il quale, credendo di effettuare dei pagamenti a fini di lucro (nella fattispecie, *trading online*), ha invece effettuato pagamenti a favore di terzi soggetti che nulla avevano a che vedere con quella realtà.

Pertanto, è facile intuire tra le righe che anche le motivazioni, che hanno indotto il ricorrente ad effettuare i pagamenti, hanno un peso decisamente rilevante, tale addirittura, in certi casi, da non prendere in considerazione gli indici di frode a tutela di questi.

In una sorta di filone aristotelico, parafrasando i concetti dell'Etica Nicomachea, possiamo quindi affermare che (anche) per l'orientamento stragiudiziale talune azioni, per quanto volontarie, ma dettate dal timore ('*φόβος*') di un pericolo imminente, sono parzialmente scusabili in presenza di negligenza tecnica da parte del PSP; diversamente, le azioni mosse da sentimenti di avidità ('*πλεονεξία*'), soprattutto se attuate nella convinzione di operare nel *trading online*, senza averne particolari conoscenze e a soli fini di lucro, addossano al ricorrente una maggiore negligenza molto spesso determinante e non meritevole di tutela.

Infine, in tema di applicabilità o meno degli indici di anomalia, il Collegio di Torino, per quanto il caso giudicato concernesse il disconoscimento da parte di una società di una serie di bonifici disposti da remoto – e, per i quali, è stata fornita dal PSP la corretta prova dell'autenticazione a due fattori (SCA) – ha rilevato che "*allo stato non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle somme di cui hanno la disponibilità sul presupposto – indimostrato ed indimostrabile – che ogni operazione anomala sarebbe di per sé truffaldina (cfr. Collegio di Torino, decisione n. 1787/2025). L'ipotesi di un obbligo in capo al PSP di intervenire ogniqualvolta il proprio utente pagatore disponga uno o più bonifici di importo anomalo non è supportata da adeguata base giuridica e, a normativa vigente, confligge*

[24]Nella fattispecie, trattavasi di undici bonifici istantanei per un totale di circa 34.000,00 euro, effettuati da remoto nell'arco di quasi sette ore.

[25] Sul tema, vd. anche Collegio di Torino, decisione n. 2684/2025.

con l'obiettivo di garantire certezza e celerità dei pagamenti, anche nell'interesse dei consumatori stessi, e con il delicato bilanciamento normativo di riparto delle reciproche responsabilità, secondo le rispettive sfere di influenza (Tribunale di Milano, sentenza n. 1596/2023)" (decisione n. 5576 dell'11/06/2025)[26].

4.2. Pagatore vs. Banca beneficiaria.

4.2.1. Il conto fittizio.

Appurato che non sempre è agevole per il ricorrente ottenere un accoglimento del ricorso, soprattutto nel caso in cui la Banca abbia assolto diligentemente ai propri obblighi ed in assenza di indici di anomalia, si segnala che il cliente-pagatore ha facoltà di rivolgere le proprie pretese anche nei confronti della Banca beneficiaria.

Sulla questione, infatti, il Collegio di Roma, nella decisione n. 851/2024, ha previsto che, nel caso di inadempimento all'obbligo di adeguata verifica della clientela nell'apertura a distanza di un rapporto di conto corrente, può sussistere, nei confronti del *solvens* vittima di frode, la responsabilità della banca di radicamento del conto dell'*accipiens*, mero titolare fittizio del conto a seguito di furto d'identità. In tali casi, il risarcimento del danno può essere limitato ex art. 1227 c.c. in ragione del concorso di colpa del danneggiato.

In primis, si ricorda la competenza dell'ABF a pronunciarsi nel caso in cui la questione verta sulla correttezza del comportamento della Banca nel dare attuazione alla normativa antiriciclaggio (vd., Collegio di coordinamento n. 1170/2023).

Circa la responsabilità risarcitoria della Banca beneficiaria ove è radicato il conto presso cui sono state fatte transitare le somme oggetto di frode, già il Collegio di Napoli[27] ha evidenziato che la mancata attuazione degli obblighi di identificazione della clientela ex art. 17 e ss. D.lgs. 231/2007, pregiudicando la possibilità per l'ordinante di recuperare le somme, si pone in relazione causale con il verificarsi dell'evento dannoso.

Nella decisione romana ricordata, preliminarmente, è stato ribadito che, sebbene non vi sia un legame contrattuale diretto tra chi effettua il pagamento e Banca del destinatario, il primo rientra comunque nella nozione di "*cliente*" di cui alle "*Disposizioni della Banca d'Italia sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*", ossia il soggetto che è entrato con essa in una non meglio precisata "*relazione*", evidentemente non

[26] A titolo di completezza, si vd. anche Trib. Ancona, sent. n. 338/2024.
[27] Vd., decisioni nn. 9801/2023 e 25262/2021.

contrattuale, ma pur sempre finalizzata alla prestazione di servizi bancari o finanziari, ivi compresi i servizi di pagamento.

Quanto al modo corretto di intendere questa "*relazione*", all'interno delle Disposizioni citate, è specificato che "*tra le ipotesi di relazione con l'intermediario per la prestazione di servizi bancari e finanziari rientrano anche le trattative precontrattuali, che possono dar luogo a controversie concernenti il rispetto delle norme in materia di trasparenza, indipendentemente dall'effettiva conclusione di un contratto*".

Sul punto, proprio la disciplina legale delle trattative precontrattuali, che impone alle parti di comportarsi secondo buona fede (art. 1337 c.c.), è ormai riconosciuta anche nella giurisprudenza di legittimità come il luogo normativo di emersione di un principio generale di tutela dell'affidamento nell'ambito del c.d. "*contatto sociale qualificato*", e cioè in tutti quei casi in cui un soggetto può legittimamente confidare nella correttezza di un altro soggetto, e perciò nella conseguente protezione della propria sfera giuridico-patrimoniale. E ciò in ragione della "*qualificazione professionale*" del soggetto col quale viene comunque a trovarsi in "*contatto*" pur in mancanza di uno specifico rapporto di prestazione.

Secondo il Collegio, un simile contatto qualificato è senz'altro riconoscibile anche in casi in cui, sulla base delle indicazioni ricevute dall'*accipiens*, il *solvens* disponga l'accredito di un pagamento su un conto corrente bancario. Anche in certi casi, infatti, il *solvens*, in virtù dello *status* professionale dell'intermediario presso cui sussiste il conto di accredito, può legittimamente confidare nell'effettiva destinazione del pagamento e nell'identità reale del destinatario di esso, dato che il PSP è tenuto a svolgere la propria attività secondo la diligenza tecnica in forza dell'art. 1176, co. 2, c.c.

Il che vuol dire che l'adempimento degli obblighi di adeguata verifica, ai sensi dell'art. 17 e ss. D.lgs. n. 231/2007, rileva non soltanto dal punto di vista (pubblicistico) delle misure "*di prevenzione e contrasto dell'uso del sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo*", ma anche al fine (privatistico) di proteggere chi utilizza un servizio bancario da possibili invasioni lesive in occasione di tale contatto sociale qualificato con l'operatore professionale.

In effetti, non sembra dubitabile che poter confidare sulla professionalità di un banchiere significa anche poter confidare sull'adeguata verifica da parte sua dell'identità della clientela, e perciò anzitutto sulla reale intestazione del conto bancario a favore del quale si dispone l'accredito di un pagamento. In altri termini, è proprio l'intermediazione professionale di un

banchiere a legittimare l'affidamento di chi paga nell'effettiva titolarità del conto indicato per l'accredito del pagamento.

Pertanto, appurata la possibilità del pagatore di far ricorso nei confronti del PSP beneficiario, la valutazione si è spostata successivamente sul piano dell'adeguata verifica in sede di accensione del conto corrente. Nel merito, il Collegio non ha ritenuto assolti detti obblighi poiché, trattandosi di un conto corrente acceso da remoto (*online*), la documentazione fornita dall'intermediario non rientrava all'interno dei casi tassativi previsti *ex lege* (art. 19 D.lgs. 231/2007[28]).

Sull'intestazione quindi '*fittizia*' del rapporto beneficiario, prosegue poi il Collegio sostenendo che "*È ben vero che un intestatario reale avrebbe comunque potuto occultare tempestivamente l'importo accreditato sul conto e che poi avrebbe potuto anche rendersi insolvente alla pretesa restitutoria esercitata dal* solvens *nei suoi confronti. È anche vero però che, in caso di intestazione reale del conto di accredito del pagamento, il* solvens *avrebbe comunque potuto far valere una pretesa restitutoria nei confronti di un*

[28] A titolo di completezza: *"(…) L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, nei seguenti casi:*
1) per i clienti i cui dati identificativi risultino da atti pubblici, da scritture private autenticate o da certificati qualificati utilizzati per la generazione di una firma digitale associata a documenti informatici, ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82;
2) per i clienti in possesso di un'identità digitale, con livello di garanzia almeno significativo, nell'ambito del Sistema di cui all'articolo 64 del predetto decreto legislativo n. 82 del 2005, e della relativa normativa regolamentare di attuazione, nonché di un'identità digitale con livello di garanzia almeno significativo, rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014, o di un certificato per la generazione di firma elettronica qualificata o, infine, identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale;
3) per i clienti i cui dati identificativi risultino da dichiarazione della rappresentanza e dell'autorità consolare italiana, come indicata nell'articolo 6 del decreto legislativo 26 maggio 1997, n. 153;
4) per i clienti che siano già stati identificati dal soggetto obbligato in relazione ad un altro rapporto o prestazione professionale in essere, purché le informazioni esistenti siano aggiornate e adeguate rispetto allo specifico profilo di rischio del cliente;
4-bis) per i clienti che, previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'articolo 4 del Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017, dispongono un bonifico verso un conto di pagamento intestato al soggetto tenuto all'obbligo di identificazione. Tale modalità di identificazione e verifica dell'identità può essere utilizzata solo con riferimento a rapporti relativi a carte di pagamento e dispositivi analoghi, nonché a strumenti di pagamento basati su dispositivi di telecomunicazione, digitali o informatici, con esclusione dei casi in cui tali carte, dispositivi o strumenti sono utilizzabili per generare l'informazione necessaria a effettuare direttamente un bonifico o un addebito diretto verso e da un conto di pagamento;
(4-ter) per i clienti già identificati da un soggetto obbligato, i quali, previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'articolo 4 del regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, consentono al soggetto tenuto all'obbligo di identificazione di accedere alle informazioni relative agli estremi del conto di pagamento intestato al medesimo cliente presso il citato soggetto obbligato in uno Stato membro dell'Unione europea. Tale modalità di identificazione e verifica dell'identità può essere utilizzata solo con riferimento a rapporti relativi a servizi di disposizione di ordini di pagamento e a servizi di informazione sui conti previsti dall'articolo 1, comma 2, lettera h-septies.1), numeri 7) e 8), del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385.
Il soggetto tenuto all'obbligo di identificazione acquisisce in ogni caso il nome e il cognome del cliente);
5) per i clienti i cui dati identificativi siano acquisiti attraverso idonee forme e modalità, individuate dalle Autorità di vigilanza di settore, nell'esercizio delle attribuzioni di cui all'articolo 7, comma 1, lettera a), tenendo conto dell'evoluzione delle tecniche di identificazione a distanza; (…).".

accipiens *identificato, mentre nel caso in questione proprio l'intestazione fittizia ha fatto sì che il* solvens *non sappia neppure chi sia il soggetto verso cui far valere il proprio diritto alla ripetizione dell'indebito, sicché si deve dire che una pretesa restitutoria sussiste solo virtualmente. Ora, poiché il rischio dell'insolvenza dell'*accipiens *non viene meno del tutto neppure in caso di intestazione reale, si può ritenere che l'entità del pregiudizio economico cagionato dall'inadempimento dell'intermediario non coincida senz'altro con il pagamento eseguito. Nondimeno, ad avviso del Collegio, deve comunque riconoscersi che l'inadempimento dell'intermediario ha aggravato in maniera determinante il pericolo del danno subìto dal ricorrente, sicché non può non ritenersi sussistente un nesso causale tra inadempimento e danno. È vero invece che anche il ricorrente con la sua condotta colpevole ha contribuito alla produzione del danno sofferto, segnatamente, come rilevato dall'intermediario, disponendo un pagamento a favore di un tale mai conosciuto di persona e senza aver avuto alcuna garanzia in ordine alla consegna del bene acquistato. Sulla base di quanto si è detto non si può tuttavia ritenere che questo dato valga ad escludere il nesso causale tra l'inadempimento dell'intermediario resistente e il danno occorso al ricorrente. E ciò perché, come si è chiarito, proprio nell'intestazione fittizia deve riconoscersi un elemento determinante della truffa perpetrata ai danni del ricorrente. Concludendo sul punto, il Collegio ritiene quindi che nel caso di specie debba riconoscersi un concorso di colpa del danneggiato con conseguente limitazione del risarcimento ai sensi dell'art. 1227, co. 1, cod. civ.*[29]".

In conclusione, le possibilità di recuperare tutto o parte della somma bonificata aumentano a favore del pagatore, a fronte del possibile mancato assolvimento degli obblighi di adeguata verifica da parte della Banca beneficiaria nei confronti del titolare del rapporto di ricezione.

4.2.2. La diversa intestazione del rapporto beneficiario.

Nei casi in cui, ad esempio, il pagatore sia convinto di eseguire un bonifico in sicurezza a favore di se stesso, ma su coordinate accese presso altro intermediario, è logico immaginare come nella contabile di pagamento compaia proprio il suo nome alla voce beneficiario.

Tuttavia, salvo furto d'identità, è improbabile che il conto destinatario sia nominativamente intestato all'ordinante. Nella quasi totalità dei casi, infatti, il conto ricevente viene intestato a persona di comodo e resta aperto per un periodo limitato (fino alla scoperta della natura fraudolenta).

[29] Nella fattispecie, è stata sancita la responsabilità nella misura di 1/3 a carico del PSP.

Come già precisato nel corso della trattazione, allo stato attuale, ciò che '*comanda*' ai fini della corretta esecuzione del bonifico sono esclusivamente le coordinate Iban (vd., art. 24 D.lgs. 11/2010).

Tuttavia, esistono fattispecie in cui l'intermediario può essere considerato responsabile nonostante il regolare accredito a favore delle coordinate indicate dal pagatore.

Sul tema, recentemente la Cassazione, nella sentenza n. 17415/2024, ha fatto luce sulla "*consapevolezza*" da parte dell'intermediario ricevente circa l'incoerenza dei dati forniti dal pagatore, ossia della non corrispondenza tra beneficiario – inserito nell'ordine di pagamento – ed effettivo titolare del conto di accredito.

È giusto pertanto dubitare del regolare operato da parte della Banca qualora, essendo già a conoscenza dell'errore da parte del pagatore, prima ancora dell'effettivo accredito a favore del beneficiario, abbia eseguito ciononostante l'accredito. Tale consapevolezza, quindi, si traduce in una sorta di colpa grave, se non addirittura dolo, a carico dell'intermediario.

Quanto sopra, tuttavia, non significa che il PSP beneficiario debba attuare – a normativa ancora attualmente vigente – un controllo circa la corrispondenza dei dati[30].

Tutt'altro. La consapevolezza in questione si può – di fatti – tecnicamente verificare, ad esempio, quando il conto beneficiario presenti già un qualsivoglia tipo di '*blocco operativo*' ancor prima di ricevere l'accredito. Alcuni tipi di blocchi procedurali, in particolare, consentono la temporanea sospensione della somma in attesa di ulteriori verifiche da parte dell'intermediario beneficiario.

Al momento si esclude comunque la possibilità di una verifica sui bonifici istantanei, in quanto la presenza di un blocco operativo sul rapporto beneficiario ne impedisce tecnicamente la contabilizzazione entro i 10 secondi canonici normativamente previsti.

Ad ogni modo, la richiesta da parte del pagatore di verifica della diretta contabilizzazione – senza, quindi, ulteriori controlli tecnici – all'intermediario beneficiario può rappresentare, talvolta, una possibilità in più circa il recupero dei fondi; soprattutto nel momento in cui il PSP abbia effettuato un controllo a fronte di blocco operativo e, nonostante l'incoerenza dei dati, senza ulteriori indagini, abbia accreditato la somma.

[30] In tal senso, vd. Cass. 21105/2025; ABF, Collegio di coordinamento, decisione n. 6886/2022; Collegio di Palermo, decisione n. 10045/2020; Corte di Giustizia UE, sez. X, sent. n. C 245/18, Tecnoservice Int.

4.2.3. Il nuovo servizio di verifica del beneficiario.

Un breve cenno finale merita l'imminente introduzione del servizio di "verifica del beneficiario" (c.d. "*verification of payee*") che, dal 09 ottobre p.v., sarà introdotto per i bonifici riguardanti i PSP situati in un Paese aventi come moneta legale l'euro[31].

In sostanza, ogniqualvolta si disporrà un bonifico, soprattutto a fini di tutela della clientela in ottica antifrode, il pagatore avrà la possibilità di farsi confermare dagli intermediari coinvolti (banca ordinante e banca ricevente) la correttezza dei dati inseriti. Qualora non dovesse esserci coerenza, anche solo parziale, il pagatore avrà la facoltà di eseguire comunque il bonifico oppure di correggerlo o annullarlo.

Ai fini di quanto esaminato nella presente trattazione, tuttavia, si ritiene che detta verifica, per quanto innovativa e a maggiore tutela dei risparmi dei consumatori, non impatterà in maniera incisiva sul fenomeno, poiché è sufficiente che il sedicente operatore convinca il cliente, tramite tecniche che con il tempo diventano ormai sempre più sofisticate, ad effettuare un bonifico a favore di un soggetto sconosciuto, ma il cui nominativo effettivamente corrisponda al titolare di quelle coordinate.

Pertanto, ed in conclusione, si ritiene più conveniente, lato pagatore, sondare il corretto assolvimento degli obblighi di adeguata verifica da parte dell'intermediario.

[31] Vd., Regolamento (UE) 2024/886 del 13/03/2024 che modifica i regolamenti (UE) nn. 260/2012 e 2021/1230 e le direttive 98/26/CE e (UE) 2015/2366 per quanto riguarda i bonifici istantanei in euro (L_202400886EN.000101.fmx.xml.).