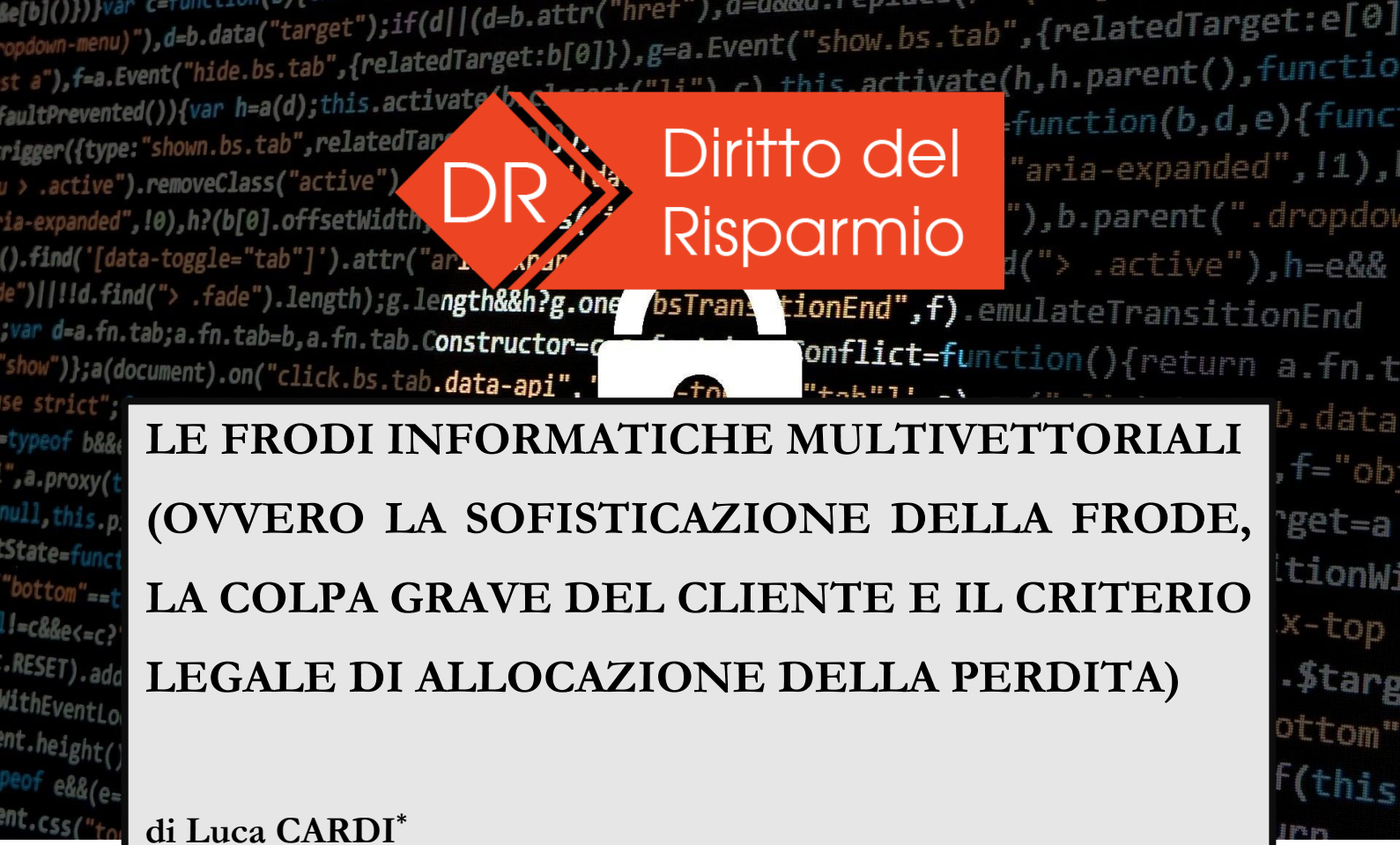

LE FRODI INFORMATICHE MULTIVETTORIALI (OVVERO LA SOFISTICAZIONE DELLA FRODE, LA COLPA GRAVE DEL CLIENTE E IL CRITERIO LEGALE DI ALLOCAZIONE DELLA PERDITA)

di Luca CARDI*

Settembre

fascicolo 3/2026

*Addetto Servizi Legali. Le tesi sostenute nel presente contributo, la selezione delle questioni affrontate, l'impostazione del ragionamento e le conclusioni interpretative sono imputabili esclusivamente all'autore. Nella preparazione ed elaborazione del lavoro ci si è avvalsi di strumenti di intelligenza artificiale generativa (nel caso di specie, Lexroom e Libra by Wolters Kluwer) quale supporto alla ricerca normativa e giurisprudenziale, al raffronto tra orientamenti e alla sistematizzazione dei materiali. La selezione delle fonti rilevanti, la lettura dei testi normativi e delle pronunce richiamate, nonché la verifica finale della coerenza argomentativa del contributo, sono state svolte personalmente dall'autore. L'impiego di tali strumenti non sostituisce l'apporto intellettuale dell'autore nelle parti del contributo che ne costituiscono espressione. Le analisi, le opinioni e le conclusioni contenute nel presente contributo sono espresse a titolo puramente personale dall'autore. Esse non impegnano in alcun modo la responsabilità, né riflettono la posizione o le strategie, dell'Istituto di Credito per il quale l'autore svolge la propria attività professionale.

ISSN 2785-3004

Rivista di Diritto del Risparmio

APPROFONDIMENTI

Le frodi informatiche multivettoriali (ovvero la sofisticazione della frode, la colpa grave del cliente e il criterio legale di allocazione della perdita)[*]

di Luca CARDI[**]

Settembre
fascicolo 3/2026

---

[*] Contributo approvato dai *referee*.

[**] Addetto Servizi Legali. Le tesi sostenute nel presente contributo, la selezione delle questioni affrontate, l'impostazione del ragionamento e le conclusioni interpretative sono imputabili esclusivamente all'autore. Nella preparazione ed elaborazione del lavoro ci si è avvalsi di strumenti di intelligenza artificiale generativa (nel caso di specie, Lexroom e Libra by Wolters Kluwer) quale supporto alla ricerca normativa e giurisprudenziale, al raffronto tra orientamenti e alla sistematizzazione dei materiali. La selezione delle fonti rilevanti, la lettura dei testi normativi e delle pronunce richiamate, nonché la verifica finale della coerenza argomentativa del contributo, sono state svolte personalmente dall'autore. L'impiego di tali strumenti non sostituisce l'apporto intellettuale dell'autore nelle parti del contributo che ne costituiscono espressione. Le analisi, le opinioni e le conclusioni contenute nel presente contributo sono espresse a titolo puramente personale dall'autore. Esse non impegnano in alcun modo la responsabilità, né riflettono la posizione o le strategie, dell'Istituto di Credito per il quale l'autore svolge la propria attività professionale.

Le frodi informatiche multivettoriali (ovvero la sofisticazione della frode, la colpa grave del cliente e il criterio legale di allocazione della perdita).

A cura di Luca CARDI.

"Meglio dallo psicanalista che dal confessore.
Per questo è sempre colpa tua,
per quello è sempre colpa degli altri."
(Marcello Marchesi)

Premettiamo, all'inizio di queste righe, che apparteniamo a coloro che, per formazione intellettuale e culturale, preferiscono il confessore allo psicanalista. Per una pluralità di ragioni che sarebbe qui difficile (e inutile, attese le finalità dello scritto) riportare. Ma una su tutte. Crediamo – sempre abbiamo creduto – che individuare con precisione le proprie e le altrui colpe serva a non confondere soluzioni giuridiche con *"percorsi assolutori"*. *"Inizio della salvezza è la conoscenza della colpa"*, ammoniva Lucio Annea Seneca nelle *Epistulae ad Lucilium*. Dal canto suo – ed è ancora più duro monito – Umberto Eco sottolineava che *"Poiché nessuno pensa che le sue sventure possano essere attribuite a una sua "pochezza"* [virgolette apposte dal redattore del contributo]*, ecco che dovrà individuare un colpevole"*.

Quadro sintetico della tesi sostenuta nel contributo e dei relativi punti qualificanti

L'articolo assume espressamente che il d.lgs n. 11/2010 configuri un modello di allocazione del rischio tendenzialmente binario (rimborso a carico del PSP ovvero esonero in presenza di dolo/frode/colpa grave dell'utente), e che la *"sofisticazione"* della frode non costituisca, di per sé, causa esimente dalla valutazione di colpa grave dell'utente. Ne discende che l'art. 1227 c.c. non opera come correttivo equitativo nel perimetro dell'art. 12 del d.lgs n.11/2010.

La responsabilità del prestatore di servizi di pagamento si radica sul piano contrattuale (artt. 1218 e 1176, co. 2, c.c.) e opera sul piano di una diligenza professionale qualificata; il decreto stabilisce un modello binario di responsabilità/esonero fondato sull'art. 12. La

nozione di *"negligenza grave"* rilevante travalica la mera disattenzione, come chiarito in giurisprudenza anche alla luce del considerando 72 della PSD2. Quanto all'onere probatorio, al PSP non basta la mera registrazione tecnica: deve provare l'autenticazione e allegare circostanze concrete idonee a far emergere la colpa grave dell'utente (dinamica della frode, contenuti di messaggi/chiamate, presidi adottati e interazione/condotta del cliente).

Le frodi multivettoriali (*smishing, vishing, sms/caller ID spoofing*) sono ormai socialmente note, sicché l'errore dell'utente medio non è automaticamente scusabile; più decisioni di merito hanno valorizzato tale notorietà nel fondare la colpa grave. In particolare, si segnalano talune pronunce (in appresso richiamate), che collegano la colpa grave alla diffusione del fenomeno e alla sua percepibilità per l'utente medio. La presenza di campagne antifrode capillari eleva ulteriormente la conoscibilità del rischio e, se disattese (divieto di comunicare codici, PIN, OTP), radica la colpa grave.

Costituiscono indicatori qualificati di colpa grave: (i) il clic su link con URL non riconducibile al dominio dell'intermediario, anche se l'SMS si inserisce nella chat genuina; (ii) la comunicazione o l'inserimento di credenziali/OTP, specie quando vanificano i presidi di sicurezza predisposti (a titolo esemplificativo: attivazione *app* su dispositivo del frodatore); (iii) l'inerzia dinanzi ad alert/notifiche e il ritardo nella segnalazione all'intermediario; (iv) la violazione di clausole contrattuali che impongono l'accesso digitando l'indirizzo della banca e vietano l'uso di link ricevuti via SMS/e-mail, condotta ritenuta autonomamente causativa del danno.

L'orientamento arbitrale e giurisprudenziale che valorizza l'*"insidiosità"* di tali tipologie di frode tende a escludere la colpa quando mancano indici percepibili; tale impostazione cede, però, se sono presenti segnali d'allarme oggettivi (*URL* anomalo, errori, richieste incoerenti e/o *"eccentriche"* rispetto alla consueta operatività e, anzi, con essa in palese conflitto) anche in contesti di *spoofing* sofisticato. La linea giurisprudenziale e arbitrale *"rigorosa"* riconduce la materia all'art. 12 del d.lgs n. 11/2010, escludendo l'uso dell'art. 1227 c.c. per riparti equitativi e imputando integralmente la perdita all'utente in caso di colpa grave accertata.

1. Premessa: la tesi e il suo rilievo sistematico.

La questione della responsabilità per operazioni di pagamento fraudolente realizzate attraverso ***smishing***, ***vishing***, ***sms spoofing*** e ***caller ID spoofing*** è oggi uno dei terreni più instabili del contenzioso bancario. Il punto davvero divisivo non è più l'astratta riconducibilità di tali fenomeni alla categoria delle *"frodi sofisticate"*, bensì la corretta individuazione del **criterio normativo di allocazione della perdita** tra prestatore di servizi di pagamento e utente.

La tesi qui sostenuta è duplice.

Da un lato, anche nelle frodi multivettoriali può ben configurarsi una **colpa grave dell'utente**, quando questi tenga condotte di cooperazione attiva o di macroscopica trascuratezza: clic su link anomali, comunicazione o inserimento di credenziali, OTP o PIN, mancata attivazione di presidi antifrode pur resi disponibili, ritardo nella segnalazione, adesione a istruzioni palesemente *eccentriche* rispetto alla fisiologia del rapporto bancario.

Dall'altro lato, una volta ricondotta la fattispecie nel perimetro degli artt. 10 e 12 del d.lgs n. 11/2010, l'innesto dell'art. 1227 c.c. appare sistematicamente improprio, poiché la disciplina speciale realizza un modello tendenzialmente **binario**: o il PSP risponde, oppure è esonerato per dolo o colpa grave dell'utente.

Ne consegue che la categoria della "sofisticazione della frode" non può trasformarsi in un criterio "*occulto*" di deresponsabilizzazione del cliente né in una base per soluzioni equitative di riparto del danno non previste dalla legge.

2. Le frodi multivettoriali: struttura fenomenologica e notorietà del rischio.

Le frodi multivettoriali si caratterizzano per la **combinazione seriale di più canali di attacco**. In termini generali:

lo ***smishing*** impiega *SMS* fraudolenti che inducono il cliente a cliccare un *link*, richiamare un numero o inserire dati riservati;

il ***vishing*** utilizza il contatto telefonico del truffatore, che si presenta come operatore bancario;

lo ***spoofing*** consente al messaggio o alla chiamata di apparire come provenienti da un mittente genuino;

il ***caller ID spoofing*** fa apparire la telefonata come proveniente dal numero della banca o di una sua filiale.

Una pronuncia del Tribunale di Monza descrive la fattispecie esaminata come ***"sms spoofing, misto a ID caller spoofing"*** *[Tribunale Di Monza, Sentenza n.2072 del 23 Luglio 2024]*. Tale sentenza sottolinea che si tratta di una tecnica *"potenzialmente più decettiva ed insidiosa rispetto al comune phishing"*. Questo dato fenomenologico, tuttavia, non equivale ancora a una conclusione in termini di assenza della colpa grave: segnala solo che la valutazione deve essere condotta con attenzione alle concrete modalità del fatto. Un punto di grande rilievo è che tali frodi non siano più eventi contraddistinti da un profilo di assoluta novità o socialmente ignoti. La loro ampia diffusione e la crescente attenzione delle campagne antifrode rendono meno plausibile una generalizzata scusabilità dell'errore. In questa prospettiva, la *"multivettorialità"* dell'attacco non elimina il dovere dell'utilizzatore di adottare le **ragionevoli misure di prudenza** richieste dal rapporto.

Prima ancora di affrontare il merito della distribuzione del rischio nel sistema del d.lgs n. 11/2010, dunque, occorre soffermarsi su un presupposto di fatto che condiziona l'intero impianto valutativo: la **conoscibilità sociale** delle frodi multivettoriali da parte dell'utenza media. Il rilievo non è accessorio. Nella struttura dell'illecito civile, la prevedibilità del pericolo è un elemento che incide sulla misura dello *standard* di diligenza esigibile: quanto più un rischio è noto, diffuso e comunicato, tanto meno è tollerabile che il soggetto esposto vi *"soccomba"* senza che la sua inerzia o imprudenza riceva una qualificazione giuridicamente significativa. Nelle frodi c.d. multivettoriali – che combinano *smishing* (*SMS* fraudolento o *"spoofato"*), *vishing* (telefonata del falso operatore) e, nelle varianti più evolute, *caller ID spoofing* (identità numerica contraffatta della banca) – questo presupposto è oggi pienamente integrato. Le principali fonti giurisprudenziali, tanto arbitrali quanto di merito, concordano nel ritenere che tali tecniche di frode abbiano raggiunto un livello di diffusione tale da renderle **conoscibili anche all'utente non specializzato**, con la conseguenza che un comportamento *"passivo"* nei loro confronti non è automaticamente scusabile per difetto di informazione.

La giurisprudenza di merito ha elaborato, con progressiva coerenza, un orientamento che valorizza esplicitamente la notorietà acquisita nel tempo da queste tipologie di frode.

Il Tribunale di Siracusa *[Sentenza n. 1538 del 26 giugno 2024]*, ricostruisce la sequenza combinata di *smishing* e *vishing*. Tre piani si intrecciano nell'argomentazione del giudice ibleo: la notorietà del fenomeno come fatto sociale; la sua percepibilità da parte dell'utente medio;

la responsabilità informativa specificamente assunta dalla banca attraverso le campagne antifrode. Tutti e tre concorrono a strutturare il giudizio di colpa grave.

In senso conforme si è pronunciato il Tribunale di Firenze *[Sentenza n. 3525 del 4 novembre 2025]* che ribadisce come, nelle ipotesi di *smishing* e *vishing* non caratterizzate da artifici eccezionalmente sofisticati, si sia consolidato l'orientamento secondo cui l'utente che asseconda il frodatore risponde a titolo di colpa grave, in ragione della *"notorietà che nel tempo"* queste frodi *"hanno acquisito"*.

Il Tribunale di Lanciano *[Sentenza n. 383 dell'11 novembre 2024]* benché incentrato su una fattispecie mista (vishing senza spoofing telefonico, seguita da smishing con spoofing del mittente), offre un passaggio di sicuro interesse nella parte in cui collega il giudizio di colpa grave dell'utente al fatto di avere *"dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa"* ormai generalizzata. Il sintagma *"capillare campagna informativa"* presuppone, anche in questa sede, che il rischio fosse già ampiamente noto alla clientela e specificamente comunicato dagli intermediari.

La medesima argomentazione si rinviene in diversi precedenti dell'Arbitro Bancario Finanziario *[cfr. ex multis: Collegio di Milano, Decisione n. 8459 dell'8 agosto 2023; Collegio di Bologna, Decisione n. 2847 del 30 marzo 2026 e Decisione n. 5788 del 16 giugno 2025; Collegio di Roma, Decisione n. 8535 del 26 settembre 2025 e Decisione n. 5850 del 17 giugno 2025]*. La Decisione n. 7145 del 19 giugno 2024 del Collegio di Roma offre una prospettiva storica aggiuntiva, recuperando il principio già enunciato dal Collegio di Coordinamento ABF con Decisione n. 3498 del 26 ottobre 2012 – citata nella giurisprudenza di merito come una delle pietre miliari del settore *[cfr. Tribunale di Palermo, Sentenza n. 2346 del 19 aprile 2024]* – secondo cui nelle forme tradizionali di *phishing* e *smishing "il cliente è vittima di una colpevole credulità"* e *"tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet."*. Il richiamo a questa massima, consolidatasi oltre dieci anni fa, conferma che la notorietà del fenomeno non è un'acquisizione recente, ma un dato giuridicamente sedimentato.

Un profilo particolarmente rilevante è quello delle **campagne informative svolte dagli intermediari**. L'esistenza di una campagna antifrode specifica, documentata e capillare eleva il livello di conoscibilità soggettiva del rischio: se il cliente ha ricevuto comunicazioni della propria banca che lo avvertivano di non comunicare mai codici di accesso, PIN o OTP a soggetti terzi – inclusi presunti operatori bancari – la successiva comunicazione di quei dati

non può essere qualificata come semplice ingenuità scusabile, ma integra la violazione di un avvertimento esplicito.

Per completezza sistematica – e per restituire un quadro realistico del contenzioso – occorre dar conto del limite entro cui l'argomento della notorietà incontra resistenza nella giurisprudenza. L'orientamento che esclude la colpa grave, o ne riduce il peso, si fonda sull'argomento della **sofisticazione eccezionale** della frode. In tali casi, la giurisprudenza arbitrale e di merito tende a ritenere che nemmeno un utente mediamente diligente avrebbe potuto percepire l'anomalia, per effetto di tecniche di contraffazione che simulano perfettamente l'identità della banca (*SMS* nella medesima chat dei messaggi autentici, numero di telefono visivamente identico a quello della banca, pagina *web* clone del sito ufficiale). Tuttavia, come si argomenterà nei paragrafi successivi, questo orientamento non inficia la tesi della responsabilità integrale dell'utente quando coesistano **indici di anomalia percepibili**: URL non riconducibile alla banca, richieste anomale di eseguire operazioni "per bloccare frodi" o per effettuare improbabili aggiornamenti, moltiplicazione dei codici richiesti. La presenza di almeno uno di tali indici trasforma la valutazione: anche nei casi di *spoofing* sofisticato, l'utente che abbia disatteso segnali di allarme concreti e percepibili non può invocare la scusabilità dell'errore.

3. Il quadro normativo del d.lgs n. 11/2010: consenso, autenticazione, onere della prova e colpa grave.

Il sistema del d.lgs n. 11/2010 si fonda su un **modello binario**: rimborso a carico del PSP oppure esonero del PSP in presenza di dolo, frode o colpa grave dell'utente. Tale inquadramento è coerente con il dato normativo e con i principi civilistici generali.

3.1. La matrice contrattuale della responsabilità del prestatore.

La responsabilità del prestatore di servizi di pagamento è, sul piano civilistico, una responsabilità contrattuale, secondo la regola generale dell'art. 1218 c.c., per cui il debitore che non esegue esattamente la prestazione è tenuto al risarcimento, salvo prova della non imputabilità. In parallelo, la diligenza esigibile dalla banca è quella qualificata dell'art. 1176, comma 2, c.c., da valutarsi *"con riguardo alla natura dell'attività esercitata"*.

Una sentenza del Tribunale di Brescia valorizza esattamente questo duplice fondamento, richiamando l'art. 12, comma 3, d.lgs n. 11/2010 e l'art. 1176, comma 2, c.c. *[Tribunale di*

Brescia, Sentenza n.5084 del 9 dicembre 2024]. Nello stesso arresto è richiamato l'orientamento di legittimità secondo cui il rischio dell'utilizzazione illecita dei codici di accesso da parte di terzi rientra nell'area del rischio professionale del prestatore, salvo dolo del titolare o comportamenti talmente incauti da non poter essere fronteggiati in anticipo.

3.2. L'onere probatorio del PSP.

Nel sistema del decreto, non basta all'intermediario provare la mera registrazione tecnica dell'operazione. Sul PSP grava la prova dell'autenticazione e, in caso di contestazione, l'onere di fornire elementi dai quali desumere la colpa grave dell'utente. Da qui discende un corollario decisivo: la banca che voglia eccepire la colpa grave non può fermarsi alla produzione dei *log*, ma deve ricostruire la sequenza fattuale della frode, il contenuto dei messaggi, la dinamica delle chiamate, gli alert disponibili, le misure di sicurezza predisposte e le modalità con cui il cliente ha interagito con esse.

3.3. Il ruolo della colpa grave dell'utente.

La colpa grave rilevante nel sistema del d.lgs n. 11/2010 non coincide con una qualunque imprudenza. Essa postula una **violazione marcata** degli obblighi di custodia e di corretto uso delle credenziali o, più in generale, un contegno che si collochi ben oltre la mera disattenzione.

La sentenza del Tribunale di Milano n. 7466 del 7 ottobre 2025 lo esprime con chiarezza, richiamando il considerando 72 della direttiva e affermando che per negligenza grave deve intendersi un comportamento *"che si spinge oltre la semplice negligenza e implica un grado significativo di mancanza di diligenza"*. La medesima pronuncia precisa che possono integrare colpa grave le condotte afferenti alla sfera di influenza dell'utente, in particolare quelle che comportano una grave violazione del dovere di adottare *"tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate"*.

4. La configurabilità della colpa grave nelle frodi multivettoriali.

Il nucleo della tesi favorevole all'intermediario consiste nel rifiuto di un automatismo opposto: non è vero che la sola sofisticazione tecnica dello *spoofing* renda il cliente, per definizione, esente da colpa grave.

4.1. Campagna informativa antifrode condotta dalla Banca.

La Decisione n. 5576 dell'11 giugno 2025 del Collegio di Torino dell'ABF valorizza espressamente il fatto che la banca avesse predisposto un sistema di autenticazione a due fattori pienamente conforme. Il Collegio rileva, inoltre, che la medesima banca avesse diffuso campagne informative sulle truffe. Di notevole importanza è il passaggio nel quale il Collegio si sofferma esplicitamente sull'assenza di un obbligo di monitoraggio della Banca per bloccare operazioni che, pur anomale, siano state disposte dal cliente stesso: "*il Collegio evidenzia 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. L'ipotesi di un obbligo in capo al PSP di intervenire ogniqualvolta il proprio utente pagatore disponga uno o più bonifici di importo anomale non è supportata da adeguata base giuridica e, a normativa vigente, confligge con l'obiettivo di garantire certezza e celerità dei pagamenti".*

Il Collegio di Roma dell'ABF, con Decisione n. 3477 del 20 marzo 2024, riconosce anch'esso che la Banca risulta aver predisposto un presidio antifrode adeguato con campagne informative capillari verso i clienti, Cionondimeno il ricorrente ha comunque ceduto i codici a fronte di una reiterata pressione esercitata dal frodatore durata complessivamente circa 25 minuti: *"Le telefonate […] duravano parecchi minuti […]. Nonostante le pressioni dell'interlocutore, la cliente rifiutava di comunicare i codici, 'ma il sedicente operatore tentava comunque di prolungare il più possibile la telefonata e, infine, [la cliente] comunicava l'ultimo codice generato"*. Il Collegio riconosce la colpa grave del cliente, ritenendo che essa tragga fondamento proprio dalla violazione dei contenuti delle campagne informative: *"il Collegio ritiene che sussistano profili di colpa grave del cliente, consistente nell'avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa posta in essere dall'intermediario".*

La Decisione n. 11142 del 22 ottobre 2024 del Collegio di Torino sottolinea, anch'essa, che la Banca aveva documentato un sistema articolato di presidio informativo: *"la Banca ha continuamente sensibilizzato sulla tematica tutta la propria base di clienti tramite un'assidua campagna antiphishing a cadenza periodica, anche inviata personalmente ai singoli clienti; l'intermediario ha anche informato i propri clienti che non vengono mai inviati via SMS link per disconoscere accessi sospetti, come avvenuto nel caso in esame".* Il Collegio riconosce il **comportamento gravemente negligente del ricorrente** che si era dimostrato *"vittima di colpevole credulità"*: *"dalla ricostruzione dei fatti appena descritta e dalle circostanze emerse, non può non rilevarsi il comportamento gravemente negligente e*

imprudente del ricorrente, il quale si è dimostrato vittima di colpevole credulità. Tutte le operazioni sono avvenute in assenza di anomalie e sono state correttamente autenticate, registrate e contabilizzate mediante il corretto inserimento del doppio fattore di autenticazione".

Il Tribunale di Lanciano *[Sentenza n. 383 dell'11 novembre 2024]* afferma che la colpa grave del cliente è provabile *"in via presuntiva"* anche per il fatto di aver dato seguito alle istruzioni del frodatore nonostante la **capillare campagna informativa** generalizzata degli intermediari: *"è predicabile (anche per prova 'in via presuntiva') di colpa grave il comportamento dell'utente (per avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa' ormai generalizzata)".*

4.2 Colpa grave del cliente per aver cliccato sul link di un SMS inseritosi nella chat genuina della Banca ma con URL palesemente falso.

Il Collegio di Milano dell'ABF, con Decisione n. 2296 del 21 febbraio 2024, affronta espressamente la questione della distinzione tra ***spoofing genuino*** e ***phishing ordinario*** quando il link contenuto nel messaggio non è riconducibile al dominio ufficiale della banca, pur essendo il messaggio inserito in una chat denominata con il nome dell'intermediario.

Il Collegio evidenzia che il *link* contenuto nell'*sms 'civetta'* non sembra riconducibile al dominio ufficiale della banca. La conclusione sistematica è netta: *"Per queste ragioni, il Collegio ritiene che nel caso di specie non si sia verificata una vera e propria truffa c.d. di spoofing, come descritta dalla giurisprudenza ABF quale truffa sofisticata; si è piuttosto verificato un normale episodio di phishing, rispetto al quale è ormai pacifica nella giurisprudenza ABF la colpa grave del cliente per avere inserito le credenziali statiche nel 'falso' sito dell'intermediario, dopo avere avuto accesso dal link indicato nel messaggio 'civetta'".*

Pertanto, la presenza del messaggio nella chat non è di per sé sufficiente a qualificare la frode come *"sofisticata"* ove il link sia palesemente falso. È la **combinazione** di chat genuina + URL autentico + errori grammaticali (nel *decisum* dell'arbitro meneghino) che costituisce lo *spoofing* sofisticato; in difetto anche di uno solo di questi elementi, la frode retrocede a phishing ordinario.

La Decisione N. 5576 del 11 giugno 2025 del Collegio di Torino dell'ABF analizza un caso in cui il messaggio *SMS* civetta presentava un *link* non riconducibile al dominio ufficiale*: "Indipendentemente dall'evidenza testuale data da anomalie grafiche nei due messaggi, tali da rendere evidente che non potevano essere stati inviati da una banca, il link contenuto nel primo SMS non poteva essere riconducibile a un sito dell'Intermediario […]".*

La Decisione N. 3477 del 20 marzo 2024 del Collegio di Roma affronta un caso in cui il messaggio civetta si era effettivamente inserito nella chat genuina dell'intermediario (*spoofing* in senso tecnico). Tuttavia il Collegio valorizza come **indici di anomalia rilevabili dall'utente mediamente attento** la presenza di un *URL* non riconducibile alla banca. Pur pervenendo a un **concorso di colpa** (non a colpa grave esclusiva) in ragione della genuinità della chat, il Collegio afferma che la presenza di indici di anomalia – tra cui il *link* anomalo – costituisce elemento che fonda la **colpa grave del cliente**: *"il Collegio ritiene che sussistano profili di colpa grave del cliente - consistente nell'avere dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa posta in essere dall'intermediario - e che essi siano tali da contribuire alla causazione dell'evento dannoso"*. Anche nel caso di genuina chat *spoofata*, la presenza di un *URL* palesemente falso è sufficiente a fondare la colpa grave del cliente.

Paradigmatico, poi, il caso esaminato dal Collegio di Torino dell'ABF *[Decisione n. 11142 del 22 ottobre 2024]*: SMS **inserito nella chat genuina + caller ID spoofing** verificato, ma con link non riconducibile all'intermediario e con errore grammaticale. Il Collegio enuncia il principio generale: *"in linea con gli orientamenti condivisi dei Collegi ABF, nello spoofing la presenza nel testo dei messaggi civetta di indici di anomalia, quale l'inequivoca non riconducibilità all'intermediario del link ivi contenuto e la presenza di evidenti errori grammaticali o sintattici, dovrebbero far allertare l'utente avveduto. In tale ipotesi si ritiene che possa rilevarsi un concorso di colpa a carico del cliente per aver agevolato il compimento della truffa"*. In questo precedente, pur essendoci genuino *spoofing* del *caller ID* e inserimento nella *chat,* la presenza del *link* falso ha **ridotto significativamente la responsabilità dell'intermediario** a un terzo, lasciando i due terzi della perdita subita in capo al cliente.

Il Collegio di Roma dell'ABF, con la Decisione n. 7491 del 27 giugno 2024, afferma espressamente che la non riconducibilità del *link* all'intermediario costituisce **anomalia del messaggio civetta** rilevante per la prova della colpa grave: *"Costituisce difatti un'anomalia del messaggio civetta l'invito a selezionare un link assolutamente non riferibile all'intermediario […]"*. E il principio generale: *"Concordemente all'orientamento condiviso tra i Collegi, può essere rilevata in via esclusiva la colpa grave del cliente (con conseguente rigetto del ricorso) laddove, oltre ad indici di anomalia come quelli già richiamati, pervenga al cliente una comunicazione ulteriore rispetto alla procedura di autenticazione forte, tale da sollecitare la sua attenzione sull'operazione che sta per autorizzare"*. In quel caso il Collegio di Roma ha deciso per il concorso di colpa per la presenza di un messaggio fittizio di storno

che aveva ingannato il cliente sulla natura dell'operazione. In assenza di tale elemento aggiuntivo, il *link* anomalo avrebbe condotto alla colpa grave esclusiva.

Il Tribunale di Lanciano *[Sentenza n. 383 dell'11 novembre 2024]* indica espressamente tra gli indici di colpa grave del cliente: *"l'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta"*.

La Corte d'Appello dell'Aquila *[Sentenza n. 1001 del 22 settembre 2025]* esamina un caso in cui si rileva un *link* non autentico e riguarda specificamente la **violazione contrattuale dell'obbligo di non usare link ricevuti via SMS** per accedere all'area personale: *"nell'art. 5 del contratto relativo al servizio di home banking prodotto dalla [banca] è previsto che l'utente si impegna ad adottare in particolare tutte le ragionevoli misure idonee e a proteggere i codici di accesso da utilizzi non autorizzati, prevedendo in particolare che il corretto accesso all'area personale del sito della Banca sia effettuato digitando nel browser l'indirizzo del sito ed effettuando il login senza utilizzare per l'accesso i link ricevuti via e-mail o tramite altri canali"*. La Corte afferma poi: *"il fatto che l'utente abbia immesso le proprie credenziali in una pagina web aperta utilizzando un link ricevuto attraverso un SMS costituisce una violazione dei suddetti obblighi, che ha originato già in sé e in via autonoma l'evento dannoso"*. E, sull'informativa antifrode della Banca, comprensiva di avvisi sul sito: *"nella guida prodotta dalla medesima Banca sono indicati, proprio al fine di tutelare i clienti, molteplici esempi di attacchi fraudolenti, tra cui l'ipotesi di SMS inviati da soggetti individuati con sigle simili a quelle della denominazione della Banca e in particolare con una sigla come quella utilizzata in questo caso. La [Banca] ha anche indicato ai clienti che il proprio numero verde è configurato per la sola ricezione e non può essere utilizzato per chiamare i medesimi clienti."*. La Corte qualifica il *clic* sul *link* ricevuto via *SMS* come **violazione contrattuale autonomamente causativa del danno**, indipendentemente dalla questione della genuinità della chat o della falsità del link.

In conclusione, il principio consolidato ABF è che la presenza del messaggio nella *chat* genuina non basta a qualificare la frode come *"sofisticata"* ove il *link* sia **palesemente non riconducibile al dominio dell'intermediario**. In tal caso la frode retrocede a phishing ordinario con conseguente **colpa grave esclusiva del cliente**. Nei casi in cui il link sia anomalo ma la chat contenga messaggi genuini precedenti e non vi siano errori grammaticali, il Collegio tende al concorso di colpa, ma fortemente sbilanciato in danno del cliente (due terzi). In ogni caso, il clic su un *link* ricevuto via *SMS* costituisce di per sé violazione contrattuale autonomamente causativa del danno, a prescindere dalla questione della genuinità del link.

4.3 Comunicazione o inserimento di credenziali, OTP e codici di sicurezza; ignorare SMS slert e segnali di allarme.

La già richiamata sentenza del Tribunale di Milano n. 7466/2025 attribuisce rilievo decisivo alla circostanza che l'attore avesse **divulgato le proprie credenziali** necessarie all'attivazione dell'*app* sul dispositivo dei truffatori, così vanificando le misure di sicurezza predisposte. La decisione conclude nel senso della **esclusiva responsabilità per colpa grave** del cliente. Questo passaggio è di particolare rilievo sistematico: anche in un contesto di frode telematica avanzata, la comunicazione delle credenziali di sicurezza resta il più tipico indice di colpa grave, salvo che il contesto fattuale dimostri l'assenza di ogni riconoscibile anomalia.

Sempre il Tribunale di Milano valorizza il fatto che il cliente avesse **"sistematicamente ignorato gli SMS alert"** e avesse atteso circa una settimana dal primo messaggio anomalo prima di rivolgersi all'assistenza *[Sentenza n. 7466/2025]*. Anche questo profilo viene ricondotto nell'area della colpa grave. L'assunto è chiaro: l'utente che riceve messaggi anomali, avvisi di attivazione, notifiche di operazioni o altri allarmi e non compie alcuna verifica minima si espone a una seria contestazione di grave negligenza.

La stessa sentenza milanese considera rilevante il ritardo dell'utente nel contattare il servizio di assistenza. Il ritardo, infatti, può assumere valore sia come indice di disattenzione qualificata, sia come fattore che consolida causalmente il danno.

4.4. La "sofisticazione" non è categoria esimente.

Proprio qui emerge il contrasto con l'orientamento più "*indulgente*". Il Tribunale di Monza, in presenza di una truffa realizzata mediante *sms spoofing* e *ID caller spoofing*, ritiene che operi una presunzione di assenza della colpa della vittima quando il truffatore adotti un sistema tecnicamente sofisticato, salvo la presenza di indici di inattendibilità o anomalia del messaggio *[Tribunale Di Monza, Sentenza n.2072 del 23 Luglio 2024]*. Nel caso concreto, il giudice valorizza il fatto che il messaggio si fosse inserito in una conversazione contenente comunicazioni genuine, che il numero verificato online corrispondesse alla filiale e che l'operatore si fosse identificato senza chiedere credenziali a voce *[Tribunale Di Monza, Sentenza n.2072 del 23 Luglio 2024]*.

Una tale impostazione, però, non appare condivisibile nella misura in cui il concetto stesso di *"sofisticazione della frode"*, nella sua aleatorietà e indefinitezza, rischia di svuotare il concetto legale di colpa grave e di spostare l'analisi dalla condotta del cliente alla maggiore abilità del truffatore. Il legislatore non conosce una categoria normativa di "errore scusabile per elevata abilità del frodatore"; conosce, invece, il problema della **custodia delle credenziali** e della **diligenza concretamente esigibile**.

5. Il contrasto giurisprudenziale: "insidiosità della frode" e "rigore del sistema speciale".

Le fonti disponibili mettono bene in luce l'attuale bipolarismo della giurisprudenza.

5.1. L'orientamento dell'"insidiosità della frode".

Il Tribunale di Monza valorizza la sofisticazione della truffa e il contesto concretamente rassicurante per la cliente. In tale prospettiva, la comunicazione delle credenziali non è di per sé sufficiente a fondare la colpa grave, poiché nel fenomeno dello spoofing essa può essere fisiologicamente indotta dal meccanismo fraudolento stesso *[Tribunale Di Monza, Sentenza n.2072 del 23 Luglio 2024]*. L'accento è posto sulla mancanza di evidenti indici di sospetto percepibili dall'utente.

5.2. L'orientamento del "rigore del sistema speciale".

Il Tribunale di Brescia, pur in una vicenda diversa, appare invece più rigoroso nel ricondurre la materia al binario normativo del decreto, insistendo sia sulla diligenza professionale del PSP sia sulla non applicabilità del concorso di colpa ex art. 1227 c.c. *[Tribunale di Brescia, Sentenza n.5084 del 9 dicembre 2024]*. La decisione afferma espressamente: *"il tenore della norma di cui all'art. 12, comma 3, D.lgs n. 11/2010 esclude che possa applicarsi la regola juris di cui all'art. 1227, comma primo, c.c."*.

Proprio questa presa di posizione consente di affermare che il sistema non tollera facilmente aggiustamenti equitativi fondati su una responsabilità *"mista"*, salvo il previo chiarimento della reale sussistenza o meno della colpa grave dell'utente.

6. L'inapplicabilità dell'art. 1227 c.c. nel sistema del d.lgs n. 11/2010.

Questo è il punto di maggiore rilievo teorico.

L'art. 1227 c.c. prevede che, se il fatto colposo del creditore concorre a cagionare il danno, il risarcimento sia diminuito secondo la gravità della colpa e l'entità delle conseguenze. Si tratta della regola generale sul concorso del fatto colposo del creditore.

Tuttavia, il d.lgs n. 11/2010, per come ricostruito, non si limita a richiamare il diritto comune: introduce una disciplina ***speciale e autosufficiente*** di allocazione della perdita, incentrata sulla distinzione tra: operazione non autorizzata con rimborso a carico del PSP ed esonero del PSP in caso di dolo, frode o colpa grave dell'utente.

Il Tribunale di Brescia recepisce in modo netto questa impostazione, negando che l'art. 1227, comma 1, c.c. possa essere utilizzato per ridurre il risarcimento in ragione di un concorso di colpa della cliente. Le ragioni della non applicabilità sono forti:

1. la disciplina speciale già tipizza **quando** e **in quale misura** la perdita grava sull'utente;
2. la previsione della colpa grave come causa di integrale sopportazione della perdita da parte dell'utilizzatore mal si concilia con un riparto equitativo intermedio.

Ne consegue che il ricorso alla previsione di cui all'art. 1227 c.c. finirebbe per introdurre un *tertium genus* non previsto dal sistema.

Il Tribunale di Milano, con la Sentenza n. 1951 del 22 febbraio 2024, si muove nel solco della medesima linea argomentativa, affermando con chiarezza che la norma speciale costituisce, rispetto all'art. 1227 c.c., non soltanto una disposizione prevalente, ma addirittura un'**applicazione positivizzata** del concorso di colpa con fissazione di un limite legale massimo alla diminuzione del risarcimento: *"Ritiene, quindi il Tribunale, esaminando le norme speciali di cui all'art. 12 del d.l.gs. n. 11/2010, come modificato dal d.lgs. n. 218/2017, che l'art. 1227 c.c. non possa venire in considerazione nell'ipotesi di cui al comma 2 ter poiché è il Legislatore che ha stabilito che in tale ipotesi il cliente non sopporta alcuna perdita e il risarcimento deve essere quindi completo; né può venire in applicazione nell'ipotesi di cui al comma 4, poiché non essendoci responsabilità della banca, l'utente sopporta tutte le perdite e quindi, non è dovuto alcun risarcimento. L'unica ipotesi potrebbe essere quella di cui al comma 3 dell'art. 12. Tuttavia, il Legislatore ha previsto che il cliente - fuori dai casi di cui al comma 2 ter e al comma 4 - può sopportare le perdite per un importo comunque non superiore a 50 euro. Ritiene, quindi il Tribunale che tale norma speciale, con il limite ivi previsto, debba prevalere sull'applicazione dell'art. 1227 comma 1 c.c. o meglio ne costituisca un'applicazione positivizzata con fissazione di un limite massimo*

alla diminuzione del risarcimento". Il valore sistematico di questa sentenza è elevato: il giudice milanese riconduce l'art. 12, comma 3, d.lgs. n. 11/2010 alla stessa *ratio* dell'art. 1227 c.c., ma ne esclude l'applicazione autonoma poiché il legislatore ha già determinato il **limite legale massimo** di imputazione al cliente (euro 50 in caso di colpa non grave). La conseguenza pratica, in senso favorevole all'intermediario, è speculare: ove sia invece accertata la **colpa grave**, la perdita è integralmente a carico del cliente e nessun correttivo equitativo ex art. 1227 c.c. è ammissibile in riduzione. Quanto alla fattispecie concreta, il Tribunale, pur ravvisando una colpa **non grave** del cliente, rimarca comunque la presenza di una condotta colposa dell'utente. La sentenza è, pertanto, rilevante sia sotto il profilo della **tesi sistematica** (art. 12 prevale su art. 1227) sia per il riconoscimento del **contributo causale del comportamento del cliente**, ancorché in quel caso qualificato come non grave.

La Corte d'Appello dell'Aquila *[Sentenza n. 1001 del 22 settembre 2025]* si è pronunciata su un caso di frode informatica tramite *home banking*, nel quale l'utente aveva colposamente selezionato il *link* di un sito civetta e, successivamente, non aveva tempestivamente segnalato la compromissione delle credenziali. La Corte afferma espressamente l'inapplicabilità dell'art. 1227 c.c. proprio in ragione dell'autonoma efficienza causale della grave negligenza dell'utente: *"con specifico riguardo alla critica degli appellanti alla sentenza di primo grado per l'omessa applicazione dell'art. 1227 c.c., si deve ribadire che le gravi negligenze dell'utente, già evidenziate, hanno avuto un'autonoma efficienza causale nella determinazione dell'evento dannoso, con la conseguente inapplicabilità dell'art. 1227 c.c. (in tal senso, tra le altre, Cass., 22 agosto 2024, n. 23024; Cass., 23 marzo 2016, n. 5679)"*. Il ragionamento seguito dalla Corte aquilana è particolarmente rilevante per l'intermediario: quando le negligenze dell'utente assurgono al rango di **causa autonoma** dell'evento dannoso, la fattispecie disciplinata dall'art. 1227 c.c. non è integrata, in quanto manca il presupposto stesso dell'applicazione della norma (il concorso causale). Se il sistema speciale attribuisce alla colpa grave la funzione di **esimente legale** per il PSP, l'efficienza causale della condotta dell'utente è già incorporata nel giudizio legale di imputazione della perdita, senza necessità – né possibilità – di un'ulteriore graduazione proporzionale. La Corte richiama a supporto due arresti della Cassazione (n. 23024/2024 e n. 5679/2016), segnalando così che la posizione non è meramente locale, ma radicata in un filone di legittimità consolidato. In fatto, la Corte evidenzia che l'utente aveva violato le disposizioni normative e contrattuali in ordine alle modalità di accesso al servizio di *home banking* e non aveva tempestivamente segnalato alla banca l'interruzione dei servizi dello

strumento di autenticazione: *"l'accesso alle credenziali è stato determinato dalla condotta gravemente imprudente del predetto, che ha violato le disposizioni normative e contrattuali in ordine alle modalità di accesso al servizio di home banking nonché in ordine alla tempestiva segnalazione alla Banca dell'interruzione dei servizi dello strumento utilizzato per il predetto accesso"*.

La Corte d'Appello di Milano *[Sentenza n. 3023 del 12 novembre 2024]* ha riformato integralmente una sentenza di primo grado che aveva riconosciuto la responsabilità della banca, escludendo ogni responsabilità dell'intermediario per effetto della **colpa grave esclusiva dell'utente**. Il caso riguardava una frode mediante *smishing* e *vishing*, nel corso della quale il cliente aveva comunicato più volte le proprie credenziali di accesso all'home banking a un interlocutore che si qualificava come operatore dell'istituto, sebbene il messaggio civetta ricevuto contenesse evidenti indici di anomalia.

La Corte valorizza espressamente tre fattori di imputazione della colpa grave al cliente:

1. la **comunicazione delle credenziali** su richiesta telefonica;
2. la **professione e l'età** dell'utente (imprenditore, 48 anni), escludenti le attenuanti connesse alla vulnerabilità;
3. la presenza di **indici di inattendibilità** nel messaggio, percepibili con ordinaria attenzione (errori grammaticali, link non riconducibile all'intermediario):

"A ciò si aggiunga – sostiene la corte meneghina – *che il testo del messaggio c.d. civetta presentava evidenti indici di dubbia attendibilità […] o anomalie (quale l'invito a selezionare un link non riferibile all'intermediario […]) che ben dovevano essere percepite dall'odierno appellato e indurlo a non assecondare la richiesta telefonica che ebbe a portarlo, poi, a comunicare le proprie credenziali necessarie per l'operatività sul conto on line"*. La conclusione è netta: *"Deve, pertanto, escludersi la responsabilità della [banca] appellante in relazione al danno sofferto dall'odierna appellata, essendo questo esclusivamente riconducibile alla colpa grave della stessa parte danneggiata"*. Questo precedente è assaia significativo nelle fattispecie "multivettoriali" in cui si rileva la presenza di **indici di anomalia oggettivamente riconoscibili** nel messaggio civetta o nella telefonata, circostanza che priva il cliente di qualsiasi scudo giuridico fondato sull'affidamento qualificato o sulla sofisticazione della frode.

Il Tribunale di Catania *[Sentenza n. 1227 del 6 marzo 2024]* ha affrontato un caso di phishing con comunicazione telefonica delle credenziali, pervenendo al **rigetto integrale della domanda del cliente** per colpa grave esclusiva dello stesso. Il giudice riconduce il caso alla categoria della condotta colposa che integra il **caso fortuito interruttivo del nesso causale**,

escludendo in radice qualsiasi responsabilità della banca: *"deve ritenersi che il correntista ha tenuto un comportamento decisamente imprudente e negligente, avendo digitato i propri codici personali - verosimilmente richiesti con una e-mail fraudolenta - in tale modo consentendo all'ignoto truffatore di successivamente utilizzarli per effettuare la disposizione sul conto e tale condotta colposa, causa esclusiva dell'operazione che ha determinato l'addebito, ha assunto i caratteri del caso fortuito che ha interrotto il nesso eziologico tra l'attività pericolosa e l'evento dannoso, con conseguente esclusione della responsabilità della banca"*. Il Tribunale specifica poi che la prova fornita dall'intermediario in ordine all'adozione di un sistema di sicurezza certificato e alla diffusione di informazioni preventive alla clientela sulle frodi informatiche è sufficiente a soddisfare la prova liberatoria: "[La banca] ha fornito la prova nei termini suddetti, in quanto, per un verso, ha dimostrato di aver adottato un sistema di sicurezza dei servizi informatici online certificato da appositi enti secondo standard internazionale [...] e, per altro verso, ha dimostrato di aver fornito, a mezzo internet, le necessarie informazioni per evitare le frodi informatiche (in particolare il phishing), con l'avvertenza, in particolare, che [la banca stessa] non richiede mai, attraverso messaggi di posta elettronica, lettere o telefonate, di fornire i propri codici personali". Quanto al tentativo del cliente di invocare il *caller ID spoofing* (telefonata proveniente dal numero ufficiale della banca), il Tribunale lo neutralizza (e verrebbe da dire: liquida) affermando che si tratta di circostanza non dimostrata: *"Non vale ad escludere la colpa della cliente [...] il fatto che la telefonata in esame provenisse dal numero ufficiale [...], trattandosi di circostanza indimostrata"*.

I precedenti individuati confermano e ampliano l'assunto del Tribunale di Brescia secondo due linee argomentative distinte ma convergenti: la prima – più vicina alla lettura sistematica proposta in precedente contributo pubblicato su questa stessa Rivista *[L. Cardi, Brevi note a margine della giurisprudenza in tema di colpa grave nell'ambito di operazioni disconosciute ai sensi del d. lgs. n. 11/2010, Diritto del Risparmio, Approfondimenti, giugno – fascicolo 2/2026]* – esclude l'applicabilità autonoma dell'art. 1227 c.c. per effetto della specialità dell'art. 12 d.lgs. n. 11/2010 *[Trib. Milano n. 1951/2024]*; la seconda – che analizza la questione da altra prospettiva afferente alla dogmatica generale – riconduce l'inapplicabilità dell'art. 1227 c.c. non alla specialità della norma, bensì all'autonoma efficienza causale della condotta gravemente negligente dell'utente, che interrompe il nesso causale o integra gli estremi del caso fortuito *[C. App. L'Aquila n. 1001/2025; Trib. Catania n. 1227/2024]*.

8. Conclusioni.

L'analisi delle fonti disponibili consente di formulare alcune conclusioni nette.

Le frodi bancarie multivettoriali costituiscono fenomeni tecnicamente insidiosi, ma la loro sofisticazione non esclude in via di principio la **colpa grave dell'utente**. Lo dimostrano i casi in cui il cliente divulga credenziali, ignora alert, trascura messaggi anomali o ritarda le segnalazioni.

Il d.lgs n. 11/2010 va letto come disciplina speciale di allocazione della perdita, secondo un modello tendenzialmente **binario**.

L'art. 1227 c.c. non appare compatibile con tale impianto quando venga usato per costruire un concorso di colpa correttivo.

L'orientamento che presume la scusabilità dell'errore in ragione della sola *"sofisticazione della frode"* non appare condivisibile, perché rischia di spostare il giudizio dalla condotta dell'utente al grado di abilità del truffatore, con perdita di certezza applicativa.

In definitiva, la soluzione più coerente con il diritto vigente non è né la deresponsabilizzazione automatica dell'utente né il riparto equitativo della perdita per via dell'art. 1227 c.c.; è, piuttosto, la rigorosa verifica della **colpa grave dell'utilizzatore** e del parallelo adempimento degli obblighi professionali del PSP, all'interno del perimetro speciale tracciato dal d.lgs n. 11/2010. **La sola *"sofisticazione"* della frode (o asserita tale) non è esimente: il giudizio resta ancorato – nella fattispecie concreta – alla verifica della colpa grave dell'utente e dell'adempimento degli obblighi professionali del PSP nel quadro speciale del d.lgs n. 11/2010**. L'art. 1227 c.c. non opera come correttivo proporzionale all'interno di tale impianto, essendo l'allocazione della perdita già compiutamente tipizzata dall'art. 12 del richiamato decreto legislativo.