DR Diritto del Risparmio

# LA PROVA CHE ASSOLVE: PERIZIE FORENSI E INVERSIONE DELL'ONERE DELLA PROVA NEI PROCEDIMENTI ABF. LA PROSPETTIVA DEL "*FORENSER*"

**di Silverio GRECO***

*Trading apps represent the "feuilletons" of the 21st century: serialized, emotional, and gamified narratives that transform investing into an engaging and immersive experience. By employing narratological techniques—such as anachronies, internal focalization, and seriality—alongside gamification, these platforms exploit cognitive biases and stimulate dopamine-driven responses, frequently overriding traditional regulatory disclosures based on the model of the rational investor.*

*This essay introduces regulatory narratology as an interdisciplinary approach to analyzing and mitigating the narrative impact on financial decision-making. It examines the risks of excessive trading and overconfidence bias and, at the systemic level, analyses how viral collective stories can generate "narrative systemic risk.*

**Giugno**
**fascicolo 1/2026**

*Docente a contratto presso l'Università del Salento, Consulente Tecnico del Ministero della Giustizia, esperto di informatica forense e analisi strategica dei dati.

ISSN 2785-3004

Rivista di Diritto del Risparmio – Fascicolo n. 2/2026
ISSN 2785-3004

*Rivista di Diritto del Risparmio*

# La prova che assolve: perizie forensi e inversione dell'onere della prova nei procedimenti ABF. La prospettiva del "*forenser*"*

**di Silverio GRECO****

---

*La società contemporanea si caratterizza per la il fatto di essere iper-connessa; a livello finanziario, le transazioni vengono effettuate quasi esclusivamente tramite servizi di pagamento digitali . Questo scenario, che comporta indubbi vantaggi sotto il profilo della gestione dei pagamenti, ha aperto nuove opportunità anche per il mondo criminale. Negli ultimi anni, infatti, il fenomeno delle frodi bancarie ha registrato una forte impennata, dovuta sia alla progressiva diminuzione dell'utilizzo del contante, sia all'avanzare della digitalizzazione dei processi.*

*La diffusione degli strumenti di pagamento elettronico — rappresentati, nella maggior parte dei casi, dai servizi bancari a portata di click (le cosiddette mobile bank) o da tutte quelle operazioni effettuabili tramite smartphone ovunque nel mondo — ha esposto gli utenti a nuove forme di rischio, alcune delle quali difficili da prevedere. Le barriere spazio-temporali che caratterizzavano i vecchi sistemi sono state superate, ma ciò ha comportato anche un aumento delle opportunità di attacco.*

*In questo contesto, l'ordinamento giuridico nazionale, e prima ancora quello europeo, ha cercato progressivamente di tenere il passo con la tecnologia, rafforzando il quadro normativo volto a garantire una maggiore sicurezza delle transazioni, una più efficace tutela dei consumatori e una più ampia accountability degli intermediari finanziari.*

**Giugno**

**fascicolo 1/2026**

---

* Contributo approvato dai *referee*.

** Docente a contratto presso l'Università del Salento, Consulente Tecnico del Ministero della Giustizia, esperto di informatica forense e analisi strategica dei dati.

# La prova che assolve: perizie forensi e inversione dell'onere della prova nei procedimenti ABF. La prospettiva del "*forenser*".

**A cura di Silverio GRECO.**

SOMMARIO: 1. Introduzione. – 1.1. Le frodi bancarie e il quadro normativo di riferimento: PSD2, D.lgs. n. 11/2010, NIS2, L. n. 90/2024. – 1.2. L'evoluzione delle frodi bancarie: dal phishing massivo allo smishing mirato e allo spoofing. – 1.3. Il ruolo dell'Arbitro Bancario Finanziario (ABF): un'alternativa rapida, ma dipendente dalla qualità della prova documentale. – 2. La responsabilità degli intermediari e l'onere della prova. – 2.1. La presunzione di responsabilità della banca: l'onere di provare la "colpa grave" dell'utente (art. 12, comma 4, D.lgs. n. 11/2010). – 2.2. Oltre la SCA (Strong Customer Authentication): perché l'autenticazione a due fattori non esclude automaticamente la responsabilità dell'intermediario. – 3. L'informatica forense in via stragiudiziale. – 3.1. *Mobile Forensics*: l'analisi dello smartphone della vittima come "scatola nera" dell'evento. – 3.2. Metodologia di acquisizione: garantire l'integrità del dato (*hash*, catena di custodia) per l'opponibilità del ricorso. – 3.3. Ricostruzione del "*customer journey*" fraudolento: analisi dei log di sistema, sms *thread* e cronologia browser. – 4. Analisi tecnica della *deception*: dimostrare l'impossibilità di distinguere il falso dal vero. – 4.1. Anatomia dello spoofing: come i criminali si inseriscono nei *thread* legittimi dei messaggi bancari. – 4.2. Il fattore umano e l'ingegneria sociale: analisi del contesto psicologico indotto dall'attaccante. – 4.3. Evidenze forensi di sofisticatezza: dimostrare che l'utente ha agito in "buona fede soggettiva" di fronte a un'interfaccia indistinguibile dall'originale. – 5. Casi pratici e orientamenti recenti dell'ABF. – 5.1. Caso 1: *Sim Swap Fraud*. – 5.2. CASO 2 – App bancaria clonata. – 6. Conclusioni. – 7. Bibliografia e sitografia.

## 1. Introduzione.

### 1.1. Le frodi bancarie e il quadro normativo di riferimento: PSD2, D. lgs. n. 11/2010, NIS2, l. n. 90/2024.

La società contemporanea si caratterizza per la il fatto di essere iper-connessa; a livello finanziario, le transazioni vengono effettuate quasi esclusivamente tramite servizi di pagamento digitali[1]. Questo scenario, che comporta indubbi vantaggi sotto il profilo della

[1] D.lgs. 11/2010 e la PSD2.

gestione dei pagamenti, ha aperto nuove opportunità anche per il mondo criminale. Negli ultimi anni, infatti, il fenomeno delle frodi bancarie ha registrato una forte impennata, dovuta sia alla progressiva diminuzione dell'utilizzo del contante, sia all'avanzare della digitalizzazione dei processi.

La diffusione degli strumenti di pagamento elettronico — rappresentati, nella maggior parte dei casi, dai servizi bancari a portata di click (le cosiddette *mobile bank*) o da tutte quelle operazioni effettuabili tramite smartphone ovunque nel mondo — ha esposto gli utenti a nuove forme di rischio, alcune delle quali difficili da prevedere. Le barriere spazio-temporali che caratterizzavano i vecchi sistemi sono state superate, ma ciò ha comportato anche un aumento delle opportunità di attacco.

In questo contesto, l'ordinamento giuridico nazionale, e prima ancora quello europeo, ha cercato progressivamente di tenere il passo con la tecnologia, rafforzando il quadro normativo volto a garantire una maggiore sicurezza delle transazioni, una più efficace tutela dei consumatori e una più ampia accountability degli intermediari finanziari.

Tra gli interventi legislativi più significativi troviamo la Direttiva UE 2015/2366, meglio conosciuta come PSD2 (Payment Services Directive 2), e il D.lgs. 11/2010, che disciplina l'esecuzione dei servizi di pagamento in Italia. Dal punto di vista della cybersicurezza, invece, l'introduzione della Legge 90/2024 ha segnato un deciso cambio di passo nella strategia italiana di difesa contro il crimine informatico: mentre le precedenti normative proteggevano i singoli pagamenti, questa nuova legge mira a salvaguardare l'intero sistema bancario, riconosciuto come "*infrastruttura critica*".

A completare il quadro interviene la Direttiva NIS2 (UE 2022/2555), recepita nel nostro ordinamento dal D.lgs. 138/2024.

La PSD2 — recepita, appunto, dal D.lgs. 11/2010 — rappresenta il nucleo della disciplina operativa in materia di frodi. Essa ha introdotto la **Strong Customer Authentication (SCA)**, ossia l'autenticazione a più fattori, al fine di convalidare le operazioni e aumentare la sicurezza. Inoltre, ha innalzato il livello di responsabilità dei prestatori di servizi di pagamento (PSP), i quali, in caso di operazione non autorizzata, sono obbligati a rimborsare immediatamente il cliente, applicando una franchigia massima di 50 euro, salvo i casi di dolo o colpa grave dell'utente.

La sicurezza delle infrastrutture è invece tutelata dalla Direttiva NIS2 (UE 2022/2555), che amplia il perimetro di sicurezza nazionale includendo un numero maggiore di soggetti e

introducendo obblighi stringenti nella gestione del rischio cyber, nonché tempi molto ridotti per la notifica degli incidenti. A ciò si aggiunge la già citata Legge 90/2024, che impone alle pubbliche amministrazioni e alle infrastrutture critiche — tra cui gli istituti finanziari — l'obbligo di segnalare all'Agenzia per la Cybersicurezza Nazionale (ACN) eventuali attacchi subiti, prevedendo sanzioni significative in caso di mancata compliance, con l'obiettivo di prevenire frodi massive derivanti da *data breach*.

### 1.2. L'evoluzione delle frodi bancarie: dal *phishing* massivo allo *smishing* mirato allo *spoofing*.

L'evoluzione delle frodi non è più rappresentata da virus o altri software/app malevoli, ma è diventata principalmente una questione di ingegneria sociale. Fino a qualche anno fa, infatti, le truffe — soprattutto quelle basate sul phishing, sia generico sia bancario — erano assimilabili a "*reti a strascico*", concepite per colpire quante più persone possibili. Oggi queste tecniche si sono evolute in forme molto più raffinate, capaci di agire con una precisione chirurgica, manipolando la percezione della vittima attraverso strumenti tecnologici sempre più avanzati che, con l'avvento dell'intelligenza artificiale, stanno diventando pressoché indistinguibili dalle comunicazioni autentiche, anche per gli utenti più esperti.

Il cosiddetto **phishing massivo**, ancora diffuso in rete, consiste nell'invio generalizzato di e-mail spesso caratterizzate da errori grammaticali e strutturali, oggi intercettabili dai filtri antispam e da una – almeno in parte – maggiore consapevolezza degli utenti. Questo lo ha reso una tecnica sempre meno efficace.

Le nuove frontiere della truffa sono invece rappresentate dallo **smishing**, condotto tramite SMS (ancora ampiamente utilizzati da molti istituti di credito per l'autenticazione a due fattori). Questa tipologia di attacco ha preso piede sfruttando la natura "*intima*" del messaggio testuale, soprattutto tra le nuove generazioni, che percepiscono l'e-mail come un mezzo "*vecchio*" e preferiscono comunicazioni immediate attraverso canali di messaggistica istantanea.

In questi attacchi, l'urgenza diventa l'elemento psicologico centrale: i messaggi contengono comunicazioni allarmistiche ("*È stato disposto un bonifico di X euro dal suo conto. Per bloccarlo, contatti immediatamente il numero*…") progettate per indurre l'utente a reagire impulsivamente.

Inoltre, queste tecniche possono essere **targettizzate geograficamente** grazie all'utilizzo di database illegali — frutto di *data breach* — che permettono ai criminali di aumentare drasticamente il tasso di conversione della frode.

Parallelamente si sta diffondendo sempre di più lo **spoofing**, particolarmente efficace in ambito aziendale (indipendentemente dalle dimensioni dell'organizzazione). Le moderne tecniche di spoofing — una forma di inganno concettualmente discussa già da Cartesio nel 1641 — consistono nel mascheramento dell'identità reale del mittente. È sufficiente pensare alle numerose telefonate provenienti da call center internazionali che, a seguito delle limitazioni imposte sull'utilizzo delle numerazioni mobili, oggi sfruttano numerazioni estere o persino numeri legittimi appartenenti a soggetti ignari, spesso con prefissi locali, eludendo così molte misure di sicurezza bancaria.

Tra le forme più diffuse troviamo il **Caller ID Spoofing**, riferito alla falsificazione del numero visualizzato nelle chiamate, e il **Sender ID Spoofing**, che riguarda invece i messaggi SMS.

L'avvento dell'intelligenza artificiale sta ulteriormente perfezionando queste tecniche, rendendole sempre più convincenti e difficili da individuare.

### 1.3. Il ruolo dell'Arbitro Bancario Finanziario (ABF): un'alternativa rapida, ma dipendente dalla qualità della prova documentale.

Nel complesso sistema di norme e di strumenti dedicati alla risoluzione delle controversie, molte persone tendono a considerare la via penale come prima forma di difesa per recuperare le somme sottratte dal proprio conto. Tuttavia, la percentuale di successo nel recupero dei fondi attraverso il procedimento penale è statisticamente talmente bassa da essere prossima allo zero.

La ragione principale di tale inefficacia risiede nella natura stessa del crimine informatico moderno, caratterizzato da un elevato livello di **anonimato** (uso di VPN, server proxy, giurisdizioni estere non collaborative) e da fenomeni quali il ***money muling***, in cui il denaro viene fatto transitare rapidamente su conti intestati a prestanomi o, in molti casi, a utenti anch'essi truffati. Questi ultimi, dopo aver perso il controllo dei propri documenti, possono ritrovarsi indagati come titolari di conti correnti di cui ignoravano l'esistenza fino alla perquisizione o alla notifica dell'avviso di conclusione delle indagini.

A complicare ulteriormente la situazione vi è il fatto che una parte consistente dei fondi sottratti viene convertita in criptovalute e trasferita su *wallet* intestati agli stessi truffati (ma senza che questi possano accedervi) oppure su account di terzi ignari.

Lo scenario cambia radicalmente quando l'attenzione si sposta non più sul truffatore, come avviene nel processo penale, bensì sulla banca, ossia su un soggetto identificabile e "*attaccabile*". In questo caso, le probabilità di successo aumentano sensibilmente e dipendono dalla solidità della prova. Negli ultimi anni, quest'ultima non è più solo documentale: l'ingresso delle prove informatiche — ancora oggi definite "***atipiche***" — nel processo civile ha rafforzato la posizione del cliente.

In ambito civile, infatti, non si discute sulla colpevolezza di un terzo, ma sulla **diligenza professionale della banca**, sull'adeguatezza delle misure tecniche di sicurezza adottate e sull'onere della prova, che — al contrario del procedimento penale, fondato sulla presunzione di innocenza — ricade sull'istituto di credito, chiamato a dimostrare la "**colpa grave**" dell'utente.

Tuttavia, questa via presenta tempi lunghi: il solo primo grado richiede mediamente due anni, tempi che possono estendersi fino a sette anni se si percorrono tutti e tre i gradi di giudizio. Il vantaggio, rispetto al procedimento penale, è che la sentenza civile costituisce titolo esecutivo e consente la **nomina di un CTU (Consulente Tecnico d'Ufficio)** per l'analisi degli aspetti tecnici.

La corsia preferenziale — ancora poco sfruttata — è rappresentata dall'**Arbitro Bancario Finanziario (ABF),** nato con l'obiettivo di garantire una procedura snella e rapida. Il tempo medio per ottenere una decisione è di circa tre/quattro mesi, con un limite massimo fissato a 180 giorni, contro i due anni del giudizio civile.

L'ABF non è un tribunale, ma un **sistema di risoluzione stragiudiziale delle controversie (ADR)**, istituito nel 2009 dall'art. 128-bis del TUB per alleggerire il carico dei tribunali e offrire ai cittadini un'alternativa efficace nelle dispute con gli istituti di credito. È un organismo indipendente costituito presso la Banca d'Italia, con composizione collegiale e membri scelti tra l'istituto stesso e le associazioni dei consumatori, garantendo imparzialità, equilibrio e un elevato livello di specializzazione.

I punti di forza dell'ABF includono:

- **altissima specializzazione** tecnica dei componenti del collegio;

- **costo di accesso estremamente ridotto** (20 euro), che vengono rimborsati dalla banca in caso di accoglimento (anche parziale) del ricorso;
- **possibilità per il cliente di presentare il ricorso autonomamente**, pur con il rischio che un'impostazione poco efficace possa compromettere l'esito, poiché il "*convincimento*" del collegio dipende dalla qualità della prova e dalle modalità con cui essa viene presentata.

La procedura è interamente online e non prevede udienze: tutto si basa sulla documentazione depositata dalle parti.
Va precisato che la decisione dell'ABF, pur autorevole, è stragiudiziale: la banca potrebbe, almeno in teoria, non adempiere spontaneamente. Si tratta però di un evento raro. In caso di inadempimento, il cliente può rivolgersi al giudice ordinario per far valere i propri diritti.
La mancata esecuzione comporta inoltre un grave danno reputazionale per l'istituto di credito, che viene inserito nella black list degli inadempienti pubblicata sul sito dell'ABF per cinque anni, e ha l'obbligo di pubblicare la notizia sulla homepage del proprio sito per sei mesi. È un forte deterrente, poiché tali informazioni vengono prese in considerazione dal mercato e dalla stessa Banca d'Italia, che vigila sulla correttezza degli intermediari.
Non sorprende, quindi, che secondo i dati ufficiali dell'ABF, la percentuale di adempimento spontaneo da parte delle banche si collochi stabilmente tra il 95% e il 98%.

## 2. La responsabilità degli intermediari e l'onere della prova.

Nel corso del tempo si è assistito, a livello europeo e quindi anche nazionale, a un'evoluzione significativa in materia di responsabilità degli intermediari. Per decenni, infatti, ha prevalso un principio di assenza di obblighi generali di sorveglianza[2], sancito dall'art. 15 della Direttiva 2000/31/CE, secondo cui gli intermediari che svolgevano attività di "*semplice trasporto*", "*memorizzazione temporanea*" o "*memorizzazione di informazioni*" non erano tenuti a vigilare attivamente sui contenuti gestiti.
In tale contesto, l'onere della prova gravava interamente sull'utente danneggiato, chiamato a dimostrare sia l'illiceità del contenuto sia la conoscenza effettiva, da parte dell'intermediario, dell'attività illecita.

[2] G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione,* Torino, Giappichelli, 2022.

La giurisprudenza della Corte di Giustizia dell'Unione Europea (ad esempio, nelle cause *eBay v. L'Oréal e Google Spain*[3]) ha poi introdotto la distinzione tra:

- **intermediario passivo**, mero fornitore tecnico che si limita al trasporto o all'hosting dei dati e che, in quanto tale, beneficia di una forma di immunità;
- **intermediario attivo**, che invece svolge attività di indicizzazione, promozione, organizzazione o ottimizzazione dei dati, perdendo così ogni forma di esenzione da responsabilità.

Ne derivava che la vittima di una truffa doveva provare non solo l'esistenza del danno, ma soprattutto che l'intermediario avesse svolto un ruolo attivo nella gestione dei contenuti o delle operazioni.
Nel 2022, con l'entrata in vigore del Digital Services Act (Regolamento UE 2022/2065), il quadro cambia radicalmente: il DSA integra e supera la logica precedente introducendo precisi obblighi di diligenza (due diligence[4]) a carico degli intermediari.
Oggi la responsabilità dell'intermediario scatta quando, ricevuta una segnalazione adeguatamente motivata, esso non interviene tempestivamente per rimuovere o disabilitare l'accesso al contenuto illecito.
Il DSA, in particolare all'art. 16, prevede che una segnalazione conforme generi una presunzione di conoscenza dell'illecito, determinando di fatto un'inversione dell'onere della prova: non è più l'utente che deve dimostrare l'effettiva consapevolezza dell'intermediario, ma è quest'ultimo che deve dimostrare di aver agito con la dovuta tempestività e diligenza.

### 2.1. La presunzione di responsabilità della banca: l'onere di provare la "colpa grave" dell'utente (art. 12, comma 4, D. lgs. n. 11/2010).

Secondo il diritto civile, e in particolare secondo quanto stabilito dall'art. 1218 c.c., il debitore è liberato da responsabilità se prova che l'inadempimento è dovuto a una causa a lui non imputabile. Applicato all'ambito dell'home banking e degli strumenti di pagamento

[3] SENTENZA CGUE: C-324/09 (L'Oréal/eBay)

[4] F. PIZZETTI, *La regolazione europea della società digitale*, Torino, Giappichelli, 2024.

elettronici (carte di debito e di credito), questo principio introduce per l'utente una tutela rafforzata, poiché egli si trova in una posizione di debolezza rispetto all'istituto bancario.
La responsabilità dei prestatori di servizi di pagamento (PSP) non è più ancorata alla semplice colpa, ma si configura come una responsabilità professionale aggravata: all'intermediario è richiesto di garantire la sicurezza dei sistemi e delle operazioni.
In questo contesto — regolato dall'art. 12, comma 4, del D.lgs. 11/2010 — all'utente è richiesto unicamente di denunciare il disconoscimento dell'operazione fraudolenta. Tocca invece alla banca provare che la transazione sia stata autenticata, correttamente registrata e contabilizzata.
Quanto alla fase di autenticazione, nonostante molte banche tendano ancora a ignorare questo passaggio previsto dalla norma, la semplice correttezza formale nell'inserimento di PIN o OTP non è sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente, né che egli abbia agito con dolo o colpa grave.
La **colpa grave non coincide con una mera distrazione**. La giurisprudenza ha chiarito che essa ricorre solo in presenza di condotte particolarmente negligenti, quali:

- il **ritardo ingiustificato** nel blocco della carta dopo il furto;
- la **comunicazione delle credenziali** in casi in cui il phishing risulti facilmente riconoscibile per errori evidenti;
- la **conservazione del PIN insieme alla carta** (evenienza difficilissima da provare in giudizio).

La banca deve quindi dimostrare la negligenza qualificata del cliente come elemento soggettivo dell'azione che ha permesso la frode. Non è più sufficiente limitarsi a formule stereotipate ("*i nostri sistemi sono sicuri*"), ancora troppo frequenti nelle risposte alle contestazioni.
Con l'introduzione della Strong Customer Authentication (SCA), l'onere probatorio a carico della banca si è ulteriormente ampliato. L'istituto di credito deve dimostrare l'effettiva implementazione e il corretto funzionamento di protocolli di sicurezza avanzati (biometria, TOTP, dispositivi di firma forte, ecc.). In mancanza di tali elementi, la banca non può imputare colpa grave all'utente né negare il rimborso.
L'orientamento dell'Arbitro Bancario Finanziario (ABF) negli ultimi anni è chiaro:

- la banca deve provare la **colpa grave** dell'utente;
- in assenza di tale dimostrazione, deve rimborsare immediatamente l'operazione disconosciuta, sottraendo solo eventuali franchigie previste dalla legge;
- l'istituto deve dimostrare che l'intrusione sia avvenuta esclusivamente per causa imputabile al cliente, escludendo ogni possibile vulnerabilità del proprio sistema.

### 2.2. Oltre la SCA (Strong Customer Authentication): perché l'autenticazione a due fattori non esclude automaticamente la responsabilità dell'intermediario.

L'introduzione della **Strong Customer Authentication (SCA)** prevista dalla Direttiva PSD2 ha rappresentato una significativa forma di tutela per le transazioni elettroniche; tuttavia, ha anche generato importanti equivoci, spesso sfruttati dalle banche nelle prime risposte ai clienti che contestano operazioni fraudolente. Molti istituti, infatti, tendono a sostenere che il semplice corretto funzionamento dell'autenticazione a due fattori (2FA) sia sufficiente a dimostrare la colpa grave dell'utente, ritenendolo automaticamente responsabile dell'autorizzazione della transazione.

La giurisprudenza e numerose decisioni dell'Arbitro Bancario Finanziario (ABF) hanno invece chiarito che la prova dell'avvenuta autenticazione forte non esaurisce l'onere probatorio della banca, ma attesta esclusivamente la regolarità formale della procedura.

La banca deve dimostrare, inoltre, che l'operazione — pur autenticata — non sia stata influenzata da malfunzionamenti tecnici, vulnerabilità non rilevate o sfruttate tramite exploit zero-day.

L'intermediario, pertanto, resta responsabile quando l'operazione fraudolenta è resa possibile da attacchi informatici avanzati, capaci di aggirare o manipolare il sistema di autenticazione "forte".

Tra gli attacchi che trasferiscono la responsabilità in capo all'istituto di credito troviamo:

- Man in the Middle (MITM);
- Man in the Mail (MITMail);
- Man in the Browser (MITB).

In questi scenari, il codice malevolo intercetta in tempo reale i codici generati dal sistema SCA, rendendo l'autenticazione formalmente corretta, ma soggettivamente non autorizzata dall'utente.

Un'altra tecnica particolarmente insidiosa è il **SIM swapping**, mediante il quale il truffatore clona la SIM della vittima per intercettare gli SMS contenenti i codici OTP.

Negli ultimi anni si è inoltre diffusa una tipologia di attacco ancora più sofisticata: l'invio di SMS apparentemente provenienti dal numero verde della banca, contenenti link anomali o file malevoli**.**

Basta una piccola distrazione affinché l'utente clicchi sul link e — inconsapevolmente — conceda all'attaccante l'accesso a dati sensibili. In una seconda fase dell'attacco, il truffatore contatta telefonicamente la vittima dallo stesso numero verde della banca (o persino dal numero della filiale), rendendo quasi impossibile distinguere un reale operatore da un impostore.

Questa tecnica *ibrida* combina:

- phishing avanzato,
- smishing,
- caller ID spoofing,
- vishing,
- sofisticate tecniche di ingegneria sociale.

Il prestatore di servizi di pagamento ha l'onere non solo di dimostrare il corretto funzionamento della SCA, ma anche di provare l'adozione di sistemi di monitoraggio delle transazioni idonei a rilevare e bloccare anomalie evidenti (bonifici verso conti esteri, operazioni ad alto importo, transazioni anomale rispetto allo storico del cliente, ecc.). L'assenza di tali misure trasferisce integralmente la responsabilità sull'istituto di credito.

In prospettiva, il sistema bancario dovrebbe orientarsi verso la cosiddetta **autenticazione continua**[5], che si basa su un processo dinamico e costante di verifica dell'identità dell'utente.

[5] MICOZZI F.P., *Sicurezza informatica – obblighi e responsabilità dopo il recepimento della NIS2 e la L. n. 90/2024*, Vicenza, Wolters Kluwer, 2024.

Non più una singola autenticazione all'inizio della sessione, ma un monitoraggio continuo basato su:

- fattori comportamentali (modo di digitare, movimento del mouse),
- dati biometrici (impronta digitale, riconoscimento facciale),
- modelli di utilizzo (abitudini di navigazione, applicazioni utilizzate).

Questo approccio riduce drasticamente il rischio di accessi non autorizzati che possono verificarsi dopo l'autenticazione iniziale e rappresenta un'evoluzione fondamentale per la sicurezza dei sistemi di pagamento digitali.

## 3. L'informatica forense in via stragiudiziale.

L'opinione pubblica, anche grazie all'influenza dei media, ha imparato a conoscere l'informatica forense, ma permane ancora lo stereotipo secondo cui questa disciplina sia applicabile esclusivamente all'ambito penale, in casi quali omicidi, traffici di droga, adescamento di minori o reati contro la persona (cyberstalking, cyberbullismo, ecc.). Solo negli ultimi anni essa ha iniziato a entrare stabilmente nel processo civile.

Già nell'aprile 2024, in occasione di un convegno sulla sicurezza dei sistemi informatici tenutosi nella "Città dei Sassi", è stato affrontato il tema della necessità di superare la visione dell'informatica forense come strumento riservato a settori di nicchia del diritto penale, mettendo in evidenza il ruolo determinante che tale disciplina può assumere nella fase stragiudiziale. L'obiettivo era sensibilizzare non solo gli operatori del settore IT, ma anche avvocati, magistrati e forze di polizia.

In questo "nuovo" ambito applicativo, l'attività di informatica forense si concretizza nell'acquisizione, analisi e conservazione dei dati digitali utili a ricostruire ciò che è accaduto prima di un'operazione disconosciuta, con lo scopo di accertare sia l'eventuale intrusione nei sistemi dell'utente sia possibili condotte negligenti da parte del cliente.

Dal punto di vista dell'intermediario finanziario, l'informatica forense assume invece il carattere di una necessità operativa — se non di un vero e proprio obbligo — in quanto

strumento essenziale per adempiere all'onere probatorio previsto dall'art. 12, comma 4, del D.lgs. 11/2010.

Senza un'analisi tecnica rigorosa e tempestiva, svolta immediatamente dopo la segnalazione dell'utente, la banca difficilmente potrà produrre in giudizio prove dotate dei requisiti fondamentali di integrità e immodificabilità. Accade spesso che vengano presentati log come prova della presunta "***colpa grave***" dell'utente, ma forniti in formati modificabili e privi di **catena di custodia**, rendendoli inidonei come prova tecnica.

Se negli ultimi anni un numero crescente di utenti finali — grazie alla maggiore attenzione di alcuni avvocati — richiede una consulenza di informatica forense, le banche risultano invece ancora molto lontane dall'adottare questa strategia di difesa tecnica.

Il cuore dell'accertamento risiede nei file di log, che rappresentano la vera "***scatola nera***" degli eventi informatici relativi alle transazioni. Perché tali file assumano valore probatorio, devono essere acquisiti secondo i protocolli della digital forensics, in particolare secondo lo standard ISO 27037, così da garantirne:

- l'immodificabilità, tramite attribuzione di hash crittografici;
- la completezza, includendo non solo l'inserimento di PIN o OTP, ma anche:
    - l'indirizzo IP di origine,
    - l'ID del dispositivo,
    - l'eventuale fingerprinting,
    - la geolocalizzazione dell'operazione,
    - l'analisi comportamentale dell'utente.

Frequentemente, infatti, gli utenti autorizzano le operazioni con sistemi biometrici; nelle frodi, invece, l'autorizzazione avviene quasi sempre tramite inserimento manuale del codice, spesso da parte di soggetti terzi.

Negli ultimi anni l'ABF ha adottato un approccio sempre più rigoroso sulla qualità della prova, ritenendo insufficienti screenshot o log prodotti unilateralmente dalle banche senza garanzie tecniche idonee.

L'informatica forense consente quindi di colmare l'asimmetria informativa tra banca e cliente:

- dal **lato della banca**, serve a dimostrare — con prove certificate — la colpa grave del cliente, provando che l'operazione sia avvenuta da un dispositivo riconosciuto e autorizzato;
- dal **lato del cliente**, permette di evidenziare anomalie nei sistemi di sicurezza dell'istituto, comportamenti ingannevoli o tecniche fraudolente difficili da individuare per un utente medio, ribaltando così le contestazioni dell'intermediario.

Infine, nell'ultimo anno, l'avvento della Direttiva NIS2 — tema che esula dal focus del presente articolo — ha ulteriormente rafforzato il ruolo dell'informatica forense nelle aziende, in particolare nelle PMI, rendendola essenziale per dimostrare, anche in sede stragiudiziale, l'assenza di responsabilità in caso di incidenti informatici e per evitare sanzioni derivanti da mancata compliance normativa.

### 3.1. *Mobile Forensics*: l'analisi dello smartphone della vittima come "scatola nera" dell'evento.

Nell'era moderna lo smartphone è diventato uno strumento imprescindibile per la maggior parte delle attività quotidiane, superando il suo ruolo originario di "*terminale di comunicazione*" e trasformandosi in un vero e proprio hub di vita digitale, incluso l'accesso ai sistemi di pagamento. Si pensi, ad esempio, che una larga parte della cosiddetta Generazione Z non utilizza più il computer tradizionale e incontra difficoltà persino nell'uso del mouse, essendo ormai completamente orientata all'interazione tramite smartphone.
In questo contesto, il dispositivo mobile è divenuto il fulcro della Strong Customer Authentication (SCA), ricoprendo contemporaneamente:

- il ruolo di possesso (il dispositivo fisico),
- il ruolo di inerenza (biometria),
- il ruolo di conoscenza (codici di sblocco, PIN, passcode, app di autenticazione).

Nel contenzioso bancario, lo smartphone assume il ruolo di vera e propria scatola nera dell'evento fraudolento: è l'unico strumento dal quale è possibile ricostruire l'intera sequenza

fenomenica che ha portato al furto delle credenziali di home banking o all'autorizzazione indebita di una transazione.

L'**analisi degli artefatti digitali** consente di assolvere o escludere — a seconda della prospettiva — l'onere probatorio relativo alla colpa grave. L'esame della cronologia, dei messaggi e delle comunicazioni ricevute permette di verificare:

- la presenza di link di phishing,
- il livello di sofisticazione dell'attacco,
- l'eventuale interazione dell'utente con tali contenuti,
- quali dati siano stati concretamente carpiti dal criminale informatico.

L'**analisi della cronologia di navigazione** consente inoltre di stabilire se l'utente sia stato indirizzato verso un sito clone dell'istituto bancario, valutando se esistessero elementi che avrebbero potuto far comprendere l'anomalia del sito rispetto a quello ufficiale.

L'**analisi delle applicazioni installate** permette invece di individuare:

- app clonate che imitano quelle reali,
- trojan bancari,
- Remote Access Tool (RAT),
- eventuali compromissioni del dispositivo a livello fisico o psicologico (social engineering).

In ambito stragiudiziale, la mobile forensics consente di incrociare i dati identificativi del dispositivo (IMEI, indirizzo MAC, ID univoco dell'app, fingerprinting del device) con quelli registrati dalla banca durante la transazione, così da evidenziare:

- eventuali discrepanze che dimostrino che l'operazione è stata eseguita da un dispositivo diverso da quello "certificato" dall'utente;
- oppure, al contrario, che l'operazione è partita dal dispositivo abituale, previa notifica push regolarmente visualizzata e autorizzata biometricamente.

Naturalmente, l'analisi — e prima ancora la copia forense — devono rispettare le più recenti pronunce giurisprudenziali e le garanzie previste dal GDPR. È quindi necessario adottare la cosiddetta "copia fine", limitando l'acquisizione ai soli dati rilevanti e abbandonando la vecchia "copia mezzo", troppo invasiva e suscettibile di violare la riservatezza degli utenti.

### 3.2. Metodologia di acquisizione: garantire l'integrità del dato (*hash*, catena di custodia) per l'opponibilità nel ricorso.

La prova digitale è, per sua natura, facilmente alterabile e, proprio per questo motivo, deve essere acquisita secondo le best practice della digital forensics, così da renderla opponibile in un eventuale giudizio o ricorso, indipendentemente dalla natura del procedimento.

Il primo pilastro dell'**acquisizione forense**[6] è l'utilizzo delle funzioni di hash, indispensabili per garantire l'integrità del dato. Anche una minima e impercettibile modifica comporterebbe la generazione di un hash completamente diverso, permettendo così di individuare qualsiasi alterazione. L'attribuzione dell'hash consente inoltre la controanalisi da parte di soggetti terzi, assicurando la genuinità dell'elemento probatorio.

Un altro aspetto fondamentale è rappresentato dalla **catena di custodia**, che — a parere dello scrivente — è spesso l'elemento in grado di far crollare interi procedimenti quando non viene predisposta in modo corretto o quando manca del tutto. La catena di custodia è un documento, preferibilmente immodificabile (quando viene generato dal sistema automaticamente), che descrive tutte le procedure tecniche, operative e metodologiche adottate per tracciare ogni passaggio della prova digitale, dal momento dell'acquisizione fino alla sua presentazione davanti all'autorità competente (giudice o organismo stragiudiziale).

La catena di custodia deve indicare con precisione:

- la fonte di prova, cioè l'origine dei dati estratti;
- il nominativo del soggetto che ha effettuato l'acquisizione;
- la strumentazione utilizzata;
- i riferimenti temporali delle operazioni;
- gli spostamenti del dato e le persone che ne sono venute in contatto;

[6] ISO/IEC 27037:2012 – *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.*

- le modalità di conservazione del materiale probatorio.

Affinché un ricorso — ad esempio davanti all'ABF — o un'azione giudiziaria abbiano successo, l'**integrità del dato** deve essere garantita sin dall'origine. Se l'interpretazione dell'informazione può differire tra i consulenti, l'estrazione e la metodologia di acquisizione devono essere inattaccabili: ciò permette di dimostrare che il dato è integro, completo e, quindi, incontestabile.

Accade spesso, invece, che in assenza di una catena di custodia rigorosa, la controparte eccepisca che il log sia stato generato o modificato ex post dall'intermediario per nascondere una vulnerabilità del sistema. Allo stesso modo, se la banca non è in grado di garantire l'integrità della prova digitale prodotta, essa non assolve all'onere probatorio previsto dalla legge. Il risultato è la soccombenza tecnica, indipendentemente dalla possibile veridicità dei fatti dichiarati.

### 3.3. Ricostruzione del "*customer journey*" fraudolento: analisi dei log di sistema, *sms thread* e cronologia browser.

Il concetto di *customer journey*, solitamente utilizzato in ambito commerciale per rappresentare il percorso dell'utente verso l'acquisto, assume in informatica forense — soprattutto nelle frodi bancarie — un significato diverso: rappresenta la ricostruzione cronologica dei passi compiuti dalla vittima e dall'attaccante, consentendo di valutare l'eventuale consapevolezza dell'utente e il livello di manipolazione subito.

L'informatico forense ha quindi l'onere di ricostruire tale percorso per stabilire se l'origine dell'evento sia imputabile a una falla tecnica o a una falla umana. Questa ricostruzione è fondamentale per determinare il grado di diligenza esigibile dall'utente ai sensi dell'art. 1176, comma 2, c.c.

I log del Prestatore di Servizi di Pagamento (PSP) rappresentano il punto di osservazione privilegiato per verificare l'integrità dei sistemi di sicurezza. La loro analisi permette di esaminare:

- le anomalie delle sessioni,
- il fingerprinting del dispositivo,
- le modalità di validazione della SCA,

- eventuali attività precedenti all'operazione fraudolenta (binding di nuovi dispositivi, modifiche dei limiti operativi, bonifici effettuati dopo il cut-off).

Tutto ciò consente una ricostruzione completa dell'evento, evitando di focalizzarsi solo sull'operazione finale (ad esempio un bonifico verso conti esteri).
La difesa dell'utente risiede spesso nell'analisi del *thread SMS*. L'inserimento di un messaggio fraudolento all'interno della conversazione legittima della banca (*Sender ID Spoofing*) altera profondamente la percezione della vittima, rendendo impossibile distinguere tra comunicazione autentica e comunicazione fraudolenta.
L'analisi dei metadati associati agli SMS è altrettanto importante, poiché questi rappresentano "*informazione nell'informazione*" e consentono di verificare:

- se il messaggio sia stato ricevuto tramite canali standard,
- se presenti anomalie nelle intestazioni,
- se vi sia manipolazione del mittente.

Quando il messaggio fraudolento appare nella stessa catena dei messaggi autentici, la colpa grave dell'utente deve essere esclusa: è il sistema di comunicazione ad aver fallito nel garantire l'autenticità del mittente, inducendo un affidamento incolpevole non rilevabile con l'ordinaria diligenza.
L'analisi della cronologia di navigazione e dei file di cache consente di individuare il momento esatto dell'attacco, verificando se l'utente sia giunto sul sito clone:

- tramite digitazione errata dell'URL, oppure
- mediante tecniche più sofisticate di manipolazione del traffico DNS.

In alcuni casi, è persino possibile recuperare i dati inseriti nei moduli HTML del sito di phishing. La prova che l'utente abbia digitato non solo le credenziali ma anche i codici OTP dimostra una manipolazione della volontà attraverso tecniche di social engineering, e permette di qualificare correttamente la condotta dal punto di vista della colpa — o di escluderla del tutto.

L'incrocio di tutti gli elementi analizzati — log, thread SMS, cronologia, metadati, fingerprinting, comportamenti anomali — consente di trasformare la difesa dell'utente da una semplice negazione ("*non sono stato io*") a una dimostrazione documentale della sofisticazione dell'attacco, escludendo in modo rigoroso ogni sua responsabilità.

## 4. Analisi tecnica della *deception*: dimostrare l'impossibilità di distinguere il falso dal vero.

Il giudizio sulla colpa grave dell'utente, quando si parla di responsabilità civile dell'intermediario[7], non può prescindere da un'analisi tecnica qualitativa dell'inganno (***deception***).

Storicamente, il phishing era caratterizzato da errori grammaticali evidenti, loghi approssimativi e pagine web facilmente riconoscibili come false. Oggi, invece, gli attacchi consentono la creazione di una simmetria percettiva quasi perfetta, grazie a interfacce fraudolente sempre più indistinguibili da quelle reali, spesso generate o ottimizzate tramite sistemi di intelligenza artificiale.

In questo scenario, il criterio della diligenza del "*buon padre di famiglia*", tradizionalmente applicato al comportamento dell'utente, deve essere necessariamente ricalibrato[8]. La crescente sofisticazione degli attacchi rende infatti in molti casi oggettivamente impossibile rilevare l'alterazione, persino per utenti esperti.

Uno degli elementi tecnici più critici della moderna *deception* bancaria è lo **spoofing dell'Alphanumeric Sender ID**. Gli attaccanti sfruttano vulnerabilità strutturali del protocollo **SS7 (Signaling System No.7)**[9], che consente loro di inviare SMS che il dispositivo mobile aggrega automaticamente all'interno del *thread* dei messaggi autentici della banca.

L'SS7, sviluppato negli anni '70 e standardizzato dall'ITU-T[10], separa il canale della segnalazione (necessario per chiamate e SMS) da quello della voce. Tuttavia, è nato in

[7] MARASÀ F., Servizi di pagamento e responsabilità degli intermediari, Milano, Giuffrè, 2020.
[8] AA.VV., *Intelligenza artificiale – Diritto, Giustizia, economia ed etica*, Torino, Giappichelli, 2025.
[9] FRALLICCIARDI A., Signalling System N.7 (Ss7) Security: Vulnerabilità Indotte Dalle Reti Ip, Sicurezza e Giustizia, (https://www.sicurezzaegiustizia.com/signalling-system-n-7-ss7-security-vulnerabilita-indotte-dalle-reti-ip/, consultato il 08.03.2026).
[10] L'ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) è il settore dell'Unione internazionale delle telecomunicazioni (ITU) responsabile della standardizzazione delle telecomunicazioni a livello mondiale.

un'epoca in cui soltanto operatori telefonici governativi o parastatali accedevano alla rete, e non prevede meccanismi robusti di autenticazione.

Dal punto di vista giuridico e di sicurezza, ciò comporta che gli istituti di credito che continuano a utilizzare gli SMS come parte della SCA adottano di fatto una tecnologia intrinsecamente insicura.

Un utente che riceve un SMS fraudolento posizionato tra due messaggi legittimi (ad esempio tra un avviso di accesso e una notifica di saldo) subisce un effetto di validazione per prossimità.

Il dispositivo, infatti, presenta il messaggio come proveniente dalla stessa fonte affidabile. L'utente, quindi:

- non ha alcun parametro tecnico per distinguere il messaggio falso;
- sta rispondendo a un comando che il suo stesso strumento di sicurezza (lo smartphone) qualifica come autentico.

In questo contesto, l'onere probatorio della banca nel dimostrare la colpa grave fallisce irrimediabilmente: l'utente non sta ignorando un rischio, ma sta reagendo nel modo che qualsiasi persona ragionevole avrebbe avuto di fronte a un messaggio che appare ufficiale.

L'attacco moderno non si limita al messaggio. Spesso si completa con una componente vocale tramite **Voice Phishing (vishing)**. Grazie alle tecniche di **VoIP Spoofing**, l'attaccante può far comparire sul display del telefono della vittima il numero ufficiale del Customer Service della banca o persino il numero della filiale locale.

Quando:

- la componente testuale (SMS),
- quella visiva (sito clone perfettamente simile all'originale), e
- quella vocale (chiamata apparente dal numero della banca)

convergono in un'unica narrazione coerente e apparentemente ufficiale, l'utente viene intrappolato in una "trappola tecnologica" che annulla la sua capacità di autodeterminazione.

L'analisi approfondita delle moderne tecniche di *deception* dimostra che gli attacchi attuali non sono, e in futuro non potranno essere, riconoscibili con la normale diligenza richiesta a un utente medio.

L'inganno, sfruttando vulnerabilità strutturali e strumenti di spoofing sempre più sofisticati, diventa così perfetto, spostando la responsabilità tecnica e giuridica sull'intermediario, che deve garantire sistemi di autenticazione realmente sicuri e non basati su tecnologie superate.

### 4.1. Anatomia dello *spoofing*: come i criminali si inseriscono nei *thread* legittimi dei messaggi bancari.

A differenza delle comunicazioni tra privati, in cui il mittente è identificato tramite un numero telefonico (MSISDN), gli istituti di credito utilizzano *alias* alfabetici denominati **Alphanumeric Sender ID** (ad es. "BANCA_XX"). Tecnicamente, questi non sono numeri di telefono, ma stringhe di testo trasmesse attraverso i centri servizi SMS (SMSC).

Il limite strutturale di questa tecnologia risiede nella mancata verifica della titolarità dell'alias: le reti di telecomunicazione trasportano la stringa indicata dal mittente senza alcun protocollo di autenticazione centralizzato, analogamente a quanto accade per il protocollo SMTP nelle e-mail.

Questa vulnerabilità, unita al comportamento dei sistemi operativi mobili (iOS e Android), permette agli attaccanti di sfruttare il raggruppamento automatico dei messaggi basato unicamente sulla stringa del mittente. Se lo smartphone riceve un SMS con un Sender ID identico a uno già presente (es. "BANCA_XX"), il sistema operativo lo aggregherà automaticamente nella stessa conversazione, inserendo il messaggio fraudolento accanto a quelli autentici.

Ciò annulla, di fatto, la capacità critica della vittima: il messaggio malevolo eredita l'autorevolezza dei messaggi legittimi precedenti, secondo un noto principio psicologico di coerenza contestuale.

Per ottenere questo risultato, l'attaccante opera a livello infrastrutturale, utilizzando provider di SMS mas-sivi situati in Paesi che non applicano controlli stringenti e che permettono l'utilizzo arbitrario del campo "Sender ID" senza alcuna autentica verifica della sua titolarità.

È opportuno segnalare che l'operatore WindTre mette a disposizione dei propri utenti una modalità (nota come sintassi K) che consente l'invio di SMS anonimi. Tale funzione — risultata ancora attiva lo scorso anno — non permette la modifica personalizzata del Sender ID come avviene nelle frodi bancarie, ma rappresenta comunque un fattore di rischio, ad esempio in contesti di stalking o comunicazioni ingannevoli.

Questa criticità evidenzia ancora una volta la fragilità intrinseca dei protocolli SMS, concepiti in un'epoca in cui non si immaginava l'attuale livello di esposizione al cybercrime.
Durante i ricorsi, molti istituti bancari eccepiscono che l'utente fosse stato avvertito di "non cliccare su link sospetti", allegando brochure, screenshot o pagine del proprio sito che illustrano campagne antifrode.
Tuttavia, l'analisi tecnica dimostra l'inadeguatezza di tali avvertimenti:

- Il messaggio arriva dal mittente ufficiale ("BANCA_XX"), quindi non appare sospetto.
- Si inserisce nella cronologia degli SMS autentici, sfruttando la validazione per prossimità.
- Il link non presenta necessariamente elementi visivi anomali, poiché l'attaccante può replicare perfettamente la sintassi utilizzata dall'istituto.
- L'utente non può controllare l'header del messaggio, a differenza di quanto avviene per le e-mail. Negli SMS non esiste un accesso diretto ai metadati di trasporto.
- Il terminale stesso — strumento su cui la banca fa affidamento per la SCA — qualifica il mittente come autentico, inducendo un affidamento del tutto incolpevole.

Ne consegue che il comportamento dell'utente non può essere ricondotto a colpa grave: l'inganno non è riconoscibile con la normale diligenza richiesta a un consumatore medio.

### 4.2. Il fattore umano e l'ingegneria sociale: analisi del contesto psicologico indotto dall'attaccante.

Nell'ecosistema digitale contemporaneo — e in particolare nell'ambito della sicurezza cibernetica — il perimetro di difesa non è più rappresentato esclusivamente da sistemi fisici (hardware e software) o da protocolli crittografici, ma sempre più dalla resilienza cognitiva dell'utente finale.
L'informatica forense, nata originariamente per raccogliere, preservare e analizzare artefatti digitali, si è progressivamente evoluta integrando competenze provenienti da altre discipline, tra cui la ***behavioural analysis***. Questo ha permesso di comprendere più a fondo le modalità

con cui gli attaccanti manipolano il fattore umano, oggi considerato il vero punto debole dell'intero ecosistema di sicurezza.
Le truffe bancarie contemporanee non si fondano infatti su "semplici" errori tecnici, ma su veri e propri hacking psicologici, studiati per ridurre o inibire il pensiero critico della vittima. Questi attacchi sfruttano:

- il senso di urgenza o di paura (ad esempio: "*il suo conto è stato violato*", "*è in corso un bonifico da X mila euro*");
- la percezione dell'autorità, attraverso un linguaggio tecnico, formale e convincente da parte dei finti operatori bancari;
- la sovraccarica cognitiva, mediante l'invio di numerose istruzioni complesse durante la telefonata, che porta la vittima ad abbassare la guardia e a farsi guidare passo passo dall'attaccante.

L'obiettivo dei criminali è semplice: sostituirsi alla capacità decisionale della vittima, facendole credere di "collaborare" alla risoluzione di un problema inesistente.
L'Intelligenza Artificiale può diventare uno strumento cruciale nel contrasto a queste tecniche, consentendo un'analisi comportamentale automatizzata e continua dell'utente, al fine di identificare anomalie o segnali di rischio che possano anticipare tentativi di frode.
Parallelamente, un approccio di ***forensics readiness***, applicato lato istituto di credito, permetterebbe di:

- acquisire e conservare log dettagliati e non solo quelli della singola transazione;
- ricostruire a posteriori l'intero evento fraudolento;
- rafforzare i sistemi di monitoraggio;
- prevenire attacchi futuri, migliorando la risposta operativa.

Questo approccio rende la banca non solo più pronta ad affrontare un eventuale contenzioso, ma anche più proattiva nel mitigare vulnerabilità sistemiche.
Un elemento irrinunciabile è il percorso formativo dell'utente, sia esso consumatore o operatore bancario. La formazione efficace dovrebbe includere:

- sessioni periodiche di simulazioni di phishing;
- campagne svolte in momenti differenti dell'anno, per evitare fenomeni di assuefazione;
- esercitazioni condotte in condizioni di stress cognitivo, per testare la capacità degli utenti di riconoscere segnali di rischio anche in condizioni realistiche.

L'obiettivo non è colpevolizzare l'utente, ma aumentare la sua resilienza comportamentale, così da ridurre il successo delle tecniche di manipolazione psicologica utilizzate dagli attaccanti.

### 4.3. Evidenze forensi di sofisticatezza: dimostrare che l'utente ha agito in "buona fede soggettiva" di fronte a un'interfaccia indistinguibile dall'originale.

Le più recenti pronunce dell'ABF e dei tribunali hanno escluso la responsabilità dell'utente finale quando l'attacco presenta un livello di sofisticazione tale da ingannare anche un soggetto diligente. In questi casi, il comportamento dell'utente non può essere qualificato come colpa grave, poiché l'inganno è tecnicamente e percettivamente irrilevabile con l'ordinaria diligenza.

Il compito dell'analista forense non è solo accertare cosa sia accaduto, ma anche ricostruire come appariva l'interfaccia utente nel momento in cui la vittima ha compiuto l'azione (tipicamente il click sul link fraudolento). L'aspetto percettivo — cioè ciò che l'utente ha realmente visto — diventa un elemento probatorio centrale.

Una delle evidenze più rilevanti è l'analisi della landing page utilizzata per la raccolta fraudolenta dei dati tramite phishing. Gli attaccanti moderni non si limitano più a copiare un logo o un'immagine: realizzano copie speculari delle pagine ufficiali, indistinguibili nello stile, nei colori, nel layout e persino in parte del codice sorgente.

L'analisi forense permette di dimostrare, tramite l'esame dei file di cache e dei fogli di stile (CSS), che:

- i **CSS** della pagina fraudolenta replicano fedelmente quelli originali;
- gli **script** includono funzioni analoghe a quelle utilizzate dalla banca;

- il **comportamento dinamico del sito** (tempi di caricamento, animazioni, messaggi di avanzamento) è deliberatamente studiato per imitare l'esperienza reale.

Questa perfetta simmetria percettiva genera un falso senso di sicurezza, poiché l'utente ritrova esattamente gli stessi elementi visivi e funzionali ai quali è abituato.
La buona fede dell'utente viene ulteriormente rafforzata dal contesto comunicativo ricostruito nei capitoli precedenti:

- Sender ID Spoofing, che inserisce il messaggio malevolo nella chat ufficiale della banca;
- siti perfettamente clonati;
- chiamate vocali spoofate provenienti dal numero del servizio clienti.

Tutti questi elementi contribuiscono a creare una narrazione unica e coerente, che qualsiasi persona ragionevole percepirebbe come autentica.
Per dimostrare la buona fede dell'utente, l'analisi forense deve ricostruire e certificare:

- la coerenza procedurale dei passaggi effettuati dall'utente;
- la loro corrispondenza con le procedure tipiche dei canali ufficiali;
- che l'utente ha seguito un flusso operativo assolutamente normale;
- che le scelte compiute sono state indotte da un sistema digitale controllato dall'attaccante e non da imprudenza.

In altre parole, la *digital forensics* deve dimostrare che l'utente ha agito in perfetta buona fede, rispondendo a stimoli che apparivano affidabili e coerenti.
L'evidenza forense di un'interfaccia indistinguibile da quella reale trasforma il correntista da presunto "***soggetto negligente***" a parte lesa di una frode evoluta.
Questo sposta inevitabilmente il baricentro della responsabilità verso:

- l'inadeguatezza dei sistemi di rilevamento dell'intermediario;
- l'insufficienza delle tecnologie di autenticazione adottate;

- la mancata capacità dell'istituto di prevenire tecniche di *deception* ormai note e diffuse.

In tali circostanze, l'onere probatorio della banca non può ritenersi assolto.

## 5. Casi pratici e orientamenti recenti dell'ABF.

L'ABF è un sistema di risoluzione stragiudiziale basato esclusivamente sulla documentazione prodotta dalle parti e, a differenza del tribunale ordinario, non ammette consulenze tecniche d'ufficio (CTU).
Per questa ragione, il punto cardine di un ricorso all'ABF diventa la consulenza tecnica di parte (CTP), che rappresenta uno strumento fondamentale per il ricorrente al fine di analizzare, interpretare e — quando necessario — superare le evidenze tecniche eventualmente presentate dalla banca.
In questo capitolo verranno illustrati alcuni casi pratici trattati dallo scrivente in qualità di CTP dei ricorrenti, sotto una duplice veste:

- quella di consulente informatico forense,
- e quella di consulente legale, spesso in supporto a studi professionali che, fino a quel momento, non si erano mai confrontati con i sistemi ADR (*Alternative Dispute Resolution* – Risoluzione Alternativa delle Controversie).

L'applicazione delle best practices della *Digital Forensics* si è dimostrata essenziale: è stato infatti possibile trasferire nell'ambito stragiudiziale tutto il bagaglio culturale e le competenze maturate negli anni nel settore penale, a partire dal 2008, anno in cui l'Italia ha ratificato la Convenzione di Budapest sul Cybercrime del 2001, dando vita alla **Legge 48/2008**, tuttora la principale colonna portante delle indagini informatiche in materia di criminalità digitale.
I casi saranno presentati in forma narrativa, con le opportune omissioni di nomi e dettagli che potrebbero rendere identificabili i ricorrenti che hanno affidato il loro caso allo scrivente.

### 5.1. Caso 1 – *Sim Swap Fraud.*

Il ricorrente lamentava la sottrazione di somme dal proprio conto corrente mediante bonifici non autorizzati che, nella casistica di chi scrive, avvengono quasi sempre in orari o giorni di chiusura delle filiali fisiche degli istituti bancari.

Nel caso di specie, le operazioni fraudolente erano state eseguite di venerdì pomeriggio, dopo il normale orario di chiusura giornaliera — e quindi settimanale — della banca.

L'utente aveva inizialmente segnalato un apparente disservizio della linea telefonica mobile, poiché sul display del proprio smartphone compariva la dicitura "Nessun segnale", fenomeno che in condizioni ordinarie non desta particolare allarme, essendo spesso dovuto a temporanee assenze di copertura di rete o a normali attività manutentive dell'operatore telefonico.

In questo caso, tuttavia, il problema era ben diverso: i truffatori avevano ottenuto un duplicato della SIM card del cliente tramite un rivenditore compiacente o poco diligente. Ottenuto il controllo della linea, avevano potuto ricevere i codici OTP sul nuovo dispositivo in loro possesso, aggirando così il sistema di autenticazione a due fattori. È il tipico schema della Sim Swap Fraud[11].

Come spesso accade, la prima risposta dell'istituto di credito seguiva un iter "*a stampo*", affermando che:

- le operazioni erano state regolarmente autenticate tramite SCA,
- il cliente era incorso in colpa grave,
- il cliente non avrebbe custodito correttamente i codici o non avrebbe bloccato la SIM con sufficiente tempestività.

Ma la vicenda va analizzata secondo una duplice prospettiva:

- Il cliente non ha mai perso il controllo dei codici OTP, semplicemente perché non li ha mai ricevuti;

[11] SATTA G., *Sim swap fraud: chi risarcisce i danni al truffato?*, Altalex.com, (https://www.altalex.com/documents/2023/10/23/sim-swap-fraud-risarcisce-danni-truffato - data consultazione 08.03.2026).

- La "*tempestività*" nel blocco della SIM non può essere stabilita astrattamente: un utente medio non può immediatamente sospettare un attacco informatico quando compare un messaggio di assenza di segnale, evento frequente e generalmente privo di connotazioni fraudolente.

Nella maggior parte dei casi, occorre tempo per comprendere la natura del problema e valutare se si tratti di un:

- disservizio di rete,
- malfunzionamento del dispositivo,
- guasto del ponte radio,
- semplice mancanza di copertura,
- o, solo in ultima analisi, una truffa in corso.

Le pronunce più recenti dell'ABF[12] confermano che:

- la mera presenza dell'OTP correttamente inserito non prova la colpa grave del cliente;
- la banca deve dimostrare di aver adottato sistemi di monitoraggio efficaci, in grado di rilevare anomalie tipiche del ***SIM swapping*** (cambio SIM, accessi da nuovi dispositivi, modifiche dei limiti);
- il cliente può e deve dimostrare, tramite consulenza tecnica di parte, che l'accesso ai propri dati sia avvenuto tramite ingegneria sociale evoluta.

Nel caso concreto, la consulenza tecnica ha permesso di dimostrare che:

- L'attacco era iniziato tramite smishing: l'utente aveva ricevuto un SMS di alert che si era perfettamente inserito nel *thread* dei messaggi ufficiali della banca (Sender ID Spoofing).
- Dopo aver cliccato sul link, l'utente aveva inserito solo nome, cognome, email e numero di telefono nella landing page fraudolenta, senza mai

[12] Tribunale di Roma, Sez. XVI, sentenza 19 luglio 2023, n. 11547 e sentenza 11 settembre 2023, n. 12832.

digitare le credenziali di home banking (Questi artefatti sono stati recuperati tramite l'analisi della cronologia di navigazione).

- Pochi minuti dopo l'inserimento dei dati, la SIM del cliente è stata disattivata e trasferita sul dispositivo dei criminali.
- I truffatori hanno quindi ricevuto gli OTP e hanno eseguito i bonifici dal nuovo device.

La linea di indagine si è concentrata sull'analisi forense del dispositivo e sulla tempistica tra:

- il distacco della SIM del cliente,
- e l'esecuzione dei bonifici.

Molti di questi bonifici risultano essere istantanei, e dunque non revocabili.
La circostanza che l'attacco sia avvenuto di venerdì pomeriggio ha aggravato ulteriormente la situazione: l'utente ha potuto recarsi in filiale solo il lunedì, quando ormai i criminali avevano completamente svuotato il conto.
Dopo aver perso il controllo della SIM, e quindi del processo di autenticazione, l'utente era stato totalmente estromesso dal proprio home banking.

### 5.2. Caso 2 – App bancaria clonata

Questo caso rappresenta una delle frontiere più insidiose delle frodi finanziarie, perché utilizza app malevole clonate. A differenza del phishing tradizionale, questa tecnica — altamente evoluta — sfrutta un malware (trojan bancario) che, una volta installato sullo smartphone della vittima, monitora e manipola tutte le attività sensibili.
Quando l'utente apre l'app ufficiale della banca (nel caso di specie, l'app BNL), il malware intercetta l'evento e sovrappone istantaneamente una schermata grafica identica a quella originale (***overlay attack***). L'utente, convinto di operare in un ambiente sicuro, inserisce credenziali, PIN e in alcuni casi perfino codici OTP, consegnando di fatto tutte le informazioni ai truffatori.

Nel caso esaminato, il primo vettore di attacco è stata una telefonata ricevuta dal numero +39 06060[13], corrispondente al servizio clienti BNL BNP Paribas, con prefisso riconducibile al distretto di Roma. Dopo questa prima chiamata, ne sono seguite altre dieci, per un totale di undici contatti.

A causa di un presunto "*disservizio dell'app*", il cliente è stato indotto a scaricare una nuova applicazione dal Play Store denominata "***Certificato Web***", che presentava:

- lo stesso logo dell'app BNL ufficiale,
- la dicitura "Banca Nazionale del Lavoro",
- una grafica perfettamente coerente a quella reale.

Un elemento particolarmente critico emerso nel caso riguarda il numero di download: alla data del 24.10.2024 l'app contava oltre 100 milioni di installazioni (100M+). Tale circostanza, nonostante l'app non fosse parte dell'ecosistema ufficiale BNL (come confermato dallo stesso istituto), avrebbe indotto in errore anche un utente esperto, data l'apparente autorevolezza della scheda Google Play.

Dall'analisi tecnica è emerso che:

- il download dell'app è avvenuto alle 17:16 del 24.10.2024,
- l'ultima chiamata dei truffatori era terminata alle 17:03 (durata 5'03"),
- l'app scaricata non risultava installata sul dispositivo.

Ciononostante, presso la filiale BNL del cliente risultava che alle 17:46 dello stesso giorno era stato disposto un bonifico ordinario, tramite Web/App, per € 22.500,00 verso un IBAN italiano intestato a un'azienda sconosciuta al cliente.

Ulteriori accertamenti hanno mostrato che il bonifico:

- era stato eseguito verso un conto presso Poste Italiane S.p.A.,
- presentava data contabile e valuta coincidenti,

[13] BNL, https://bnl.it/it/Individui-e-Famiglie/Internet-e-Mobile/Banca-via-Telefono (data consultazione 08.03.2026).

- risultava disposto oltre il ***cut-off bancario*** (ore 17:00 secondo foglio informativo BNL).

Questa combinazione di fattori è stata ritenuta anomala e meritevole di approfondimento.
Le verifiche ***OSINT*** hanno confermato che la società beneficiaria del bonifico era realmente esistente, con sede nel Veneto. Questo elemento è tipico delle frodi sofisticate: utilizzare soggetti reali per velocizzare il trasferimento e rendere meno sospetta la transazione.
Pochi minuti dopo l'esecuzione dell'operazione, la vittima ha contattato il servizio clienti BNL, nuovamente al medesimo numero *spoofato*:

- alle 18:02 e 18:03, con l'assistenza dell'operatore "Roberto", con numero operatore "12345",
- ha richiesto ed ottenuto un numero di blocco, riportato anche nella denuncia presentata quello stesso giorno.

Il mattino successivo, alle 09:15, la vittima si è recata fisicamente presso la propria filiale per richiedere un ulteriore blocco del bonifico, classificato come operazione fraudolenta[14].
L'operazione presenta elementi tecnici che sollevano dubbi sulla regolarità del sistema BNL:

- Il bonifico è stato eseguito alle 17:46, oltre il cut-off delle 17:00.
- È stato comunque registrato con data valuta coincidente, come se fosse istantaneo.
- Non è stato revocato, nonostante la richiesta effettuata 16 minuti dopo, alle 18:03.
- Il beneficiario apparteneva a un altro istituto (Poste Italiane).
- L'app fraudolenta sul Play Store presentava logo, nome e descrizione identici all'originale.

Gli elementi combinati suggeriscono, a parere dello scrivente, una doppia vulnerabilità:

[14] ZICCARDI G., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali. Vol. 2*, Milano, Giuffrè, 2012.

- **ID *Calling Spoofing***: i truffatori hanno simulato perfettamente il numero del call center dell'istituto di credito.
- **Possibile falla del sistema bancario**: il bonifico ordinario oltre il *cut-off* è stato trattato anonimamente come se fosse immediatamente eseguibile.

Nonostante la tempestività del cliente — che ha chiesto il blocco 16 minuti dopo la disposizione e ha reiterato la richiesta il giorno successivo — non ha più ricevuto alcun riscontro dalla banca.
Questo solleva dubbi sull'efficacia dei sistemi di protezione e revoca dell'istituto nell'ambito della prevenzione delle frodi.

## 6. Conclusioni.

L'analisi condotta evidenzia come la consulenza informatica forense non rappresenti più un elemento accessorio, ma il cuore pulsante del procedimento davanti all'Arbitro Bancario Finanziario (ABF). In un sistema di risoluzione stragiudiziale (ADR) privo di udienze e di Consulenze Tecniche d'Ufficio (CTU), la Consulenza Tecnica di Parte (CTP) diventa l'unico strumento capace di colmare l'asimmetria informativa tra istituto di credito e cliente.
L'efficacia deflattiva dell'ABF — che garantisce tempi di definizione rapidi, fino a un massimo di 180 giorni — dipende direttamente dalla qualità della prova documentale depositata. Una perizia informatica rigorosa, redatta secondo gli standard internazionali (come ISO 27037) e corredata da catena di custodia e funzioni di hash, trasforma il ricorso da una semplice contestazione a un dossier tecnico inattaccabile. Questo approccio incrementa in modo significativo le probabilità di adempimento spontaneo da parte delle banche (oggi tra il 95% e il 98%) e riduce la necessità di adire la giustizia ordinaria, contribuendo ad alleggerire il carico dei tribunali civili.
L'avvento dell'Intelligenza Artificiale ha inaugurato una nuova era di hacking psicologico, in cui tecniche di *deception* come:

- lo *spoofing* dell'*Alphanumeric Sender ID*,
- la clonazione di app bancarie,
- l'inserimento di SMS fraudolenti nei *thread* ufficiali,
- il *vishing* con numeri spoofati del servizio clienti,

rendono l'inganno indistinguibile dall'esperienza reale dell'utente. In questo contesto, la difesa tecnica deve evolversi verso una multidisciplinarietà specialistica: l'analista forense non deve limitarsi a estrarre log, ma deve saper integrare analisi comportamentale e valutazione del contesto percettivo, dimostrando la buona fede soggettiva dell'utente di fronte a trappole tecnologiche ormai perfette.

Alla luce dei moderni vettori d'attacco, diventa evidente che la tradizionale Strong Customer Authentication (SCA), pur rappresentando un passo avanti rispetto al passato, non è più sufficiente da sola a prevenire le frodi.

La sicurezza dei sistemi bancari deve evolvere verso il paradigma della autenticazione continua, già analizzato nei capitoli precedenti.

A differenza dell'autenticazione "una tantum" in fase di accesso, la autenticazione continua:

- monitora costantemente l'identità dell'utente durante l'intera sessione,
- analizza parametri biometrici e comportamentali (ritmo di digitazione, movimenti touch, postura del dispositivo),
- verifica anomalie di contesto (geolocalizzazione, *device fingerprinting*, pattern d'uso),
- identifica variazioni improvvise del comportamento come possibili attività fraudolente.

L'integrazione dell'autenticazione continua nei sistemi di home e mobile banking rappresenta il futuro della sicurezza applicativa, poiché riduce drasticamente il rischio di compromissione dopo l'autenticazione iniziale — rischio emerso in quasi tutti i casi trattati.

La mancanza di tali sistemi di monitoraggio aumenta il peso dell'onere probatorio in capo alla banca, che non può limitarsi a dimostrare l'avvenuta SCA, ma deve provare di aver adottato misure realmente idonee, come previsto dalla normativa vigente.

Il futuro dei procedimenti ADR richiede una maggiore standardizzazione delle prove tecniche, seguendo il percorso già tracciato in ambito penale dalla Legge 48/2008, che ha introdotto nel sistema italiano regole chiare per l'acquisizione e la conservazione della prova digitale.

Solo tramite protocolli certi di acquisizione — che includano:

- analisi dei metadati,
- valutazione della cronologia browser,
- estrazione degli SMS *thread*,
- *fingerprinting* del dispositivo,
- ricostruzione del *customer journey* digitale,
- verifica della presenza di trojan, RAT o app clonate,

sarà possibile garantire che il dato digitale sia considerato integro, completo e incontestabile. Questo approccio, oltre a tutelare il diritto dell'utente, spingerà gli istituti bancari verso una seria adozione di modelli di *Forensics Readiness*, indispensabili per prevenire frodi evolute e per gestire correttamente gli incidenti di sicurezza.
La sfida dei prossimi anni non sarà più solo "custodire le chiavi", ossia proteggere credenziali e codici OTP, ma garantire la resilienza dell'intero ecosistema digitale contro minacce cyber sempre più simmetriche, pervasive e sofisticate.

- La combinazione di:
- analisi forense strutturata,
- autenticazione continua,
- standardizzazione delle prove digitali,
- formazione comportamentale,
- sistemi di monitoraggio evoluti,

rappresenta il nuovo paradigma di sicurezza bancaria, necessario per difendere un utente che si muove in un ambiente in cui la linea di confine tra reale e fraudolento è ormai sottilissima.

## 7. Bibliografia e sitografia.

**AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)**, Rapporti annuali sulle minacce cyber in Italia (www.acn.gov.it).
**AA.VV.**, Intelligenza artificiale – Diritto, Giustizia, economia ed etica, Torino, Giappichelli, 2025.

**BANCA D'ITALIA - ARBITRO BANCARIO FINANZIARIO**, Relazione annuale anno 2024, 18 giugno 2025 e portale delle decisioni (www.arbitrobancariofinanziario.it).

**FRALLICCIARDI A.**, Signalling System N.7 (Ss7) Security: Vulnerabilità Indotte Dalle Reti Ip, Sicurezza e Giustizia, (https://www.sicurezzaegiustizia.com/signalling-system-n-7-ss7-security-vulnerabilita-indotte-dalle-reti-ip/, consultato il 08.03.2026).

**MARASÀ F.**, Servizi di pagamento e responsabilità degli intermediari, Milano, Giuffrè, 2020.

**MICOZZI F.P.**, Sicurezza informatica – obblighi e responsabilità dopo il recepimento della NIS2 e la L. n. 90/2024, Vicenza, Wolters Kluwer, 2024.

**PIZZETTI F.**, La regolazione europea della società digitale, Torino, Giappichelli, 2024.

**SARTOR G.**, L'informatica giuridica e le tecnologie dell'informazione, Torino, Giappichelli Editore, 2022.

**SATTA G.**, *Sim swap fraud: chi risarcisce i danni al truffato?*, Altalex.com, (https://www.altalex.com/documents/2023/10/23/sim-swap-fraud-risarcisce-danni-truffato - data consultazione 08.03.2026).

**ZICCARDI G., PERON G.**, Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali. Vol. 2, Milano, Giuffrè, 2012.