

A BETTER FINANCE Stocktake on Investment Scams

Outpacing Investment Scams: Shared
Responsibility for Financial Fraud

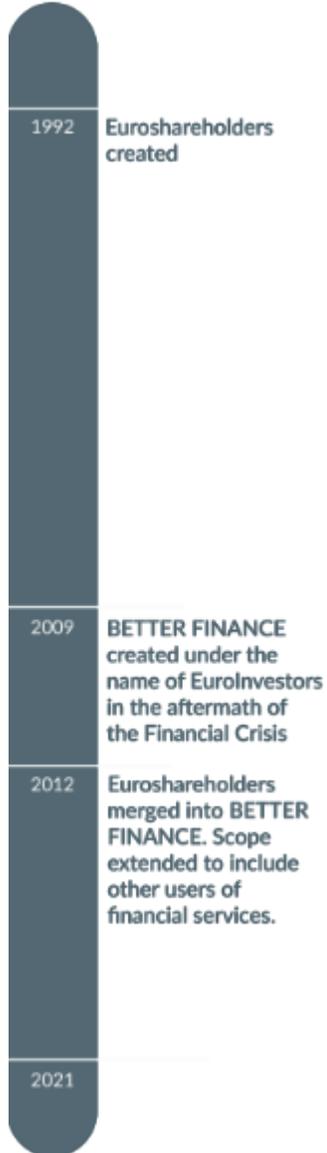
* * * * *

Briefing as part of the event: *"From Fraud to Accountability: Tackling Financial Crime Across Europe"* that took place on 9th December 2025.

BF **BETTER FINANCE**

The European Federation of Investors and Financial Services Users
Fédération Européenne des Épargnants et Usagers des Services Financiers

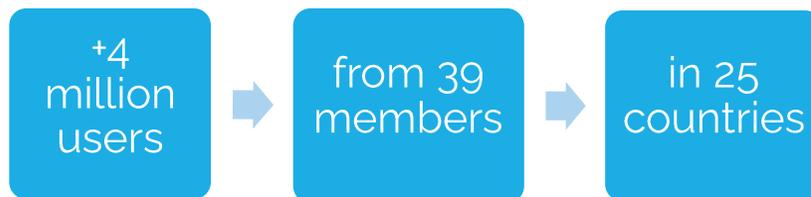
AN INDEPENDENT FINANCIAL ADVOCACY AND EXPERTISE CENTRE TO THE DIRECT BENEFIT OF EUROPEAN FINANCIAL SERVICES USERS



BETTER FINANCE was created in 2009 in the aftermath of the 2008 financial crisis to give consumers of financial services a voice. **BETTER FINANCE's** predecessor, Euroshareholders, was created in 1992 and gathered about 30 individual shareholder organisations in Europe. Euroshareholders merged with **BETTER FINANCE** in 2012 to become the [Federation of retail investors and financial services users](#).

BETTER FINANCE activities are independent, supported by the European Union since 2012 (SMP Grant) and by its member organisations. We produce policy positions and research reports, advocacy campaigns, educational material, organise policy debates, engage with policymakers and stakeholders.

BETTER FINANCE directly benefits European end-users of financial services (and non-industry stakeholders) as its members are dedicated non-profit European financial services user organisations themselves. Our constituency includes individual and small shareholders, fund and retail investors, savers, pension fund participants, life insurance policy holders, borrowers — we have the best interest of all European citizens at heart.



BETTER FINANCE represents about **4 million financial services users through 39 organisations in 25 countries, including 20 EU Member States.**



Provide access to independent investment advice



Facilitate access to simple, cost-efficient and pan-European investment products



Effectively address the pensions time bomb



Further involve, consult and empower EU citizens as financial users and investors, and their representative organisations



Ensure equal access to collective redress



Support the ESG transition with investment products that truly aim at having an impact

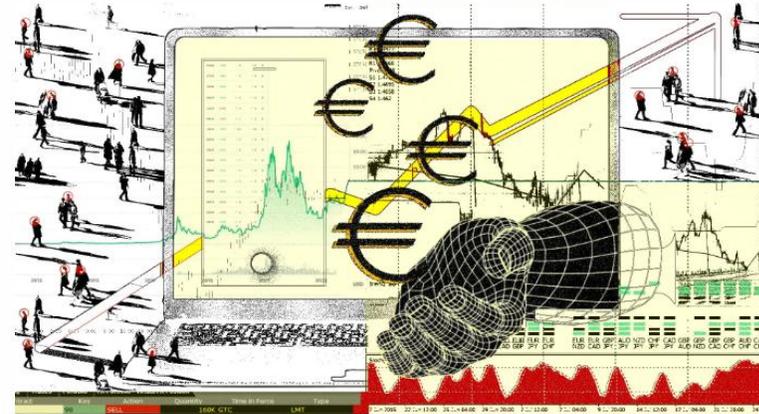


Drive a consumer-centric digital transition

Fraud takes different forms and has been able to **adapt** to evolving legal frameworks by **harnessing** new **technologies** and broadening its scope, techniques and strategies.

[Unchecked Power](#) / [Scam Europe](#)

Investment scammers slip through cracks in EU Big Tech law



International takedown of cryptocurrency fraud network laundering over EUR 700 million

Scam Network Crackdown Takes Aim At Firms Behind Fraudulent Ads

NEWS

Two arrested as authorities in Europe and Israel target companies linked to ad campaigns for fake online investment platforms.

Key figures | Scams are systemic, not marginal

56%

of Europeans adults faced a scam/fraud attempt and

39%

experienced "Monetary Fraud"

Source: EC Consumer Barometer of 2020

Over **€20bn** lost in scams

€4.2bn

alone were loss in "payment fraud" in the EEA — **43%** in cross-border credit transfer fraud

Source: ECB/EBA 2025

But it's merely the tip of the iceberg, as it leaves out:

- Non-transactional scams (e.g., pyramid schemes, land banking)
- Misrepresented investments (e.g., rare assets)
- Crypto scams outside traditional systems, and some recovery room fraud. (e.g. €700 m Europe seizing of money laundering of investment scams)

➤ **Need to Focus on investment scams:** the second most common defrauded credit-transfer type, but cause the highest average losses, making them a critical risk for the SIU.

Example: by Q2 2025 Belgium counts **1,289 cases of investment fraud** (reported), with €15M in losses — with an average loss per victim of €37k (users' complaint; likely under-reported)

Authorised-firm: fraud or misconduct

Typically: Mis-selling cases, misconduct or breach of duty by *licensed* firms (investment firms, banks, insurers, fund managers). Yet consumers are protected by:

- Conduct supervision & enforcement (NCAs, ESMA/EBA/EIOPA), civil liability/redress,
- Investor and deposit-guarantee schemes (if accredited firm), Ombudsman.

Core Focus: The Growing sophistication in the fraud landscape led to the surge of..

...scams by unaccredited actors :

Scams take many forms and may lead either to **unauthorised payment transactions** (e.g., through credential compromise) or to **authorised transactions** where the payer is deceived into initiating the payment.

Investment scams = *Provision of investment services by an unauthorised actor, operating outside the financial regulatory perimeter.*

The counterparty behind the offer is thus unregulated, victims can therefore only rely on:

- payment-chain rules (PSD2-3/PSR, APP-fraud liability),
- platforms and ad-tech duties (e.g. DSA),
- Criminal enforcement & complex cross-border cooperation.

Some of the **novelties** include:

- Increasingly **hybrid**: scams **start on platforms**, executed through payments, passing through crypto/CASPs, and often **ending in untraceable jurisdictions**
- The **post-covid retail investment surge** resulted in an unprecedented **prominence of online investment scams**.

The latest trends – Authorised Push Payment Based (APP)

- **Authorised Push Payment (APP) fraud initiated by clients** is growing in sophistication due to improvement in social engineering techniques.
Ex: Banking & Payments Federation Ireland (BPMFI) show a **42.5% increase in volume** and an **82.2% increase in total losses** compared to 2022.
- The Bank of Ireland reported a 28.8% increase in card payments since 2023, with **card fraud** rising another 8.2% in the same timeframe, rising to **95% of the total volume of fraudulent transactions**.
- Similar trends are visible in EU-wide data (in the graphs below), with fraud volume increasing at a higher pace than value loss per transaction

Chart 1 - Volume and value of SCT instant in % of SCT transactions

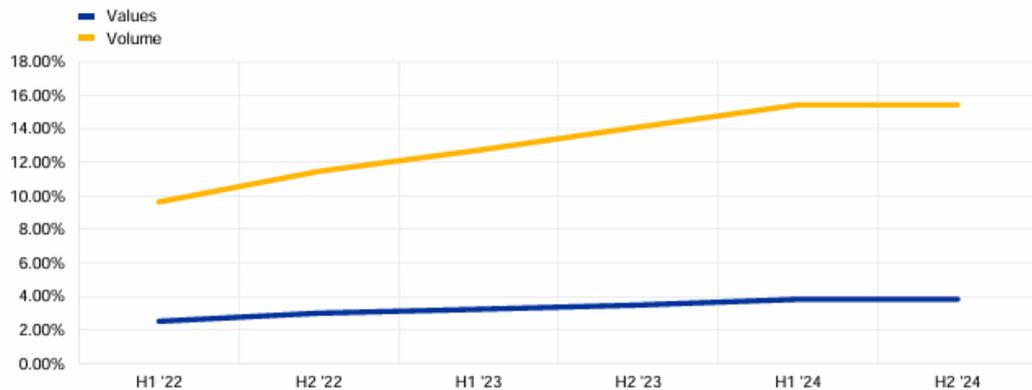
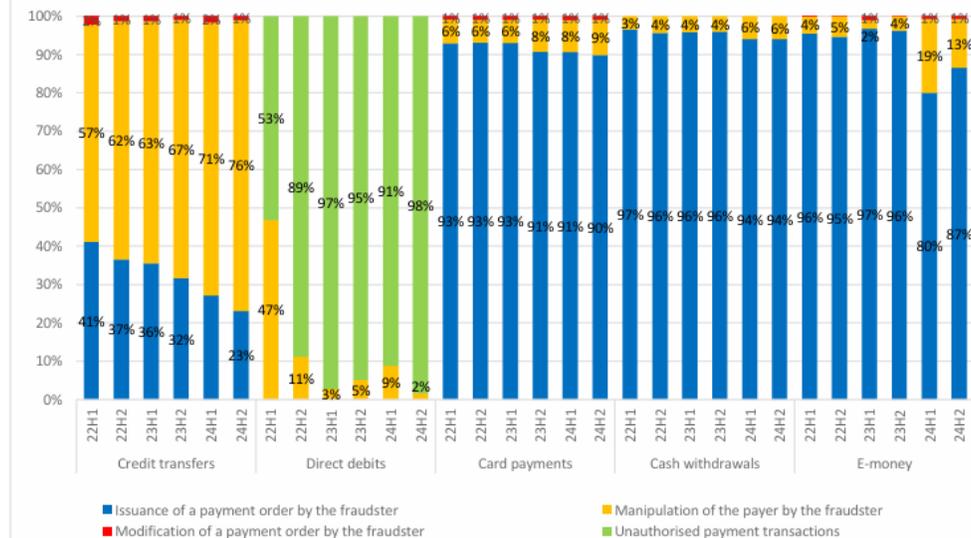


Chart 5: Composition of the value of fraud by main types of fraud
(value of fraudulent transactions by main fraud type in % of the total value of corresponding fraud)

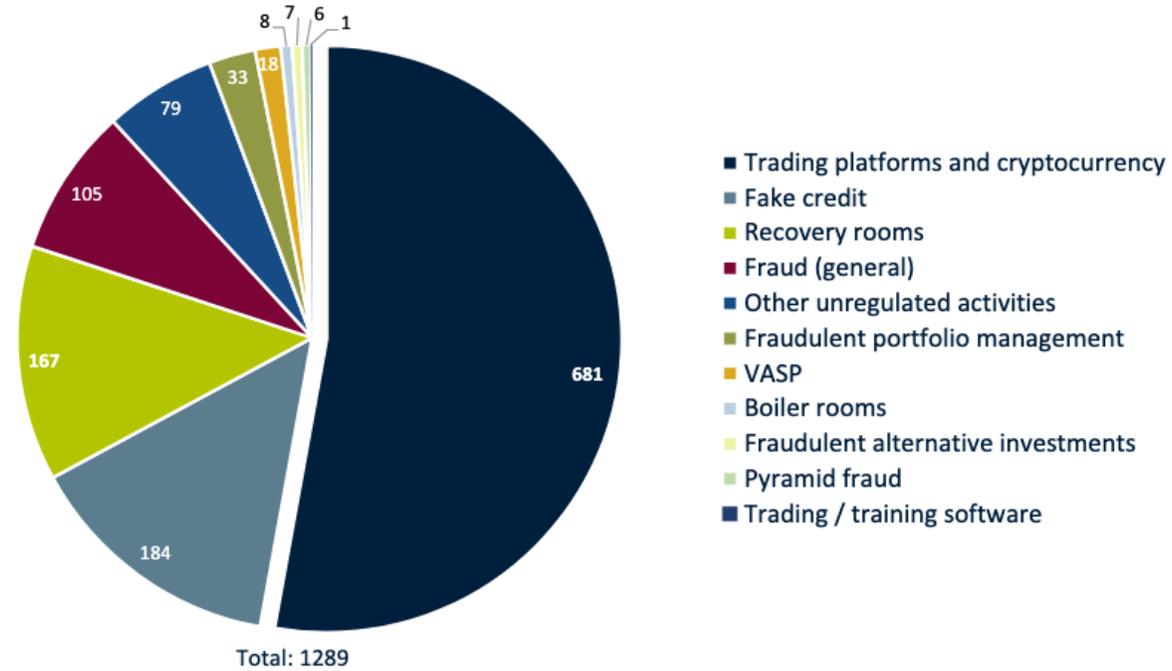


A snapshot from Belgium

FSMA **Unlawful offers: statistics for the first half of 2025**

1. Evolution of the forms of fraud: main trends

Unlawful offers: statistics for the first half of 2025 (number of reports received by the FSMA)*



Belgium H1 2025: €15M fraud losses
 €12M (80%) from fake crypto trading platforms
 €1.2M from fraud 'recovery scams'

Pervasiveness of Investment Scams via fraudulent trading platforms.

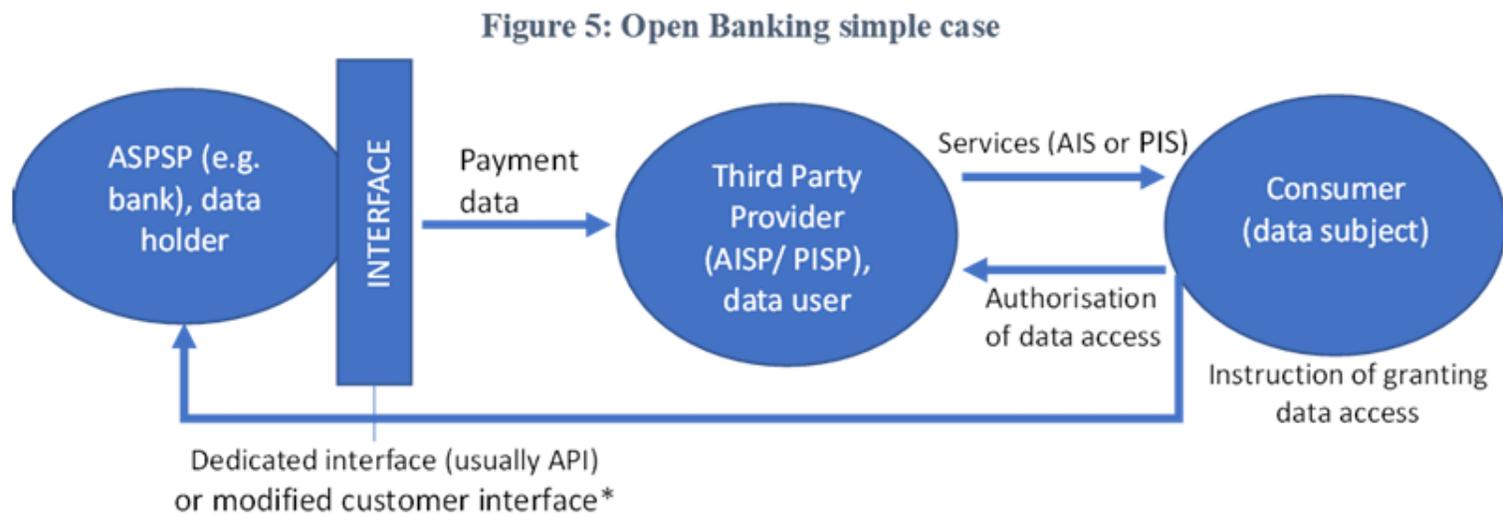
Discrepancies in data are **vast** and so is the amount and quality of information provided by NCAs in the EU. Consequently, EU-wide reports jointly issued by the EBA and the ECB offer **patchy data**.

A question necessarily arises, **how so?**

The answer bears different layers, in brief:

- Fast-paced technological updates allow **scammers** to offer fraudsters **evolving weapons** to **circumvent** existing legislation and **adapt** to new trends.
- **Legislation** has **large margins of improvement** at the European level and is **not harmonized** at the national level, resulting in PSPs limited data-sharing with banks and, consequently, with MS. This results in NCAs having access to different datasets and some of them only receiving partial information, thus the lack of pan-European data and the macroscopic differences depending on the source.
- **Complexity** inherent to Open Banking and Account Information Services **exacerbates** both the previous aspects.

Fuzzy for retail investors, hunting ground for fraudsters



* The modified customer interface is also known as the fallback interface or the contingency mechanism

The overly complicated Open Banking landscape, caused by non-optimal legislation, produces **inefficiencies for users** and makes **information sharing much more difficult**. The EBA has been underlining such issues since 2022-2023, when the revision of the PSD3/PSR started being drafted.

Mirror Trade WhatsApp Scam (BaFin Warning)

- Fraudsters pose as "B2 Akademie" on WhatsApp, **impersonating a licensed firms** (identity fraud)
- They lure investors with free stock tips => pressure to join trading platforms (mirrortrade.top)
- Trust is built over weeks => pitch "crypto tokens" or "high-return investments"
- Initial small withdrawals allow to build credibility
- Then impossible withdrawal conditions are applied, and larger deposits are demanded via crypto/foreign accounts

**Not authorised
by BaFin**

Quantum Banc Identity Fraud (BaFin Warning)

- Website quantum-banc(.)world fraudulently claims to be "Quantum Banc UK"
- Falsely uses FCA registration number assigned to Saxo Capital Markets UK Ltd (no connection)
- Offers unauthorised financial, investment and crypto services

**Not authorised
by BaFin**

Retail investors across Europe are increasingly targeted by fraudulent tactics

Fraud **exploits the digital transformation** of financial services. Social media advertising & search engines activity connect users and scammers, with the latter leveraging AI and any other tool that can help them **deceive and manipulate** the former. Domain names, keywords, aggressive marketing, all aspects that can be part of a strategy aimed at reeling retail investors into a scam.

Fake Trading Platforms ("Fake-Tech"). Unregulated platforms promoting "high-risk products" (e.g., Forex, derivatives) – passing appropriateness assessments.

Misleading Copy Trading. Targets retail investors via fake crypto ("shitcoins"), pump-and-dump schemes, Rug pull, churning, etc..

Social Engineering & Phishing. Fake ads or emails designed to steal personal, financial, or asset-related information.

'Communities' Schemes/Messaging. Facilitate pump-and-dump, Ponzi schemes, and misleading webinars to manipulate asset prices and exploit investors.

Clone Firms & Impersonation. Rising misuse of reputable financial institutions' names, posing significant reputational risks.

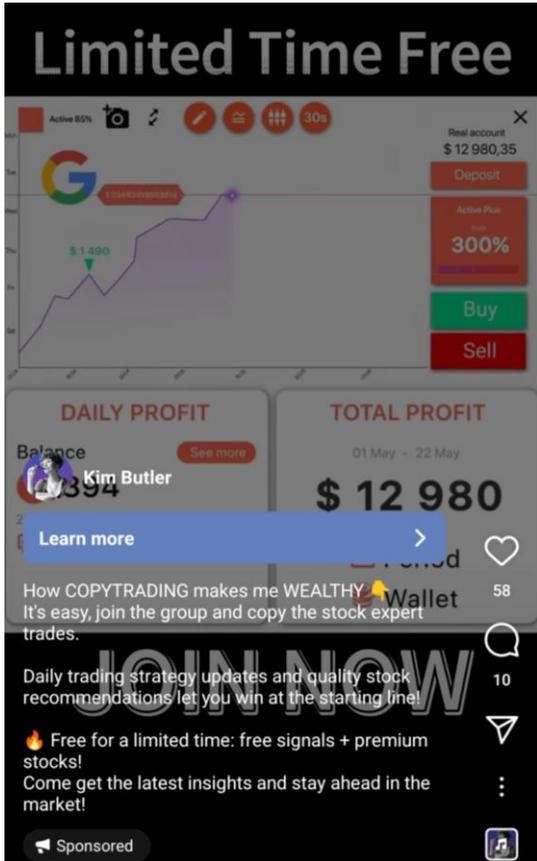
Cryptocurrency Fraud. Dominates EU fraud reports, leveraging AI-driven trading claims or disguised Forex strategies, with millions lost annually (Europol/IOCTA).

Recovery Scams. Fraudsters impersonate authorities or lawyers, falsely offering to recover lost funds for victims.

Celebrity or influencers/endowment scams

➤ Concentration of EU scam-related user search activity (first half of 2024): 86% in Germany, France, Poland, Italy, and the Netherlands (cf. *BrokerChooser*).

The central role of BigTech and Social Media (search and ads)

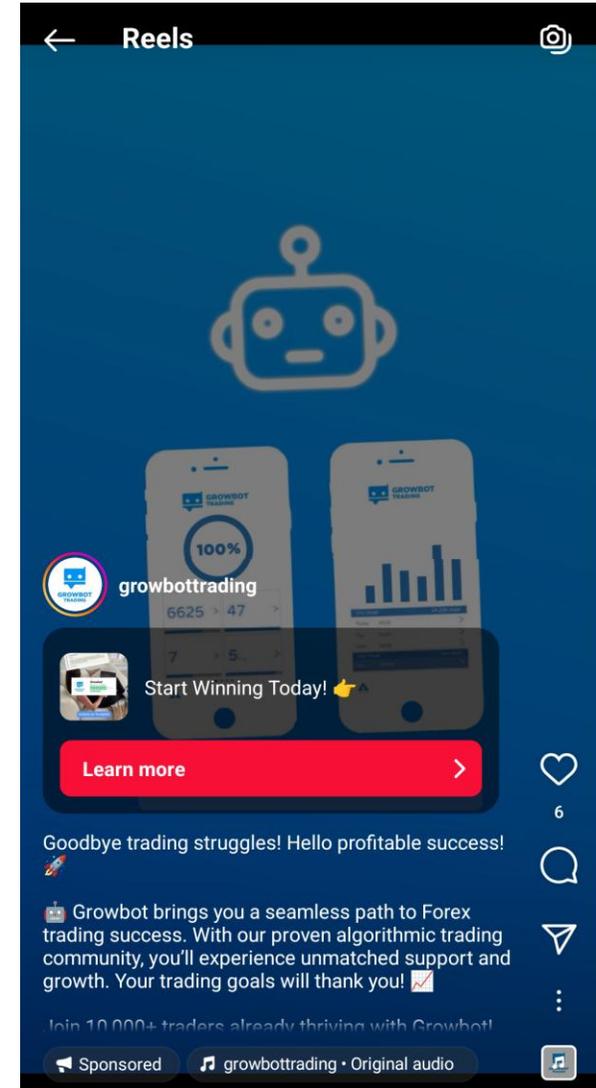


Exploitation of Digital Platforms
Scammers leverage social media ads/impression, posts (sometimes via non-diligent 'FinFluencers,') and search engines to amplify deceptive ads and schemes, targeting retail investors.

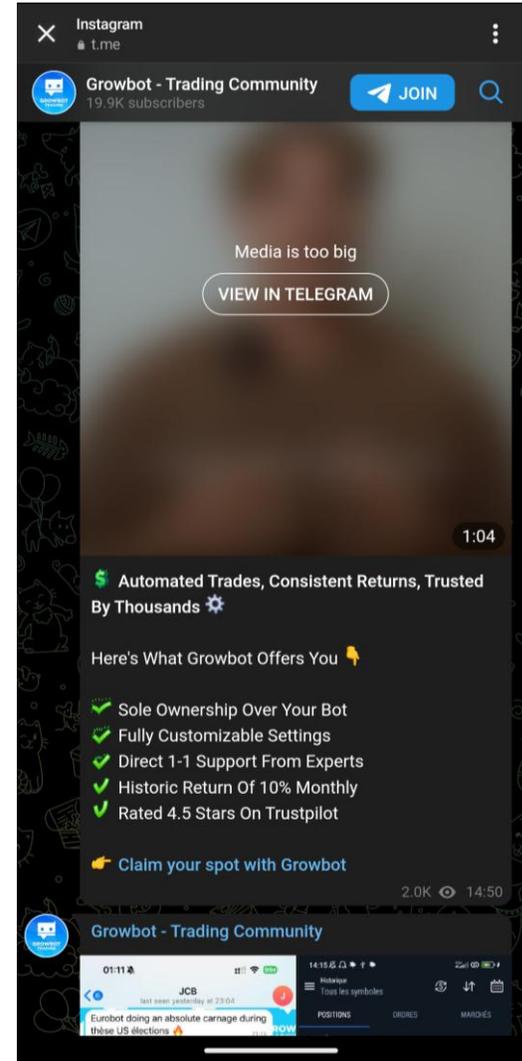
High Search Visibility
Fraudulent entities generated *1.3M Google search impressions targeting EU citizens (BrokerChooser).*

Social Media Profiling
Increased use of social platforms and ads by fraudsters highlights the need for data on impressions to ascertain ad activity from regulated vs. unregulated firms.

Emotional Manipulation
Fraudsters exploit emotional triggers like FOMO and unrealistic return promises to lure victims into "get-rich-quick" schemes.



Examples of scam-like advertisements channels



Scams are an encompassing threat to trust in capital markets

Trust and confidence are necessary for capital markets to thrive, and by **taking advantage** of them scammers are making damage to a degree that is hard to quantify. The metaphor of **cat and mice** encapsulates the dynamic whereby national and European enforcement authorities and lawmakers are trying to take down scammers that operate **transnationally** with seamless ease and that can afford to **target all demographics** with different means and strategies.

Some considerations on the **victims** and on the **legal backdrop** are required to understand how to **tackle the issue**

➡ The victim's perspective

The **demographics** of scam victims are extremely **wide**: they span **across** different **ages**, levels of **education** and more. The same can be said about the reaction to scam: some individuals **divest**, some others become more **risk tolerant** (in search for casino-like gains to make up for the loss), some others turn to **expensive financial advice** or reliable **low-yield investments** and others even **fail to divest** their frauded funds. Responses are very often **irrational** and triggered by victimisation, that does nothing but harm.

Against this, **financial literacy** can be a **curbing** factor, but consumers should not really be the policy focus, as they only represent part of the problem and should not be blamed for other factors like the lack of transparency throughout the investment journey

- Policy-makers should strike a balance between trying to make citizens more aware of the investment landscape and making the landscape itself more transparent, so as to not provoke an instinctive loss of trust.

Current practice:

- **UK [Ad Approval] - FCA collaboration with Google, Meta, Microsoft Bing, and X to allow only:**
 - FCA-authorized firms to advertise financial services online.
 - Functions as a de facto "pre-approval" mechanism for financial advertisements.
 - FCA mandates rigorous processes and risk warnings, especially for crypto and Forex ads.

- **Italy [Search/Indexing] – Consob actions to prevent fraudulent platforms and ensures rapid search engine removals.**
 - **Italian FinTech Decree** (*Digital Issuance and Circulation Register*): Provides Consob enforcement powers, including warnings, blackouts, and sanctions.
 - **Google Collaboration:** Requires advertisers to declare Consob authorisation and facilitates fast removal of unauthorized activity.

- Towards an EU Framework (PSR & DSA)?

The vulnerabilities of payment systems

While scammers operate smoothly between national borders, enforcement authorities are forced to navigate a **complex transnational legislations**, ensuring **privacy provisions** put in place by the GDPR are respected.

PSPs benefit from instant payments, but the quick execution does **not** give them enough **time** to run the appropriate **fraud detention** and **prevention** activities.

Currently PSPs work in silos with **marginal disclosures**, communicating through **different jargons** and referring to **different taxonomies**. National and international authorities must comply with **fragmented regulations** while gathering intelligence, which adds to the problem.

The PSD2 is outdated and despite its relative success thanks to the implementation of SCA, it still falls short when faced with today's challenges. It leaves PSPs **too much discretion** and too **few obligations** and it does **not protect vulnerable individuals** from the fraud threat.

A shift in focus is needed, and new legislation must take into account the multilayered and cross-border complications of fraud

- From a standing start, SEPA instant credit transfers have gone from 0 per cent of all conventional SEPA credit transfers (SCT) in 2018 to about 14 per cent in Q1 2023.

What agenda?

RIS/SIU does not address scams (only elements on financial literacy or influencers rules)

Warning lists (ESMA/NCAs/IOSCO) are not operationalised; uptake by search engines remains voluntary.

Investor Journey: digital engagement rules may help, but impact on scam resilience unclear; a consumer-centric approach, the way-forward to combat fraudulent offers?

EU policy discussions acknowledge fraud only indirectly (literacy, influencers, DSA enforcement).

AML/KYC: Tackling at the inception of the payment or onboarding process; a circuit breaker?

AI Act: not consumer-oriented, rely on the duties on high-risk systems, ex-post risk management by providers leaves consumers exposed during the first—and most harmful—wave of misuse.

MiCA: captures crypto-asset issuers/exchanges, but scam tokens & off-platform promotions remain untouched. Divergent national enforcement leads to uneven consumer exposure.

Enforcement varies heavily across Member States; NCAs seldom cooperate on scam typologies.

DSA: a step, but significant loopholes remain – as currently:

- Platforms can retain “safe harbour” despite enabling systematic deceptive ads.
- Illegal ads persist and up to 10% of platform ad revenue reportedly linked to fraudulent financial content.

PSD2: Mainly bolstered protection against unauthorised transactions via SCA, while liability may still shift to consumers in cases of fraud or gross negligence (notably problematic as many scams involve authorised payments). PSD2 also did not mandate IBAN/name verification, leaving misdirected transfers without an EU-wide preventive check.

Key shifts expected with IPR & PSD3/PSR



Mandatory reimbursements in cases of impersonation (unless customer gross negligence is proven).



Stronger duties on PSPs to **detect, block, and refund** certain APP scams. “**Gross negligence**” refusals are more limited, and reimbursement is subject to **set timelines (10 business days)**



Supervisory **convergence**; **harmonised** EU-level fraud reporting (EBA); **balanced** security standards.



Instant Payments Regulation **mandates VoP (IBAN–name check)**; PSD3/PSR add broader risk-based monitoring and fraud data-sharing measures



Positions payments as the **first** point of **intervention** in the scam cycle.



Clarifies allocation of liability between sending and receiving PSPs, supporting *systemic responsibility*. Online platforms accountability is introduced (social media, search engine), strengthening liability chain of actors without excessive burden of proof on clients.

Online platforms are often used as hunting ground by scammers

Stronger **obligations** on search engines and social media:

- Removing illegal content; assessing systemic risks; providing algorithmic transparency.

...despite

Persistent **limitations**:

- Paid scam ads still circulate despite “know-your-business-customer” requirements.
- No hard obligation to pre-screen financial promotions or integrate NCA warning lists.

Organic Content & Finfluencers

- Scams increasingly rely on non-paid channels!
- Fraudulent “success stories”, trading groups (whatsapp), unverified testimonials.
- Finfluencers often lack licensing: de facto investment promotion outside MiFID

1. Prevent :

- Mandatory pre-screening of financial ads by platforms/search engines.
- Integration of regulator warning lists into search results “by default” (automated ingestion).
- Algorithmic downranking of high-risk content; mandatory scam-risk indicators.
- Stronger oversight of influencers: transparency, remuneration disclosure, anti-inducement rules.
- Investor Awareness and Education
- Effective early-fraud payment prevention

2. Protect

- Shared EU database of fraudulent IBANs, wallets, domains, ads with mandatory reporting by PSPs/platforms.
- Strengthened cooperation between NCAs, EBA, ESMA, Europol.

3. Repair

- PSR/PSD3 reimbursement logic is important, when platform or PSP fails to prevent foreseeable harm or are impersonated. Gross must remain narrow; the bank or PSP should act on behalf of client.
- Liability for platforms benefiting from fraudulent ads or failing to take reasonable preventive steps.
- Clear, EU-wide dispute mechanism (ADR/ODR).

- Scam activity is, cross-border, and digitally amplified.

Retail investors remain structurally exposed because the EU's prevention, liability, and repair tools are fragmented.

A coherent framework is essential to:

- **Restore trust & Strengthen market participation**
- **Protect household financial resilience**

Key Outcomes to achieve: Prevention first, protection always, reparation guaranteed.

- ECB, EBA, *ECB and EBA Report on Payment Fraud 2025* (2025), <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf>.
- Europol, "Fraud against Payment Systems," Europol, accessed December 23, 2025, <https://www.europol.europa.eu/crime-areas/online-fraud-schemes/fraud-against-payment-systems>.
- Nat Shum, "Authorised Push Payments Fraud – Theorising a Loss Allocation Model," *UCL Journal of Law and Jurisprudence* 14, no. 1 (2025): 1988, <https://doi.org/10.14324/111.444.2052-1871.1988>.
- European Commission, "Impact Assessment Report SWD(2023) 231 Final," European Commission, June 28, 2023, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2023:0231:FIN:EN:PDF>.
- "FraudSMART Payment Fraud Report 2023," *Banking & Payments Federation Ireland*, n.d., accessed December 23, 2025, <https://bpfi.ie/publications/fraudsmart-payment-fraud-report-2023/>.
- Lynn A. Stout, *The Investor Confidence Game*, 68, no. 2 (2002): 407–37.
- Umit G. Gurun et al., "Trust Busting: The Effect of Fraud on Investor Behavior," *The Review of Financial Studies* 31, no. 4 (2018): 1341–76.
- Rich Lewis et al., *Consumer Decision-Making in Retail Investment Services: A Behavioural Economics Perspective*, n.d.
- Jeremy Burke et al., *Can Educational Interventions Reduce Susceptibility to Financial Fraud?*, n.d.
- AlInvest, "The Growing Risk of Financial Fraud and Its Impact on Investor Behavior and Asset Allocation," AlInvest, accessed February 10, 2026, <https://www.ainvest.com/news/growing-risk-financial-fraud-impact-investor-behavior-asset-allocation-2509/>.

- Johannes Hagen and Amedeus Malisa, "Financial Fraud and Individual Investment Behavior," *Journal of Economic Behavior & Organization* 203 (November 2022): 593–626, <https://doi.org/10.1016/j.jebo.2022.09.015>.
- Nanne Johanna Taavitsainen, *Trust to Exploitation: The Legal and Societal Implications of Payment Fraud and the Path Toward Stronger Protections*, n.d.
- Mark Button et al., "Fear of Fraud amongst Older Adults: A Hidden Epidemic?," *Security Journal* 38, no. 1 (2025): 44, <https://doi.org/10.1057/s41284-025-00485-1>.
- Steven James Lee, "Does Fixed Income Buffer against Fraud Shocks?," *Journal of Risk and Financial Management* 14, no. 10 (2021): 479, <https://doi.org/10.3390/jrfm14100479>.
- "Tightening the Reins on Payment Fraud: How the EU's New Regulations Aim to Protect Consumers," News Item, Faculteit Rechtsgeleerdheid En Criminologische Wetenschappen, accessed July 29, 2025, https://www.law.kuleuven.be/ccm/blog/posts/payment_fraud_regulation.
- Annick Moes and Meral Ruesing, "A Pan-European Fraud Taxonomy : Do You Speak Fraud?," *Journal of Payments Strategy & Systems* 18, no. 1 (2024): 61, <https://doi.org/10.69554/XOFK3234>.



BF BETTER FINANCE

The European Federation of Investors and Financial Services Users
Fédération Européenne des Épargnants et Usagers des Services Financiers

@ policy@betterfinance.eu

 betterfiance.eu

