Crypto & TradFi

Special feature on investor protection: crypto scams and operational vigilance

Unravelling the regulations for investors

Following the MiCA grandfathering clause: practical steps to take in the face of crypto scams

Previous editions of the Regulatory Brief have outlined the European regulatory framework in successive layers: the AI Act and its Omnibus (Seqlense Regulatory Brief Issue #7), its relationship with the GDPR (Issue #8), the post-quantum transition (Issue #9), technological sovereignty (Issue #10), the convergence of AI and cybersecurity (Issue #11), dual supervision of market abuse and AML/CFT (Issue #12), the end of the MiCA grandfathering clause (Issue #13), heightened vigilance regarding market abuse (Issue #14), the global regulatory acceleration of AI (Issue #15) and the European Parliament's vote on dollar-pegged stablecoins (Issue #16). This seventeenth edition draws out the most concrete practical implications for savers: the end of the MiCA grandfathering clause on 1 July 2026 now places the protection of retail investors at the heart of the European framework, and the French authorities, in particular the AMF, are supporting this with a renewed educational initiative.

On 27 July 2026, the AMF updated the homepage of its educational section on crypto-assets, with a structure organised around six key areas: investing in Bitcoin (caution), choosing a professional, practical precautions, watching out for scams, participating in a public offering of crypto-assets, and investing in a crypto treasury company. This framework complements the resources dedicated to protecting victims of scams (how to file a complaint) and verification tools: whitelists (authorised PSCA entities), blacklists, ESMA and Regafi. The last major thematic update to the scams section dates from 30 June 2025. Taken together, these resources now form a comprehensive decision-support framework for retail investors in a crypto market which, with the expiry of the MiCA grandfathering clause, no longer relies on residual national regimes but on a harmonised European framework.

The context of this edition is particularly significant. According to the AMF Barometer of June 2026 (see Edition #11), 33 per cent of French investors in crypto-assets reported using AI as a source of information prior to making an investment; the profiles most exposed to risk are thus the very same ones that most frequently rely on tools of varying reliability. At the same time, the AMF, the AFM and the ESAs have been warning since June 2026 about the industrial-scale proliferation of malicious campaigns accelerated by AI (see Issue #11), and in July 2026 the ESRB classified the cyber risk associated with cutting-edge AI models as 'severe' (see Issue #15). The interconnection between investor protection, the regulation of investment firms and cyber governance has never been so close.

For retail investors and the regulated entities that serve them, such as investment firms, investment advisors, distributors and trading platforms, this edition offers an operational overview based on the AMF's educational resources, which were updated this week.

The main signal

With the end of the MiCA grandfathering clause and thus the transition period, investor protection has become the regulator's operational focus: the 'whitelist' is no longer a mere convenience, but the gateway to the European crypto market.

The most fundamental element of the AMF framework, updated on 27 July 2026, lies in a simple yet often misunderstood operational distinction. An investor wishing to buy, sell or have crypto-assets held in custody must use a service provider featured on the white list of authorised crypto-asset service providers (PSCAs). This list is public, accessible and legally binding. This 'white list first' approach replaces the former fragmented system of national regimes, under which an investor could legitimately use providers with various legal statuses. Since 1 July 2026, the rule has been harmonised across Europe: this is the gateway to the market.

A direct consequence of this is that the blacklist published by both the AMF and ESMA is a useful tool, but an insufficient one. It lists operators identified as unauthorised or fraudulent, but by its very nature it is not exhaustive: a service provider not included on this list is not necessarily trustworthy. The only robust approach is therefore to check whether a provider appears on the PSCA whitelist, supplemented by the Regafi register for CFDs on crypto-assets and by the ESMA register of white papers for the crypto-assets themselves. This hierarchy of checks now underpins every investment decision involving crypto-assets, and regulated providers who can present it clearly to their clients gain a competitive advantage.

Focus 1 - The verification process: four registers to be aware of

The first component of the AMF's framework is a verification system structured around four complementary registers, which every retail investor would do well to be familiar with and use systematically.

• The **AMF-authorised PSCA whitelist**: lists crypto-asset service providers authorised under MiCA in France. It also includes operators authorised in another Member State who, through a European passport, may provide their services in France. This register is the benchmark for any custody service, or the buying/selling of crypto-assets for legal tender, or the exchange of crypto-assets.

• The **ESMA white paper register**: to be admitted to a trading platform, a crypto-asset must have been the subject of a white paper detailing the project and the associated risks. The AMF or the ACPR is notified but does not approve the white paper: the person applying for admission remains solely responsible for its content. The register is maintained by ESMA at European level.

• The **Regafi register**: used to verify the authorisation of an investment services provider (ISP) offering CFDs (contracts for difference) on crypto-assets. A useful reminder: since 1 August 2018, the marketing of CFDs on crypto-assets to retail investors has been limited to a leverage of 2.

• The **AMF and ESMA blacklists**: these list operators identified as unauthorised or flagged. They are useful for immediately disqualifying a counterparty, but are by their very nature not exhaustive. The AMF points out: "an institution or platform that does not appear on these lists is not necessarily reliable for that reason alone". Verification must be carried out first and foremost via the whitelist.

Key points to watch

- Changes to the **ESMA register of authorised CAPSs** as authorisations are granted across all 27 Member States following the expiry of the grandfathering clause.
- • The **upcoming AMF awareness campaigns** and their alignment with the European Banking Authority's (EBA) factsheet on crypto scams published in January 2026.
- • The**possible emergence of aggregated lists at European level** to facilitate cross-border verification for retail investors.

Focus 2 - Anatomy of crypto scams: the typologies documented by the AMF

The second part of the updated AMF guidance is a detailed typology of scam scenarios, illustrated by several accounts received by AMF Épargne Info Service. This typology is useful because it documents the techniques observed and enables investors to recognise a pattern or modus operandi before it takes hold.

The first scenario involves a well-rehearsed pitch. Fraudsters contact their targets by email, telephone, social media or instant messaging, often after the target has provided their contact details via an online form (see the AMF warning of November 2024 on forms, social media and dating sites). They build a sense of trust, mobilise a network of fake ‘industry professionals’ and dangle the prospect of attractive returns. The victim is encouraged to make an initial small investment; a first withdrawal of the so-called profits is granted, a crucial step in turning mistrust into trust. The victim then invests larger sums, which will never be recovered. The scammers become unreachable or cite technical problems, hold-ups or the payment of fake taxes as excuses.

Three key variants complement this core scheme. The refund scam (a scam within a scam): once they realise they have been exposed, the fraudsters orchestrate a second scam involving someone posing as a lawyer, banker or authority figure, who contacts the victim and promises to recover their funds in exchange for a further payment. The romance scam: fraudsters use dating apps, social media or private messaging services to build a seemingly genuine relationship (‘romantic relationship’, ‘friendship’, ‘concern for the victim’s personal situation’), before steering the victim towards a fraudulent investment scheme. Impersonation: fake websites, fake social media accounts and articles use the image of public figures, newspapers or news channels. Fake paid online courses have also been identified as a means of directing people towards fraudulent platforms.

The three case studies published by the AMF illustrate the scale of the individual losses. Mr C. invested €1,000 and avoided losing a further €50,000 thanks to his scepticism regarding the promise of a miracle profit. Ms A. paid a total of €53,000 before her contacts stopped responding. Mr V. invested €70,000 and was then asked to pay fictitious ‘taxes’ in order to recover his funds. The common thread running through these three cases is that there were no obvious warning signs at the initial point of contact, the pressure was gradually ramped up, and the victims realised what was happening too late. The AMF reiterates a simple yet robust warning sign: guaranteed high returns of more than 2-3 per cent simply do not exist.

Key points to watch

• The evolution of **social engineering campaigns amplified by AI** (deepfakes, personalised chatbots), following on from the ESRB’s July 2026 assessment (see Issue #15) and the AMF/AFM alerts from spring 2026.

• The **new channels identified by AMF Épargne Info Service** through user reports, which are likely to inform future AMF warnings.

• The **international coordination of blacklists** (AMF, ESMA, EBA, counterpart authorities) to tackle the cross-border nature of fraudulent campaigns.

Focus 3 - Technical precautions: beyond the choice of service provider

The third aspect of the AMF's guidance concerns the technical precautions specific to investing in crypto-assets, which are distinct from those relating to the choice of counterparty. Price volatility and the risk of scams are the first to be mentioned, but the AMF's guidance emphasises that investing in crypto-assets also entails specific IT and technical risks that do not exist, or exist in a different form, when investing in traditional financial instruments.

This section is structured around three categories of precautions. Security of custody: crypto-assets may be held on a platform (in which case security depends on the service provider's IT systems), in a hot wallet (connected to the internet), or in a cold wallet (offline). Responsibility for managing private keys and recovery phrases is a critical factor which, ultimately, rests with the holder in the case of self-hosted wallets. Any loss or compromise of these elements carries a risk of irreversible loss of assets. Protection against phishing and social engineering: systematically verifying URLs, being wary of unsolicited communications, and using multi-factor authentication on platform accounts. And understanding the nature of the services used: buying and selling, custody, staking, lending; each involves a different risk, different regulation and different exposure.

An important point to bear in mind concerns deposit protection. Unlike traditional financial instruments, crypto-assets are not covered by the Deposit Guarantee and Resolution Fund (FGDR), even when held with a PSCA authorised by the AMF. Crypto-assets are covered neither by the FGDR's deposit guarantee nor by its securities guarantee; MiCA obligations do not constitute a compensation mechanism. In the event of the insolvency of an authorised platform, protection depends on the provider's internal asset segregation arrangements and its own guarantees, as well as the applicable MiCA framework. This structural difference from traditional financial instruments must be understood and factored into investment decisions.

Key points to watch

• Future **guidance from ESMA and the EBA on asset segregation and the custody of crypto-assets** by crypto-asset service providers (PSCAs), in line with MiCA.

• The **additional measures proposed by certain service providers** (private insurance, contractual guarantees) to compensate for the lack of FGDR cover; their legal and operational soundness warrants careful scrutiny.

• The **roll-out of tools simplifying the secure management of portfolios** for retail investors (cold wallets for the general public, assisted management of recovery phrases).

Focus 4 - In the event of doubt or a dispute: remedies and points of contact

The fourth part of the AMF's guidance concerns remedies and points of contact in the event of doubt, a dispute or proven loss. The fundamental distinction, which is often overlooked, lies in whether the platform in question is authorised or not, and this directly determines the available avenues of redress.

• For **any questions or preliminary queries**, the first point of contact is **the AMF Épargne Info Service (telephone: 01 53 45 62 00)** or its online contact form. An additional service, **the Assurance Banque Épargne Info Service (34 14), can also be contacted for matters falling within the remit of** several authorities.

• In the event of a **dispute with a platform authorised in France**, the **AMF mediator** may intervene to attempt an amicable resolution. This is a free, independent and confidential process.

• In the event of a dispute with a **platform authorised in another European Union Member State**, the platform's terms and conditions set out the dispute resolution procedure and the competent supervisory authority.

• In the event of a dispute with an **illegal (unauthorised) platform**, the only recourse is to **file a complaint with the police or the gendarmerie**. The AMF is clear: "in this case, the chances of recovering your money are very slim, as the fraudsters are usually based abroad". This is precisely why carrying out due diligence (Focus 1) is crucial.

A universal precaution: generally speaking, neither the AMF, nor a bank, nor any public authority will contact an investor out of the blue to offer to recover lost funds in return for payment. No legitimate organisation will ask for upfront fees, codes or transfers to 'recover' the funds. Any solicitation of this kind is, by definition, a second scam ('refund scam').

Key points to watch

• The growing coordination between **the AMF Ombudsman, European ombudsmen and ESMA's centralised supervisory role** as the Market Integration and Supervision Package is rolled out (see Issue #10).

• The **consolidated statistics on cases handled by the AMF Ombudsman** relating to crypto-assets, expected in the next annual report.

• The **potential European one-stop shop for retail investors**, as direct European supervision of PSCA providers progresses.

Key takeaways

Five key principles should now be adopted:

• Always **check the PSCA whitelist first**: this list can be regarded as a gateway to the European crypto market. The blacklist is complementary but not exhaustive.

• Treat any guaranteed return exceeding 2-3 per cent as an **almost certain warning sign**, as well as any unsolicited approach presenting an urgent opportunity.

• Remember that **crypto-assets are not covered by the FGDR guarantee**, even on a platform authorised by the AMF; protection depends on the provider's internal arrangements and the MiCA framework.

• If in doubt, **contact the AMF Épargne Info Service (01 53 45 62 00)**; in the event of a dispute with a platform authorised in France, refer the matter to **the AMF ombudsman**; if approached with an offer of 'reimbursement assistance' following a scam, refuse it systematically as it is very likely to be a second scam.

• Take into account the **new risks amplified by AI** (deepfakes, personalised social engineering, identity theft), which were explicitly highlighted by the AMF, the AFM and the ESAs in spring 2026, and described as 'severe' by the ESRB in July 2026.

Conclusion

The expiry of the MiCA grandfathering clause has brought the European crypto-asset market under a unified regulatory framework. For retail investors, this means that protection now relies primarily on two operational mechanisms: the prior verification of service providers (first via the PSCA whitelist, then via supplementary registers) and the recognition of the types of scams documented by the AMF. In addition to these two mechanisms, investors should be aware of the available redress options (Épargne Info Service, the AMF ombudsman, and filing a complaint) and take the technical precautions specific to crypto-assets, notably the lack of FGDR cover. This edition does not introduce any new regulatory requirements; it reiterates and outlines essential public resources at a time when the growing sophistication of malicious campaigns, amplified by AI, makes managing them more critical than ever. For authorised PSCA firms, this presents an opportunity: investing in education and the clarity of client information is not merely a MiCA requirement; it is a key differentiator against fraudulent operators. For investors, there is a simple rule: if in doubt, contacting the AMF is quicker and less costly than acting without verifying the facts.

Main sources

- AMF, *« Investir dans les crypto-actifs (bitcoin, etc.) »*, page d'entrée de l'espace pédagogique consacré aux crypto-actifs, actualisée le 27 juillet 2026 (amf-france.org).
- AMF, *« Crypto-monnaies (bitcoin, etc.) : attention aux arnaques ! »*, article pédagogique, dernière mise à jour thématique du 30 juin 2025.
- AMF, *« Investir en crypto-actifs : quel professionnel choisir ? »*, article de doctrine pédagogique sur le choix des PSCA.
- AMF, *« Investir en crypto-actifs : les précautions pratiques »* et *« Investir dans le bitcoin : prudence ! »*, articles pédagogiques complémentaires.
- AMF, *« Faire les vérifications »*, page transversale sur les registres de vérification utilisables par les investisseurs.
- AMF, *Listes blanches (PSCA, PSFP, biens divers)* et *listes noires et mises en garde* (amf-france.org).
- ESMA, *Registre européen des livres blancs sous MiCA* et *liste des acteurs signalés / non autorisés* (esma.europa.eu).
- ACPR, *Regafi* — registre des agents financiers, utilisé notamment pour vérifier les PSI proposant des CFD sur crypto-actifs.
- EBA, *Fiche pratique des autorités européennes sur les arnaques liées aux crypto-actifs*, version française publiée en janvier 2026 (eba.europa.eu).
- Règlement (UE) 2023/1114 (MiCA) — cadre européen des crypto-actifs ; règles applicables aux PSCA et aux offres au public de crypto-actifs.
- AMF, *Baromètre AMF de l'épargne et de l'investissement 2025 – édition spéciale IA* (Édition #11 du Regulatory Brief).
- AMF, *Épargne Info Service (01 53 45 62 00)* et Assurance Banque Épargne Info Service (34 14), points de contact pour les épargnants.

.***

The Seqlense Regulatory Brief - Crypto & TradFi · Issue #17