



# Newsletter – Financial services

## Fall 2026

*Contrary to FATF standards on beneficial ownership transparency, the United States abolished the federal beneficial ownership register for U.S. entities in August and announced the deletion of previously collected data. FinCEN will instead rely on alternative information-gathering mechanisms. This policy shift may attract FATF scrutiny, as deficiencies in access to accurate, up-to-date beneficial ownership information are a recurring reason for grey-listing.*

*This growing divergence may also complicate beneficial ownership checks by European financial institutions on certain U.S. counterparties.*

*Also in the United States, legislation formally adopted in mid-September<sup>1</sup> authorises tariffs of up to 500% on Russian-origin goods and 100% on imports from certain purchasers of Russian oil. However, national-interest waivers leave the executive branch considerable discretion over implementation.*

*Although the digital euro's legislative framework remains uncertain, the ECB continues to build its operational infrastructure. It has selected 36 PSPs for a pan-European pilot beginning in 2027 and unveiled key features of the digital euro application. The project is thus moving from regulation to operational testing as private tokenisation and euro-denominated stablecoin initiatives accelerate.*

### 1. **Financial Sanctions against Russia**

The EU's 21st sanctions package against Russia and Belarus, adopted on 23 July 2026<sup>2</sup> strengthens restrictions targeting Russia-linked banks, payment networks and crypto-asset service providers. Financial institutions should accordingly reassess their sanctions screening, KYC and sanctions-evasion detection frameworks. On 12 October, two implementing regulations produced the largest expansion to date of the list of sanctioned persons and entities<sup>3</sup>.

EU sanctions are also increasingly addressing digital financial crime. Under its global human rights regime, the EU has targeted private operators involved in organised cybercrime, cryptocurrency fraud and the exploitation of trafficking victims. Its cyber sanctions regime has likewise been extended in response to hybrid threats attributed to certain States.

### 2. **Fight against money laundering (AML/CFT)**

#### 2.1 **European developments**

Beyond the June 2026 update of the FATF Recommendations<sup>4</sup> and the regular updates to the FATF grey list<sup>5</sup> the most significant AML/CFT developments at EU level concern the draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) published by the new European Anti-

---

<sup>1</sup> The Lindsey O. Graham Sanctioning Russia and Iran Act of 2026.

<sup>2</sup> Other than amendments to the EU Regulations targeting Iran.

<sup>3</sup> The first implementing regulation targets individuals and entities providing material support to Russia's war effort, while the second sanctions persons involved in legitimising the annexation and occupation of Ukrainian territories through the organisation and conduct of electoral processes in occupied regions of Ukraine.

<sup>4</sup> The revised FATF Recommendations confirm that certain humanitarian activities may benefit from exemptions to asset-freezing measures and complement the developments introduced in 2025 regarding the risk-based approach and payment transparency.

<sup>5</sup> As of 19 June 2026, Algeria and Namibia were removed from the FATF grey list, while Iraq and Bosnia and Herzegovina were added.



Money Laundering Authority (AMLA), which will become applicable from 10 July 2027. Since our [previous newsletter](#), AMLA has notably published:

- draft RTS on the assessment of the inherent and residual risk profiles of obliged entities in the financial sector (in addition to parallel RTS applicable to non-financial sectors); and
- draft ITS establishing a harmonised European format for suspicious transaction reports (STRs), including the information and supporting documentation to be provided to Financial Intelligence Units.

These draft ITS significantly expand the information expected to accompany suspicious transaction reports when compared with the current French reporting framework applicable to reports submitted to Tracfin. They are closely linked to the enhanced customer due diligence requirements introduced by the Anti-Money Laundering Regulation (AMLR)<sup>6</sup> which are more extensive than those currently applicable under French law. As a result, obliged entities should start reviewing the scope of information collected from customers and identify any gaps between current onboarding practices and the requirements that will apply from 10 July 2027<sup>7</sup>.

It should also be noted that AMLA's draft Guidelines on ongoing monitoring, published earlier this summer, move away from a compliance framework primarily focused on transaction monitoring and periodic reviews. Instead, they promote a dynamic, risk-based approach to monitoring the business relationship as a whole, based on events, behavioural indicators and changes in risk profile. While the new framework introduces a greater degree of proportionality, it also raises expectations regarding the timely identification of material changes affecting customers.

In addition, the EU AML package marks a further step towards harmonising the treatment of cross-border activities. The AMLR is expected to reduce regulatory discrepancies between Member States in areas that have historically been governed by sometimes divergent national AML/CFT rules. Institutions operating in multiple Member States will therefore need to ensure the consistent application of customer due diligence, transaction monitoring and suspicious transaction reporting frameworks across all their European activities.

Following France's proposal to establish a register of fraudulent bank accounts (the FNC-RF), previously discussed in our newsletter, Luxembourg and Spain are also experimenting with secure information-sharing mechanisms relating to fraudulent accounts and fraud typologies. These initiatives reflect a broader European trend towards making anti-fraud data sharing a cornerstone of payment security, in anticipation of the forthcoming PSD3/PSR framework.

In September 2026, the FATF drew attention to the increasing sophistication of informal value transfer systems such as hawala networks. The report highlights that such schemes frequently rely on bank accounts, payment service providers, commercial companies, virtual IBANs and crypto-assets. FATF's analysis shows that the most significant indicator of such networks is no longer the use of cash itself, but rather the combined use of bank accounts, PSPs, corporate structures, vIBANs and crypto-assets in a manner disconnected from the underlying economic reality of the transactions concerned.

## 2.2 National developments

A confidential report issued by the French judicial police and referred to in the press during the summer highlighted the growing interconnection between the criminal economy and the legitimate economy. According to the report, criminal organisations increasingly rely on commercial companies, informal settlement networks, false invoicing schemes, real estate transactions and crypto-assets to disguise illicit activity. For AML/CFT obliged entities, this development underscores the importance of assessing

---

<sup>6</sup> Article 28 of the AML Regulation (AMLR).

<sup>7</sup> For example, the obligation to collect information relating to all nationalities held by a customer.

not only a customer's identity and profile, but also the economic rationale of transactions and the origin of funds, including where transactions are channelled through structures that appear entirely legitimate.

Meanwhile, the publication of the first part of Tracfin's annual report on suspicious transaction reporting and related enforcement activity reveals two noteworthy developments. First, the French Financial Intelligence Unit exercised its blocking power for the first time in order to freeze crypto-assets. Secondly, the number of crypto-related disclosures transmitted to prosecutorial authorities doubled compared with 2024, confirming the growing importance of crypto-assets in both suspicious transaction reporting and law enforcement activity.

### **3. Payment services**

#### **3.1 European developments**

The digital euro project is entering a more operational phase. Following the completion of the preparation phase, the European Central Bank (ECB) has moved to the next stage of the initiative. Large-scale testing could begin as early as 2027, with a potential issuance date from 2029. As part of this process, the ECB has selected its main technology providers, finalised an advanced version of the digital euro rulebook applicable to payment service providers (PSPs) and confirmed a number of key features, including offline payments, conditional payments ("programmable payments") and open standards designed to facilitate integration by PSPs. The ECB has also selected 36 PSPs to participate in beta testing of the digital euro.

In the crypto-asset sector, a position published by the European Securities and Markets Authority (ESMA) earlier this summer was followed by an update to the AMF's supervisory guidance of the *Autorité des marchés financiers* (AMF) at the end of July<sup>8</sup>. The revised position clarifies that a financial investment adviser (*Conseiller en investissements financiers* - CIF) may consider crypto-assets as an asset class when advising on portfolio allocation, provided that the analysis stops short of recommending a specific crypto-asset or crypto-asset service. Accordingly, a CIF may include crypto-assets within a broader wealth diversification strategy, for example through exposure ranges or allocation scenarios, without holding a Crypto-Asset Service Provider (CASP) authorisation, provided that no specific crypto-asset or crypto-asset service is recommended.

In July 2026, the Court of Justice of the European Union (CJEU) confirmed that guarantee mechanisms involving fund transfers only on an ancillary basis do not fall within the scope of payment services regulation. Earlier, in June 2026, the Court was also called upon to clarify the extent of payment service providers' liability for unauthorised transactions where strong customer authentication had not been implemented. Taken together, these developments illustrate the continuing evolution of EU case law regarding both the scope of payments regulation and the level of protection afforded to users against insolvency and fraud-related risks.

#### **3.2 National developments**

The rollout of Click to Pay, a payment solution enabling consumers to complete online purchases without manually entering their card details, could become a commercial reality by the end of 2026, subject to approval under France's domestic CB card scheme<sup>9</sup>. Payment service providers (PSPs) are already updating their terms and conditions to reflect this new functionality, which is expected to significantly streamline the online payment experience.

---

<sup>8</sup> These developments come shortly after the full application of the European MiCA regime and the expiry of the transitional period available to market participants.

<sup>9</sup> Groupement Cartes Bancaires (CB). It should be noted that banks issuing payment cards that are not co-badged have already started rolling out this solution.

As the adoption of the PSD3/PSR package approaches, market participants are already reviewing and strengthening their fraud prevention frameworks, information-sharing mechanisms and processes for handling unauthorised payment transactions.

Judicial decisions delivered in June and July 2026 concerning the reimbursement of unauthorised payment transactions confirm a tightening of judicial scrutiny over PSPs. The most significant development relates to the burden of proof. The debate is gradually shifting away from the sole question of whether the customer acted with "gross negligence" and towards the PSP's ability to demonstrate the integrity and security of the authentication journey. Courts are increasingly examining the entire technical chain that enabled the fraud to occur, including beneficiary creation, trusted-device changes, password resets, spending-limit increases, the registration of a new trusted device and similar events. PSPs are therefore expected to provide evidence that their security mechanisms functioned properly throughout the transaction process.

#### **4. Investment services and asset management**

In late September 2026, the AMF amended its General Regulation and related supervisory guidance on the quarterly obligation of UCITS and AIF depositaries to report any significant anomaly or irregularity identified in the course of their duties. This development forms part of the AMF's broader effort to enhance the reporting and detection of operational and governance weaknesses within investment funds.

In September 2026, the AMF also published its first feedback on the cyber resilience of asset management companies and other investment firms under the new regulatory framework. The regulator observed that 87% of major incidents reported by management companies in 2025 originated from a failure or cyberattack affecting a third-party service provider. This confirms that cyber risk is increasingly a digital supply-chain risk, explaining DORA's focus on the governance and oversight of ICT providers. The report also highlights that operational resilience can no longer be assessed solely through the robustness of internal systems, but must increasingly take into account dependencies on external technology providers.

#### **5. Sustainable finance**

In late July 2026, the European legislator published the implementing measures for the Regulation on ESG rating providers, establishing a comprehensive regulatory framework subject to the direct supervision of the European Securities and Markets Authority (ESMA)<sup>10</sup>. The new regime is intended to enhance the reliability, comparability and integrity of ESG ratings across the European Union.

In addition, at the end of September 2026, the European legislator published the Delegated Regulation of 3 July 2026 on sustainability reporting, adopted under the Corporate Sustainability Reporting Directive (CSRD). The regulation simplifies sustainability reporting requirements for financial years beginning on or after 1 January 2027. While maintaining the principle of double materiality, whereby companies must report both on their impacts on people and the environment and on the financial risks arising from sustainability-related matters, the new framework streamlines implementation through a more proportionate materiality assessment process and a reduction in the number of mandatory disclosures.

Particular attention has also been paid to interoperability with other European regulatory frameworks, including SFDR, the EU Taxonomy Regulation, the Capital Requirements Regulation (CRR) and the emerging corporate sustainability due diligence regime. In practical terms, information disclosed once

---

<sup>10</sup> The relevant Delegated Regulations specify the information required for the authorisation or recognition of ESG rating providers, governance and conflict-of-interest requirements, organisational separation between rating activities and other commercial activities, transparency obligations relating to methodologies, data sources, assumptions and models, as well as the arrangements governing supervisory fees and the procedural framework applicable to inspections, fines and periodic penalty payments.

in a sustainability report should increasingly be capable of being reused for the purposes of complying with several overlapping European reporting obligations, thereby reducing duplication and reporting burdens.

## **6. Other European or national developments impacting financial services**

In mid-July 2026, the European Commission presented its vision for a more competitive and better integrated European banking sector. While no immediate legislative measures were announced, the communication confirms an evolution in the EU policy agenda towards greater prudential proportionality, regulatory simplification and deeper cross-border integration of banking groups. The first legislative initiatives reflecting this policy direction are expected from 2027 onwards.

Pending those reforms, the European Banking Authority (EBA) continued implementing the new CRD VI framework through two texts published in July 2026 concerning branches of third-country banks. Having identified the regulatory arbitrage risks arising from divergent national regimes, the EBA has developed a harmonised framework based on common requirements relating to authorisation, governance, liquidity, capital and prudential disclosures. The reform represents a significant strengthening of the prudential framework applicable to third-country branches operating within the European Union and gradually brings their regulatory treatment closer to that applicable to European credit institutions.

The French transposition of the European cyber resilience framework, including the NIS2 Directive, is finally entering its decisive phase. As France is currently the subject of infringement proceedings before the Court of Justice of the European Union (CJEU) for failing to transpose the Directive within the prescribed timeframe, the relevant bill is expected to be examined by the National Assembly in the coming weeks. For affected entities, the question is no longer whether the new regime will apply, but rather how to prepare for the strengthening of governance, cyber risk management and incident reporting requirements that will result from the reform.

In the insurance sector, the Autorité de contrôle prudentiel et de résolution (ACPR) published guidance in late July 2026 clarifying access to the new proportionality regime introduced by the revision of Solvency II. The notice details the criteria that may justify the refusal of prudential simplifications, including weaknesses in governance arrangements, the existence of supervisory measures, activities presenting a heightened degree of complexity or a risk profile that is not considered sufficiently low. The publication provides welcome clarity regarding supervisory expectations in the context of the implementation of the revised Solvency II framework.

Finally, in the consumer credit sector, the second wave of implementing measures relating to the new Consumer Credit Directive will enter into force on 20 November 2026. The texts published in August and September further strengthen requirements relating to creditworthiness assessments and their documentation and traceability. They also provide additional clarification regarding early repayment provisions and the regulatory thresholds used for calculating French usury rates.