Newsletter – Financial services

Spring 2024

At its plenary session, late April, the European Parliament voted one last time before the EU elections in early June 2024. This hyper legislative has triggered a slight delay in the release of our newsletter.

The key development of this last session for the financial sector is the final adoption of the regulatory package on anti-money laundering and combating the financing of terrorism (AML/CFT), just as the trial in Panama of some thirty personalities associated with the Panama Papers (including the heads of the now liquidated Mossack Fonseca law firm) drew to a close.

The European legislator did not limit itself to AML/CFT: the expected adoption of avalanche of Regulations and Directives did take place at this last session: other regulatory moves included the revision of the banking package, revised Directive for resolution (banking and insurance), the package for payment services (including the Regulation governing instant transfers), but also the important topics of European digital identity, sustainable finance and cyber resilience.

1. Financial Sanctions against Russia

The European legislator is preparing a 14th set of sanctions after releasing its 13th in February 2024. The expansion of the blacklist of sanctioned persons (Regulation 269/2014) has pushed the number of entries over the 2,000 mark. In terms of trade restrictions (Regulation 833/2014), the changes made first concerned the management of frozen assets of the Central Bank of Russia before limiting Russia's capture of technologies allocated to the construction of military equipment, including by targeting Russian or third-country entities involved in this trade (whether or not the latter is linked to circumventing European sanctions). It is this last regulatory move which calls for the strengthening of contracts with counterparties likely to trade with Russia, in addition to the risk of Russian transit.

As part of the sanctions against Russia, in April 2024 the Commission provided practical clarifications on, in particular, the mandatory reporting by the financial sector, from July 2024, of certain transfers of funds outside the EU of more than €100,000 cumulated during the 1st half of 2024[1].

A Directive adopted at the end of April 2024 (n°2024/1260) on the recovery and confiscation of assets[2] foreshadows the increased risk of confiscation of Russian assets, in the context of the so-called "Cyprus Confidential" affair. The form of confiscation in question is distinct from that of the profits generated by frozen assets, on which the EU Council reached agreement in principle early May 2024[3].

As mentioned above in previous newsletters, these developments should not overshadow sanctions regimes targeting (i) other States or (ii) various individuals[4].

[1] In addition to the obligation for persons on the EU sanctions list to declare their assets in the EU.
[2] Its implementation is expected by 23 November 2026 at the latest; it replaces a 2014 Directive on the same subject. It strengthens EU law on attempts to circumvent European sanctions (it requires Member States' criminal law to tackle the violation of sanctions and to confiscate), as does another Directive adopted on the same day (no. 2024/1226) harmonising criminal offences and penalties for breaches of EU sanctions, which must be transposed into national law by 20 May 2025.
[3] Eventually formalized in a Regulation adopted on 21 May 2024. As a reminder, the EU had already obliged central securities depositories to record windfall profits separately so that they could be used to finance the reconstruction of Ukraine.
[4] E.g. Because of their responsibility for human rights violations, under Regulation (EU) 2020/1998, itself amended at the beginning of April 2024, or the Regulation on specific restrictive measures to combat terrorism (amended in February 2024).

2. Fight against money laundering (AML/CFT)

2.1 European developments

It is interesting to note that while the European Parliament adopted its final position[5] on the AML/CFT package[6].the European Commission published (i) its report on the implementation of the 4th European Directive and (ii) its application to the European Banking Authority (EBA) to draft the regulatory technical standards (RTS)[7] tied to the recast of the said package.

With respect to the said package, financial institutions will first and foremost enjoy being able to build their AML/CFT vigilance on the basis of a uniform regulatory framework, rather than on divergent national implementations. Without even waiting for the Regulation to come into force, they will also be able to update their risk classifications based on the factors suggested by the Regulation, revealing a potentially higher (or lower) risk of money laundering or terrorist financing. They can also take into account the fact that some of their existing customers will themselves become subject to the AML/CFT: the list has been extended to include traders in "high-value" goods[8], and soccer clubs[9].

Various institutions in the financial sector may benefit from exemptions from AML/CFT liability, depending on the decisions taken by the Member State to which they belong. Payment/electronic money institutions and crypto asset service providers shall continue designating a central contact point in a Member State when they carry out cross-border activities.

The transparency of EU registers for ultimate beneficial owners (UBOs) is a key measure of the 6th Directive[10]. However, the legislator validated the principle that information is accessible upon payment of a fee[11]. Unfortunately, the Directive failed to tie the equivalence of third countries' AML/CFT rules to the availability of their registers of UBOs. Another change in the 6th Directive is the obligation for EU countries to upkeep registers of accounts[12] by mid-2029, which must (i) include crypto asset accounts and (ii) be interconnected between competent authorities of EU countries[13].

It should be noted that the Regulation resulting from the AML package sets the threshold for the admissibility of digital identities at the "substantial" eIDAS level, extending the French rule currently contained in the French Monetary and Financial Code; this is an important milestone in the context of pan-European marketing of financial services.

2.2 National developments

In France, the French financial intelligence unit (TRACFIN) has rolled out its new version of the reporting form for suspicious transactions. While it is regrettable that the new form will take longer to fill in, it is hoped that the increased data on the form will lead to criminal proceedings in line with the record number of reports in 2023 (190,000). This hope should be seen in the context of a final reorganization of the State's law enforcement agencies[14].

---

[5] A legislative package adopted at the end of April 2024, awaiting final adoption by the EU Council.
[6] The 6th Directive and related texts. They should come into force in mid-2027, with a directly applicable regulation on the substantive rules and another on the future European authority 'AMLA', the headquarters of which will be in Frankfurt. The AMLA will exist as of this year and begin its activities in mid-2025.
[7] A report published on 11 March 2024 and a request from the Commission to the EBA dated 12 March 2024.
[8] This includes art market players, luxury car dealers (over €250,000), aircraft manufacturers (aircraft over €7.5m) and shipyards (boats over €7.5m).
[9] Unless they benefit from a national exemption on the basis of annual sales < €5m.
[10] With rules designed to prevent nominees from becoming shareholders or directors.
[11] Limited "*to what is strictly necessary to cover the costs to guarantee the quality of the information*".
[12] Referred to in the Directive as BARIS (Bank Account Registers' Interconnection System).
[13] See the European Parliament's position of 23 April 2024 on an amending Directive.
[14] With the creation of the Anti-fraud agency (ONAF); it will replace the Financial Judicial Investigation Service.

3. Digital identity

The political agreement reached at the end of 2023 on the draft Regulation amending the European framework for digital identity (eiDAS2) was followed by its publication at the end of April 2024. It will be completed by implementing acts on the setting of reference standards by 21 May 2025. Compliance with these standards will be subject to supervision of national supervisory authorities (e.g. ANSSI).

The eIDAS2 Regulation supplements a number of new features in the area of trust services, notably the creation of new "electronic archiving" and "electronic register" services[15]. Their use could is likely to grow given their probative value[16]. It also then lays the foundations for the future European digital identity wallet, notwithstanding that it requires the "high" eIDAS level, whereas institutions in the banking and financial sector generally limit themselves to the "substantial" level (as mentioned above in connection with AML). This more stringent requirement is likely to hamper the development of the EU wallet.

4. Payment services

The European Parliament's adoption of the PSD3 package at the end of April 2024 brings to a close a busy season in which the European legislator also released in mid-March its Instant Transfer (IP) Regulation. This latter publication sets in motion a major countdown for financial institutions offering traditional single credit transfers (SCT). By 8 October 2025[17], they will have to offer their customers (i) the option of issuing IPs at the same price as SCTs and (ii) the option of associating with IPs a service for verifying the match between IBANs entered and the associated names of the beneficiaries[18].

The latter service should put an end to the current practice of disclaiming liability in the event of discrepancies, even though this disclaimer is already challenged in court[19]. Professional customers will likely be invited to opt out when submitting bulk payment orders[20].

What is most striking about the IP Regulation's presentation of the IBAN/payee matching service is that the legislator has entrusted the service's European interoperability to standards established at European level, whereas such a service does not currently exist in all EU countries[21].

Additional implementing standards for the Regulation on Crypto Asset Providers (MiCA) were adopted in February 2024, following on from those already mentioned above. In the context of the emergence

[15] Its definition is aimed directly at distributed registers (the Blockchain).
[16] Provided that the service providers reach the 'qualified' level. In this context, the electronic archive or register benefits from a presumption of reliability, both in terms of the sequential chronological classification of the data and its integrity, which is likely to encourage cloud service providers widely used in the financial sector to offer archiving services at the 'qualified' eiDAS level, which is essential in the context of the deployment of cybersecurity imposed by the DORA Regulation. It is also this 'qualified' level that should give greater prominence to private or hybrid blockchain rather than public blockchain.
[17] Or by 9 July 2027 for payment or electronic money institutions (PI/EMI) or banks outside the eurozone (or even by 9 June 2028 for the latter).
[18] These same service providers will have to be ready to receive PIs from 8 January 2025 (9 April 2027 for PIs/EMIs). The matching service is in addition to the obligation to compare the list of beneficiaries pre-registered by the customer with the blacklists of financial sanctions (national or EU).
[19] See our article on this subject published in 2022 in *Revue Banque et Droit* (recently confirmed by a decision of the Rennes Court of Appeal on 16 April 2024). We regretfully note that the IP Regulation wrongfully claims that a transaction executed despite a discrepancy not brought to the customer's attention would be a 'wrongly executed' transaction, whereas it seems to us to be indicative of an 'unauthorised' transaction. Another decision by the French Supreme Court on 14 February 2024 (22-11.654) deserves attention: it limits the bank's liability if the disputed payment transaction is not unusual in the customer's commercial practice.
[20] This exemption seems astonishing; it is hard to see what would justify a bank and its employer client not ensuring that salaries are paid to the employees of this employer client rather than to other people.
[21] Under the aegis of the European Payment Council (EPC) and its Rulebooks. It is within this framework that the French interbank service (Sepamail Diamond) has joined the STET group, which is better placed to ensure this integration. Other companies have claimed to be in a position to provide such European service

of these crypto assets, in January 2024 the French Ministry of the Economy took up the critical conclusions of the French *Cour des Comptes* on the need for a better framework to address tax consequences to the transfer of such crypto assets. The latter seem too often associated with the laundering of tax fraud. At the same time, on 22 April 2024, the French legislator passed a law empowering the Government to adjust the regulatory framework associated with crypto asset service providers, thus taking into account (i) the MiCA Regulation and (ii) the Regulation on information accompanying transfers of funds and certain crypto assets.

5. Insurance

While the third pillar of the Banking Union – the European deposit guarantee[22] – has yet to be fully adopted, the insurance sector will closely monitor to the rise of the second pillar of the Insurance Union: the one establishing the rules ensuring the recovery and resolution of insurance companies[23].

A delegated regulation adopted at the end of 2023 but published in March 2024 and applicable from October 9, 2024 raises the basic amounts for professional indemnity insurance and the financial capacity of insurance intermediaries.

In France, at the end of March 2024, the industry's supervisory authority (ACPR) published its 2023 assessment of the checks carried out on the competence and good repute of managers in the banking and insurance sectors, publishing certain governance indicators in both sectors as well as those for management bodies and key function managers in insurance.

Finally, the financial sector will be paying close attention to the ACPR's reminder to insurers to continue their efforts to clarify cyber risk coverage in their contracts[24], particularly with regard to their management of implicit guarantees. The ACPR's aim is to reduce uncertainty about the existence and scope of coverage, which poses a financial risk for insurers and their policyholders.

6. Sustainable finance

At its plenary session on 24 April 2024, the European Parliament adopted the final version of the draft Regulation governing rating providers on environmental, social and governance (ESG)[25]. Firstly, it reinforces the integrity of these providers by laying down rules to prevent conflicts of interest. Above all, when they offer their services to investors and companies in the EU, they must apply for a license, under the supervision of the European Securities and Markets Authority (ESMA). Although the Regulation amends the Sustainable Finance Disclosure Regulation (SFDR), the European Commission is expected shortly to propose its recast, while the French securities regulator (AMF) was calling a recast in mid-February 2024.

The other adoption on the same day was related to the Directive on Corporate sustainability due diligence (CSDD)[26]. After some intense discussions tied to intense lobbying, the adopted Directive eventually excluded asset managers (AIFM and UCITS), although they were initially subject to the underlying requirements. The Regulation is more stringent than French law, but less than the initial draft[27].

[22] EDIS (European Deposit Insurance Scheme). However, the EP adopted its position on 23 April 2024.
[23] Adoption by the European Parliament on 23 April of the draft Directive amending Solvency 2; the French ACPR had earlier released in March 2024 an important explanatory memorandum.
[24] Communication of 11 March 2024.
[25] Applicable from 18 months after its entry into force, expected in summer 2024.
[26] In the same terms as the text adopted by the Council on 15 March 2024. Given the 2-year implementation period, application is anticipated as from mid-2027.
[27] Broadly speaking, companies with more than 1,000 employees (instead of 500 initially) and turnover of more than €450 million (€150 million initially) may be held liable for damages resulting from violations to human rights or the environment that are not properly anticipated (lack of vigilance).

In addition, companies subject to the Corporate Sustainability Reporting Directive (CSRD) will be reporting for the 2024 financial year in 2025 in compliance with guidelines on interoperability between European and international sustainability reporting standards, which were released on 2 May 2024.

7. Investment services and asset management

In the sector of investment services and asset management, the European legislator adopted the final version of texts governing investment services (MiFID3/MiFIR2)[28], pending amendment of the level 2 Regulations. In particular, the reform aims to centralize the provision of data on the key elements of transactions on which investment decisions are based: instrument prices, volume, date and time of transactions, to selected and limited operators (Consolidated Tape Providers). It also aims to publish transactions already carried out (post-trade transparency) as close to real time as possible.

The other major change is the revision of asset management texts (AIFMD2 and UCITS5)[29] in March 2024, to come into force by April 16, 2026. Induced changes concern (i) the framework governing liquidity management tools, (ii) that of funds providing credit to companies, and (iii) introduces reinforced rules applicable to delegation by portfolio managers to third parties.

8. Other European or national developments impacting financial services

There are other developments impacting financial services, including the reform of the banking resolution framework[30], pending a further amendment on early intervention measures, the conditions for triggering a resolution procedure and the financing of resolution measures[31].

On 24 April 2024, the European Parliament also adopted the “banking package”, consisting of a Regulation (CRR3) and a Directive (CRD6) that integrate emerging risks such as those linked to climate change or banks' exposure to crypto assets into the prudential framework[32].

Companies in the financial sector that use cloud providers will be paying close attention to changes in the European cybersecurity certification framework (scheme) for cloud providers[33], following the publication of the Implementing Regulation on 7 February 2024. Cybersecurity is also a key issue, with delegated regulations adopted in February 2024[34] and March 2024[35].

[28] Adopted on 28 February, released in the OJ on 8 March 2024; implementation is due by 29 September 2025.
[29] In addition to four implementing regulations on AIFMD or UCITS on cross-border activities, adopted at the end of 2023 but released in the OJ on 25 March 2024, which have already partially come into force.
[30] Directive of 11 April 2024 on minimum capital requirements and eligible commitments. It should be noted that the ACPR published a useful operational document on 16 January 2024 on the implementation of the bail-in instrument in France, which is part of the regulatory technical standards published in February 2024 on the minimum elements to be included in a business reorganisation plan and the criteria it must meet to be approved by the resolution authority.
[31] Adoption by the European Parliament on 24 April 2024.
[32] A communication from the ACPR in March 2024 sets out the underlying developments.
[33] EU Cybersecurity Certification Scheme on Cloud Services (EUCS) applicable from 27 February 2025.
[34] On (i) the amount of supervisory fees to be collected by the lead supervisor from critical third-party ICT service providers and the terms of payment of these fees and (ii) the definition of criteria for designating third-party IT service providers as critical for financial entities.
[35] On the technical regulatory standards specifying (i) the tools, methods, processes and policies for managing the risk associated with IT service providers, (ii) the criteria for classifying ICT-related incidents and cyber threats and (iii) the detailed content of the policy concerning contractual agreements on the use of IT services supporting critical or important functions.