Identomat

COMPLIANCE GUIDE

# Banking & Digital Banking Compliance in France

COUNTRY France

INDUSTRY Banking & Digital Banking

LAST UPDATED 29 October 2026

KEY REGULATORS Autorité de contrôle prudentiel et de résolution · Tracfin · European Central Bank

## Key takeaways

- Taking deposits from the public in France requires a credit institution licence. The European Central Bank grants it on the proposal of the French banking supervisor (Autorité de contrôle prudentiel et de résolution, ACPR). Taking deposits without one is a criminal offence.
- Banks must identify every customer, and verify that identity, before opening an account. Fully remote account opening is allowed, with no special approval, if the bank uses one of the verification methods the law lists.
- Online, the two main routes are a government-grade digital identity (for example France Identité, used through FranceConnect+) or two checks combined, such as a remote identity service certified by the national cybersecurity agency (ANSSI) plus a copy of the ID document. A video call does not count as seeing the original document in person.
- Suspicious transactions must be reported to Tracfin, the French financial intelligence unit, before they are carried out. There is no minimum amount. Since May 2026 banks must also record accounts they suspect of fraud in a national file kept by the Banque de France.
- New EU anti-money laundering rules apply from 10 July 2027. They will replace much of the French detail with one EU rulebook, require customer data to be refreshed at least every year for high-risk customers, and bring the largest cross-border groups under direct EU supervision from 2028.

---

France is open to digital and branch banking alike, and its rules are largely channel-neutral: the same customer due diligence obligations apply whether an account is opened in a branch or in an app. What changes online is the list of acceptable verification methods, and France has written that list into its monetary and financial code in more detail than most EU countries, including a national certification scheme for remote identity verification providers.

The ACPR authorises and supervises banks, payment and e-money institutions, and is their anti-money laundering supervisor. Tracfin receives suspicious transaction reports, the Directorate General of the Treasury keeps the national asset-freeze register, and the CNIL (Commission nationale de l'informatique et des libertés) supervises personal data processing.

For a new entrant, the biggest obstacle is the licence itself: an ECB authorisation with a capital requirement of between €1 million and €5 million, a head office in France and at least two effective managers. Partnering with a licensed bank, or operating as a payment or e-money institution, are the usual alternatives.

CONTENTS


1 Who regulates this sector
2 Licensing and authorisation
3 AML, KYC and customer due diligence
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
▪ Sources


## 1 Who regulates this sector

| Authority | Remit | Level | Official site |
|---|---|---|---|
| European Central Bank (ECB) | Grants and withdraws credit institution licences on the ACPR's proposal; prudential supervision of significant banks | EU | CMF L511-10 |
| Autorité de contrôle prudentiel et de résolution (ACPR) | Licence proposals, prudential supervision, conduct of business, AML/CFT supervision and sanctions for banks, payment and e-money institutions | National | acpr.banque-france.fr |
| Banque de France | Central bank; hosts the ACPR; manages the right-to-an-account procedure and the national fraud-risk accounts file | National | banque-france.fr |
| Tracfin | Financial intelligence unit: receives suspicious transaction reports, can block transactions | National | economie.gouv.fr/tracfin |

| | | | |
|---|---|---|---|
| Direction générale du Trésor | National asset-freeze register (national, EU and UN measures) | National | gels-avoirs.dgtresor.gouv.fr |
| ANSSI (Agence nationale de la sécurité des systèmes d'information) | Certifies remote identity verification providers (PVID) and electronic identification means | National | cyber.gouv.fr |
| CNIL | Data protection, including biometrics and authentication | National | cnil.fr |
| Anti-Money Laundering Authority (AMLA) | EU AML/CFT authority; took over the European Banking Authority's AML/CFT mandates on 1 January 2026; direct supervision of selected groups from 2028 | EU | amla.europa.eu |

The Autorité des marchés financiers (AMF) supervises AML/CFT for asset management companies, financial investment advisers and certain market infrastructures (CMF L561-36); this guide focuses on deposit-taking institutions.

## 2 Licensing and authorisation

**The banking monopoly.** Only a credit institution may receive repayable funds from the public on a regular basis or provide banking payment services, and only a credit institution or a financing company (société de financement) may lend on a regular basis (Code monétaire et financier, CMF, L511-5). Breaching the monopoly carries three years' imprisonment and a €375,000 fine (L571-3).

**Who grants the licence.** Under CMF L511-10 (in force since 10 April 2026), the ECB grants the licence to companies with their registered office in France, on the ACPR's proposal. The ACPR itself authorises branches of banks from outside the EU and EEA.

- Initial capital of €1 million to €5 million depending on the licence, set by ministerial order (L511-11).
- Registered office and central administration in France, and at least two effective managers (L511-13).

- Membership of the deposit guarantee and resolution fund, the Fonds de garantie des dépôts et de résolution (L312-4), which covers up to €100,000 per depositor per institution (standard depositor information form, arrêté of 27 October 2015).

**Digital models.** There is no separate licence for a digital-only bank: a neobank that takes deposits needs the same licence. Many app-based providers are instead payment or e-money institutions, also obliged entities under L561-2. In banking-as-a-service, a firm relying on a partner's checks stays responsible (L561-7).

**Third-country branches.** Ordonnance n° 2026-255 of 8 April 2026 transposed Directive (EU) 2024/1619. From 11 January 2027 (article 81 II of the ordonnance), CMF L511-10 I requires non-EU banks to serve French clients through an authorised branch, except for business with credit institutions and financing companies, entities of the same group, and clients who approached the bank on their own initiative. Marketing other products to those clients still requires a branch.

## 3 AML, KYC and customer due diligence

**Scope.** Credit institutions, including branches of foreign banks, are obliged entities under CMF L561-2 1°. The obligations apply to every customer; there is no size threshold.

### Risk assessment

Classify risks by product, transaction, distribution channel, customer and geography, and set due diligence accordingly (L561-4-1).

### Identification

Identify and verify the customer and any beneficial owner before the relationship starts (L561-5). For an individual: surname, first names, date and place of birth (R561-5).

### Know your customer

Collect and update information on the purpose and nature of the relationship, adapted to risk (L561-5-1, R561-12).

### Ongoing monitoring

Examine transactions for consistency with what the bank knows of the customer (L561-6).

If due diligence cannot be completed, the bank must not execute any transaction or open or continue the relationship, and may report to Tracfin (L561-8). Where risk appears low, verification may be completed while the relationship is being established (L561-5 IV). Anonymous accounts are prohibited (L561-14).

**Occasional customers.** CMF R561-10 requires verification before any suspicious transaction, money transfer or safe-deposit rental, manual currency exchange above €1,000 (any amount if the customer is not physically present), cash or e-money transactions above €10,000, and any other transaction above €15,000, counting linked transactions.

**Enhanced due diligence.** Additional measures are mandatory for politically exposed persons and their families and close associates, products that favour anonymity, and transactions with high-risk countries listed by the FATF or the European Commission (L561-10). A person remains politically exposed for one year after leaving office (R561-18). Onboarding them needs senior approval and a review of the origin of wealth and funds (R561-20-2).

**Beneficial owners.** The beneficial owner is the natural person who ultimately controls the customer (L561-2-2); for a company, anyone holding directly or indirectly more than 25% of capital or voting rights, or exercising control by other means (R561-1). Companies declare beneficial owners to the trade register (L561-46), and since 31 July 2024 access is limited to supervisors, obliged entities and persons with a legitimate interest.

**Reporting.** Banks report to Tracfin sums and transactions they know, suspect or have good reason to suspect derive from an offence punishable by more than one year's imprisonment or are linked to terrorist financing, including attempts (L561-15). Reports are filed before execution (L561-16), with no minimum amount, through the ERMES platform. Tracfin may defer a transaction for ten working days (L561-24).

**Freezes and records.** Banks must apply freeze measures without delay and inform the Minister of the Economy immediately (L562-4). Joint guidelines of the Directorate General of the Treasury and the ACPR (updated 16 March 2026) expect screening before onboarding, re-screening of the customer base without delay whenever measures change (weekly is not enough), transaction screening before settlement and fuzzy matching. Records are kept for five years after the relationship ends (L561-12), and each bank appoints a senior AML/CFT officer (L561-32).

## 4 Identity verification and onboarding

CMF R561-5-1 (in force since 5 April 2021) lists the primary verification methods; any one is enough: an electronic identification means certified or attested by ANSSI at eIDAS level "substantial" or "high", or notified by another member state at those levels; an electronic identification means presumed reliable under article L102 of the Code des postes et des communications électroniques; for an individual physically present, the original of a valid

official photo document plus a copy; for a company, a registry extract less than three months old.

Where none can be used, R561-5-2 requires **at least two** of six measures that together verify every identification element: a copy of an official document; certification of that copy by an independent third party; a first payment from or to an account in the customer's name at a regulated institution in the EU, EEA or an equivalent country; confirmation from a qualifying third party; a service certified by ANSSI at the "substantial" level of Implementing Regulation (EU) 2015/1502; or an advanced or qualified electronic signature or seal based on a qualified certificate. Evidence of each measure must be kept.

### Certified remote identity verification (PVID)

Under the arrêté of 28 March 2021, ANSSI publishes the technical framework for remote onboarding services and lists certified remote identity verification providers (prestataires de vérification d'identité à distance, PVID), at the "substantial" level, for both agent-assisted and automated services.

### Documents, biometrics and video

The ACPR's guidelines on identification and verification (16 December 2021) allow biometrics and videoconferencing to verify identity, but presenting the original document requires the customer to be physically in the same place as the bank's staff, which excludes videoconference.

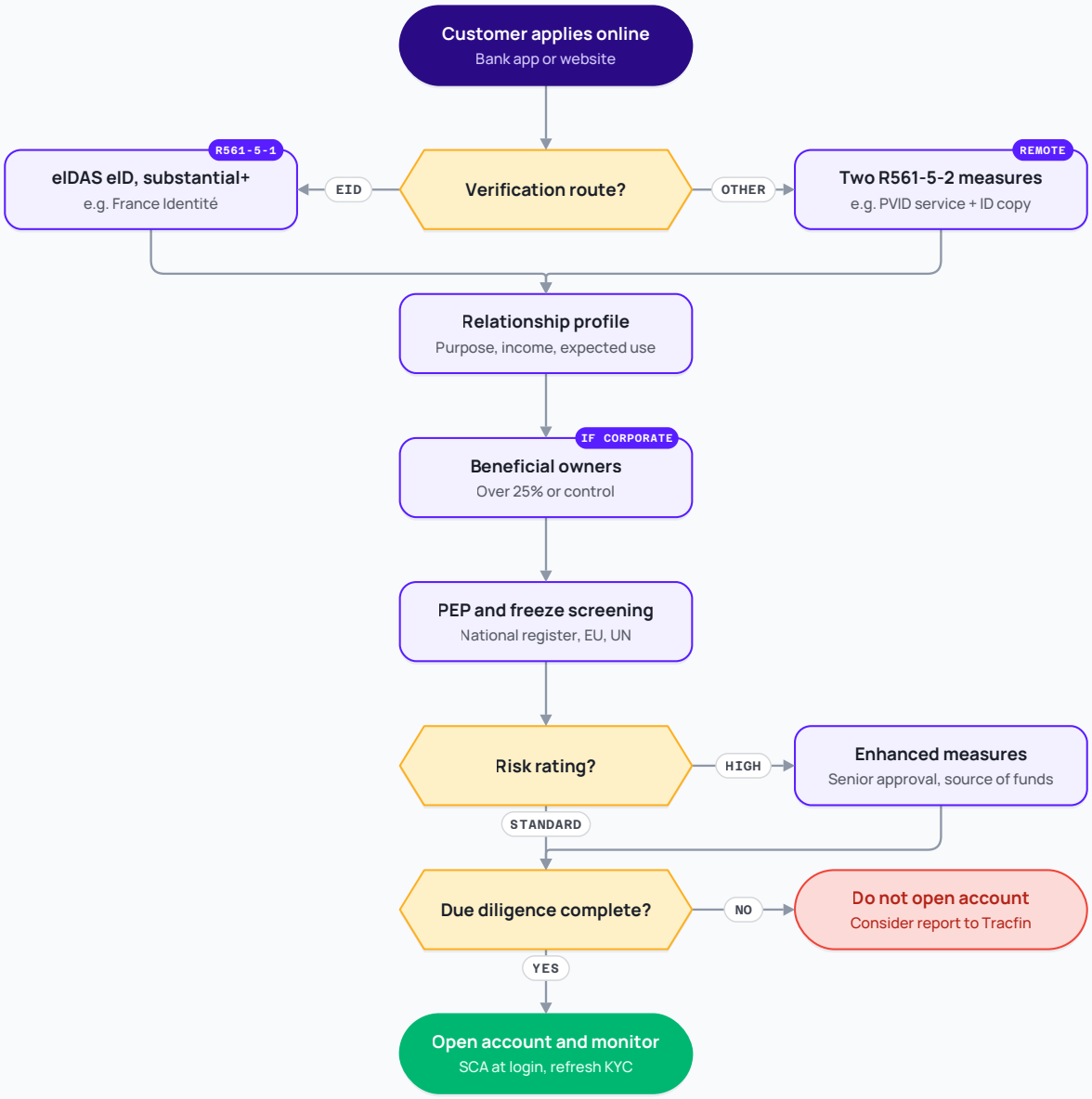



Figure 1. Remote account opening at a French bank under CMF R561-5-1 and R561-5-2.

## National digital identity

France Identité, the Ministry of the Interior's app for holders of the new identity card, was certified by ANSSI at eIDAS level "high" on 7 February 2024. Through FranceConnect+, identities are offered at "substantial" or "high"; basic FranceConnect is level "low", which does not meet R561-5-1. Only France Identité and La Poste's digital identity are available on FranceConnect+. A bank can be authorised to use FranceConnect for its due diligence duty under CMF L561-5, and only within that scope.

## 5 Digital channels: what's different

**Bottom line:** due diligence obligations are channel-neutral, but online the bank must use a certified electronic identity or combine two listed measures; showing an ID to a camera is not the same as showing the original in a branch.

| Requirement | In person / branch | Online / remote | Difference |
|---|---|---|---|
| **Permission to onboard** | Permitted | Permitted, no prior approval (R561-5-1, R561-5-2) | Same |
| **Identity data collected** | Names, date and place of birth | Same (R561-5) | Same |
| **Verification method** | Original photo ID plus a copy | eIDAS eID at substantial or high, or two R561-5-2 measures | Differs |
| **Video presentation of the original ID** | Not applicable | Does not count as physical presence (ACPR guidelines) | Differs |
| **Risk treatment** | Risk-based; channel is a risk factor | Not an automatic enhanced due diligence trigger (L561-10) | Same |
| **Timing of verification** | Before the relationship starts | Same; deferral only for low risk (L561-5 IV) | Same |
| **Account access** | Not applicable | Strong customer authentication for online account access (L133-44) | Differs |
| **Reliance on third parties** | Permitted; bank remains responsible | Same (L561-7) | Same |
| **Evidence retention** | Five years | Five years, including evidence of each remote measure (R561-5-2, L561-12) | Same |

### Remote opening is not automatically high risk

The mandatory enhanced measures in CMF L561-10 (version in force since 24 December 2025) cover politically exposed persons, anonymity-favouring products and high-risk countries, not non-face-to-face onboarding. Channel remains a factor in each bank's own risk classification (L561-4-1).

### Account security

CMF L133-44 requires strong customer authentication when a customer accesses an online account, initiates an electronic payment or takes a risky remote action, dynamically linked to amount and payee for remote payments.

### What is changing

Regulation (EU) 2024/1624 `Adopted, applies 10 Jul 2027` allows verification by an identity document plus reliable independent sources, or by eIDAS identification at "substantial" or "high" (Article 22(6)). Under Regulation (EU) 2024/1183 `Adopted, applies 36 months after implementing acts`, banks must accept European Digital Identity Wallets at the user's request within 36 months of the relevant implementing acts, the first of which entered into force on 24 December 2024.

## 6 Data protection and biometrics

The GDPR and the Loi Informatique et Libertés apply, supervised by the CNIL. Customer due diligence rests on a legal obligation: the CNIL confirms that banks keep a copy of identity documents for five years after the relationship ends (CMF L561-12). The national social security number (NIR) may not be used to identify customers; the framework decree allows it in AML and freeze processing only where the number itself appears on a freeze or sanctions list (décret 2019-341, article 2 D 11°).

Biometric data are sensitive under Article 9 of the GDPR. The CNIL considers that biometrics rest on explicit consent unless a legal text requires or expressly authorises them, and cannot be imposed without an alternative (recommendation on multi-factor authentication, 20 March 2025). It treats matching a selfie to the ID photo for remote account opening as one-to-one authentication, which raises fewer issues than identification, and favours templates stored on the user's device (November 2019). For remote identity verification, ANSSI committed to require an Article 9(2) basis for any biometric processing and to prohibit keeping fingerprints (CNIL deliberation 2022-027). An impact assessment is required for large-scale biometric processing (GDPR Article 35(3)(b)) or when two of the CNIL's nine risk criteria are met. Biometric verification that only

confirms a claimed identity is outside the AI Act's high-risk biometric category (AI Act, Annex III, 1(a)).

## 7 Sector-specific obligations

### Right to an account

Anyone domiciled in France, EU residents acting as consumers and French nationals abroad who have no French deposit account are entitled to one with basic services (CMF L312-1). Subject to AML/CFT checks, the bank opens it within six working days of a complete file and explains any refusal in writing.

### National fraud-risk accounts file In force

CMF L521-6-1, created by loi n° 2025-1058 of 6 November 2025 and applicable six months after the law's promulgation, set up a Banque de France file of accounts that payment service providers, including banks, consider likely to be fraudulent. Under an arrêté of 24 April 2026 (in force since 29 April 2026), banks record the IBAN, fraud category and any identity-theft complaint, refresh their local copy at least daily or before any new payment, and investigate flagged accounts they hold without delay. A listing does not by itself block payments or justify closing the account.

### Instant payments

Under Regulation (EU) 2024/886, euro-area banks have verified the payee before every credit transfer since 9 October 2025 (Article 5c), and banks offering instant transfers screen their whole customer base against EU restrictive measures at least daily instead of screening each transfer (Article 5d).

## 8 Risk indicators and red flags

BANKING TYPOLOGIES FROM TRACFIN AND THE ACPR

- **Sanctions circumvention**: correspondent flows linked to Russia or Iran via Central Asia, Southeast Asia, Hong Kong or the UAE (Tracfin, 2025).
- **Foreign-coded virtual IBANs**: automatic redirection that hides the underlying account holder (Tracfin and ACPR, April 2026).
- **Repeat "occasional" customers**: frequent walk-in transactions never reclassified as a business relationship (ACPR, November 2025).
- **Rebound accounts**: new, mostly remotely opened accounts, often first funded by someone else's card, that pass fraud proceeds straight on (ACPR, July 2025).
- **Shell-company pass-through accounts**: new companies at domiciliation addresses, onboarded with forged documents, whose inflows from unrelated firms leave for abroad at once (Tracfin, 2025, case 16).
- **Cash-for-transfer swaps**: transfers between unrelated companies, cash withdrawals from abroad and a lifestyle out of line with declared income (Tracfin, 2025, case 18).
- **Missing beneficial owner data**: corporate customers with no recorded director or owner, defeating freeze screening (ACPR, June 2025).
- **Identity theft at account opening**: accounts opened in another person's name, to be flagged in the national fraud file.

Tracfin received 278,484 suspicious transaction reports in 2025, 163,630 of them from banks and credit institutions, up 45% on 2024.

## 9 Enforcement and penalties

The ACPR's Sanctions Committee hears AML/CFT cases. Under CMF L561-36-1 (version in force since 1 July 2026), it can impose the disciplinary sanctions listed in L612-39 and, instead or in addition, a fine of up to the higher of €100 million or 10% of total turnover.

Managers and the AML/CFT officer can be sanctioned personally, including temporary bans of up to ten years.

- **Banque Chaabi du Maroc** (7 November 2025): reprimand and €250,000 fine. About 63% of 38,020 alerts were unprocessed and suspicious transaction reports were filed on average 768 days late.
- **Banque Delubac & Cie** (19 June 2025): reprimand and €600,000 fine for monitoring, enhanced due diligence, reporting and asset-freeze failings, including a €1,000 screening threshold that left about 65,000 transfers unscreened.
- **BRED** (27 June 2024): reprimand and €2.5 million fine for monitoring, enhanced due diligence and reporting failings.

## 10 Recent changes and what to watch

- **2 December 2027**: AI Act high-risk obligations for Annex III systems `Adopted, applies 2 Dec 2027`, including AI credit scoring of individuals (Regulation (EU) 2026/1744).
- **10 July 2027**: EU AML Regulation 2024/1624 `Adopted, applies 10 Jul 2027`. One EU rulebook; customer data refreshed at least yearly for higher-risk customers and every five years for others.
- **1 July 2027**: AMLA selection for direct supervision `Adopted, starts by 1 Jul 2027`. Large cross-border groups may come under EU supervision from 2028.
- **11 January 2027**: third-country branch requirement `Adopted, applies 11 Jan 2027`. Non-EU banks serving French clients need an authorised branch unless exempt.
- **May 2026**: national fraud-risk accounts file `In force`. Banks must declare and consult flagged accounts; operating rules applied from 29 April 2026.
- **1 January 2026**: AMLA takes over EBA AML/CFT mandates `In force`. EBA guidelines, including on remote onboarding, stay in force until replaced.

## 11 What this means for identity verification

- Map every remote journey to R561-5-1 (eIDAS eID at substantial or high) or to a documented pair of R561-5-2 measures covering all identification data.
- A document and selfie flow counts as one measure only if it is PVID-certified by ANSSI; otherwise it needs a second measure.

- Keep evidence of each measure for five years after the relationship ends, within CNIL limits on biometrics.
- Screen against the national freeze register and, for instant payments, at least daily.
- Re-verify on changed circumstances, fraud-file entries or suspected identity theft, and plan for AMLR refresh cycles from July 2027.

IDENTOMAT

## How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote KYC onboarding with ID document capture and verification (including NFC), face match and biometric liveness, configurable to combine the measures listed in CMF R561-5-2.
- Video KYC for agent-assisted remote onboarding journeys.
- KYB and beneficial owner verification for corporate customers.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring.
- A no-code workflow builder and an audit trail of each check to support the five-year evidence retention requirement.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

## Sources

- **Code monétaire et financier, articles L561-4-1 to L561-14-2 (customer due diligence)**, versions in force on 28 October 2026, Légifrance, legifrance.gouv.fr

- **Code monétaire et financier, Book V, Title VI, Chapter I (AML/CFT obligations, including L561-36, L561-2, L561-2-2, L561-15, L561-15-1, L561-16, L561-24, L561-32, L561-36-1, L561-46)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, articles R561-5 to R561-22-2 (identification and verification, occasional customers, PEPs)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L511-5 (banking monopoly)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, articles L511-9 to L511-20 (authorisation)**, version of L511-10 in force since 10 April 2026, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L511-20-1 (significant acquisitions)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L571-3 (criminal penalties)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L312-1 (right to an account)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L312-4 (deposit guarantee and resolution fund)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L133-44 (strong customer authentication)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L521-6-1 (national fraud-risk accounts file)**, version in force since 27 June 2026, Légifrance, legifrance.gouv.fr
- **Arrêté du 24 avril 2026 définissant les modalités techniques de fonctionnement du fichier mentionné à l'article L. 521-6-1 du code monétaire et financier** [order on the technical operation of the fraud-risk accounts file], Légifrance, legifrance.gouv.fr
- **Arrêté du 28 mars 2021 relatif à la certification de conformité des services d'entrée en relation d'affaires à distance** [order on certification of remote onboarding services], Légifrance, legifrance.gouv.fr
- **ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle** [guidelines on identification, verification and knowledge of customers], 16 December 2021, paragraphs 32 to 49, acpr.banque-france.fr
- **ACPR Commission des sanctions, decision 2024-01 (Banque Chaabi du Maroc)**, 7 November 2025, acpr.banque-france.fr
- **ACPR Commission des sanctions, decision 2024-02 (Banque Delubac & Cie)**, 19 June 2025, acpr.banque-france.fr
- **ACPR press release, Commission des sanctions decision regarding BRED**, 28 June 2024, acpr.banque-france.fr
- **ACPR, Recueil des sanctions** [register of sanctions decisions], acpr.banque-france.fr
- **Tracfin, Quand et comment déclarer un soupçon ?** [when and how to report a suspicion], economie.gouv.fr
- **Tracfin, 2025 Activité et impact, Tome 1** [2025 activity and impact report], pages 12 to 17, economie.gouv.fr

- **Tracfin and ACPR, Panorama et analyse des services d'IBAN virtuels offerts en France** [virtual IBAN services in France], 10 April 2026, economie.gouv.fr
- **Direction générale du Trésor and ACPR, Lignes directrices conjointes sur la mise en œuvre des mesures de gel des avoirs** [joint guidelines on asset freezes], updated 16 March 2026, paragraphs 108 to 126, acpr.banque-france.fr
- **INPI, FAQ on beneficial owners**, inpi.fr
- **ANSSI, Prestataires de vérification d'identité à distance (PVID)** [remote identity verification providers], cyber.gouv.fr
- **France Identité, press kit on the general availability of France Identité**, February 2024, france-identite.gouv.fr
- **FranceConnect, conditions générales d'utilisation, version 1.8** [user terms], applicable from 20 February 2026, franceconnect.gouv.fr
- **CNIL, Recommandation relative à l'authentification multifacteur** [recommendation on multi-factor authentication], adopted 20 March 2025, cnil.fr
- **CNIL, Ma banque peut-elle faire une copie de ma pièce d'identité ?** [can my bank copy my ID?], CNIL Direct, cnil.fr
- **CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux** [facial recognition], 15 November 2019, pages 3 to 6, cnil.fr
- **CNIL, Délibération n° 2022-027 du 3 mars 2022** [opinion on certification of electronic identification means], Légifrance, legifrance.gouv.fr
- **CNIL, Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)** [data protection impact assessments], cnil.fr
- **Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du NIR** [NIR framework decree], article 2, version in force since 1 January 2026, Légifrance, legifrance.gouv.fr
- **Regulation (EU) 2016/679 (GDPR), Articles 9 and 35**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1689 (AI Act), Annex III points 1(a) and 5(b)**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2026/1744 (Digital Omnibus on AI)**, 8 July 2026, EUR-Lex, eur-lex.europa.eu
- **FranceConnect, Fournisseurs d'identité** [identity providers], docs.partenaires.franceconnect.gouv.fr
- **Code monétaire et financier, article R561-1 (beneficial owner of a company)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L562-4 (application of freeze measures)**, version in force since 26 February 2022, Légifrance, legifrance.gouv.fr
- **Ordonnance n° 2026-255 du 8 avril 2026 relative à la transposition de la directive (UE) 2024/1619**, articles 2 and 81, Légifrance, legifrance.gouv.fr
- **Loi n° 2025-1058 du 6 novembre 2025 visant à renforcer la lutte contre la fraude bancaire** [law strengthening the fight against banking fraud], article 1, Légifrance, legifrance.gouv.fr

- **Arrêté du 27 octobre 2015 relatif à l'information des déposants sur la garantie des dépôts** [order on depositor information], annex, Légifrance, legifrance.gouv.fr
- **ACPR, Rapport sur la prévention des comptes rebonds** [report on preventing rebound accounts], July 2025, pages 2 to 34, acpr.banque-france.fr
- **Tracfin, LCB-FT : état de la menace 2024-2025, Tome 3** [AML/CFT threat assessment], 29 September 2025, case 16 (pages 44 to 45) and case 18 (pages 48 to 49), economie.gouv.fr (report page: economie.gouv.fr)
- **FranceConnect, Conditions d'éligibilité des fournisseurs de service** [service provider eligibility], docs.partenaires.franceconnect.gouv.fr
- **Commission Implementing Regulations (EU) 2024/2979 and 2024/2981 (EUDI Wallet integrity and certification)**, EUR-Lex, 2024/2979 and 2024/2981
- **Regulation (EU) 2024/1624 (AMLR), Articles 22, 26, 90**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1620 (AMLA Regulation), Article 13(4) and recital 86**, EUR-Lex, eur-lex.europa.eu
- **Directive (EU) 2024/1619 (CRD6), Article 2 and Article 21c of Directive 2013/36/EU as amended**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 (European Digital Identity Framework), Article 5f**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/886 (instant payments), Articles 5c and 5d**, EUR-Lex, eur-lex.europa.eu
- **AMLA, EBA and AMLA complete handover of AML/CFT mandates**, 19 January 2026, amla.europa.eu
- **EBA, Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15)**, 22 November 2022, eba.europa.eu