



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in France

COUNTRY **France**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **29 October 2026**

KEY REGULATORS **Autorité de contrôle prudentiel et de résolution (ACPR) · Tracfin · Direction générale du Trésor**

Key takeaways

- Providing payment services or issuing e-money in France requires an authorisation (agrément) from the banking and payments supervisor, the Autorité de contrôle prudentiel et de résolution (ACPR), or an EU licence used in France through the passport; operating without one is a criminal offence.
- Payment and e-money firms are fully covered by French anti-money laundering rules: they must identify and verify every customer before the relationship starts, monitor activity, report suspicions to the financial intelligence unit (Tracfin) and apply asset freezes without delay.
- Fully remote onboarding is allowed. The cleanest route is a government-grade digital identity at the European "substantial" or "high" level; otherwise the firm must combine at least two checks from a fixed legal list, such as a state-certified remote identity verification service plus a first payment from the customer's own bank account.
- A video call does not count as meeting the customer in person, and showing a bank account number is not enough on its own: the first payment must actually come from, or go to, that account.
- From 10 July 2027 the EU Anti-Money Laundering Regulation replaces most of these national rules, and a draft EU standard would make document-and-selfie onboarding a fallback that firms must justify case by case (proposed, not yet law).

France is open to online payment, e-money and money transfer businesses, including firms licensed elsewhere in the European Economic Area that operate through agents or distributors. The ACPR authorises and supervises them, including for anti-money laundering; Tracfin receives suspicious transaction reports; the Direction générale du Trésor runs the national asset-freeze register.

The biggest obstacle for a new entrant is the verification design. French law lists the remote methods it accepts, and the ACPR has sanctioned payment firms for weak customer knowledge, monitoring and oversight of agent networks, so an onboarding flow built only for conversion will not pass supervision.

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

Regulator	Remit	Level	Official site
Autorité de contrôle prudentiel et de résolution (ACPR)	Authorises and supervises payment and e-money institutions, registers agents and account information providers, supervises anti-money laundering compliance, imposes sanctions	National	acpr.banque-france.fr
Banque de France	Gives its opinion on authorisation applications; oversees the security of means of payment	National	banque-france.fr
Tracfin	Financial intelligence unit: receives suspicious transaction reports and systematic reports on money transfers	National	economie.gouv.fr/tracfin
Direction générale du Trésor	Asset-freeze policy and the national register of freezes	National	gels-avoirs.dgtresor.gouv.fr
Agence nationale de la sécurité des systèmes d'information (ANSSI)	Certifies electronic identification means and remote identity verification providers	National	cyber.gouv.fr

Commission nationale de l'informatique et des libertés (CNIL)	Data protection, including biometric data	National	cnil.fr
Anti-Money Laundering Authority (AMLA)	EU anti-money laundering standards; took over the European Banking Authority's AML mandates on 1 January 2026	Supranational (EU)	amla.europa.eu

2 Licensing and authorisation

The Code monétaire et financier (CMF) reserves payment services and e-money issuance to authorised providers. The main routes for a non-bank are:

Payment institution

Before providing payment services, a payment institution must obtain an agrément from the ACPR, issued after the Banque de France's opinion, and only to a legal person (art. L522-6 CMF). The ACPR notifies its decision within three months (art. R522-1). Minimum capital is €20,000 for money remittance only, €50,000 for payment initiation only and €125,000 for other payment services (arrêté of 29 October 2009, art. 4).

Simplified payment institution

A lighter agrément is available where forecast payment volume stays below a ceiling set by decree (art. L522-11-1): three million euros per month, averaged over twelve months (art. D522-1-1).

E-money institution

Issuing and managing e-money requires an ACPR agrément, again after the Banque de France's opinion (art. L526-7), and minimum capital of €350,000 (arrêté of 2 May 2013, art. 4).

Account information services

Account information service providers register with the ACPR instead of seeking full authorisation (art. L522-11-2), and must hold professional liability insurance (art. L522-7-1).

Agents, distributors and passporting

A payment service provider may act through agents, which it must register with the ACPR (art. L523-1). The provider "demeure pleinement responsable" (remains fully responsible) for its agents and must bring them within its internal control and anti-money laundering framework (art. L523-3). EU payment and e-money institutions that use agents or distributors in France are themselves obliged entities under French anti-money laundering law (art. L561-2, 1^o quater).

Exclusions and penalties

Limited-network instruments are excluded, but must be notified to the ACPR once twelve-month volume exceeds one million euros (art. L521-3). Providing payment services without authorisation is punishable by three years' imprisonment and a fine of €375,000 (art. L572-5); the same penalties apply to unauthorised e-money issuance (art. L572-13).

3

AML, KYC and customer due diligence

Payment institutions and e-money institutions are obliged entities under art. L561-2 CMF (1^o bis and 1^o ter). Their core duties are:

- **Identify and verify before onboarding.** Before entering a business relationship, firms identify the customer and any beneficial owner and verify these elements "sur présentation de tout document écrit à caractère probant" (on presentation of any reliable written document) (art. L561-5). For a natural person, identification data are surname, first names, and date and place of birth (art. R561-5).
- **Occasional customers.** Money remittance (transmission de fonds) requires identification and verification before the transfer whatever the amount; other occasional operations are caught above €15,000, cash or e-money operations above €10,000, or on suspicion (art. R561-10).
- **Knowledge and monitoring.** Firms keep constant vigilance over the relationship and check that operations match their up-to-date knowledge of the customer (art. L561-6). If they cannot complete due diligence, they must not execute any operation or start or continue the relationship (art. L561-8).
- **Enhanced due diligence.** Additional measures apply to politically exposed persons, anonymity-favouring products and high-risk countries; since 24 December 2025 their intensity and frequency must match the customer's risk profile (art. L561-10). Remote onboarding is not on this list.

- **Beneficial owners.** A beneficial owner is a natural person holding more than 25% of capital or votes, or otherwise controlling the company. Since 31 July 2024, access to the beneficial ownership register kept by INPI (the national business register) is limited to supervisors, obliged entities and persons with a legitimate interest.
- **Asset freezes.** Freezes apply without delay (art. L562-4). The joint DG Trésor and ACPR guidelines (updated 16 March 2026) expect screening before onboarding, customer-base screening as soon as a list changes (weekly screening is insufficient) and screening of transfers before settlement.
- **Retention.** Customer and due diligence records are kept for five years after the account is closed or the relationship ends, and transaction records for five years after execution (art. L561-12).

E-money exemption and simplified measures

Simplified measures may be applied where risk is low (art. L561-9). E-money issuers may skip identification and verification only if every condition of art. R561-16-1 is met: the e-money buys consumer goods or services only (not crypto-assets), stores no more than €150 and, if reloadable, is capped at €150 of storage and payments per 30 days and used only in France; it cannot be loaded with cash (with narrow exceptions) or with unverified e-money; and the issuer monitors transactions. Cash redemptions over €50, and payments initiated online or by remote device over €50 per transaction, always require full due diligence.

Reporting

Firms report to Tracfin any sums or operations 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 (art. L561-15). Tracfin states that there is no reporting threshold and that the report must normally be filed before the transaction is executed, through its ERMES platform. Money remittances funded by cash or e-money are also reported systematically from €1,000 per operation or €2,000 per customer per calendar month, within 30 days after the month of payment (art. R561-31-1).

4

Identity verification and onboarding

Art. R561-5-1 CMF lists the methods that verify identity on their own:

- an electronic identification means certified or attested by ANSSI at the eIDAS "substantiel" or "élevé" level, or issued under a scheme notified to the European Commission at those levels (1°);

- an electronic identification means presumed reliable under the postal and electronic communications code (2°);
- for a customer physically present, the original of a valid official photo document, with a copy taken (3°);
- for a legal person, an official register extract less than three months old (4°).

Where none of these can be used, art. R561-5-2 requires at least two of six measures: 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 EU, EEA or equivalent institution; confirmation of identity by a qualifying regulated third party; a remote identity verification service certified by ANSSI at the "substantial" level of the EU identity-proofing requirements (Implementing Regulation (EU) 2015/1502); or an advanced or qualified electronic signature, seal or qualified registered delivery service.

How the ACPR reads these rules

The ACPR's identification guidelines (16 December 2021) set three limits. Physical presence "exclut le recours à la vidéoconférence" (rules out videoconference) (para. 35). The first-payment measure "ne saurait néanmoins reposer sur la simple présentation d'un RIB au nom du client" (cannot rest on merely showing a bank details slip in the customer's name): the firm must check that the payment actually comes from that account; e-money wallets do not qualify, and for a card payment the firm checks that the card is not linked to an e-wallet and that the cardholder holds the account (para. 46). Biometrics and videoconference may be used if they meet R561-5-1 or R561-5-2 (para. 48).

Certified remote verification and EU guidelines

ANSSI certifies remote identity verification providers (prestataires de vérification d'identité à distance, PVID) against its requirements framework (v1.1 of 1 March 2021) and publishes the list of certified providers. A certified service checks the document's authenticity, detects that the user in the video is live, and compares the face with the document photo or with the photo in the document's chip. Only passports and identity cards of EU, EEA and Swiss nationals and listed residence permits and travel documents are accepted. The European Banking Authority's guidelines on remote customer onboarding (EBA/GL/2022/15), with which the ACPR has declared compliance for all obliged entities it supervises, apply since 2 October 2023 and require liveness detection in unattended flows, capture during the session, comparison with the document photo and time-stamped records.

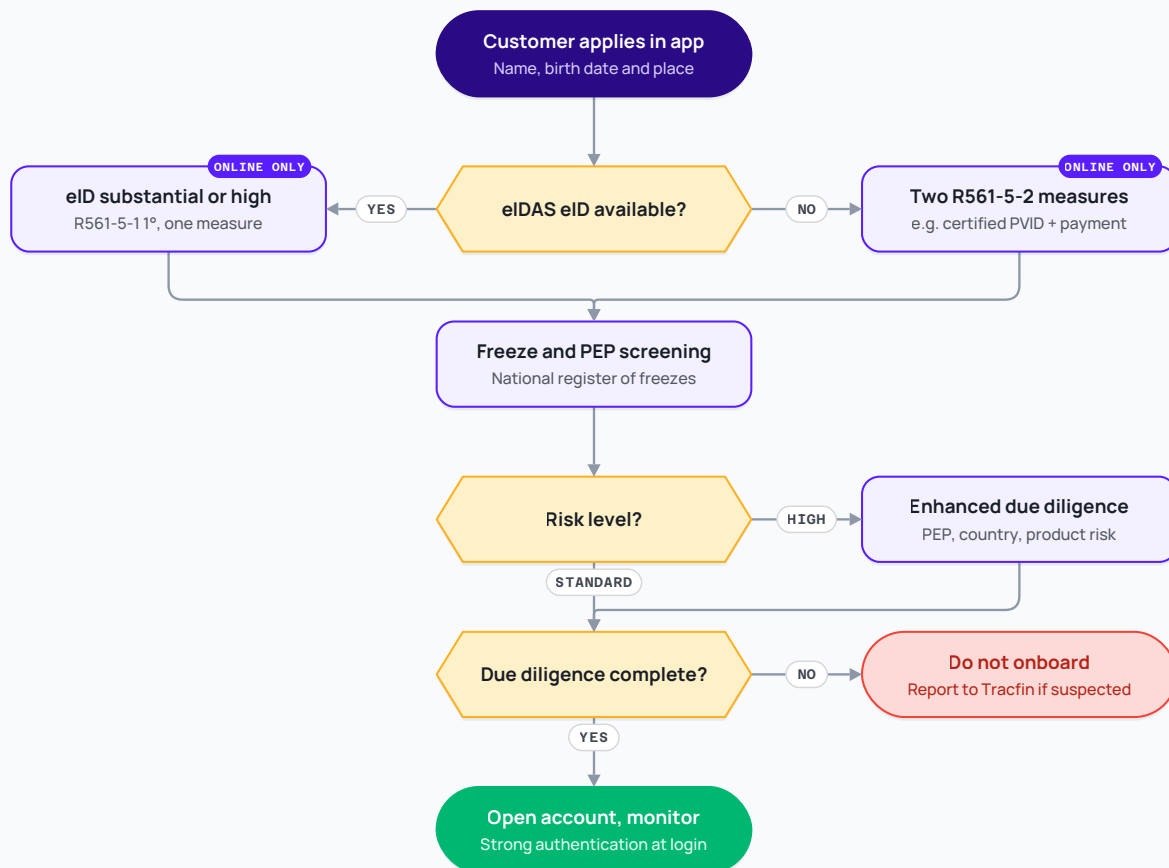


Figure 1. Remote onboarding of a retail customer by a French payment or e-money institution.

5

Digital channels: what's different

Bottom line: remote onboarding is not treated as higher risk in France, but it must use one of the verification methods the CMF lists, and a video call or a copied document alone never replaces meeting the customer in person.

Requirement	In person / land-based	Online / remote	Difference
Verification method	Original photo ID plus a copy	eIDAS substantial or high eID, or two listed measures	Differs
Video call	Not applicable	Not physical presence; usable only within listed measures	Differs

Risk classification	Risk-based	Risk-based; remote is not an automatic enhanced due diligence trigger	Same
Anonymous e-money	Up to €150 within the R561-16-1 conditions	Online payments over €50 need full due diligence	Differs
Account access	No statutory rule	Strong customer authentication for online access	Differs
Reliance on a third party's checks	Permitted; firm stays responsible	Permitted; firm stays responsible	Same
Suspicious transaction reporting	To Tracfin, no threshold	To Tracfin, no threshold	Same
Asset freezes	Apply without delay	Apply without delay	Same
Record retention	Five years	Five years; EBA expects time-stamped capture records	Same

Remote is not, by itself, high risk

Art. L561-10 CMF does not list non-face-to-face onboarding among its enhanced due diligence triggers; the ACPR guidelines treat the channel, including the internet, as one factor in the firm's risk classification.

Strong customer authentication

Payment service providers must apply strong customer authentication when the payer accesses a payment account online, initiates an electronic payment or acts remotely in a way that carries a fraud risk; for remote electronic payments, it must dynamically link the amount and the payee (art. L133-44 CMF).

Pending changes

The AMLR **Adopted, applies 10 Jul 2027** allows verification by an identity document plus reliable independent sources, or by eIDAS electronic identification at the substantial or high level (art. 22(6)). AMLA's final draft standard on customer due diligence

Draft, not adopted would allow other remote document-based solutions only where the customer cannot present a document in person and has no access to qualifying electronic identification, with documented justification.

Data protection and biometrics

Biometric data used to identify a person uniquely are sensitive data, prohibited unless an exception applies (GDPR art. 9; Informatique et Libertés law, art. 6). The CMF does not itself authorise face matching, so firms rely on explicit consent, which the CNIL considers valid only if "le recours à la biométrie" is not "imposé sans alternative" (biometrics are not imposed without an alternative); the eID and two-measure routes can serve as that alternative. The CNIL prefers templates stored on the user's device and treats selfie-to-document matching for remote account opening as authentication, not identification. An impact assessment is likely required for large-scale sensitive data (GDPR art. 35(3)(b)), and credit scoring and payment-fraud processing are on the CNIL's mandatory list. Face matching used only to confirm a claimed identity falls outside the AI Act's high-risk biometric category; creditworthiness scoring becomes high-risk from 2 December 2027.

Sector-specific obligations

Oversight of agents and distributors

The ACPR's December 2025 review of eight money transfer providers found agent oversight "largement perfectible" and expects risk-based agent controls and anti-money laundering training before agents start and every year.

Operational resilience

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) has applied since 17 January 2025 to payment institutions, account information service providers and e-money institutions, covering ICT risk, incident reporting and oversight of ICT providers such as onboarding vendors.

Instant payments

Under Regulation (EU) 2024/886, euro-area providers have had to offer payee verification since 9 October 2025, and instant transfer providers screen their own users against EU sanctions after each list change and at least daily, instead of screening each instant payment. Payment and e-money institutions must offer sending and receiving instant euro transfers by 9 April 2027 [Applies 9 Apr 2027](#).

Buy now, pay later

Ordonnance n° 2025-880 of 3 September 2025 transposes the revised EU Consumer Credit Directive and brings split and deferred payments within consumer credit rules, with stronger creditworthiness assessment and pre-contractual information

Adopted, effective 20 Nov 2026 .

8

Risk indicators and red flags

PAYMENT, E-MONEY AND MONEY TRANSFER TYPOLOGIES (ACPR AND TRACFIN)

- **Shared identifiers:** the same identity document or phone number used by several customers.
- **Multiple identities:** one customer operating under several identifiers.
- **Fan-out transfers:** one sender paying many beneficiaries.
- **Romance and pension fraud:** large transfers to Africa linked to romance scams or abuse of elderly people's pensions.
- **Shell companies:** newly created firms at a domiciliation or coworking address moving large sums quickly through payment accounts.
- **Prepaid cards:** cards reloaded with prepaid coupons, which Tracfin calls a favoured laundering and terrorist financing vehicle.
- **Organised networks:** patterns linked to organised crime detected by payment account managers.

9

Enforcement and penalties

The ACPR's Commission des sanctions may impose sanctions ranging from a warning or reprimand (blâme) to withdrawal of authorisation, and, instead or in addition, a fine of up to €100 million or 10% of annual net turnover for breaches of the anti-money laundering chapter, EU anti-money laundering rules and restrictive measures. Unauthorised activity is a criminal offence (section 2).

- **MoneyGram International SA (15 April 2026, procedure n° 2024-06):** a Belgian payment institution operating in France through an agent network (1,156 retail agents at the time of inspection) received a reprimand and a €1.3 million fine for inadequate

customer knowledge, miscalibrated monitoring, missing enhanced reviews, late and missing reports to Tracfin and weak agent oversight.

- **Treezor (9 April 2024)**: a reprimand and a €1 million fine for weak customer risk profiling and deficient transaction monitoring.

10 Recent changes and what to watch

- **10 July 2027**: **Adopted, applies 10 Jul 2027** the AMLR applies. Its e-money exemption (art. 19(7)) covers only non-reloadable instruments up to €150, narrower than today's French exemption.
- **20 November 2026**: **Adopted, effective 20 Nov 2026** consumer credit reform covering split and deferred payments. Buy now, pay later products need creditworthiness checks and new disclosures.
- **30 September 2026**: **Draft, not adopted** AMLA final report on the customer due diligence standard, to be sent to the European Commission. Remote document-based verification would become a justified fallback.
- **16 March 2026**: **In force** updated DG Trésor and ACPR asset-freeze guidelines. Screening must follow every list change; weekly batch screening is not enough.
- **1 January 2026**: **In force** AMLA takes over the EBA's anti-money laundering mandates; EBA guidelines stay in force until replaced.
- **9 October 2025**: **In force** payee verification and daily sanctions screening of users for euro instant transfers.
- **EU Payment Services Regulation**: **Political agreement, not adopted** the deal was agreed on 27 November 2025 and approved by Parliament's economic committee on 5 May 2026; it would require payee name and IBAN matching, make providers liable for fraud losses where prevention is inadequate and require refunds in some bank-impersonation scams.

11 What this means for identity verification

- **Offer an eID route first.** An eIDAS substantial or high identity (for example France Identité's digital identity, certified at the high level; FranceConnect admits banks case by case for their due diligence obligations) satisfies verification in one step, and the AMLR and the draft EU standard favour it.

- **Design the fallback as two measures.** Document capture alone is one measure; pair it with an ANSSI-certified service, a verified first payment from the customer's own account, or a qualified electronic signature.
- **Verify the first payment, not the account number.** Match the incoming payment to an account in the customer's name, and exclude e-money wallets.
- **Plan for 2027.** Reloadable anonymous e-money and default document-plus-selfie flows may need redesign under the AMLR and the draft standard.

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 chip reading, face match and biometric liveness, with time-stamped evidence for the five-year retention period.
- KYB and beneficial owner verification for business customers and merchants.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring, so new asset-freeze listings are picked up quickly.
- Transaction monitoring and configurable risk-based workflows built in the no-code workflow builder, with an audit trail for each check.
- E-signatures and phone and email verification to complete multi-measure remote verification flows.

[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, art. L561-4-1 to L561-14-2 (customer due diligence, including L561-5, L561-6, L561-8, L561-9, L561-9-1, L561-10, L561-12), Légifrance, versions in force at 29 October 2026, legifrance.gouv.fr
- Code monétaire et financier, art. R561-5 to R561-20-5 (identification and verification, R561-5-1, R561-5-2, R561-10, R561-16-1), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L561-2 (obliged entities), Légifrance, in force since 5 August 2026, legifrance.gouv.fr
- Code monétaire et financier, art. L561-15 and L561-15-1 (reporting to Tracfin), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L521-1 to L521-6-1 (payment service providers, L521-3), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L522-6 to L522-13 (payment institution authorisation), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. R522-1 and D522-1-1, Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L523-1 to L523-6 (agents), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L526-1 and following (e-money institutions, L526-7), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L572-5 and L572-13 (criminal penalties), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L612-39 (ACPR sanctions), Légifrance, in force since 10 April 2026, legifrance.gouv.fr
- Code monétaire et financier, art. L133-44 (strong customer authentication), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L562-4 (asset freezes), Légifrance, legifrance.gouv.fr
- Rapport au Président de la République relatif à l'ordonnance n° 2025-880 du 3 septembre 2025 relative au crédit à la consommation [report on the consumer credit ordinance], Journal officiel, legifrance.gouv.fr
- Regulation (EU) 2024/1624 (AMLR), art. 19(7), 22(6) and 90, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/886 (instant payments), art. 5a, 5c and 5d as inserted in Regulation (EU) 260/2012, EUR-Lex, eur-lex.europa.eu
- Proposal for a Regulation on payment services in the internal market, COM(2023) 367, procedure 2023/0210/COD, EUR-Lex, eur-lex.europa.eu
- AMLA, Final Report, Draft RTS under Article 28(1) AMLR, 30 September 2026, art. 6, 7 and 26, amla.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, paras 26, 41, 47 to 49, eba.europa.eu
- ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle [guidelines on identification, verification and customer knowledge], 16 December 2021 (page updated 24 September 2026), paras 35, 46, 48, acpr.banque-france.fr
- ACPR, Bilan des actions de contrôle portant sur le dispositif LCB-FT des acteurs de la transmission de fonds [review of money transfer providers' AML controls], December 2025, acpr.banque-france.fr
- ACPR Commission des sanctions, decision, procedure n° 2024-06 (MoneyGram International SA), 15 April 2026, acpr.banque-france.fr
- ACPR, "La Commission des sanctions de l'ACPR sanctionne la société Treezor", 16 April 2024, acpr.banque-france.fr
- Tracfin, "Quand et comment déclarer un soupçon ?" [when and how to report a suspicion], economie.gouv.fr
- Tracfin, LCB-FT : activité des professions déclarantes, bilan 2024 (Tome I), pp. 33 to 35, economie.gouv.fr
- ANSSI, Prestataires de vérification d'identité à distance (PVID), cyber.gouv.fr; Référentiels de qualification (PVID référentiel d'exigences v1.1), cyber.gouv.fr
- France Identité, press kit on the generalisation of France Identité, 2024, france-identite.gouv.fr
- FranceConnect, conditions générales d'utilisation v1.8 [user terms], applicable 20 February 2026, franceconnect.gouv.fr
- Direction générale du Trésor, "Le registre national des gels se transforme", 18 March 2021, tresor.economie.gouv.fr; Registre national des gels, gels-avoirs.dgtresor.gouv.fr
- Code monétaire et financier, art. R561-31 to D561-32-1 (content and transmission of reports, R561-31-1), Légifrance, legifrance.gouv.fr
- Arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement [prudential rules for payment institutions], art. 4, Légifrance, legifrance.gouv.fr
- Arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique [prudential rules for e-money institutions], art. 4, Légifrance, legifrance.gouv.fr
- Regulation (EU) 2022/2554 (DORA), art. 2 and 64, EUR-Lex, eur-lex.europa.eu
- ACPR, Avis: mise en œuvre des orientations de l'ABE sur l'utilisation de solutions d'entrée en relation d'affaires à distance (EBA/GL/2022/15) [notice implementing the EBA remote onboarding guidelines], 14 June 2023, acpr.banque-france.fr
- Lignes directrices conjointes de la Direction générale du Trésor et de l'ACPR sur la mise en œuvre des mesures de gel des avoirs [joint asset-freeze guidelines], version updated 16 March 2026, paras 122 to 126, acpr.banque-france.fr
- Tracfin, LCB-FT : état de la menace 2024-2025 (Tome III), case 16, pp. 45 to 46, economie.gouv.fr
- ANSSI, Prestataires de vérification d'identité à distance: référentiel d'exigences, v1.1, 1 March 2021, annex 4, cyber.gouv.fr

- FranceConnect, Conditions d'éligibilité (service providers), partenaires.franceconnect.gouv.fr
- Regulation (EU) 2016/679 (GDPR), art. 4(14), 9 and 35, EUR-Lex, eur-lex.europa.eu
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 6, Légifrance, legifrance.gouv.fr
- CNIL, Recommandation relative à l'authentification multifacteur [multi-factor authentication recommendation], adopted 20 March 2025, section 3.3, cnil.fr
- CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux [facial recognition paper], 15 November 2019, cnil.fr
- CNIL, Liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise [list of processing requiring an impact assessment], délibération n° 2018-327 of 11 October 2018 as amended by n° 2019-011, cnil.fr
- 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.europa.eu
- European Parliament, "Payment services deal: More protection from online fraud and hidden fees", 27 November 2025, europarl.europa.eu; Legislative Train, Payment services regulation, updated 20 September 2026, europarl.europa.eu
- INPI, FAQ on beneficial owners, inpi.fr