



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in the United Kingdom

COUNTRY United Kingdom

INDUSTRY Fintech & Digital Payments

LAST UPDATED 16 October 2026

KEY REGULATORS Financial Conduct Authority · Payment Systems Regulator · HM Revenue and Customs

Key takeaways

- Moving money or holding customer balances in the UK needs permission from the Financial Conduct Authority (FCA) first: a payment institution or electronic money (e-money) institution licence, or a lighter registration for small firms. Operating without one is a criminal offence.
- Every new customer must be identified and verified before the relationship starts. Onboarding through an app is allowed, and electronic identity checks count as valid evidence if they are secure and give enough confidence that the person is who they claim to be.
- Remote onboarding is not automatically high risk in the UK, but onboarding someone you never meet without safeguards is a risk factor you must manage. App-based payments also need strong customer authentication: two independent checks, such as a passcode plus the phone or a fingerprint.
- From 30 June 2026 the money laundering thresholds are in pounds: identity checks apply to one-off transfers over £800 and other one-off transactions of £12,000 or more, and the low-value e-money exemption is capped at £150.
- Expect more change: buy-now-pay-later lending became FCA-regulated on 15 July 2026, new safeguarding rules for customer funds apply from 7 May 2026, and the government plans to fold the Payment Systems Regulator into the FCA (this needs a new law, not yet passed).

The UK is open to app-only payment and e-money businesses, and remote onboarding is common. The rules are UK-wide: payment services, e-money and money laundering law apply in England and Wales, Scotland and Northern Ireland alike.

The FCA authorises and supervises payment and e-money institutions, including for anti-money laundering (AML). The Payment Systems Regulator sets the authorised push payment (APP) scam reimbursement rules, and HM Treasury writes the underlying regulations.

The biggest obstacle for a new entrant is authorisation itself: the FCA expects a UK head office, safeguarding arrangements for customer funds and financial crime controls that work at scale from launch.

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 for fintech and payments	Level	Official site
Financial Conduct Authority (FCA)	Authorises payment and e-money institutions and consumer credit firms; conduct rules, safeguarding, Consumer Duty; AML supervisor for e-money institutions and authorised firms	UK-wide	fca.org.uk
Payment Systems Regulator (PSR)	Payment systems; APP scam reimbursement requirement for Faster Payments and CHAPS	UK-wide	psr.org.uk
HM Treasury	Makes the Payment Services, E-Money and Money Laundering Regulations	UK-wide	gov.uk
HM Revenue and Customs (HMRC)	AML supervisor for money service businesses and certain payment providers not supervised by the FCA	UK-wide	gov.uk
National Crime Agency (UK Financial Intelligence Unit)	Receives suspicious activity reports	UK-wide	nationalcrimeagency.gov.uk

Office of Financial Sanctions Implementation (OFSI)	Financial sanctions list and enforcement	UK-wide	gov.uk
Information Commissioner's Office (ICO)	Data protection, including biometric data used in onboarding	UK-wide	ico.org.uk
Financial Ombudsman Service	Consumer complaints, including disputed payments and terminated accounts	UK-wide	financial-ombudsman.org.uk

2 Licensing and authorisation

Regulation 138 of the Payment Services Regulations 2017 (PSRs) prohibits providing payment services in the UK unless the provider is an authorised or small payment institution, a registered account information service provider, an e-money institution, a bank or another listed exempt body. Regulation 63 of the Electronic Money Regulations 2011 (EMRs) does the same for issuing e-money. Both offences carry up to two years' imprisonment on indictment.

Route	Typical business	Key condition	Initial capital
Authorised payment institution	Money remittance, acquiring, payment accounts, payment initiation	Full authorisation; safeguarding mandatory	€20,000 (remittance only), €50,000 (payment initiation), €125,000 (other services)
Small payment institution	Smaller payment or remittance firms	Monthly average payment volume over 12 months must not exceed €3 million; no account information or payment initiation services	None set by the PSRs
Authorised e-money institution	Wallets, prepaid cards, stored-value accounts	Full authorisation; safeguarding mandatory	€350,000

Small e-money institution	Smaller e-money issuers	Average outstanding e-money must not exceed €5 million; payment volume cap of €3 million a month	2% of average outstanding e-money where it reaches €500,000
Registered account information service provider	Open Banking data aggregation	Registration only	Not applicable
Consumer credit permission (FSMA Part 4A)	Lending apps, and buy-now-pay-later since 15 July 2026	FCA authorisation under the Financial Services and Markets Act 2000	Set by FCA rules

These euro amounts remain in the PSRs and EMRs as of October 2026; the 2026 sterling conversion applied only to the Money Laundering Regulations.

Agents and buy-now-pay-later

A payment institution may only act through an agent that the FCA has entered on the register, and the application must describe the agent's money laundering controls (PSRs regulation 34). Buy-now-pay-later agreements that were exempt from consumer credit regulation became regulated credit agreements on 15 July 2026 under the Financial Services and Markets Act 2000 (Regulated Activities etc.) (Amendment) Order 2025, as amended by a second 2025 Order. The Order provides a temporary permission route for firms that registered for it.

3

AML, KYC and customer due diligence

Payment institutions, e-money institutions and money service businesses are "financial institutions" and therefore relevant persons under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), regulation 10. The FCA supervises e-money institutions and authorised firms; HMRC supervises money service businesses and certain bill payment and telecommunication, digital and IT payment providers that the FCA does not supervise (regulation 7).

When customer due diligence applies

Under regulation 27, as amended from 30 June 2026, a firm must apply CDD when it:

Business relationship

Opens any account, wallet or ongoing relationship, at any value.

Occasional transfer

Executes a one-off transfer of funds over £800 (previously €1,000).

Occasional transaction

Carries out any other one-off transaction of £12,000 or more, single or linked (previously €15,000).

Suspicion or doubt

Suspects money laundering or terrorist financing, or doubts earlier identity information.

CDD means identifying and verifying the customer, any person acting for them and any beneficial owner, and understanding the purpose of the relationship (regulation 28). Since 18 November 2025 a firm cannot meet the beneficial ownership duty by relying solely on information filed at Companies House (regulation 28(9)). Monitoring must be ongoing.

Enhanced and simplified due diligence

Enhanced due diligence is mandatory for high-risk cases, for relationships or transactions involving a "FATF call for action country" (the term that replaced "high-risk third country" on 30 June 2026), for politically exposed persons, where false or stolen identity documents are detected and the firm continues, and for unusually complex or large transactions (regulation 33). Simplified due diligence is permitted only where the firm has assessed the risk as low (regulation 37). For pooled accounts opened from 30 June 2026, firms must also understand the account's purpose and intended use (regulation 29).

Reporting and records

Suspicions are reported to the National Crime Agency under Part 7 of the Proceeds of Crime Act 2002. A payment or e-money institution operating an account does not commit a money laundering offence for transactions involving criminal property below £3,000 (section 339A, raised from £1,000 on 31 July 2025), so a defence request is needed only above that amount. There is no general cash transaction reporting threshold. CDD and transaction records are kept for five years from the end of the relationship, with transaction records capped at ten years, then deleted unless an exception applies (regulation 40).

The MLRs do not list accepted documents. "Verify" means checking against documents or information from a reliable source independent of the customer, and documents issued by an official body count as independent even when the customer supplies them (regulation 28(18)). In practice this covers passports, national identity cards and driving licences, together with data checks against independent sources.

Regulation 28(19) expressly allows electronic identification: information can be treated as reliable and independent where it comes from an electronic identification process, including electronic identification means or a trust service, that is secure from fraud and misuse and gives the assurance needed to manage the money laundering risk. The MLRs set no specific liveness standard or assurance level. The FCA's Financial Crime Guide (FCG 3.2) asks firms how their approach gives confidence for non-face-to-face customers and how they test onboarding technology, and expects firms to understand the limits of electronic verification and cater for customers without common identity documents.

Verification must be completed before the relationship is established (regulation 30(2)). A financial institution may open an account first if no transactions are carried out until verification is complete (regulation 30(4)).

Reliance on other firms

A firm may rely on another regulated firm's CDD but remains liable for any failure, must obtain the information immediately and must be able to get copies of the evidence on request (regulation 39). Reliance on a firm in a FATF call for action country is not allowed. Using an identity verification vendor is outsourcing, not reliance: the firm stays fully responsible.

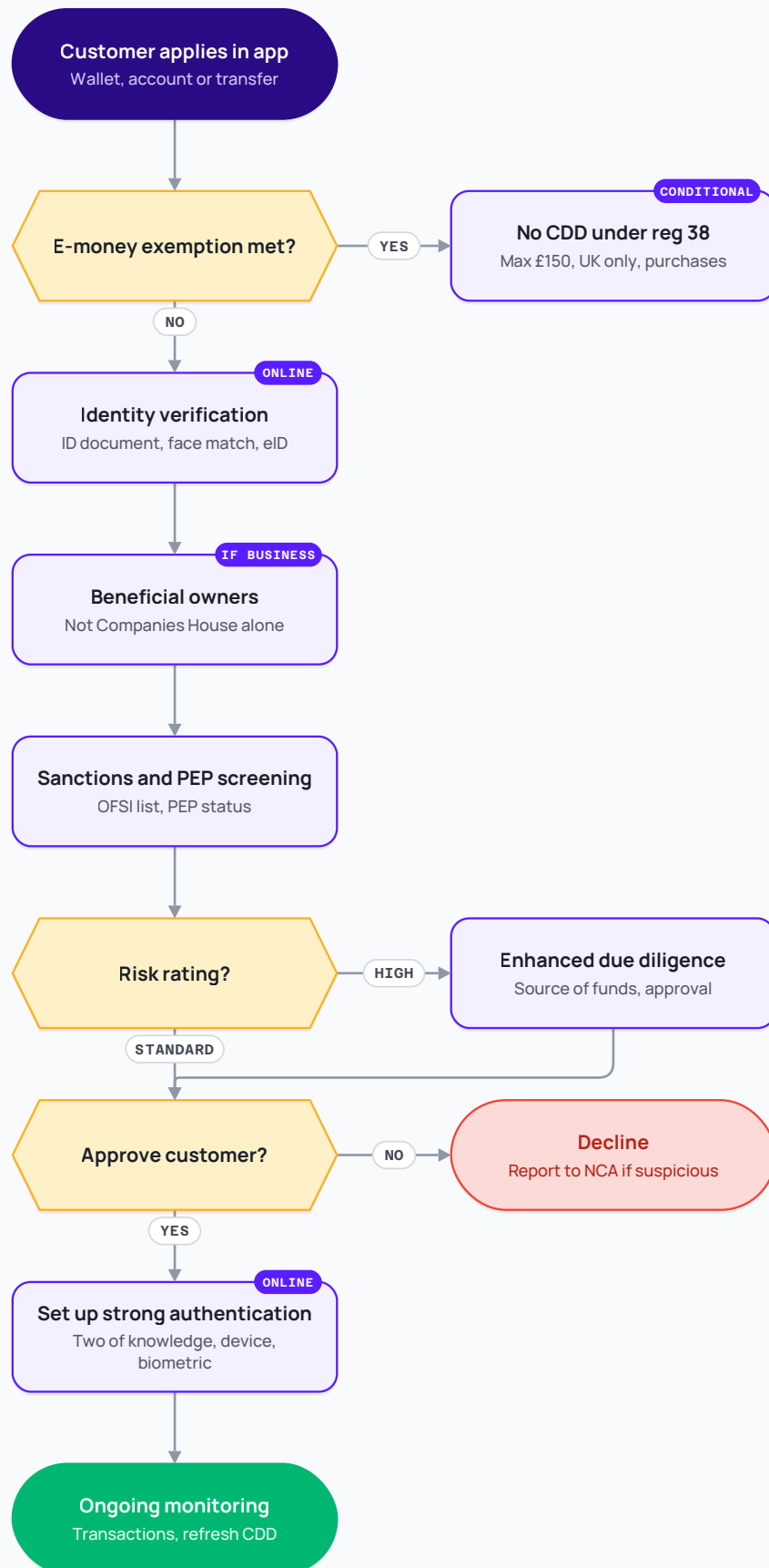


Figure 1. Remote onboarding for a UK payment or e-money app.

Bottom line: the AML rules are largely channel-neutral and allow electronic identification, but remote relationships without safeguards are a named risk factor, and strong customer authentication and the e-money remote redemption limit apply specifically to online activity.

Requirement	In person / agent	Online / remote	Difference
Licence needed	PI or EMI authorisation; agents must be registered	Same authorisation; no separate online licence	Same
When CDD applies	Relationship, transfer over £800, transaction of £12,000+	Same triggers	Same
Risk treatment	Assessed on customer, product and geography	Non-face-to-face without safeguards is a listed risk factor	Differs
Evidence accepted	Documents from reliable independent sources	Also electronic identification processes meeting reg 28(19)	Differs
Timing of verification	Before the relationship	Before the relationship	Same
E-money exemption	Cash redemption over £50 needs CDD	Remote payment over £50 per transaction needs CDD	Differs
Customer authentication	No SCA duty for physical counter cash	SCA for online account access and remote payments	Differs
Reliance and outsourcing	Firm remains liable	Firm remains liable	Same
Record retention	Five years after relationship ends	Five years after relationship ends	Same

Remote onboarding is a risk factor, not an automatic EDD trigger

MLRs regulation 33(6)(b)(iii) lists "non-face-to-face business relationships or transactions, without certain safeguards, such as an electronic identification process" meeting regulation 28(19) among the factors a firm must weigh. Robust electronic identification is the named safeguard. Enhanced due diligence is not automatic for app customers, but the firm must be able to show its supervisor that its controls match the risk (regulation 28(16)).

Strong customer authentication

PSRs regulation 100 requires strong customer authentication when a customer accesses a payment account online, initiates an electronic payment or acts through a remote channel in a way that may imply fraud risk. It must use two or more independent elements from knowledge, possession and inherence (regulation 2). Remote payments must be dynamically linked to the amount and payee. Exemptions are set in technical standards under regulation 106A.

Low-value e-money

Regulation 38 lets an e-money issuer skip CDD where the stored amount is at most £150, the instrument is non-reloadable or limited to £150 a month and usable only in the UK, it is used only to buy goods or services, and it is not funded by anonymous e-money. The exemption ends for cash redemptions over £50 and remote payment transactions over £50, and the issuer must still monitor for suspicious activity.

Certified digital identity services

The UK digital identity and attributes trust framework became the statutory trust framework for digital verification services under the Data (Use and Access) Act 2025 on 1 December 2025. Certification is voluntary for fintech firms; the MLRs test in regulation 28(19) still governs what counts as reliable evidence.

6 Data protection and biometrics

Identity data is governed by the UK GDPR and the Data Protection Act 2018, supervised by the ICO. Two points are specific to fintech onboarding:

- **AML purpose limitation.** Personal data obtained for the MLRs may be used only to prevent money laundering, terrorist financing or proliferation financing unless another

law permits or the customer consents, and new customers must be told this before onboarding (MLRs regulation 41).

- **Biometrics.** Biometric data used to uniquely identify a person is special category data under UK GDPR Article 9, so a selfie-to-document face match needs an Article 9 condition. The usual options are explicit consent or a Data Protection Act 2018 Schedule 1 condition, such as compliance with regulatory requirements relating to unlawful acts (paragraph 12). The ICO states its biometric recognition guidance is under review following the Data (Use and Access) Act 2025.

Retention follows MLRs regulation 40: delete identity data after the five-year period unless another law, legal proceedings or consent justify keeping it.

7 Sector-specific obligations

Safeguarding customer funds

Authorised payment institutions and all e-money institutions must safeguard customer funds, either by segregation or by insurance or a comparable guarantee (PSRs regulation 23, EMRs regulation 20); small payment institutions may opt in. From 7 May 2026, CASS 15 and CASS 10A of the FCA Handbook add rules on reconciliations, record keeping, third-party oversight, annual safeguarding audits and a resolution pack. Firms that safeguard must also send monthly safeguarding returns within 15 business days of month end.

Authorised push payment scams

Since 7 October 2024, the PSR's reimbursement requirement covers Faster Payments and CHAPS transfers by individuals, microenterprises and charities. Sending and receiving firms share reimbursement of up to £85,000 per claim, normally within five business days, and the firm must reach an outcome within 35 business days. An optional excess of up to £100 cannot be applied to vulnerable customers. A payer's provider may delay an outbound payment until the end of the fourth business day where it has reasonable grounds to suspect fraud, and must tell the payer why (PSRs regulation 86(2A) to (2D), inserted in October 2024).

Consumer Duty and account closures

The Consumer Duty (FCA Handbook PRIN 2A) applies to payment and e-money firms serving retail customers. For framework contracts entered into on or after 28 April 2026, a provider ending an open-ended contract must give at least 90 days' notice with specific

reasons and complaint routes (PSRs regulation 51B), subject to exceptions where other legal requirements prevail.

8

Risk indicators and red flags

FINTECH AND PAYMENTS RED FLAGS (FROM THE MLRS, FCA AND PSR)

- **Implausible onboarding data:** PO boxes, landmark addresses or foreign addresses with UK postcodes, as found in the FCA's 2025 Monzo enforcement.
- **Returning exited customers:** people opening new accounts after earlier accounts were closed for financial crime concerns.
- **False or stolen identity documents:** detected at onboarding or later, which triggers mandatory enhanced due diligence if the firm continues.
- **Mule-like inbound payments:** accounts receiving funds from unknown or unassociated third parties and moving them on quickly.
- **Anonymity-favouring products:** prepaid or reloadable instruments used to cash out or move value outside expected patterns.
- **High-risk geographies:** customers or counterparties in a FATF call for action country or a sanctioned jurisdiction.
- **Unusual transactions:** unusually complex or large payments, or patterns with no apparent economic purpose.

9

Enforcement and penalties

Under MLRs regulation 76 the FCA or HMRC may impose a penalty of whatever amount it considers effective, proportionate and dissuasive, publish a censure, and fine officers knowingly concerned. There is no statutory cap or per-violation tariff. The supervisor must take into account whether the firm followed FCA guidance or Treasury-approved guidance. Breaching a relevant requirement is also a criminal offence carrying up to two years' imprisonment (regulation 86). The FCA has separate penalty powers under the PSRs and EMRs, and providing payment services or issuing e-money without authorisation is a criminal offence.

The leading remote-onboarding case is the FCA's 8 July 2025 fine of £21,091,300 on Monzo Bank, after a 30% settlement discount. The FCA found the app-based bank's onboarding,

customer risk assessment and transaction monitoring did not keep pace with growth, that it accepted implausible addresses, and that it onboarded over 34,000 high-risk customers despite a restriction. The FCA's February 2025 letter to payments firms names financial crime controls, safeguarding and Consumer Duty implementation as supervisory priorities.

10 Recent changes and what to watch

- **6 October 2026:** HM Treasury's consultation on modernising payment services regulation, covering tokenised, Open Banking and agentic payments, closed.
Consultation closed, response pending Expect proposals to reshape the PSRs and EMRs.
- **15 July 2026:** buy-now-pay-later agreements became regulated credit. **In force**
Lenders need FCA permission or temporary permission.
- **30 June 2026:** Money Laundering and Terrorist Financing (Amendment) Regulations 2026 converted thresholds to sterling, added pooled account duties and introduced FATF call for action countries. **In force** Update CDD trigger logic and e-money tier limits.
- **7 May 2026:** CASS 15 safeguarding rules took effect. **In force** Daily-reconciliation, audit and resolution-pack processes are now rules.
- **28 April 2026:** 90-day notice with reasons for ending payment contracts. **In force**
Applies to contracts made from this date.
- **21 April 2026:** HM Treasury confirmed it will abolish the PSR and move its functions to the FCA through a Financial Services and Markets Bill. **Bill, not enacted** The PSR keeps its powers, including APP reimbursement, until the law is in force.
- **31 July 2025:** account-operating threshold under the Proceeds of Crime Act raised to £3,000. **In force** Fewer defence requests for low-value transactions.

11 What this means for identity verification

Onboarding flows should verify identity before any transaction, or use regulation 30(4) to open an account but block transactions until verification completes. Document checks combined with independent data or electronic identification satisfy regulation 28, provided the firm can show the process resists fraud; liveness and face matching are the usual way to link the person to the document remotely, and testing that technology is an FCA expectation. Biometric matching needs an Article 9 condition and a privacy notice including the MLRs regulation 41 statement.

Tiered wallets should apply the regulation 38 limits exactly, with full CDD triggered as soon as the stored balance, monthly limit or £50 redemption limit is exceeded. Business customers need beneficial owner verification beyond the Companies House register. Re-verification is required where the firm doubts earlier information, and risk refreshes should follow monitoring alerts. Evidence, including images and check results, should be kept for five years after the relationship ends and then deleted.

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 that verifies identity before the first transaction, with ID document capture and verification (including NFC), face match and biometric liveness.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring as lists change.
- KYB and beneficial owner verification for business customers, going beyond the Companies House register.
- A no-code workflow builder to apply risk-based tiers, such as low-value e-money limits and step-up to enhanced due diligence.
- Transaction monitoring and an audit trail of each check to support record keeping and supervisory review.

[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

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692), regulations 7, 10, 27, 28, 29, 30, 33, 37, 38, 39, 40, 41, 76 and 86, [legislation.gov.uk](https://www.legislation.gov.uk)
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2026 (SI 2026/621), made 9 June 2026, [legislation.gov.uk](https://www.legislation.gov.uk)
- The Payment Services Regulations 2017 (SI 2017/752), regulations 2, 14, 23, 34, 51B, 86, 100 and 138 and Schedule 3, [legislation.gov.uk](https://www.legislation.gov.uk)
- The Electronic Money Regulations 2011 (SI 2011/99), regulations 13, 20 and 63 and Schedule 2, [legislation.gov.uk](https://www.legislation.gov.uk)
- Proceeds of Crime Act 2002, section 339A, [legislation.gov.uk](https://www.legislation.gov.uk); Proceeds of Crime (Money Laundering) (Threshold Amount) (Amendment) Order 2025 (SI 2025/877), [legislation.gov.uk](https://www.legislation.gov.uk)
- The Financial Services and Markets Act 2000 (Regulated Activities etc.) (Amendment) Order 2025 (SI 2025/859), [legislation.gov.uk](https://www.legislation.gov.uk); (Amendment) (No. 2) Order 2025 (SI 2025/1154), [legislation.gov.uk](https://www.legislation.gov.uk)
- UK GDPR, Article 9, [legislation.gov.uk](https://www.legislation.gov.uk); Data Protection Act 2018, Schedule 1 Part 2, [legislation.gov.uk](https://www.legislation.gov.uk)
- FCA Handbook, CASS 15 Payment services and electronic money: relevant funds (effective 7 May 2026), [handbook.fca.org.uk](https://www.handbook.fca.org.uk)
- FCA Handbook, PRIN 2A The Consumer Duty, [handbook.fca.org.uk](https://www.handbook.fca.org.uk)
- FCA Handbook, FCG 3.2 Financial Crime Guide: money laundering, [handbook.fca.org.uk](https://www.handbook.fca.org.uk)
- FCA, Safeguarding requirements for payment and e-money institutions, [fca.org.uk](https://www.fca.org.uk)
- FCA, Priorities for payments portfolio firms, letter of February 2025, [fca.org.uk](https://www.fca.org.uk) (PDF)
- FCA, FCA fines Monzo £21m for failings in financial crime controls, press release, July 2025, [fca.org.uk](https://www.fca.org.uk)
- Payment Systems Regulator, APP fraud reimbursement protections, [psr.org.uk](https://www.psr.org.uk)
- HM Treasury, A Streamlined Approach to Payment Systems Regulation: consultation and response (21 April 2026), [gov.uk](https://www.gov.uk)
- Regulatory Policy Committee, RPC opinion: impact of Financial Services and Markets Bill (4 June 2026), [gov.uk](https://www.gov.uk)
- HM Treasury, Modernising Payment Services Regulation, consultation, 14 July to 6 October 2026, [gov.uk](https://www.gov.uk)
- DSIT, UK digital identity and attributes trust framework (0.4), page updated 9 June 2026, [gov.uk](https://www.gov.uk)
- ICO, Biometric data guidance: Biometric recognition, [ico.org.uk](https://www.ico.org.uk)