



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in the United Kingdom

COUNTRY United Kingdom

INDUSTRY Banking & Digital Banking

LAST UPDATED 16 October 2026

KEY REGULATORS Prudential Regulation Authority · Financial Conduct Authority · HM Treasury (Office of Financial Sanctions Implementation)

Key takeaways

- Taking deposits in the UK requires authorisation from the Prudential Regulation Authority (PRA), which can only grant it with the Financial Conduct Authority's (FCA) consent. A complete application gets a decision within six months; new banks can start in a restricted "mobilisation" phase capped at £50,000 of deposits.
 - Fully remote account opening is allowed. Online onboarding is a risk factor rather than an automatic trigger for enhanced checks, provided the identity process is secure against fraud and gives enough assurance that the applicant is who they claim to be.
 - A bank may open an account before identity verification is finished, but no money can move until verification is complete.
 - Money laundering rules changed on 30 June 2026: euro thresholds became sterling, new checks apply to pooled accounts, and a new rule lets banks onboard customers of a failed bank quickly. A further change for crypto correspondent relationships applies from 1 February 2027.
 - Face matching during onboarding is "special category" biometric data under UK data protection law, so banks need a specific legal condition, a data protection impact assessment and a non-biometric alternative where they rely on consent.
-

The UK is open to digital-only banks, and the regime is the same for app-based and branch-based banks: there is no separate digital banking licence. Authorisation is dual. The PRA judges safety and soundness, the FCA judges conduct and financial crime controls, and the FCA also supervises every bank's anti-money laundering compliance.

The biggest practical obstacle for a new entrant is not the licence itself but proving that financial crime controls will keep pace with growth. A recent FCA fine against a digital bank turned on onboarding controls that accepted thin or implausible customer information at scale.

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

Financial services, anti-money laundering (AML), sanctions and data protection law apply across the whole UK (England and Wales, Scotland and Northern Ireland). There is no separate devolved banking regulator.

Regulator	Remit for banks	Level	Official site
Prudential Regulation Authority (Bank of England)	Authorises deposit-takers; capital, liquidity, deposit protection rules	UK-wide	bankofengland.co.uk
Financial Conduct Authority	Conduct, consents to authorisation, AML supervisor for banks under the Money Laundering Regulations	UK-wide	fca.org.uk
HM Treasury and the Office of Financial Sanctions Implementation (OFSI)	AML legislation; financial sanctions and reporting	UK-wide	gov.uk/ofsi
National Crime Agency, UK Financial Intelligence Unit	Receives suspicious activity reports; decides on defence requests	UK-wide	nationalcrimeagency.gov.uk
Information Commissioner's Office (ICO)	Data protection, including biometric data in onboarding	UK-wide	ico.org.uk

Office for Digital Identities and Attributes (OfDIA)	Statutory trust framework and register for digital verification services	UK-wide	gov.uk/ofdia
Companies House	Register of beneficial owners (people with significant control); identity verification of directors	UK-wide	gov.uk/companies-house

The Payment Systems Regulator and the Financial Ombudsman Service also oversee banks' payment and complaint handling.

2 Licensing and authorisation

Accepting deposits by way of business is a regulated activity. Carrying it on without permission breaches the general prohibition in the Financial Services and Markets Act 2000 (FSMA) and is an offence under section 23, punishable on indictment by up to two years' imprisonment, a fine or both.

Authorisation is dual. The PRA decides the application but may only authorise with the FCA's consent, and a successful bank receives a Part 4A permission. Both regulators test the firm against their threshold conditions: a UK-incorporated bank must keep its head office in the UK, hold appropriate financial and non-financial resources, be fit and proper and be capable of effective supervision. The PRA sets capital and liquidity requirements from the firm's own capital and liquidity assessments, and requires proof that capital is in place before authorisation.

Timeline

The regulators have six months to decide a complete application and twelve months for an incomplete one. An optional pre-application stage of three meetings comes first.

Mobilisation

New banks may be authorised with restrictions for up to twelve months, with total deposits capped at £50,000, while they finish building systems.

People

At minimum a chief executive, a chair and one other executive senior manager must be approved under the Senior Managers Regime at authorisation.

The Bank of England's application guidance asks for the customer journey, including onboarding and know-your-customer processes, and for early drafts of the financial crime policy even before mobilisation. Eligible deposits are protected by the Financial Services Compensation Scheme up to £120,000 per depositor per bank for failures on or after 1 December 2025.

3

AML, KYC and customer due diligence

Banks are credit institutions and therefore "relevant persons" under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the MLRs). The FCA's Handbook adds binding systems and controls rules in SYSC 6.3: a director or senior manager must hold overall responsibility for AML, and a money laundering reporting officer must be appointed with sufficient authority and independence.

When customer due diligence applies

Customer due diligence (CDD) is required when a bank establishes a business relationship, carries out an occasional transaction of £12,000 or more, or an occasional transfer of funds above £800, suspects money laundering, or doubts earlier identification data (regulation 27). CDD means identifying and verifying the customer from reliable, independent sources, understanding the purpose of the relationship and, for companies, verifying name, registration number and registered office and taking reasonable measures to understand ownership and control (regulation 28). Beneficial owners must be identified and verified on a risk basis, and banks cannot rely solely on the Companies House register to do so.

Enhanced due diligence

Enhanced due diligence (EDD) is mandatory for high-risk cases, customers established in a country on the Financial Action Task Force call for action list, correspondent relationships with third-country institutions, politically exposed persons (PEPs), customers who supplied false or stolen identity documents, and transactions that are unusually complex

or unusually large given their nature (regulation 33). For domestic PEPs, the starting point is a lower level of risk than for foreign PEPs (regulation 35(3A)). Banks must not set up anonymous accounts or deal with shell banks (regulations 29 and 34).

Reporting and records

Reporting is suspicion-based under Part 7 of the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000. Where a bank needs a defence before handling suspected criminal property, the National Crime Agency has a notice period of seven working days, followed by a 31-day moratorium if consent is refused (POCA section 335). Since 31 July 2025, banks may process transactions on an account involving suspected criminal property below £3,000 without a defence request. CDD records must be kept for five years after the relationship ends, transaction records for no more than ten years, and personal data then deleted (regulation 40).

4

Identity verification and onboarding

The MLRs do not list mandatory documents. "Verify" means confirming identity on the basis of documents or information from a reliable source independent of the customer; documents issued by an official body count as independent even when the customer supplies them (regulation 28(18)). Information from an electronic identification process also counts, if the process is secure from fraud and misuse and gives assurance that the person is who they claim to be to the degree the money laundering risk requires (regulation 28(19)).

The FCA has regard to whether a bank followed the HM Treasury-approved guidance of the Joint Money Laundering Steering Group when judging its controls (SYSC 6.3.5), and courts must consider such guidance in criminal proceedings (MLR regulation 86(2)). SYSC 6.3.7 also expects identification procedures not to deny access unreasonably to people who cannot produce detailed evidence of identity.

Banks may rely on another UK regulated firm, or an equivalent overseas firm, to carry out CDD, but remain liable for any failure and must be able to obtain the underlying data immediately (regulation 39). Using a technology vendor is outsourcing, not reliance, and liability stays with the bank. Corporate onboarding gets easier as Companies House identity verification of directors and people with significant control takes effect; its transition year ends in November 2026.

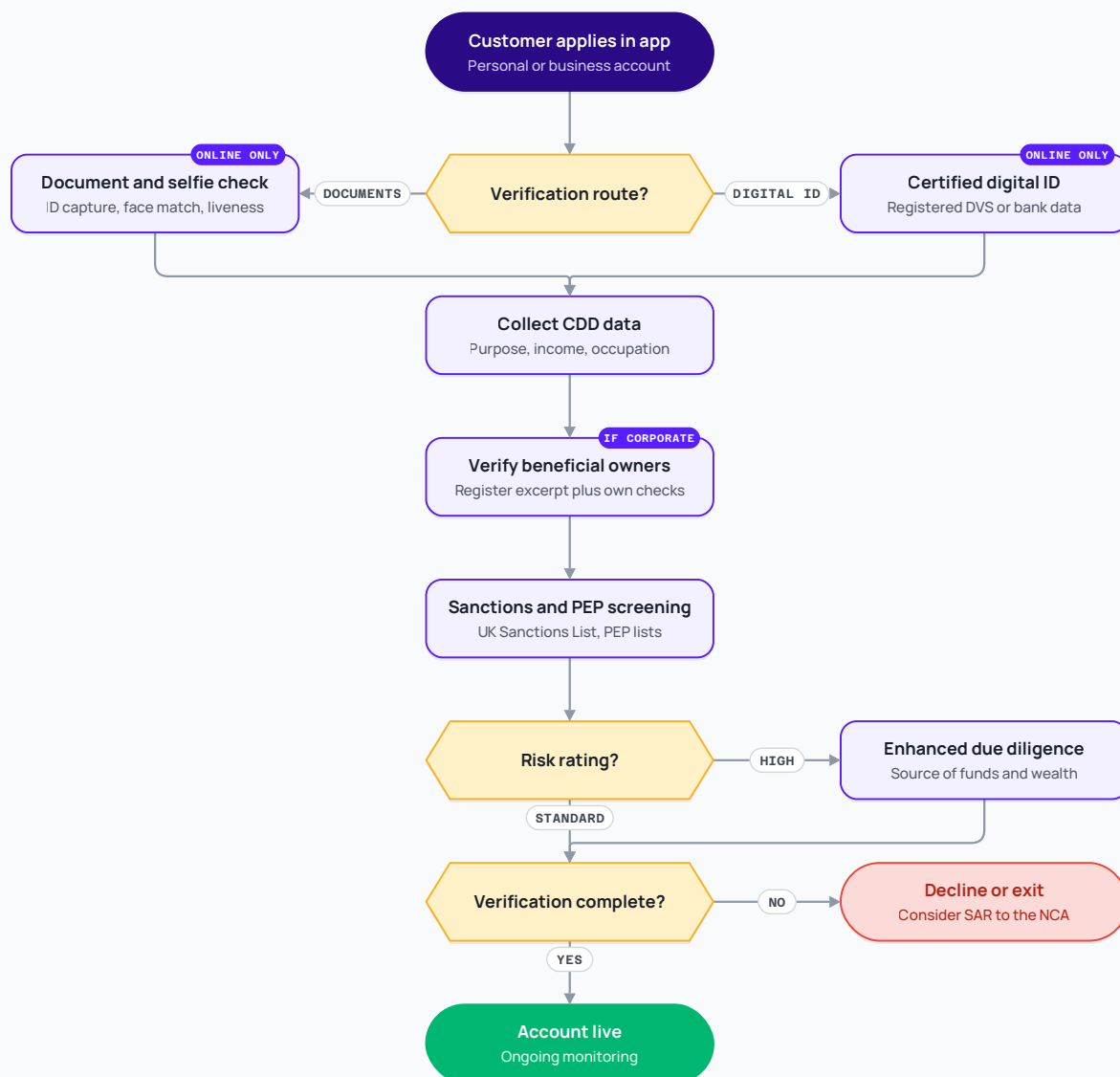


Figure 1. Remote personal and business account opening at a UK bank.

5

Digital channels: what's different

Bottom line: the rules are channel-neutral, but a remote relationship becomes a higher-risk factor unless the bank uses an electronic identification process that is secure from fraud and gives sufficient assurance of identity.

Requirement	In person / branch	Online / remote	Difference
-------------	--------------------	-----------------	------------

Licence	PRA authorisation with FCA consent	Same authorisation; no digital-only licence	Same
Permission to onboard remotely	Not applicable	Permitted under the MLRs	Same
Risk treatment	Risk-based	Non-face-to-face is a risk factor unless safeguards apply (reg 33(6)(b)(iii))	Differs
Accepted evidence	Official documents, independent sources	Also electronic identification meeting reg 28(19)	Differs
Timing of verification	Before relationship; account may open first with no transactions	Same rule (reg 30)	Same
Reliance on third parties	Permitted, bank stays liable	Same; vendors are outsourcing	Same
Biometric data	Rarely processed	Face matching is special category data	Differs
Record retention	Five years after relationship ends	Same, including digital evidence	Same

Electronic identification as a safeguard

Regulation 33(6)(b)(iii) lists non-face-to-face relationships "without certain safeguards" as a risk factor, and names an electronic identification process meeting regulation 28(19) as such a safeguard. A bank that uses a strong remote process therefore need not treat every app customer as high risk. Regulation 33(7) adds that one risk factor does not on its own make a situation high risk.

Speed versus completeness

The FCA's review of challenger banks found that fast onboarding attracted money mule networks and that most firms did not collect income or occupation, leaving them unable to assess the purpose of the relationship. It also found that transaction monitoring cannot substitute for CDD at onboarding. Good practice it observed included video selfies, mobile geolocation data, passport images, fraud database checks and monitoring of customers using multiple devices.

Certified digital identity

Part 2 of the Data (Use and Access) Act 2025 created a statutory trust framework and public register for digital verification services, in force since 1 December 2025. Version 1.0 of the framework, published on 9 June 2026, was due to take effect from 1 September 2026 subject to accreditation of certification bodies. OfDIA says it is working with AML regulators on guidance for using registered services in customer due diligence; the MLRs do not yet require certified providers.

Proposed, consultation closed 5 May 2026 The government's national digital ID proposal would add a government-issued credential; there would be no legal obligation to hold or present it.

6 Data protection and biometrics

The UK GDPR and Data Protection Act 2018 apply, supervised by the ICO. The MLRs restrict use of CDD data to preventing money laundering, terrorist financing and proliferation financing unless another law or the customer's consent allows more, and require a statement to that effect before onboarding (regulation 41).

The ICO's biometric recognition guidance (February 2024) treats face matching of a selfie against an ID photo as special category biometric data from the moment of collection. It says a data protection impact assessment is highly likely to be required, biometric data must be encrypted, retention periods must be clear, and explicit consent is likely to be the most appropriate condition in many cases, with a non-biometric alternative offered. Regulation 41(8) of the MLRs points to the Schedule 1 conditions of the 2018 Act for sensitive processing done for AML purposes; the ICO accepts that the prevention or detection of unlawful acts condition can apply where the processing is necessary and an appropriate policy document is in place. Banks should document which condition they rely on.

7 Sector-specific obligations

Pooled accounts

In force 30 June 2026 For new pooled accounts, banks must understand the purpose and intended use, assess the risk, and consider controls on the account. The account holder must supply the identity of underlying customers on request and keep records of payments for five years (regulation 29(10) to (18)).

Customers of a failed bank

In force 30 June 2026 Within 30 days of a bank insolvency order, a credit institution may let former customers of the failed bank open and use an account after identifying them but before completing verification, provided full CDD follows as soon as practicable (regulation 30ZA).

Correspondent banking and sanctions

Correspondent relationships with third-country institutions require information on the respondent's business, its supervision and AML controls, senior management approval and documented responsibilities (regulation 34). As a firm with Part 4A permission, a bank is a "relevant firm" that must report known or suspected designated persons, breaches and frozen assets to OFSI as soon as practicable, and report frozen assets held at 30 September each year by 30 November.

Failure to prevent fraud

Since 1 September 2025, large organisations, including banks, commit an offence if an associated person commits a specified fraud for their benefit and they lacked reasonable fraud prevention procedures (Economic Crime and Corporate Transparency Act 2023).

Risk indicators and red flags

DIGITAL BANKING TYPOLOGIES (FCA FINDINGS AND MLR RISK FACTORS)

- **Money mule recruitment:** fast app onboarding used to open accounts that move stolen funds.
- **Implausible addresses:** landmarks, PO boxes or foreign addresses with UK postcodes.
- **Repeat applicants:** customers exited for financial crime reopening accounts under the same or new details.
- **Multiple devices:** one customer operating an account from many devices, or many customers from one.
- **Profile mismatch:** turnover inconsistent with stated income or occupation.
- **Unassociated payers:** payments received from unknown or unassociated third parties (MLR regulation 33(6)(b)(iv)).
- **Pooled account misuse:** client money accounts receiving unvetted funds from unknown third parties.

Enforcement and penalties

The FCA can fine banks without limit under FSMA and the MLRs. Under DEPP 6.5A it calculates a penalty in five steps: disgorgement of any benefit, a seriousness figure of 0% to 20% of revenue from the business area during the breach, adjustment for aggravating and mitigating factors, an uplift for deterrence where needed, and a 30% discount for early settlement. Breaching a relevant MLR requirement is also a criminal offence carrying up to two years' imprisonment (regulation 86), with a defence of having taken all reasonable steps.

In July 2025 the FCA fined Monzo £21,091,300 for inadequate financial crime controls between 2018 and 2020, including onboarding customers with obviously implausible information, and for opening over 34,000 accounts for high-risk customers while a requirement prohibited it.

10 Recent changes and what to watch

- **November 2026** **In force, transition ending** Companies House's 12-month identity verification transition for directors and people with significant control ends; verified status becomes the norm in business onboarding.
- **9 June 2026** **Adopted, effective 1 Sep 2026 subject to accreditation** Digital verification services trust framework 1.0 published.
- **30 June 2026** **In force** MLR amendments (SI 2026/621): sterling thresholds, pooled accounts, failed-bank customers and revised EDD triggers.
- **1 February 2027** **Adopted, effective 1 Feb 2027** EDD for crypto exchange and custodian correspondent relationships (regulation 34A); relevant to banks serving those firms.
- **10 March 2026** **Proposed, consultation closed** National digital ID consultation; a government response is awaited.
- **1 December 2025** **In force** Deposit protection limit rose to £120,000.
- **31 July 2025** **In force** POCA threshold for operating accounts with suspected criminal property raised to £3,000.

11 What this means for identity verification

Design the remote journey so that it qualifies as a safeguard under regulation 28(19): document authenticity checks, face match and liveness detection, or a certified digital verification service, with assurance matched to the product's risk. Collect purpose, income and occupation at onboarding, because the FCA treats their absence as a CDD failure. Validate addresses and detect duplicate applicants and device anomalies. Allow accounts to open before verification completes only if transactions are blocked until it does.

For business accounts, take a register excerpt, verify beneficial owners independently and report material discrepancies to Companies House. Keep verification evidence for five years after the relationship ends, record the data protection condition used for biometrics, offer a non-biometric route, and re-run CDD when circumstances change or doubts about earlier data arise.

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.
- KYB and beneficial owner verification for business accounts.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring.
- KYC questionnaires to collect purpose, income and occupation, and a no-code workflow builder for risk-based EDD routes.
- Cloud, on-premises or hybrid deployment with an audit trail of every check.

[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 27 to 41 and 86, legislation.gov.uk, legislation.gov.uk
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2026 (SI 2026/621), made 9 June 2026, legislation.gov.uk
- Proceeds of Crime Act 2002, section 335, legislation.gov.uk
- The Proceeds of Crime (Money Laundering) (Threshold Amount) (Amendment) Order 2025 (SI 2025/877), legislation.gov.uk
- Financial Services and Markets Act 2000, Part II, section 23, legislation.gov.uk
- FCA Handbook, SYSC 6.3 Financial crime, handbook.fca.org.uk
- FCA Handbook, DEPP 6.5A The five steps for penalties imposed on firms, handbook.fca.org.uk

- Bank of England, New bank authorisation process, updated 2 February 2026, bankofengland.co.uk
- Bank of England, PRA confirms FSCS deposit limit to be increased to £120,000, 18 November 2025, bankofengland.co.uk
- FCA, Financial crime controls at challenger banks, multi-firm review, fca.org.uk
- FCA, FCA fines Monzo £21m for failings in financial crime controls, 8 July 2025, fca.org.uk
- ICO, Biometric data guidance: biometric recognition, version 1.0, 23 February 2024, ico.org.uk
- OfDIA 2026 Annual Report on the operation of Part 2 of the Data (Use and Access) Act 2025, 14 July 2026, gov.uk
- Cabinet Office, Making public services work for you with your digital identity, consultation, 10 March 2026, gov.uk
- Companies House, Verify your identity for Companies House, updated 30 April 2026, gov.uk
- OFSI, Reporting information to OFSI: what to do, updated 17 July 2025, gov.uk
- Home Office, Offence of failure to prevent fraud introduced by ECCTA, updated 10 October 2025, gov.uk