



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in the United Kingdom

COUNTRY United Kingdom

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 16 October 2026

KEY REGULATORS Financial Conduct Authority · HM Treasury · Office of Financial Sanctions
Implementation

Key takeaways

- Any business that exchanges or holds crypto for customers in the UK must register with the Financial Conduct Authority (FCA) before it starts trading. The FCA actively shuts down and prosecutes unregistered operators.
 - A second, fuller licence regime starts on 25 October 2027. Every crypto firm, including those already registered, must apply for FCA authorisation; the application window runs from 30 September 2026 to 28 February 2027, and there is no automatic conversion.
 - Every customer must be identified and verified before they are onboarded. Onboarding entirely online is allowed, but it counts as a higher-risk factor unless the electronic identity check is secure and reliable.
 - Before a retail customer's first purchase, the app must show a personalised risk warning, wait at least 24 hours, classify the investor and test their knowledge. Crypto transfers must carry sender and recipient details (the "Travel Rule"), with extra data from £800.
 - From 1 January 2026, platforms must also collect tax details (such as a National Insurance number) from every user and report them to HM Revenue and Customs (HMRC), with the first report due by 31 May 2027.
-

The UK is open to crypto businesses, but tightly gated. Today the FCA supervises crypto firms for anti-money laundering purposes and polices how crypto is marketed to consumers; from October 2027 it will authorise and supervise them in the same way as other financial firms. HM Treasury writes the underlying rules, the Office of Financial Sanctions Implementation (OFSI) enforces sanctions, and HMRC collects tax data.

The biggest obstacle for a new entrant is timing. A firm that is not registered today and does not apply for authorisation in the current window faces a narrow route into the market, and firms that do not apply at all must wind down their UK business before the new regime starts.

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

Crypto regulation is UK-wide: the Money Laundering Regulations, the Financial Services and Markets Act 2000 and sanctions law apply equally in England and Wales, Scotland and Northern Ireland.

Regulator	Remit for crypto firms	Level	Official site
Financial Conduct Authority (FCA)	Registration and anti-money laundering supervision under the Money Laundering Regulations; financial promotions; authorisation under the new regime from 25 October 2027	UK-wide	fca.org.uk
HM Treasury	Makes the Money Laundering Regulations and the cryptoasset legislation under the Financial Services and Markets Act 2000	UK-wide	gov.uk
Office of Financial Sanctions Implementation (OFSI)	Financial sanctions, mandatory breach reporting by crypto firms	UK-wide	gov.uk
National Crime Agency (UK Financial Intelligence Unit)	Receives suspicious activity reports	UK-wide	nationalcrimeagency.gov.uk

HM Revenue and Customs (HMRC)	Cryptoasset Reporting Framework: collection and reporting of users' tax data	UK-wide	gov.uk
Bank of England	Joint approach with the FCA to stablecoin issuers recognised as systemic	UK-wide	bankofengland.co.uk
Information Commissioner's Office (ICO)	Data protection, including biometric data used in onboarding	UK-wide	ico.org.uk

2 Licensing and authorisation

Today: registration under the Money Laundering Regulations In force

A cryptoasset exchange provider (exchanging crypto for money or for other crypto, including as issuer, and operating crypto ATMs) or a custodian wallet provider (safeguarding crypto or private keys for customers) that acts by way of business in the UK must register with the FCA before starting any in-scope service ([MLRs reg. 14A](#); [FCA, Cryptoassets: AML/CTF regime](#)). Registration is not an endorsement, and firms must not suggest it is. Because most cryptoassets are not specified investments, customers usually lack access to the Financial Ombudsman Service and the Financial Services Compensation Scheme, and firms must say so before starting a relationship or transaction ([reg. 60A](#)). Registered firms file an annual financial crime return (REP-CRIM) within 60 business days of their accounting reference date.

Anyone acquiring or increasing control of a registered firm must notify the FCA and wait for approval; completing the deal without approval is a criminal offence. Since 30 June 2026 the change-in-control test also captures holdings of 10% or more of shares or voting power, aligning it with the authorisation regime ([SI 2026/621, reg. 37](#)).

From 25 October 2027: authorisation under FSMA Adopted, effective 25 Oct 2027

The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 ([SI 2026/102](#)), made on 4 February 2026, create new regulated activities. Trading platforms, intermediaries, custodians, stablecoin issuers and firms arranging staking will need FCA authorisation, and the FCA published its final rules on 30 June 2026, applying the Consumer Duty and capital and stress-testing requirements to crypto firms ([FCA, 30 June 2026](#)).

Apply in the window

The application period opened on 30 September 2026 and closes on 28 February 2027. If the FCA has not decided an application by commencement, a saving provision lets the firm keep trading until it is finally determined.

Apply late

A firm that applies after 28 February 2027 but is not authorised by 25 October 2027 enters a transitional provision: it may only service pre-existing contracts and cannot take on new UK customers.

Do not apply

The firm must run off its UK business before 25 October 2027 or risk breaching the general prohibition in section 19 of the Act.

Registered firms are not converted automatically; already-authorised firms must vary their permissions ([FCA, How the gateway will operate](#)). The FCA advises against applying for registration after 31 July 2027, because its three-month determination period would run past commencement ([FCA, Registration under the MLRs ahead of the new regime](#)). Security tokens are already specified investments, so firms dealing in them need authorisation today.

3

AML, KYC and customer due diligence

Cryptoasset exchange providers and custodian wallet providers are relevant persons under [reg. 8\(2\)\(j\) and \(k\)](#) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), and the FCA is their supervisor ([reg. 7](#)). The core duties are:

Customer due diligence (CDD)

Identify and verify the customer, understand the purpose of the relationship, identify beneficial owners and take reasonable measures to verify them, and verify anyone acting on the customer's behalf ([reg. 28](#)). The Companies House register alone is not enough for beneficial ownership ([reg. 28\(9\)](#)).

Enhanced due diligence (EDD)

Mandatory for high-risk cases, politically exposed persons, customers using false or stolen identity documents, unusually complex or large transactions, and relationships with countries on the FATF "call for action" list ([reg. 33](#)). The FATF list test replaced the broader high-risk third country test on 30 June 2026.

Ongoing monitoring and reporting

Scrutinise transactions, including source of funds where necessary (reg. 28(11)). A nominated officer must receive internal reports, and suspicions go to the National Crime Agency under Part 7 of the Proceeds of Crime Act 2002 or Part 3 of the Terrorism Act 2000 ([reg. 19\(4\)\(d\)](#), reg. 21(3)).

Record keeping

Keep CDD and Travel Rule records for five years from the end of the relationship or the occasional transaction, with a ten-year cap for transaction records, then delete personal data unless another basis applies ([reg. 40](#)).

From 1 February 2027, a new **Adopted, effective 1 Feb 2027** reg. 34A requires crypto firms with correspondent relationships with third-country crypto providers to gather information on the respondent, assess its controls, obtain senior management approval and avoid shell banks ([SI 2026/621, reg. 20](#)).

4

Identity verification and onboarding

The MLRs do not prescribe a document list. Verification must use 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 (reg. 28(18)). Information from an electronic identification process, including an electronic identification means or a trust service, also qualifies, provided the process is secure from fraud and misuse and gives assurance that the person is who they claim to be to the degree needed to manage the money laundering risk (reg. 28(19)). Verification that a person acting for a customer is authorised to do so is required separately (reg. 28(10)).

A firm may rely on another regulated firm's CDD, or use an outsourced identity provider, but it remains liable for any failure and must be able to obtain the underlying identity data immediately on request ([reg. 39](#)). Reliance on a third party established in a FATF call-for-action country is not allowed.

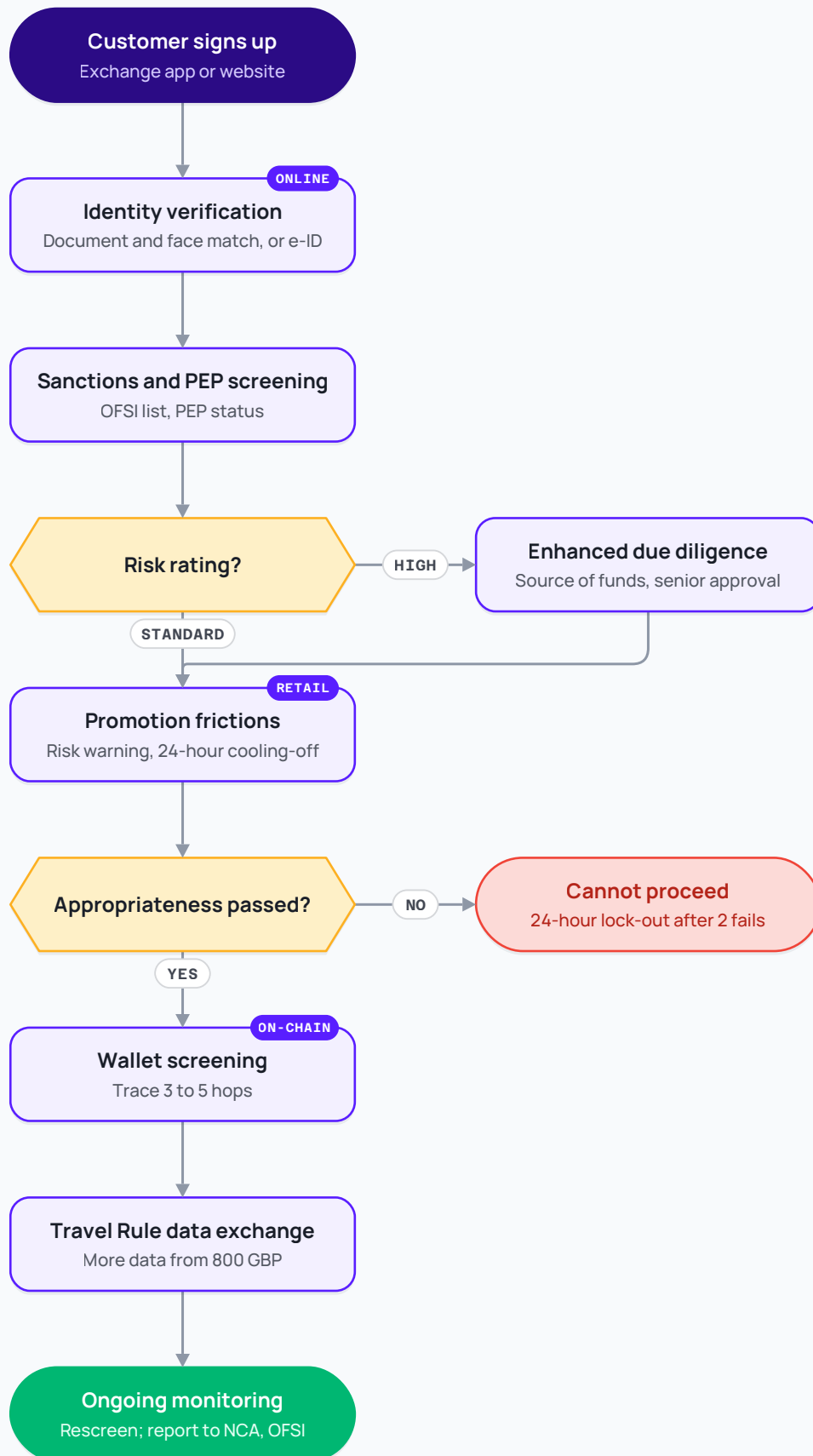


Figure 1. Online onboarding and first transfer at a UK crypto platform.

Bottom line: the UK crypto rules are largely channel-neutral, but remote onboarding without a secure electronic identification process is a listed higher-risk factor, so the quality of the online identity check decides how much extra due diligence a firm must apply.

Requirement	In person (crypto ATM, desk)	Online / app	Difference
Registration with the FCA	Required (ATMs named in reg. 14A)	Required	Same
CDD measures	Reg. 28 applies	Reg. 28 applies	Same
Risk treatment	Standard risk-based approach	Non-face-to-face without safeguards is a high-risk factor	Differs
Verification evidence	Documents from independent source	Also electronic identification meeting reg. 28(19)	Differs
Travel Rule data	Applies to transfers	Applies to transfers	Same
Location checks	Customer physically present	VPN use is an OFSI red flag; geolocation tools recommended	Differs
Reliance and outsourcing	Permitted, firm stays liable	Permitted, firm stays liable	Same
Record retention	Five years	Five years	Same
Biometric data	Not usually processed	Face matching is special category data	Differs

Remote onboarding is permitted, with a risk signal

Nothing in the MLRs requires a face-to-face meeting. When assessing risk, however, firms must take account of whether a situation involves non-face-to-face relationships or transactions "without certain safeguards, such as an electronic identification process" meeting reg. 28(19) ([reg. 33\(6\)\(b\)\(iii\)](#)). Products that might favour anonymity are a

separate risk factor (reg. 33(6)(b)(ii)), which matters for privacy coins and unhosted wallet flows.

Location and VPN masking

No UK rule mandates geolocation for crypto platforms. OFSI's July 2025 threat assessment lists VPN usage that masks a counterparty's location as a red flag and suggests geolocation tools as part of counterparty exposure assessment ([OFSI, Cryptoassets Threat Assessment](#)).

Unhosted wallets

For transfers to or from a self-hosted wallet, a firm may request originator or beneficiary details from its own customer on a risk basis, and must not make the crypto available if requested information is not received ([reg. 64G](#)).

6 Data protection and biometrics

The UK GDPR and the Data Protection Act 2018 govern identity data. The ICO treats any system that compares a selfie with a document photo to verify identity as processing special category biometric data from the moment of collection, which requires both a lawful basis and an Article 9 condition ([ICO, Biometric recognition](#)); the ICO notes that this guidance is under review following the Data (Use and Access) Act 2025. The MLRs add three constraints: personal data collected for AML may be used only to prevent money laundering, terrorist financing or proliferation financing unless another law permits or the customer consents; customers must be told this before onboarding; and the data must be deleted once the retention period ends ([regs. 40\(5\) and 41](#)).

7 Sector-specific obligations

Financial promotion frictions In force since 8 Oct 2023

Qualifying cryptoassets are restricted mass market investments. Before a retail customer receives a direct offer, the firm must give a personalised risk warning, apply a cooling-off period of at least 24 hours, categorise the client as restricted, high net worth or certified sophisticated (restricted investors limit high-risk investments to 10% of net assets; categorisation lasts 12 months) and run an appropriateness assessment. A customer who

fails two consecutive assessments is locked out for at least 24 hours ([FCA, good and poor practice, August 2024](#)).

Travel Rule In force; threshold changed 30 Jun 2026

Every transfer between crypto businesses must carry the names of the originator and beneficiary and their account numbers or a unique transaction identifier. Where any business in the chain is outside the UK and the transfer is £800 or more (previously 1,000 euros), the originator's address, date and place of birth, identity document number or customer number must also accompany it. Originator data must be verified, and the receiving firm must check the data before releasing funds ([regs. 64C and 64D](#)). Where a counterparty's country has no Travel Rule, the FCA expects UK firms still to collect, verify and store the data ([FCA statement](#)).

Tax reporting under the Cryptoasset Reporting Framework

In force since 1 Jan 2026

Platforms must collect, for each individual user, name, date of birth, home address, country of residence and a National Insurance number or Unique Taxpayer Reference (or a foreign tax identification number), plus entity details and controlling persons, and verify them through due diligence ([HMRC](#)). The first report covers 2026 and is due between 1 January and 31 May 2027.

Sanctions reporting

Since August 2022, crypto firms have been "relevant firms" that must report to OFSI when they know or suspect they have dealt with a designated person or a breach. OFSI recommends tracing at least three to five hops of transaction history and expects frozen assets to be restricted and reported.

8 Risk indicators and red flags

OFSI states that two or more of the following should trigger increased due diligence ([OFSI, July 2025](#)):

CRYPTO SANCTIONS AND LAUNDERING RED FLAGS

- **Mixer inflows:** concentrated deposits from mixers, darknet or ransomware wallets, followed by immediate withdrawal.
- **Chain hopping:** cross-chain bridges or transfers to privacy-focused blockchains to obscure the trail.
- **Address farming:** one account generating hundreds or thousands of deposit addresses through an API.
- **Structuring:** large cumulative volumes built from many transfers under £10,000.
- **Dormant wallets:** new or long-inactive wallets suddenly receiving large transfers.
- **Location masking:** VPN use hiding a counterparty's true location.
- **Unregulated counterparties:** exposure to services without KYC or AML procedures, or to nested exchanges.
- **Inconsistent source of assets:** unexplained or shifting explanations of where funds came from.

9

Enforcement and penalties

Under the MLRs the FCA may impose a penalty "of such amount as it considers appropriate", meaning effective, proportionate and dissuasive, publish a censure, and fine officers knowingly concerned in a breach; there is no fixed cap or per-violation tariff, and a firm that took all reasonable steps has a defence ([reg. 76](#)). CARF failures carry penalties of up to £300 per user ([HMRC](#)). From 25 October 2027, carrying on crypto activities without authorisation breaches the general prohibition in section 19 of the Act.

Recent actions show where the FCA focuses. In July 2024 it fined CB Payments Limited, a Coinbase Group e-money firm that acted as a gateway to crypto trading, £3,503,546 for onboarding 13,416 high-risk customers in breach of a voluntary restriction ([FCA](#)). On 10 September 2026 the FCA, HMRC and the Metropolitan Police served cease and desist letters at three London premises suspected of unregistered peer-to-peer crypto trading; the FCA has previously secured a four-year sentence for the operator of an illegal crypto ATM network ([FCA, September 2026](#)).

10 Recent changes and what to watch

- **30 September 2026** **Open until 28 Feb 2027** : the FCA authorisation gateway for the new regime opened. Firms that miss the window lose the saving provision.
- **16 September 2026** **Published** : the FCA issued perimeter guidance (PS26/18) on which activities need authorisation. Check your business model against it before applying.
- **30 June 2026** **In force** : SI 2026/621 cut the Travel Rule threshold to £800, limited mandatory country-based EDD to the FATF call-for-action list and widened change-in-control notifications. Update transfer logic and country risk tables.
- **30 June 2026** **Adopted, effective 25 Oct 2027** : the FCA published final rules for crypto firms, including stablecoin, prudential and market abuse rules. Build compliance programmes now.
- **1 January 2026** **In force** : CARF data collection began; the first HMRC report is due by 31 May 2027.
- **1 February 2027** **Adopted, effective 1 Feb 2027** : EDD for crypto correspondent relationships with third-country providers (reg. 34A) applies.
- **Later in 2026** **Consultations expected** : the FCA plans to consult on decentralised finance guidance and Financial Crime Guide updates, and with the Bank of England on systemic stablecoin issuers. No rules are yet proposed.

11 What this means for identity verification

UK crypto onboarding is fully remote in practice, so the design of the electronic check carries the regulatory weight. A document check paired with face matching and liveness, or a recognised electronic identification means, helps a firm show that its process meets the reg. 28(19) standard and avoids the non-face-to-face risk factor; a weaker process pushes more customers into enhanced due diligence. Biometric matching brings special category data duties, so firms need an Article 9 condition, a clear privacy notice and deletion at the end of the retention period.

Identity data now serves three regimes at once: CDD, Travel Rule originator data (which must be verified) and CARF tax fields such as a National Insurance number or foreign tax identification number. Capturing all of them at onboarding avoids later outreach. Re-verification triggers include doubts about earlier documents, signs of false identity (an EDD case under reg. 33(1)(e)), an appropriateness or categorisation refresh after 12 months, and on-chain alerts such as exposure to sanctioned addresses. Reliance on an

identity provider is permitted, but the firm stays liable and must be able to retrieve evidence immediately.

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.
- AML screening against sanctions, PEP, adverse-media and watchlists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate and institutional crypto clients.
- KYC questionnaires and a no-code workflow builder to capture tax and source-of-funds data and route high-risk users to enhanced checks.
- Cloud, on-premises or hybrid deployment with an audit trail for each 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), regs. 7, 8, 14A, 19, 28, 33, 39 to 41, 60A, 64A to 64H, 76, legislation.gov.uk (revised text, up to date to October 2026), legislation.gov.uk
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2026 (SI 2026/621), made 9 June 2026, and Explanatory Memorandum, legislation.gov.uk

- The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102), legislation.gov.uk
- FCA, A new regime for cryptoasset regulation (updated 30 September 2026), fca.org.uk
- FCA, Cryptoassets: How the gateway will operate (updated 30 September 2026), fca.org.uk
- FCA, Cryptoasset firms: Registration under the MLRs ahead of the new FSMA regime (updated 16 September 2026), fca.org.uk
- FCA, Cryptoassets: AML/CTF regime (updated 12 February 2026), fca.org.uk
- FCA, FCA sets landmark crypto rules, press release, 30 June 2026, fca.org.uk
- FCA, Assessing firms' compliance with 'back end' cryptoasset financial promotions rules, good and poor practice, 7 August 2024, fca.org.uk
- FCA, Expectations for UK cryptoasset businesses complying with the Travel Rule, statement, 17 August 2023, fca.org.uk
- FCA, First enforcement action against firm enabling cryptoasset trading (CB Payments Limited), 25 July 2024, fca.org.uk
- FCA, FCA and partners continue crackdown on illegal crypto trading, 17 September 2026, fca.org.uk
- OFSI, Cryptoassets Threat Assessment, July 2025, pp. 6 to 19, gov.uk
- HMRC, Collecting cryptoasset user and transaction data (updated 1 January 2026), gov.uk
- HMRC, Reporting cryptoasset user and transaction data (updated 3 June 2026), gov.uk
- ICO, Biometric data guidance: Biometric recognition, ico.org.uk